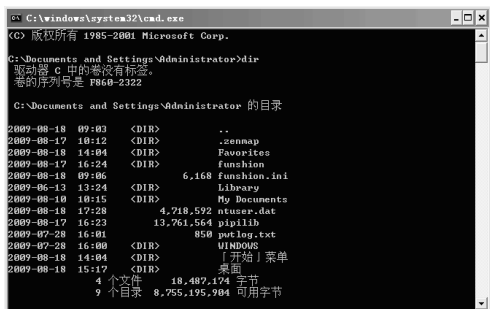


3.1 基本 DOS 命令

在 DOS 应用中,一些基本的命令是必须掌握的,例如查看目标主机的资源、路径的切换等。下面归纳了一些基本的 DOS 命令,帮助用户更好地学习 DOS。

3.1.1 Dir 命令

Dir 命令是显示磁盘目录命令。在命令提示符窗口中输入 Dir 命令,然后按下 Enter 键,即可查看当前目录下的资源列表。



```
C:\windows\system32\cmd.exe
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>dir
驱动器 C 中的卷没有标签。
卷的序列号是 F860-2322

C:\Documents and Settings\Administrator 的目录

2009-08-18 09:03 <DIR>      .
2009-08-17 18:12 <DIR>      ..
2009-08-18 14:04 <DIR>      Favorites
2009-08-17 16:24 <DIR>      Funshion
2009-08-18 09:06      6,168 Funshion.ini
2009-06-13 13:24 <DIR>      Library
2009-08-18 10:15 <DIR>      My Documents
2009-08-18 17:28      4,718,592 ntuser.dat
2009-08-17 16:23      13,761,564 pipilab
2009-07-28 16:01      850 putlog.txt
2009-07-28 16:00 <DIR>      WINDOWS
2009-08-18 14:04 <DIR>      [开始] 菜单
2009-08-18 15:17 <DIR>      桌面
          4 个文件      18,487,174 字节
          9 个目录      8,755,195,904 可用字节
```

根据资源列表中显示的文件/文件夹名称,可以轻松调用其中的文件资源,还可以进行路径的切换。对于一名黑客来说,必须记住 Dir 命令的/a 参数,该参数是查看目标主机中带有隐藏性质的文件,例如木马程序、病毒程序等。

使用 Dir 命令的格式为 DIR+盘符+路径+P+/W。

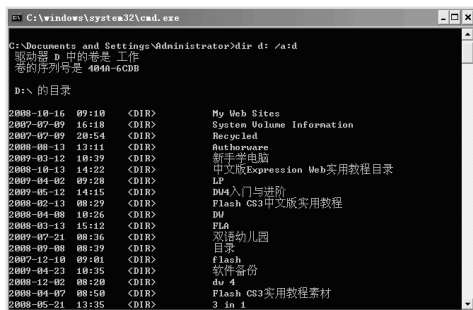
/P 作用是当要查看的目录太多,无法在一屏显示完屏幕会一直往上卷,不容易看清,加上/P 参数后,屏幕上会分面一次显示 23 行的文件信息,然后暂停,并提示 Press any key to continue(按下任意键继续)。

