快速通道

文档分类
- 红盟公告
- 新手上路
- 漏洞分析
- 工具介绍
- 安全配置
- 编程技术
- **安全技术** <=
- 业界动态

本类热门
- 如何利用黑客技术跟踪并分析一名目标人物
- 有关无线安全与黑客的话题
- 让我们回归(by 默难)
- 通用ShellCode深入剖析[转]
- Format String 漏洞介绍/总结(一)
- 结合实例解读ELF文件-阅读笔记(1)

# Guest权限突破

提交文章： 天地成双
提交日期： 2004-08-20
文章属性： 转载
文档类别： 安全技术
浏览次数： 今101次/总498次

Guest权限提升方法总结：

现在的入侵是越来越难了，人们的安全意识都普遍提高了不少，连个人用户都懂得防火墙，杀毒软件要装备在手，对于微软的补丁升级也不再是不加问津。因此现在我们想在因特网上扫描弱口令的主机已经几乎是痴心妄想了。（这可是一件大大的好事啊。）

但是这也使得我们作黑客的进行入侵检测达到了一个前所未有的难度。通过各种手段，我们通常并不能直接获得一个系统的管理员权限。比如我们通过某些对IIS的攻击，只能获得IUSR-MACHINENAME的权限（如上传asp木马，以及某些溢出等）。这个帐号通常可是系统默认的guest权限，于是，如何拿到系统管理员或者是system权限，便显得日益重要了。

于是，我就总结了一下大家所经常使用的几种提升权限的方法，以下内容是我整理的，没有什么新的方法，写给和我一样的菜鸟看的。高手们就可以略去了，当然，你要复习我不反对，顺便帮我查查有什么补充与修改：

1、社会工程学。

对于社会工程学，我想大家一定不会陌生吧？（如果你还不太明白这个名词的话，建议你去找一些相关资料查查看。）我们通常是通过各种办法获得目标的敏感信息，然后加以分析，从而可以推断出对方admin的密码。举一个例子：假如我们是通过对服务器进行数据库猜解从而得到admin在网站上的密码，然后借此上传了一个海洋顶端木马，你会怎么做？先翻箱倒柜察看asp文件的代码以希望察看到连接SQL的帐号密码？错错错，我们应该先键入一个netstat －an命令察看他开的端口（当然用net start命令察看服务也行）。一旦发现他开了3389，犹豫什么？马上拿出你的终端连接器，添上对方IP，键入你在他网站上所获得的用户名及密码……几秒之后，呵呵，进去了吧？这是因为根据社会工程学的原理，通常人们为了记忆方便，将自己在多处的用户名与密码都是用同样的。于是，我们获得了他在网站上的管理员密码，也就等同于获得了他所有的密码。其中就包括系统admin密码。于是我们就可以借此登入他的3389拉！

即使他并没有开启3389服务，我们也可以凭借这个密码到他的FTP服务器上试试，如果他的FTP服务器是serv-u 5.004 以下版本，而帐号又具有写权限，那么我们就可以进行溢出攻击了！这可是可以直接拿到system权限的哦！（利用serv-u还有两个提升权限的方法，我待会儿会说的）

实在不行，我们也可以拿它的帐号去各大网站试试！或许就能进入他所申请的邮箱拿到不少有用的信息！可以用来配合我们以后的行动。

还有一种思路，我们知道，一个网站的网管通常会将自己的主页设为IE打开后的默认主页，以便于管理。我们就可以利用这一点，将他自己的主页植上网页木马……然后等他打开IE……呵呵，他怎么也不会想到自己的主页会给自己种上木马吧？
其实利用社会工程学有很多种方法，想作为一个合格黑客，这可是必学的哦！多动动你自

己的脑子，你才会成功！

2、本地溢出。

微软实在是太可爱了，这句话也不知是哪位仁兄说的，真是不假，时不时地就会给我们送来一些溢出漏洞，相信通过最近的MS-0011大家一定又赚了一把肉鸡吧？其实我们在拿到了Guest权限的shell后同样可以用溢出提升权限。最常用的就是RunAs.exe、 winwmiex.exe或是PipeUpAdmin等等。上传执行后就可以得到Admin权限。但一定是对方没有打过补丁的情况下才行，不过最近微软的漏洞一个接一个，本地提升权限的exploit也会出来的，所以大家要多多关心漏洞信息，或许下一个exploit就是你写出来的哦！

