黑客防线

2002（下册）

精华本

双光盘

http://www.hacker.com.cn

超值：60例《黑客防线》原创全程攻防录像演示

赠送：2001年《黑客防线》精华本的电子版

超值大奉送

- 名家专访
- 专题综述
- 系统安全
- 服务器安全
- 数据库安全
- 网站安全
- 网管之家
- 编程解析
- 安全方案

- 经验交流
- 病毒前线
- 拒绝服务
- QQ专栏
- 恶意攻击防范
- 案例分析
- 攻防工具
- 网吧攻略
- 密界寻踪

邮电出版社
ELECOMMUNICATIONS PRESS

黑客防线精华本

2002（下册）

《黑客防线》编辑部　编

人民邮电出版社

目 录

九、密界寻踪

Windows 下 Ping 命令详解及使用小技巧

资料整理/iceblood

对于 Windows 下 Ping 命令相信大家已经再熟悉不过了，但是能把 Ping 的功能发挥到最大的人却并不是很多，在此我总结了一些小经验，和大家分享一下。

先罗嗦两句 Ping 的最基本使用，Windows 用户可用：开始->运行，输入“command” 调出 command 窗口使用此命令，或者直接进入 ms-dos 模式下输入：

Ping IP 地址或域名，显示如图 1。

图 1

Ping 命令通过向计算机发送 ICMP 回应报文并且监听回应报文的返回，以校验与远程计算机或本地计算机的连接。对于每个发送报文， Ping 最多等待 1 秒，并打印发送和接收报文的数量，比较每个接收报文和发送报文，以校验其有效性。默认情况下，发送 4 个回应报文，每个报文包含 64 字节的数据（周期性的大写字母序列）。

现在我就参照Ping命令的帮助说明来给大家说说我使用 Ping 时会用到的技巧，Ping 只有在安装了 TCP/IP 协议以后才可以使用：

```
Ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j computer-list] | [-k computer-list]] [-w timeout] destination-list
```

-t (Ping the specified host until stopped. To see statistics and continue - type Control-Break; To stop - type Control-C.)

不停地 Ping 地方主机，直到你按下 Control-C 。

此功能没有什么特别的技巧，不过可以配合其他参数使用，将在下面提到。

-a (Resolve addresses to hostnames.)

解析计算机 NetBios 名。

```
示例：C:\>Ping -a 192.168.1.21
Pinging iceblood.yofor.com [192.168.1.21] with 32 bytes of data:
Reply from 192.168.1.21: bytes=32 time<10ms TTL=254
Reply from 192.168.1.21: bytes=32 time<10ms TTL=254
Reply from 192.168.1.21: bytes=32 time<10ms TTL=254
Reply from 192.168.1.21: bytes=32 time<10ms TTL=254
Ping statistics for 192.168.1.21:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

从上面就可以知道IP为192.168.1.21的计算机 NetBios名为iceblood.yofor.com。

-n (count Number of echo requests to send.)

发送 count 指定的 Echo 数据包数。

在默认情况下，一般都只发送 4 个数据包，通过这个命令可以自己定义发送的个数，对衡量网络速度很有帮助，比如我想测试发送 50 个数据包的返回平均时间为多少，最快时间为多少，最慢时间为多少，就可以通过以下获知：

```
C:\>Ping -n 50 202.103.96.68
Pinging 202.103.96.68 with 32 bytes of data:
Reply from 202.103.96.68: bytes=32 time=50ms TTL=241
Reply from 202.103.96.68: bytes=32 time=50ms TTL=241
Reply from 202.103.96.68: bytes=32 time=50ms TTL=241
```

```
Request timed out.
.....
Reply from 202.103.96.68: bytes=32 time=50ms
TTL=241
Reply from 202.103.96.68: bytes=32 time=50ms
TTL=241
Ping statistics for 202.103.96.68:
Packets: Sent = 50, Received = 48, Lost = 2 (4%
loss),Approximate round trip times in milli-seconds:
Minimum = 40ms, Maximum = 51ms, Average =
46ms
```

从以上我可以知道,在给202.103.96.68发送50个数据包的过程当中，返回了48个，其中有两个由于未知原因丢失，这48个数据包当中返回速度最快为40ms，最慢为51ms，平均速度为46ms。

-l (size Send buffer size.)

定义echo数据包大小。

在默认的情况下，Windows的Ping发送的数据包大小为32byt，我们也可以自己定义它的大小，但有一个大小的限制，就是最大只能发送65500byt。也许有人会问为什么要限制到65500byt。因为Windows系列的系统都有一个安全漏洞（也许还包括其他系统），就是当向对方一次发送的数据包大于或等于65532时，对方就很有可能当机，微软公司为了解决这一安全漏洞，于是限制了Ping的数据包大小。虽然微软公司已经做了此限制，但这个参数配合其他参数以后危害依然非常强大，比如我们就可以通过配合-t参数来实现一个带有攻击性的命令（以下介绍带有危险性，仅用于试验） ：