/W 作用是只显示文件名,至于文件大小及建立的日期和时间则都省略。加上参数后,每行可以显示 5 个文件名。

【例 3-1】在命令提示符窗口中使用 Dir 命令来查看 D 盘中的资源。

☒ 教学视频 ☐ 源文件

01 打开命令提示符窗口,输入 Dir d: /a:d 命令,按下 Enter 键,即可查看 D 盘下的所有文件目录。

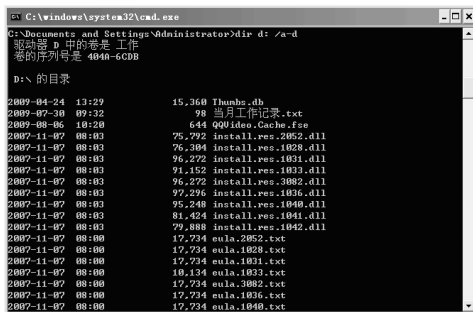


```
C:\windows\system32\cmd.exe
C:\Documents and Settings\Administrator>dir d: /a:d
驱动器 D 中的卷是 工作
卷的序列号是 4040-C0DB

D:\ 的目录

2008-10-16 09:10 <DIR>      My Web Sites
2009-07-09 16:18 <DIR>      System Volume Information
2009-07-09 20:54 <DIR>      Recycled
2008-08-13 13:11 <DIR>      Authware
2009-05-12 10:30 <DIR>      新手指南
2008-10-13 14:22 <DIR>      中文版Expression Web实用教程目录
2009-04-02 09:28 <DIR>      LP
2009-05-12 14:15 <DIR>      DM4入门与进阶
2008-02-13 08:29 <DIR>      Flash CS3中文版实用教程
2008-04-08 10:26 <DIR>      DM
2008-03-13 15:12 <DIR>      FLA
2009-07-21 08:36 <DIR>      目录
2008-09-08 08:39 <DIR>      Flash
2009-04-23 14:35 <DIR>      软件备份
2008-12-02 08:20 <DIR>      du 4
2008-04-07 08:50 <DIR>      Flash CS3实用教程素材
2008-05-21 13:35 <DIR>      2 in 1
```

02 输入 Dir d: /a-d 命令,按下 Enter 键,即可查看 D 盘下的所有文件。



```
C:\windows\system32\cmd.exe
C:\Documents and Settings\Administrator>dir d: /a-d
驱动器 D 中的卷是 工作
卷的序列号是 4040-C0DB

D:\ 的目录

2009-04-24 13:29      15,360 Thumb.db
2009-07-30 09:32      98 当月工作记录.txt
2009-08-06 18:20      644 QQIdeo.Cache.rse
2009-11-07 08:03      75,792 install.res.2052.dll
2009-11-07 08:03      76,304 install.res.1028.dll
2009-11-07 08:03      96,272 install.res.1031.dll
2009-11-07 08:03      91,152 install.res.1033.dll
2009-11-07 08:03      96,272 install.res.3082.dll
2009-11-07 08:03      97,296 install.res.1036.dll
2009-11-07 08:03      95,248 install.res.1040.dll
2009-11-07 08:03      81,424 install.res.1041.dll
2009-11-07 08:03      79,888 install.res.1042.dll
2009-11-07 08:00      17,734 amla.2052.txt
2009-11-07 08:00      17,734 amla.1028.txt
2009-11-07 08:00      17,734 amla.1031.txt
2009-11-07 08:00      18,134 amla.1033.txt
2009-11-07 08:00      17,734 amla.3082.txt
2009-11-07 08:00      17,734 amla.1036.txt
2009-11-07 08:00      17,734 amla.1040.txt
```

3.1.2 CD 命令

CD(Change Directory)命令是改变目录命令,可以用于切换路径目录。

CD 命令的使用主要有以下 3 种方法。

CD PATH: PATH 是路径的意思,例如输入 CD C:\Windows、CD \C:等。主要路径存在,在 CD 后面就可以输入该路径,否则提示错误信息。

CD..: CD 后面加上两个“.”号表示

回到上级父目录,例如当前命令提示符路径为 D:\users\administrator,输入 CD..命令,按下 Enter 键后,将会返回到上一级目录,即 D:\users 目录。

CD\ :表示当前提示符的路径无论在哪个子级目录下,立即返回根目录。

3.1.3 批处理

如果希望一次性执行多条命令,可以使用批处理文件。

批处理(Batch)也称为批处理脚本。顾名思义,就是对某对象进行批量的处理。DOS 批处理是基于 DOS 命令,用来自动地批量地执行 DOS 命令以实现特定操作的脚本。