3、利用scripts目录的可执行权限。

这也是我们以前得到webshell后经常使用的一招，原理是Scripts目录是IIS下的可运行目录，权限就是我们梦寐以求的SYSTEM权限。常见的使用方法就是在U漏洞时代我们先上传idq.dll到IIS主目录下的Scripts目录，然后用ispc.exe进行连接，就可以拿到system权限，不过这个是在Microsoft出了SP3之后就行不通了，其实我们仍可以利用此目录，只要我们上传别的木马到此目录，我举个例子就比如是winshell好了。然后我们在IE中输入：

http://targetIP/Scripts/木马文件名.exe

等一会，看到下面进度条显示“ 完成 ”时，可以了，连接你设定的端口吧！我这里是默认的5277，连接好后就是SYSTEM权限了！这时你要干什么我就管不着了……嘿嘿

4、替换系统服务。

这可是广大黑友乐此不疲的一招。因为windows允许对正在运行中的程序进行改动，所以我们就可以替换他的服务以使得系统在重启后自动运行我们的后门或是木马！首先，通过你获得的guest权限的shell输入：net start命令，察看他所运行的服务。此时如果你对windows的系统服务熟悉的话，可以很快看出哪些服务我们可以利用。

C:\WINNT\System32\>net start
已经启动以下 Windows 服务:

COM+ Event System
Cryptographic Services
DHCP Client
Distributed Link Tracking Client
DNS Client
Event Log
Help and Support
IPSEC Services
Logical Disk Manager
Logical Disk Manager Administrative Servic
Network Connections
Network Location Awareness (NLA)
Protected Storage
Remote Procedure Call (RPC)
Rising Process Communication Center
Rising Realtime Monitor Service
Secondary Logon
Security Accounts Manager
Shell Hardware Detection
System Event Notification
System Restore Service
Telephony
Themes
Upload Manager
WebClient
Windows Audio
Windows Image Acquisition (WIA)
Windows Management Instrumentation
Windows Time
Wireless Zero Configuration
Workstation

命令成功完成。

我先在我的机器上运行一下命令做个示范（大家别黑我呀），注意我用红色标注的部分，那是我安装的瑞星。Rising Process Communication Center服务所调用的是CCenter.exe，而Rising Realtime Monitor Service服务调用的是RavMonD.exe。这些都是第三方服务，可以

利用。（强烈推荐替换第三方服务，而不要乱动系统服务，否则会造成系统不稳定）于是我们搜索这两个文件，发现他们在D:\ rising\rav\文件夹中，此时注意一点：如果此文件是在系统盘的Program Files目录中时，我们要知道，如果对方是使用的NTFS格式的硬盘，那么系统盘下的这个文件夹guest权限是默认不可写的，还有Windows目录、Documents and Settings目录这些都是不可写的，所以我们就不能替换文件，只能令谋途径了。（这也是为什么我不建议替换系统服务的原因之一，因为系统服务文件都在Windows\System32目录中，不可写）但如果是FAT32格式就不用担心，由于它的先天不足，所有文件夹都是可写的。

于是就有人会问：如果是NTFS格式难道我们就没辙了吗？

当然不是，NTFS格式默认情况下除了对那三个文件夹有限制外，其余的文件夹、分区都是everyone完全控制。（也就是说我即使是IPC$的匿名连接，都会对这些地方有可写可运行权限！）所以一旦对方的第三方服务不是安装在那三个文件夹中，我们就可以替换了！我就拿CCenter下手，先将它下载到本地机器上（FTP、放到IIS主目录中再下载等等……）然后拿出你的文件捆绑机，找到一个你最拿手的后门……呵呵，捆绑好后，上传，先将对方的CCenter.exe文件改个名CCENTBAK.exe，然后替换成自己的CCenter。现在只需要等对方的机器重启，我们的后门就可以运行了！由于Windows系统的不稳定，主机在一个礼拜后就会重启，（当然如果你等不及的话，可以对此服务器进行DDOS攻击迫使他重启，但我并不赞同！）此时登上你的后门，就是System权限了！