```
C:\>Ping -l 65500 -t 192.168.1.21
Pinging 192.168.1.21 with 65500 bytes of data:
Reply from 192.168.1.21: bytes=65500 time<10ms
TTL=254
Reply from 192.168.1.21: bytes=65500 time<10ms
TTL=254
.....
```

这样它就会不停地向192.168.1.21计算机发送大小为65500byt的数据包，如果你只有一台计算机，也许没有什么效果，但如果有很多计算机，那么就可以使对方完全瘫痪。我曾经就做过这样的试验，当我同时使用10台以上计算机Ping一台Windows 2000Pro系统的计算机时，不到5分钟，对方的网络就已经完全瘫痪，网络严重堵塞，HTTP和FTP服务完全停止，由此可见威力非同小可 。

-f (Set Don't Fragment flag in packet.)

在数据包中发送“不要分段”标志。

在一般情况下，你所发送的数据包都会通过路由分段再发送给对方，加上此参数以后路由就不会再分段处理。

-i (TTL Time To Live.)

指定TTL值在对方的系统里停留的时间。

此参数同样是帮助你检查网络运转情况的。

-v (TOS Type Of Service. 0

将“服务类型”字段设置为 tos 指定的值。

-r (count Record route for count hops.)

在“记录路由”字段中记录传出和返回数据包的路由。

在一般情况下，你发送的数据包是通过一个个路由才到达对方的，但到底是经过了哪些路由呢？通过此参数就可以设定你想探测经过的路由的个数，不过限制在9个，也就是说你只能跟踪到9个路由。如果想探测更多，可以通过其他命令实现，我将在以后的文章中给大家讲解。以下为示例 ：

```
C:\>Ping -n 1 -r 9 202.96.105.101 （发送一个数
据包，最多记录9 个路由）
Pinging 202.96.105.101 with 32 bytes of data:
Reply from 202.96.105.101: bytes=32 time=10ms
TTL=249
Route: 202.107.208.187 ->
202.107.210.214 ->
61.153.112.70 ->
61.153.112.89 ->
202.96.105.149 ->
202.96.105.97 ->
202.96.105.101 ->
202.96.105.150 ->
61.153.112.90
Ping statistics for 202.96.105.101:
Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 10ms, Maximum = 10ms, Average =
10ms
```

从上面可以知道,从我的计算机到202.96.105.101一共通过了202.107.208.187 ,202.107.210.214,

Windows 2000 终端服务使用技巧

文／王智雄

Windows 2000终端服务器有两种运行模式："应用程序模式(Application Server Mode)"和"远程管理模式(Remote Administration Mode)"。前者为终端客户提供应用程序共享服务，在此模式下，客户机以仿真终端机的身份访问并显示服务器桌面，还可运行服务器上的应用程序。后者为系统管理员提供了一种远程管理服务器的强有力的方法。系统管理员可以通过任何TCP/IP连接对服务器进行远程管理。这两种模式适用于不同的场合，但不能同时运行。

在中小型局域网中，为了简化网络管理、减轻系统管理员负担、降低软件升级和维护的费用，通常使用"应用程序模式"为客户机提供应用程序共享服务。本文主要讨论在该模式下管理网络时常见问题的解决方法。

一、判断终端服务器的运行模式

如前所述，Windows 2000终端服务器可以运行在"应用程序模式"或"远程管理模式"之下，那么，如何判断终端服务器运行在何种模式之下呢？我们可以使用下述方法。

选择"开始"->"程序"->"管理工具"->"终端服务配置"，点击"服务器设置"，点击左面窗口中的"服务器设置"项，在右面窗口中的"终端服务器模式"行的"属性"列中将显示出当前的模式。

二、在"应用程序模式"和"远程管理模式"之间切换

61.153.112.70，61.153.112.89，202.96.105.149，202.96.105.97这几个路由。

-s(count Timestamp for count hops.)

指定count跃点数的时间戳。

此参数和-r差不多，只是这个参数不记录数据包返回所经过的路由，最多也只记录4个。

-j(host-list Loose source route along host-list.)

利用 computer-list 指定的计算机列表路由数据包。连续计算机可以被中间网关分隔（路由稀疏源）IP 允许的最大数量为 9。

-k (host-list Strict source route along host-list.)

利用 computer-list 指定的计算机列表路由数据包。连续计算机不能被中间网关分隔（路由严格源）IP 允许的最大数量为 9。

-w (timeout Timeout in milliseconds to wait for each reply.)

指定超时间隔，单位为毫秒。

此参数没有什么其他技巧。

Ping命令的其他技巧：在一般情况下还可以通过Ping对方让对方返回给你的TTL值大小，粗略地判断目标主机的系统类型是Windows系列还是UNIX/Linux系列，一般情况下，Windows系列的系统返回的TTL值在100~130之间，而UNIX/Linux系列的系统返回的TTL值在240~255之间。当然，TTL的值在对方的主机里是可以修改的，Windows系列的系统可以通过修改注册表以下键值实现：