批处理是一种简化的脚本语言,它应用于 DOS 和 Windows 系统中,它是由 DOS 或者 Windows 系统内嵌的命令解释器(通常是 COMMAND.COM 或者 CMD.EXE)解释运行。类似于 Unix 中的 Shell 脚本。批处理文件具有 .bat 或者 .cmd 的扩展名,例如逐行书写在命令行中会用到的各种命令。更复杂的情况,需要使用 if、for、goto 等命令控制程序的运行过程,类似于 C#、Basic 等中高级语言。如果需要实现更复杂的应用,利用外部程序是必要的,这包括系统本身提供的外部命令和第三方提供的工具或者软件。批处理文件,或称为批处理程序,是由一条条的 DOS 命令组成的普通文本文件,可以用记事本直接编辑或用 DOS 命令创建,也可以用 DOS 下的文本编辑器 Edit.exe 来编辑。在命令提示下输入批处理文件的名称,或者双击该批处理文件,系统就会调用 Cmd.exe 运行该批处理程序。一般情况下,每条命令占据一行;当然也可以将多条命令用特定符号(如: &、&&、|、||等)分隔后写入同一行中;还有的情况就是像 if、for 等较高级的

命令则要占据几行甚至几十几百行的空间。系统在解释运行批处理程序时,首先扫描整个批处理程序,然后从第一行代码开始向下逐句执行所有的命令,直至程序结尾或遇见 exit 命令或出错意外退出。

1. 创建批处理文件

要创建批处理文件,可以使用记事本和 Copy con 命令实现。

【例 3-2】使用记事本创建批处理文件。

☒ 教学视频 ☐ 源文件

01 打开一个记事本,输入 dir、md text 和 dir 命令,每个命令之间使用 Enter 键换行。

02 保存文档名称为 p1.bat。



(3) 生成的批处理文件如下图所示。

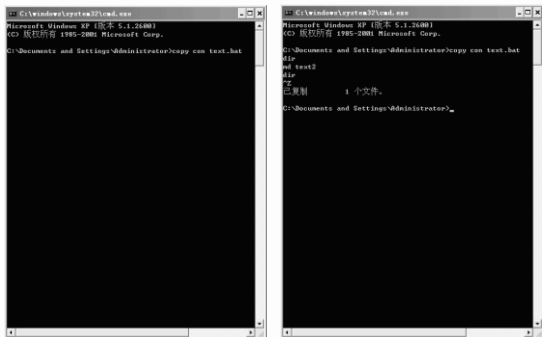


2. 使用 Copy Con 命令

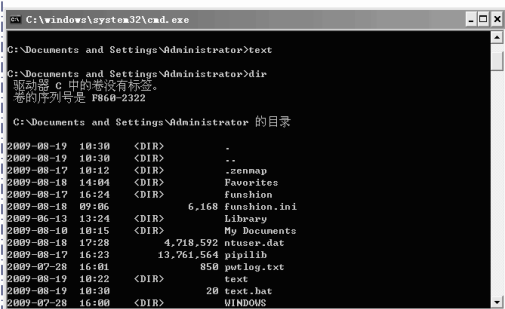
使用 copy con 命令创建批处理文件的方法很简单。打开命令提示符窗口,输入命令 Copy Con text.bat,然后按下 Enter 键。