5、替换admin常用程序。

如果对方没有你所能利用的服务，也可以替换对方管理员常用的程序，例如QQ，MSN等等，具体替换方法与替换服务一样，只是你的后门什么时候可以启动就得看你的运气了。

6、利用autorun .inf或desktop.ini。

我们常会碰到这种事：光盘放进光驱，就会自动跳出来一段FLASH，这是为什么？呵呵，你到光盘的根目录中看看，是否有一个autorun.inf的文件？用记事本打开来看看，是不是有这么一句话：autorun=xxx.exe 这就是你刚才所看到的自动运行的程序了。

于是我们就可以利用这个来提升我们的权限。先配置好一个后门，（我常用的是winshell，当然你不用这个也行）上传到他D盘下的任意一个文件夹中，然后从你那个自运行的光盘中把autorun.inf文件也上传，不过上传前先将autorun=xxx.exe 后面的xxx.exe改为你配置的后门文件途径、文件名，然后再上传到d盘根目录下，加上只读、系统、隐藏属性。OK就等对方admin浏览D盘，我们的后门就可以启动了！（当然，这必须是在他没有禁止自动运行的情况下才行。）

另外有相同作用的是desktop.ini。大家都知道windows支持自定义文件，其实它就是通过在文件夹中写入特定文件——desktop.ini与Folder.htt来实现的，我们就可以利用修改这文件来达到我们的目的。

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！（如果你不放心，可以多设置几个目录）

7、Serv-U提升权限

利用Serv-U提升权限共有三种方法，溢出是第一种，我之前已经说过，这里就不介绍了。我要讲的是其余两种办法。

办法一：要求：对Serv-u安装目录有完全控制权。

方法：进入对方的Serv-U目录，察看他的ServUDaemon.ini，这是Serv-U的配置文件，如果管理员没有选择将serv- u的所有配置写入注册表的话，我们就可以从这个文件中看到Serv-U的所有信息，版本、IP、甚至用户名与密码！早些版本的密码是不加密的，但是后来是经过了MD5加密。所以不能直接得到其密码。不过我们仍然有办法：先在本地安装一个Serv-U（版本最好新点），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。我们新建一个用户，什么组不重要，重要的是将他的主目录改为对方的系统盘，然后加上执行权限！这个最重要。更改完后应用，退出。再将你更改过的ServUDaemon.ini 文件上传，覆盖掉他的文件，然后就等他的Serv-U重启更新配置，之后我们就可以登入他的FTP。进入后执行以下命令：

Cd windows
Cd System32
Quote site exec net.exe user wofeiwo /add
Quote site exec net.exe localgroup administrators wofeiwo /add
Bye

然后你就有了一个叫wofeiwo的系统管理员了，还等什么?登陆3389，大功告成！

办法二：Serv-u开了两个端口，一个是21，也就是ＦＴＰ了，而另一个是43958，这个端口是干什么的？嘿嘿，这个是Ｓｅｒｖ－Ｕ的本地管理端口。但是默认是不准除了１２７．０．０．１外的ｉｐ连接的，此时就要用到FPIPE.exe文件，这是一个端口转发程序，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，之后提升权限的方法参考办法一。我就不赘述了。

8、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，因为MSSQL是默认的SYSTEM权限。
要求：你得到了对方MSSQL管理员密码（可以从他的连接数据库的ASP文件中看到）,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。

唔……升个懒腰，好累阿，终于写完8个方法了，发发牢骚……（以下省略N字符）

总之，以上的8种方法并不是绝对的，最主要的是你的思路，每种方法互相结合，才能发挥其应有的效应。

返回上页

Copyright © 2000-2004 **HUC** All Rights Reserved.
中国红客网络技术联盟 www.cnhonker.com
webmaster@cnhonker.net