```
[HKEY_LOCAL_MACHINE\SYSTEM\
CurrentControlSet\Services\Tcpip\Parameters]
"DefaultTTL"=dword:000000ff
255---FF
  128---80
  64----40
  32----20
```

好了，Ping命令基本上完全讲解完了。当然还有一些其他的使用技巧，就有待于各位朋友自己去发掘。

可以按下述步骤在“应用程序模式”和“远程管理模式”之间切换。

选择“开始”->“设置”->“控制面板”，双击“添加/删除程序”，点击“添加/删除Windows 组件”图标，在“选择Windows组件”对话框中不改变任何选项而直接点击“下一步”，在“终端服务安装程序”对话框中，两种模式都会显示出来，当前运行的模式处于选中状态。你可以直接选择另一模式，然后点击“下一步”，重新启动计算机即可。

三、在安装模式与执行模式之间切换

在Windows 2000终端服务器上安装应用程序有两种方式：“安装模式(install mode)”和“执行模式(execute mode)”。这两种安装方式是有区别的，在“安装模式”下安装的应用程序允许所有终端服务用户使用，而在“执行模式”下安装的程序只能由安装该程序的用户使用，其他用户不能使用。因此，如果要为所有用户安装程序，必须要利用“安装模式”来安装。进入“安装模式”的方法有两种：

方法一：利用“控制面板”中的“添加/删除程序”安装应用程序时，可以使得终端服务器自动进入“安装模式”。

方法二：可以按下述步骤进行：

1、选择“开始”->“运行”，输入命令“cmd”后点击“确定”；

2、在命令行中输入下列命令后回车：

change user /install

运行该命令后，终端服务器即进入“安装模式”，接下来可以为用户安装应用程序；

3、应用程序安装完成后，可以使用下列命令退出“安装模式”而进入“执行模式”：

change user /execute

4、可以使用下述命令测试终端服务器处于何种模式之下：

change user /query

四、使用户从终端服务客户机登录到服务器

在默认情况下，任何一个在终端服务器上建立的用户都具有从终端服务客户机登录到服务器的权利。然而，也可以按下述步骤为一个用户赋予该权利：

选择“开始”->“程序”->“管理工具”->“计算机管理”。

展开“系统工具”分支及其下的“本地用户和组”分支，然后点击“用户”选项。

双击即将要赋予该权限的用户名，在“终端服务配置文件”选项卡中选择“允许登录到终端服务器”复选框后，点击“确定”，关闭“计算机管理”对话框。

选择“开始”->“程序”->“管理工具”->“终端服务配置”，打开“连接”文件夹，选择“RDP-Tcp”。

选择“操作”->“属性”，在“权限”选项卡中加入需要赋予该权限的用户或组后，点击“确定”。

五、在Windows 2000终端服务器上安装Office 2000 CD1

在Windows 2000终端服务器上安装Office 2000时，必须在安装之前做一些准备工作，才能使安装顺利完成，否则将会出现如下错误信息：

“Microsoft Office 2000安装程序的一些默认设置不能在终端服务器上正常工作。要想在终端服务器上安装Office 2000，必须要使用Office 2000 Resource Kit光盘中或网站http://www.microsoft.com/office/ork中所提供的指令和工具。”

因为Office 2000在Windows 2000终端服务器上安装时，需要使用一个转换程序termsrvr.mst，当将Office 2000光盘插入计算机之后，将自动运行安装程序，从而无法使用该转换程序，因而引起了上述错误。因此，我们应该在安装Office 2000时使用转换程序termsrvr.mst。

在安装Office 2000之前，应首先做好以下两项准备工作。

1、终端服务器运行在“应用程序模式”之下，并且已经安装和启动了终端服务功能，以便使多个终端服务客户可以同时使用Office 2000。

2、已经得到了终端服务转换程序termsrvr.mst，并且已将其放置于硬盘某一个目录之下。该文件可通过以下几种方式得到：

(1) 可以在Office 2000 Resource Kit光盘中的ORK\PFiles\ORKTools\Toolbox\Tools\TermSrvr目录下找到。

(2) 如果已安装了Office 2000资源工具包，可以在硬盘的<drive:>\Program Files\ORKtools\Toolbox\Terminal Server Tool

目录下找到。其中< drive:>默认是Windows 2000所在磁盘。

(3) 如果没有Office 2000 Resource Kit光盘，也可以到Microsoft公司的网站下载，下载文件名为orktools.exe，是一个自解压包，其中包含了termsrvr.mst文件。下载地址为:http://www.microsoft.com/office/ork/2000/download/ORKTools.exe。

在做好了上述准备工作之后，可以按下述步骤在终端服务器上成功安装Office 2000的第一张光盘 。

1、“在控制面板”中双击“添加/删除程序”，点击“添加新程序”，然后点击“光盘或软盘”，点击“下一步”按钮，点击“浏览”按钮。

2、在Office CD1的根目录下选择setup.exe并点击“打开”按钮。setup.exe将出现在“运行安装程序”对话框的命令行。

3、在“运行安装程序”对话框的命令行输入“setup.exe”命令之后键入一个空格，然后再键入以下内容：

TRANSFORMS=< path>\Termsrvr.mst

其中< path>是存放文件termsrvr.mst所在的路径 。

4、点击“下一步”按钮，输入用户信息后点击“下一步”按钮。

5、同意最终用户协议后点击“下一步”按钮，点击“安装”按钮。

6、当出现成功安装的信息后，点击“确定”按钮、“下一步”按钮，然后点击“完成”按钮即可。

六、解决在启动终端服务功能后不能使用Office 2000