接着输入 dir、md text、dir 命令,每个命令使用 Enter 键换行,输入完毕后按下 Ctrl+Z

键结束输入。按下 Enter 键，会显示“已复制 1 个文件”完毕内容，表示成功创建批处理文件。



创建批处理文件后，输入文件名称 text，按下 Enter 键，即可运行创建的批处理文件。



3.2 DOS 命令应用

在了解了 DOS 命令的一些基础知识后，下面介绍黑客在攻击时常用的一些命令，帮助用户更好地学习黑客攻防知识。

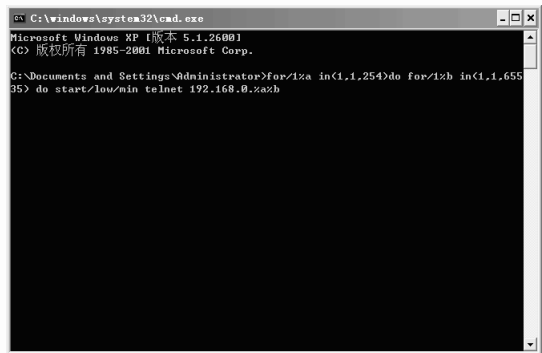
3.2.1 使用 DOS 命令扫描端口

如果没有扫描工具，就可以使用 DOS 命令对一个网段的所有端口进行扫描。下面通过实例来介绍使用 DOS 命令扫描端口的方法。

【例 3-3】使用 DOS 命令扫描端口。

☒ 教学视频 ☐ 源文件

01 打开命令提示符窗口，输入命令 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。



02 按下 Enter 键，即可扫描 192.168.0.x 这个网段所有开放的 3389 端口主机，同时尝试对主机进行 Telnet 登录，若登录失败则会在 5 秒内

自动退出。


3.2.2 Arp 命令

Arp 命令是黑客和网络管理员都常用的命令，可以通过此命令进行 IP 地址和 MAC 地址的欺骗，当然也可以使用该命令来修改 ARP 缓存表。

Arp 命令设计本意是用于显示和修改地址解析协议(ARP)缓存中的项目。ARP 缓存中包含一个或多个表，它们用于存储 IP 地址及其经过解析的以太网或令牌环物理地址。电脑上安装的每一个以太网或令牌环网络适配器都有自己单独的表。如果在没有参数的情况下使用，则 arp 命令将显示帮助信息。

1. Arp 命令语法

Arp 命令的语法为 arp[-a [InetAddr] [-N IfaceAddr]] [-g [InetAddr] [-N IfaceAddr]] [-d InetAddr [IfaceAddr]] [-s InetAddr EtherAddr [IfaceAddr]]。其中参数的含义如下。

 -a [InetAddr] [-N IfaceAddr]: 显示所有接口的当前 ARP 缓存表。要显示特

01章

02章

03章

04章

05章

06章

07章

08章

定 IP 地址的 ARP 缓存项, 请使用带有 InetAddr 参数的 arp -a, 此处的 InetAddr 代表 IP 地址。如果未指定 InetAddr, 则使用第一个适用的接口。要显示特定接口的 ARP 缓存表, 请将 -N IfaceAddr 参数与 -a 参数一起使用, 此处的 IfaceAddr 代表指派给该接口的 IP 地址。-N 参数区分大小写。

- ❶ -g [InetAddr] [-N IfaceAddr]: 与 -a 参数相同。
- ❷ -d InetAddr [IfaceAddr]: 删除指定的 IP 地址项, 此处的 InetAddr 代表 IP 地址。对于指定的接口, 要删除表中的某项, 请使用 IfaceAddr 参数, 此处的 IfaceAddr 代表指派给该接口的 IP 地址。要删除所有项, 请使用星号 (*) 通配符代替 InetAddr。
- ❸ -s InetAddr EtherAddr [IfaceAddr]: 向 ARP 缓存添加可将 IP 地址 InetAddr 解析成物理地址 EtherAddr 的静态项。要向指定接口的表添加静态 ARP 缓存项, 使用 faceAddr 参数。IfaceAddr 代表指派给该接口的 IP 地址。

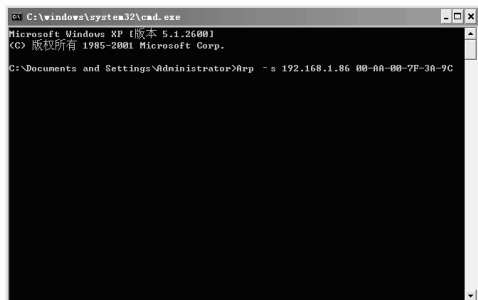
2. Arp 命令应用

当黑客入侵内部网络后, 可以在任意一台主机中使用 Arp -a 命令显示 ARP 缓存表。此外黑客也可以伪造 MAC 地址并与 IP 地址绑定, 下面通过实例介绍将 IP 地址与物理地址绑定的方法。

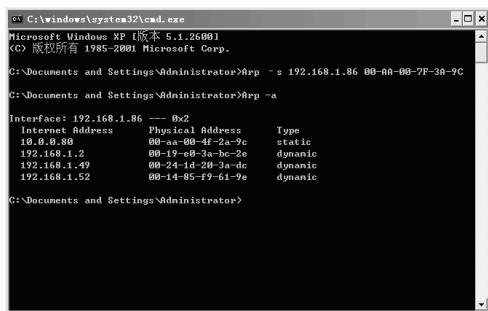
【例 3-4】使用 Arp 命令将 IP 地址与物理地址相互绑定。

☒ 教学视频 ☐ 源文件

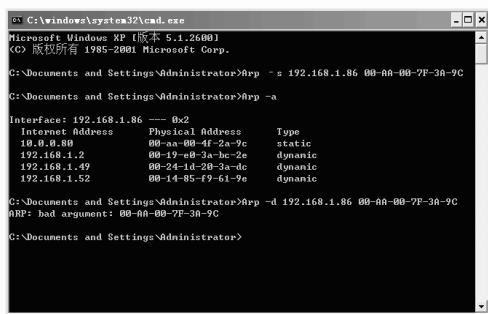
❶ 打开命令提示符窗口, 输入命令 Arp -s 192.168.1.86 00-AA-00-7F-3A-9C, 然后按下 Enter 键。



❷ 继续输入命令 Arp -a, 然后按下 Enter 键, 可以查看到 IP 地址与物理地址已经绑定。

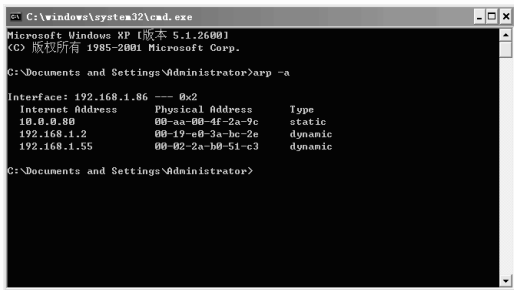


❸ 如果要删除 ARP 缓存中的 IP 地址与物理地址的绑定记录, 输入命令 Arp -d 192.168.1.86 00-AA-00-7F-3A-9C, 然后按下 Enter 键即可。



高手点拨

如果想要批量获取局域网中所有电脑的 MAC 地址, 首先使用 Ping 命令测试所有需要获取局域网中所有电脑的 MAC 地址, 然后输入 Arp -a 命令, 按下 Enter 键即可获得 Ping 过的局域网中所有电脑网卡的 MAC 地址和对应的 IP 地址。



3. 解决并防止 ARP 欺骗

采用双向绑定的方法可以有效地解决并且防止 ARP 欺骗。

首先获得安全网关的内网的 MAC 地址(例如 HiPER 网关地址 192.168.16.254 的 MAC 地址为 0022aa0022aa), 然后编写一个批处理文件 rarp.bat, 命令如下。

@echo off

Arp -d

Arp -s 192.168.16.254 00-22-aa-00-22-aa

将文件中的网关 IP 地址和 MAC 地址更改为实际使用的网关 IP 地址和 MAC 地址即可。最后将这个批处理软件移至【开始】菜单的【所有程序】|【启动】栏中。

4. Arp 常用命令

Arp 命令除了以上的应用外, 还有一些常用的命令, 有关命令与作用如下表所示。

命 令	作 用
Arp -a 或 arp -g	用于查看高速缓存中的所有项目。-a 和-g 参数的结果是一样的, 多年来-g 一直是 UNIX 平台上用来显示 ARP 高速缓存中所有项目的选项, 而 Windows 用的是 arp -a(-a 可被视为 all, 即全部的意思), 但它也可以接受比

较传统的-g 选项

(续表)

命 令	作 用
Arp a IP	如果有多个网卡, 那么使用 arp -a 加上接口的 IP 地址, 就可以只显示与该接口相关的 ARP 缓存项目
Arp -s IP 物理地址	可以向 ARP 高速缓存中人工输入一个静态项目。该项目在计算机引导过程中将保持有效状态, 或者在出现错误时, 人工配置的物理地址将自动更新该项目
Arp -d IP	人工删除一个静态项目