在Windows 2000服务器上启动终端服务功能后，Office 2000应用程序可能不能运行。当安装Office 2000新组件或第一次使用时需要安装的组件时，将出现以下提示信息：“Microsoft Office 2000安装程序的一些默认设置不能在Windows 2000终端服务器上正常工作。要想在终端服务器上安装Office 2000，必须要使用Office 2000 Resource Kit光盘中或站点http://www.microsoft.com/office/ork中的有关指令和工具。”

当利用终端服务转换程序重新安装Office 2000时，将会出现以下错误信息：“在终端服务器上安装应用程序时必须要进入安装模式。使用控制面板中的‘添加/删除程序’安装应用程序时，可以使终端服务器自动地进入安装模式。”

事实上，你将不能在安装模式下(通过控制面板中的“添加/删除程序”安装)利用终端服务转换程序termsrvr.mst重新安装Office 2000。

出现这种情况的原因是终端服务功能只能在安装了Office 2000之后才能安装。你可以先删除终端服务功能，然后卸载Office 2000，接下来再启动终端服务功能，再利用终端服务转换文件重新安装Office 2000。具体操作步骤如下：

1、删除终端服务功能

选择“开始”->“设置”->“控制面板”，双击“添加/删除程序”，点击“添加/删除Windows组件”。清除“终端服务”和“终端服务授权”复选框中的选中标记，点击“下一步”按钮，若提示重新启动计算机，则重启计算机 。

2、卸载Office 2000

选择“开始”->“设置”->“控制面板”，双击“添加/删除程序”，在当前已安装的应用程序列表中选中Office 2000，然后点击“删除”按钮。点击“是”按钮确认后，即删除Office 2000。

3、启动终端服务功能

选择“开始”->“设置”->“控制面板”，双击“添加/删除程序”，点击“添加/删除Windows组件”，选择“终端服务”。如果需要，还可以选择“终端服务授权”，点击“下一步”按钮，选择“应用程序服务模式”。选择“与Windows 2000用户兼容的权限”，然后点击“下一步”按钮。如果选择了“终端服务授权”选项，需要指定相关信息将计算机安装为许可证服务器，然后点击“下一步”按钮。点击“完成”按钮即可进行安装，如果需要，可重启计算机。

4、安装Office 2000

使用终端服务转换程序termsrvr.mst安装Office 2000，这一安装过程与问题5中所述安装过程相同，不再重述。

以上一些方法是我在实际学习和操作过程中得出来的，希望对大家有所帮助。

Windows 自带的网络信息查询命令

文／一水

一、WinIPcfg：看自己IP的小工具，既然是98自带，我们就不用费劲下载了，在NT里则在网络监视器里就可以看见IP。用法很简单，直接在DOS下键入就可以了！没有什么参数。

二、Tracert：是验证同往远程主机路径的实用程序。格式：

tracert [-d][-h maximum_hops][-w timeout] target_name

-d:不将IP转换主机名

-h：最大跟踪数量

-w：time out：(time out的时间)

最简单的例子：tracert hostname，hostname可以是计算机名也可以是IP

三、NET：非常棒的东西，由于网上的非常全，在这里只是简单说两句吧：）

NET HELP SERVICES：列出用户可以起用的网络服务

NET HELP SYNTAN：解释如何阅读NET HELP语法行

NET HELP COMMAND|MORE：逐屏显示帮助

1．Devicename：指定一个名字，以便与资源连接或指定要切断的设备，有两种类型的设备名：磁盘驱动器（D：—Z：）和打印机（LPT1：—LPT3：）

(1) \\computername:指控制共享资源的计算机的名字，如果计算机名中包含空字符，就要将双斜线”\\“和计算机名一起用引号括起来

(2) share name：一看名字就知道是共享受资源的网络名

(3) \volume：指定一个服务器上的NETWARE卷，但用户必须安装NETWARE

(4) password：多么敏感的字眼，指访问共享资源所需要的密码

(5) *：进行密码提示，因为在密码提示符下输入密码是，密码是不会显示的

2．/user：指定连接时的一个用户

3．domainname：指定另一个域如果缺省域，就用当前登录的域

4．username：登录用户名

5．/home：将用户与他们的宿主目录相连

6．/delete：取消一个网络连接，从永久连接列表中删除连接

7．/persistent：控制对永久网络连接的使用，缺省时为最近使用的设置

YES：在连接产生的时候保存它们，并在下次登录的时候恢复他们

NO：不保存正在产生的连或后继接的连接，现有的连接可以在下次登录时被恢复

file///***.***.***.***\c$ 则网上共享C盘的内容就像使在FTP中一样清楚

四、AT：指定在特定的日期和时间运行某些命令和程序

先启动schedule服务

c:\>net start schedule

schedule 正在启动服务...

schedulw 服务启动成功

AT[\\computername][[id][/delete]|/delete[/yes]]

AT[\\computername]time[]/interactive][/every:date[,...]/next:date[,...]]

computername：远程计算机名

/yes：用于删除所有作业

id:指定给派顶进度命令的识别号

time：命令运行时间

/delete：删除某个已排定进度的命令所有由排定进度的命令都删除（缺省的情况下）

in：允许作业在运行是与用户通过桌面交互

/every：data[,...]指定什么时候运行什么命令

最近，《黑客防线》应广大读者反映刊登了一些UNIX系统的入侵实例，但有些读者却因为不熟悉UNIX系统的命令而影响了阅读。因此我们列举了UNIX下常用的命令供读者参考，希望可以起到辅助阅读的作用。

需要知道的UNIX命令

文／银蜥蜴

这里有一些你需要学习的基本命令和一些能帮你登录或者保持你的权限的UNIX程序。

一、基本命令

我希望你能有一些基本的DOS知识，这样会对你有一些帮助，而且在写这篇文章时，我会假设你已经具备一些DOS基础了。

经常使用的DOS命令如下：

（记住：UNIX是区分大小写的，所以，如果我使用小写，你也得使用小写，如果我使用空格，你也得使用空格。DOS会忽略大小写，但是UNIX不会！）