3.2.3 AT 命令

AT 即 Attention, AT 指令集是从终端设备(Terminal Equipment, TE)或数据终端设备(Data Terminal Equipment, DTE)向终端适配器(Terminal Adapter, TA)或数据电路终端设备(Data Circuit Terminal Equipment, DCE)发送的。通过 TA、TE 发送 AT 指令来控制移动台(Mobile Station, MS)的功能, 与 GSM 网络业务进行交互。用户可以通过 AT 指令进行呼叫、短信、电话本、数据业务、传真等方面的控制。

1. AT 命令语法

AT 命令列出了在指定的时间和日期计算机运行的已计划命令或程序。必须正在运行计划服务才能使用 AT 命令。它的语法如下:

at [\computername] [[id] [/delete] | /delete [/yes]]
at [\computername] time [/interactive] [/every:date[,...]] /next:date[,...]] command

2. AT 命令参数

有关 AT 命令语法参数的具体含义如下。

01章

02章

03章

04章

05章

06章

07章

08章

- ❶ `\\computername`: 指定远程计算机。如果省略该参数, 命令将安排在本地计算机。
- ❷ `id`: 指定指派给已计划命令的识别码。
- ❸ `/delete`: 取消已计划的命令。如果省略了 `id`, 计算机中已计划的命令将被全部取消。
- ❹ `/yes`: 当删除已计划的事件时, 对系统的查询强制进行肯定的回答。
- ❺ `Time`: 指定运行命令的时间。将时间以 24 小时标记的方式表示, 即为小时:分钟。
- ❻ `/interactive`: 允许作业与在作业运行时登录用户的桌面进行交互。
- ❼ `/every:date[,...]`: 在每个星期或月的指定日期(例如, 每个星期四或每月的第三天)运行命令。将 `date` 指定为星期的一天或多天(M,T,W,Th,F,S,Su), 或月的一天或多天(使用 1~31 的数字)。用逗号分隔多个日期项。如果省略了 `date`, 将假定为该月的当前日期。
- ❽ `/next:date[,...]`: 在重复出现下一天(例如, 下个星期四)时, 运行指定命令将 `date` 指定为星期的一天或多天(M,T,W,Th,F,S,Su), 或月的一天或多天(使用 1~31 的数字)。用逗号分隔多个日期项。如果省略了 `date`, 将假定为该月的当前日期。
- ❾ `Command`: 指定要运行的 Windows 2000 命令、程序(.exe 或 .com 文件)或批处理程序(.bat 或 .cmd 文件)。当命令需要路径作为参数时, 请使用绝对路径, 也就是从驱动器号开始的整个路径。如果命令在远程计算机上, 请指定服务器和共享名的 UNC 符号, 而不是远程驱动器号。如果命令不是

可执行(.exe)文件, 必须在命令前加上 `cmd /c`, 例如: `cmd /c dir > c:\test.out`

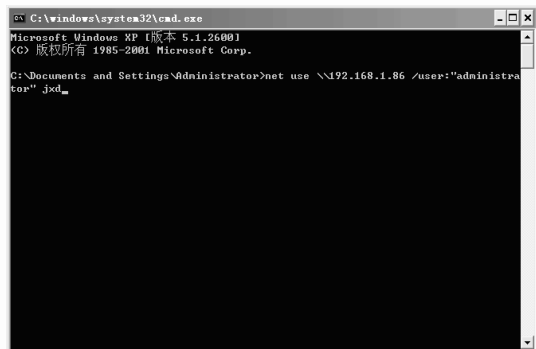
3. AT 命令应用

下面通过实例介绍 AT 命令的应用, 设置 IP 为 192.168.1.86 这台远程电脑在 12 点执行 `srv.exe` 程序。

【例 3-5】使用 AT 命令控制远程电脑执行程序。

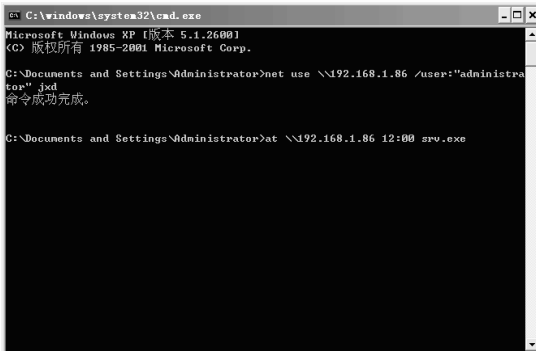
☒ 教学视频 ☐ 源文件

❶ 打开命令提示符窗口, 输入 `net use \\192.168.1.86 /user:"administrator" jxd` 命令, 其中 `administrator` 是帐户名称, `jxd` 是帐户密码, 但必须先确定 192.168.1.86 这台远程电脑有该帐户的存在。



❷ 按下 Enter 键, 当提示“命令成功完成”内容后, 表示已经成功登录 192.168.1.86 远程电脑。

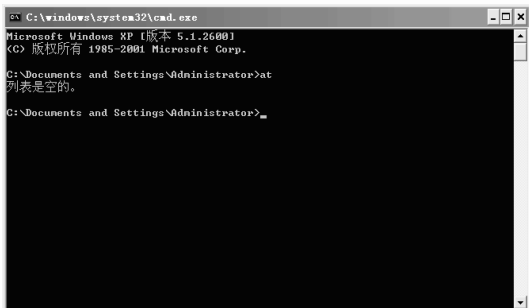
❸ 输入命令 `at \\192.168.1.86 12:00 srv.exe`, 按下 Enter 键完成操作。



高手点拨

如果提示“服务尚未开启”，表示远程电脑的 Task Scheduler 服务被关闭。

此外，在命令提示符窗口中输入 AT 命令，然后按下 Enter 键，可以查看本机正在执行的所有任务，如果没有创建任何任务，会提示“列表是空的”文本内容。



知识点滴

在使用 AT 命令时，Task Scheduler 服务必须已经运行。此外，必须成功登录远程电脑以获取执行 AT 命令的权限。

3.2.4 Del 命令

Del 即 Delete(删除)的缩写，它的作用就是删除文件。在黑客攻击目标主机时，首先使用的就是删除命令，使用 Del 命令，可以删除指定的文件，常用于在命令行中完成文件夹或文件的删除任务。

Del 命令的语法为 Del [Drive:][Path]FileName [...][p][f][s][q][a[:Attributes]]，其中各参数的作用如下。

- 🔗 [Drive:][Path]FileName：指定要删除的文件或文件来的位置和名称。FileName 是必需的。如果要使用多个文件名，可以使用空格、逗号或分号隔开文件名。
- 🔗 /P：删除每一个文件之前提示确认。
- 🔗 /F：强制删除只读文件。
- 🔗 /S：从所有子目录删除指定文件。

- 🔗 /Q：安静模式。删除全局通配符时，不要求确认。
- 🔗 /A：根据属性选择要删除的文件。
- 🔗 Attributes：可以是下列文件中的任意一种，r 为只读，a 为存档，s 为系统，h 为隐藏，- 为前缀标明“非”。

在了解了语法和参数作用后，如果要删除 D 盘分区中的 text 文件中所有文件，以下几种命令都可以实现。

- 🔗 Del d:\text
- 🔗 Del d:\text*.*
- 🔗 Del d:\text\.*.*

需要注意的是，使用 Del 命令删除的文件将不会保留在【回收站】中。

3.2.5 RD 命令

除了使用 Del 命令外，还可以使用 Rmdir(RD)命令删除目录或子目录。该命令语法为：

Rmdir [Drive:]Path[/s][q]
Rd [Drive:]Path[/s][q]

其中各参数作用如下。

- 🔗 [Drive]Path：指定要删除目录的位置和名称。
- 🔗 /s：删除指定目录和所有子目录以及包含的所有文件。
- 🔗 /q：在安静模式中运行 Rmdir，无需确认即可删除目录。