```
DIR/W       = ls
DIR         = ls -l
DIR/AH      = ls -al  AH=(hidden) -al=(include
hidden files as well as regular)
RENAME      = mv
ATTRIB      = chmod
MD          = mkdir
RD          = rmdir
DEL         = rm
COPY        = cp
```

以上这些全是基本的命令，我建议你在UNIX外壳的帮助页面查找一下这些命令。你可以输入“man command”去查找。

每一个命令都有参数，比如：cp -R，拷贝文件和目录。你可以输入“man cp”来得到cp命令的所有参数。

cd｛然后按回车｝可以回到你的主目录。

cp 文件名 $HOME 拷贝文件到你的主目录。

cd ~用户名 进入这个用户的主目录，但是前提条件是你必须有访问权限。

pwd｛按回车｝显示你现在所在目录。

二、Telnet

Telnet是一个能在外壳环境下使用的命令，或者是一个在Windows,OS/2,Windows 95和其他一些操作系统下的exe文件（telnet.exe），它可以让你通过网络连接上另一台计算机。在这里，你还可以学到其他一些程序，比如：FTP和Rlogin。但是现在我们先来看看Telnet。

如果知道你想连接的计算机的IP地址或者主机名，你可以使用Telnet。用Telnet程序连接那个IP或者主机，你应该使用下面这个命令：

Telnet netxxx.com or telnet 206.xxx.xx.xx

好了，现在登录：

```
telnet machxxx.com
trying...
Connected to machxxx.com
Linux 2.0.28 (machxxx.com) (ttyp0)
machine login:username
password:########
bash$
```

你的提示符可能会不一样，但是我们以现在这个来讲。

注意上面的那个“bash$”，这意味着，你已经登录成功，并且进入系统。如果你已经收集到大量的口令文件，那么你就可以使用Telnet了。在破解密码文件以前，最好用telnet看看对方运行的是什么系统。这里还有另外一种方法，就是让Telnet的标题持续显示。telnet domain.name.com，在你看清楚后，再用“Ctrl]”来结束连接。

首先，把你所有的Linux口令文件都集中起来

破解。我们所需要的也就是一个系统中的账号，我们几乎可以肯定，我们将在那台机器上得到root权限。

三、UNIX 文件许可

```
bash$
bash$ cd /tmp
bash$ ls -l
total 783
-rwx------   1 wood      users          1 Jan
25 18:28 19067haa
-rw-r--r--   1 berry     mail           1 Jan
16 12:38 filter.14428
-rw--------  1 rhey19    root      395447 Jan
24 02:59 pop3a13598
-rw--------  1 rhey19    root      395447 Jan
24 03:00 pop3a13600
drwxr-xr-x   4 root      root        1024 Jan
12 13:18 screens
```

首先注意到，我们使用一个“/”而不是“\”来改变目录！UNIX使用“/”作为根目录，所以这一点与DOS不同。

注意，我们输入“ls -l”来查看长目录。如果我们输入“ls”，我们将得到如下显示：

```
bash$ ls
19067haa      filter.14428  pop3a13598    pop3a13600
screens
```

以上看到的输出结果不能让我们了解详细信息，所以，一般情况下，我们都会使用“ls -al”，使用参数“-al”，我们还将看到隐藏文件，隐藏文件和目录名将总是以一个“.”开头。看如下显示：

```
bash$ ls -al
total 794
drwxrwxrwt   4 root      root        8192 Jan
25 23:05 .
drwxr-xr-x  22 root      root        1024 Dec
28 18:07 ..
-rw-r--r--   1 berry     users          6 Jan
25 23:05 .pinetemp.000
drwxr-xr-x   2 berry     users       1024 Jan
25 23:05 .test
-rwx------   1 wood      users          1 Jan
25 18:28 19067haa
-rw-r--r--   1 berry     mail           1 Jan
16 12:38 filter.14428
-rw--------  1 rhey19    root      395447 Jan
24 02:59 pop3a13598
-rw--------  1 rhey19    root      395447 Jan
24 03:00 pop3a13600
drwxr-xr-x   4 root      root        1024 Jan
12 13:18 screens
.pinetemp.000 is a hidden file, and .test is a hidden
directory.
-rw-r--r--   1 berry     mail           1 Jan
16 12:38 filter.14428
row 1        row2        row3
```

现在，我们需要学习一些关于文件许可、用户和组群的知识。

Row #1 是文件许可。

Row #2 是文件权限。

Row #3 是文件的组群所有者。

文件许可被群组在3个不同的组群中。如果某一行开头为一个“ d”，那么这是一个目录；如果不是“d”，那么就是一个文件。

```
- ---  ---  ---
|| |  |--------> 其它 = 任何人都能访问
|| |-----------> 组群 = 通过验证的组群能够
访问
||-------------> 用户 = 只有所有者才能访
问
|-------------> 目录标志

- rw-  r--  r--
|| |  |--------> 其它 = 只能读文件
|| |-----------> 组群 = 只能读文件
||-------------> 用户 = 读写文件
|-------------> 这不是一个目录

- rwx  rwx  r-x
|| |  |--------> 其它 = 能读和执行文件
|| |-----------> 组群 = 能读写并且执行文件
||-------------> 用户 = 能读写并且执行文
件
|-------------> 这不是一个目录
```

所有者是在row #2中的用户名，而组群所有者是在row #3中的名字。

在DOS下，文件通常都有例如：a.exe,.

com，或者.bat的扩展名来执行，但是在UNIX下，你所需要的就是你的用户的组群、其他和组群中的“－－x”。

如果你拥有这些文件或者root权限，你就可以改变这些文件许可。

chmod oug+r filename 使所有3个组的文件许可都变成可读。

chmod og-r filename 使文件所有者对文件只能读(注意：－ or ＋ 设置文件许可是或否)。

chmod +x filename 使文件能够被所有人执行 。

chown username filename 使文件被另一个用户所有。

chgrp groupname filename 使文件被另一个组群所有。

确定保持文件许可和组群的原样！否则，你将被查出来，并且被系统踢出！改变系统配置可能会破坏其他的进程，所以，收好你的“爪子”！只做你肯定的事情；只使用你熟知的命令。你可能会发现你自己会在例如：“chown -R username /*”的命令上花去一年的时间。

四、Rlogin（远程登录命令）

这里，你还可以使用另一个命令，我们用Rlogin可以不使用口令而进入某个系统。

现在，去看看有关“Rlogin”的帮助信息。

这个命令的格式是：

```
rlogin -l username hostname
connecting....
password:
bash$
```

Rlogin需要用户在其主目录下有一个文件，来告诉他们对方是什么系统。在这个文件里，远程主机会做出如下显示：

```
username hostname (or) hostname
```

如果你在这个文件里加了 ＋ ＋，它将允许任何用户不需口令进入任何主机。

这个文件如下：

```
------cut here-------
+ +
------cut here-------
```

如果他们已经有了登录权限，你就能在他们的主目录下加入“＋ ＋”，但是记住：现在他们可能会注意到，他们不需要口令也能登录了。你最好瞄准那些还没有.rhosts文件的用户。

五、FTP(File Transfer Protocol，文件传送[输]协议)

另一种登录方法就是FTP了。你能在Windows环境下登录，也能在UNIX环境下登录：

ftp ftp.domain.com

这个协议允许你在对方站点上下载和上传文件。在登录后，别忘了在系统中的xferlog消除你的登录记录。记住：千万别FTP或者Telnet上一个已经被黑了的站点。如果你使用的是自己的系统，或者使用的是一台肉鸡，你可能会在那个站点上留下你的登录用户名和口令。那里可能已经被放了一个特洛伊木马或者嗅探器。所以，现在一旦你登录，就会留下你的登录用户名和口令。如果对方是系统管理员的话，还可能对你轻易进行报复 。

在UNIX环境下使用FTP，我建议使用几个命令 。

在你登录，并且出现提示符后，输入下面这几个命令：

```
prompt
hash
bin
```

提示符将允许你输入类似于（mget *）或者（mput *）的命令，而且能够在没有所有文件权限的时候传送整个活动目录。

hash标志

当目录还在传送时，你能看到hash在屏幕上显示 ＃＃＃＃＃＃＃＃＃＃＃＃，并且知道当前的传送速度。

bin将让你通过正确的方式得到文件，如果调用一个二进制文件，就可以肯定：它们都是没压缩的。

调用命令比较容易，get filename、put filename、使用mput，或者mget即可。

巧用IE的分级审查 拒绝恶意网站

文／志勇

现在恶意网站有增多的趋势，他们的行为很招人反感，开始时仅仅修改IE的主页，篡改IE的标题，如IE窗口的标题原来是“欢迎访问黑客防线——Microsoft Internet Explorer”，被恶意网站改为：“欢迎访问黑客防线——欢迎访问*****，www.***.com”，让人生厌。这还好办，解决办法大家都知道。可是后来这类恶意网站做的越来越过分了：点击按钮弹出无限IE窗口，使IE速度变慢，冻结IE的窗口，格式化访问者的硬盘，恶意修改注册表，使Windows 95/98/Me死机，使IE拒绝服务，访问者的硬盘被共享……。有关上述现象的描述，大家可以看看《黑客防线》2002年第4、5期劲风朋友的文章《网页恶意代码大曝光》，在此笔者就不赘述了。

对付这类网站，一般都是修改注册表（现在一般都有专用的工具，如兔子魔法、金山的一个专用工具等），进行IE设置，初级菜鸟看后多半会一愣一愣的（笔者没有贬低菜鸟的意思）。不过，即使这样辛辛苦苦修改完了，以后万一不小心又访问了该网站，岂不是又重蹈覆辙？

笔者在此讲述利用IE的分级审查功能来拒绝恶意网站，那些高手就不要看了吧，呵呵，本来就是给菜鸟们看的。*^o^*

Internet 是提供各类信息的广阔天地。但是，并非所有信息都适合浏览者。例如，要禁止小孩查看包含暴力或性等内容的网站。为此，微软公司在IE中添加了分级审查功能。

想想看，其实我们可以用分级审查的功能来拒绝恶意网站。只要我们网友互相交流互为补充，列个恶意网站黑名单，拒绝访问它们就可以了。

要使用分级审查功能，在“控制面板”中，打开Internet选项。

在“内容”选项卡上，在“分级审查”中，单击“启用”按钮（图1）。

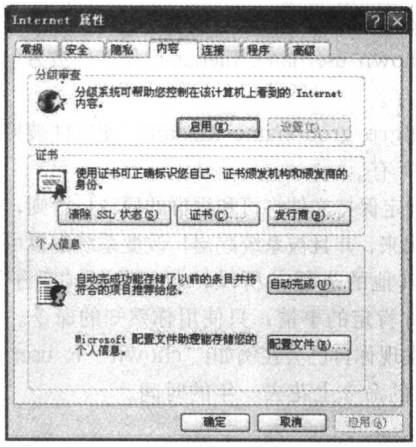

图1

如果已经启用“分级审查”（按钮显示为“禁用（E）…”的时候），请单击“设置”按钮，然后键入监督人密码（图2）。

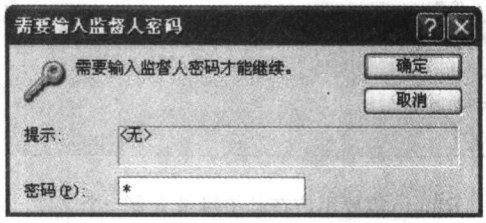

图2

单击“许可站点”选项卡（图3），在“允许该网站”中键入恶意网站的Internet地址，然后点击右边的“从不”按钮，让访问者从不能访问该恶意站点。对需要设置拒绝访问的每个恶意网站都重复该过程。

如果此前没有设置过监督人密码的话，这时候会让你设置一个（图4），完成以后弹出提示窗口（图5）。

这样，就可以预防登录被列入黑名单的恶意网

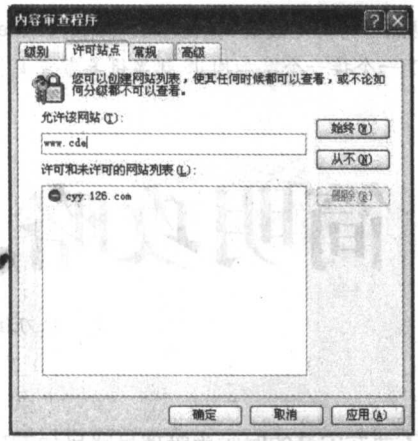

图 3

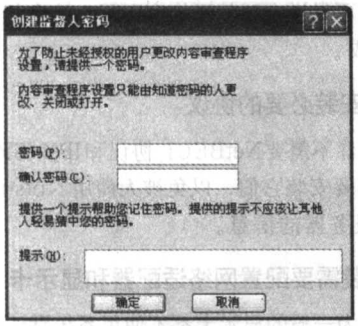

图 4

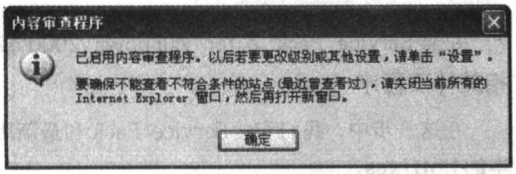

图 5

站了，当访问者登录已被列入黑名单的网站的时候，IE 会自动弹出这个窗口拒绝登录这个网站（图 6）——我们的目的达到了。

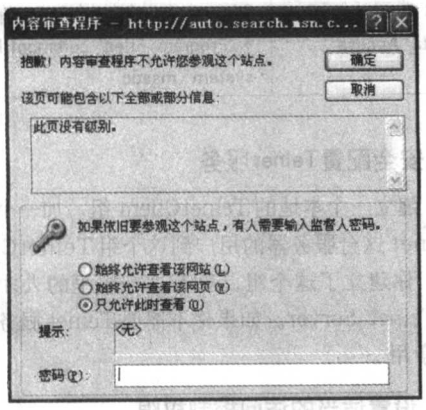

图 6

笔者写此文的本意是提供一个思路，鉴于菜鸟朋友不熟悉注册表，有些菜鸟的机器不够档次，安装能预防恶意网页代码的杀毒工具会过多消耗机器宝贵的资源，所以，用 IE 的分级审查功能不失为一个好的办法，关键在于广大网友互相通气，不断更新恶意网站黑名单。

声明：被列入恶意网站黑名单的所有者，跟提供者没有任何瓜葛，只是他们的所作所为惹怒了广大网友，被网友披露而曝光的。黑名单中的网站，笔者并没有一个一个验证，既然有很多网友揭发，也就被列入了黑名单，不排除后来又改邪归正的可能。笔者希望广大做网站的朋友，好自为之，不要再做这些无谓的事情，共同创造一个清洁健康的网络环境。

在此感谢广大热心网友的无私提供。让那些恶意网站如老鼠过街，人人喊打吧！

由于某种原因，笔者不便在此公开黑名单。不过，这类黑名单在网上就能找到，请读者发扬 DIY 精神，自己在网上搜索吧。

小知识

如何限制应用程序的使用？

只运行允许的 Windows 应用程序，可以防止在你的机器上运行你不想运行的程序。但使用该项功能时前，一定要谨慎，一旦有个程序没有列出，就无法运行它，所以 Regedit.exe 应首先列进去，不然将来想改可就改不回来了。在进行注册表操作的时候一定要注意：备份它！下面我们来看看具体的步骤吧：

1．找开注册表编辑器；

2．找到 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 下建立 RestrictRun，类型为 REG_DWORD；

3．设置其值为 1；

在 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\RestrictRun 下面建立 1，2，3 等项目，项目中包括应用程序名，只要应用程序名就可以了，不要路径，下面是一个例子：

建立值名 1 为的项目，它的类型为 REG_SZ，里面填一个应用程序名 X，这时候 X 是被允许运行的，其它程序不能被运行！