1. 删除当前目录

如果要删除当前目录，必须返回到其上一级目录下，例如命令提示符路径为 C:\a\b，要删除 b 这个目录，就必需退回到 C:\a 目录下。

知识点滴

在执行删除当前目录操作之前，必须首先清空目录中的内容。

01章

02章

03章

04章

05章

06章

07章

08章

2. 删除所有文件和子目录

要删除当前目录下的所有文件和子目录，例如删除路径 C:\a\b，输入命令 `RdC:/s/a`，然后按下 Enter 键即可。

该命令相当于 `Deltree` 命令，可以一次性将所需删除目录下的所有资源全部删除，需要注意的是，不能删除包含隐藏文件或系统文件的目录。

3.2.6 Systeminfo 命令

使用 `Systeminfo` 命令可以快速获取目标主机的各种信息，例如操作系统版本、安装的 SP 版本号等。

`Systeminfo` 命令的语法为：

`SYSTEMINFO [/S system [/U username [/P password]]] [/FO format] [/NH]`，其中各参数的作用如下。

- `/S system`：指定要连接的远端系统。
- `/U [domain]user`：指定要执行命令的使用者内容。
- `/P [password]`：指定提供的使用者内容的密码。
- `/FO format`：指定输出的显示格式。有效值为 `TABLE`、`LIST` 或 `CSV`。
- `/NH`：指定"Column Header"是否显示输出。

打开命令提示符窗口，输入 `Systeminfo` 命令，然后按下 Enter 键，即可显示本机操作系统信息。

```
命令提示符
C:\Documents and Settings\Administrator>systeminfo

主机名: CHINA-20F6B5D2D
OS 名称: Microsoft Windows XP Professional
OS 版本: 5.1.2600 Service Pack 3 Build 2600
OS 制造商: Microsoft Corporation
OS 配置: 独立工作站
OS 硬件类型: Multiprocessor Free
注册的所有人: USER
注册的组织: CHINA
产品 ID: 76481-648-8834885-23854
初始安装日期: 2002-6-1, 18:10:41
系统启动时间: 0 天 1 小时 49 分 57 秒
系统制造商: F4M80P
系统类型: x86-based PC
安装: 1 个处理器
处理器: [01]: x86 Family 15 Model 4 Stepping 9 GenuineIntel ~3054 Mhz
BIOS 版本: F4M80P - 42302e31
Windows 目录: C:\windows
系统目录: C:\windows\system32
启动设备: \Device\HarddiskVolume1
系统区域设置: zh-cn; 中文(中国)
输入法区域设置: zh-cn; 中文(中国)
时区: 默认
```

如果要查看远程电脑的系统信息，例如 IP 地址为 192.168.1.86，输入命令 `Systeminfo /s 192.168.1.86`，然后按下 Enter 键即可。

```
命令提示符

[05]: File 1
[06]: File 1
[07]: File 1
[08]: File 1
[09]: File 1
[10]: G147222
[11]: KB9246782_WMP10
[12]: KB923689
[13]: KB958215-IE7
[14]: KB960714-IE7
[15]: KB98461 - Update
[16]: KB94263 - Update
[17]: kb950259 - Update
[18]: KB950760 - Update
[19]: KB950762 - Update
[20]: KB951376 - Update
[21]: KB951698 - Update
安装了 1 个 NIC:
[01]: Realtek RTL8139 Family PCI Fast Ethernet NIC
连接名: 本地连接
启用 DHCP: 否
IP 地址: [01]: 192.168.1.86

C:\Documents and Settings\Administrator>
```

在显示的信息列表中，用户可以查看操作系统的名称、内部版本号以及 SP 补丁包的版本情况。在【角色】中分别是默认值为 1 的域控制器；默认值为 2 的成员服务器；默认值为 3 的工作组，这些信息对于黑客来说非常重要，通过这些探测信息可以决定攻击的方法。

3.2.7 Ipconfig 命令

`Ipconfig` 命令用于显示当前的 TCP/IP 配置的设置值。这些信息一般用来检验人工配置的 TCP/IP 设置是否正确。如果希望快速获取当前电脑的所有网络配置信息，就必须掌握 `Ipconfig` 命令。

1. Ipconfig 命令常用参数

下面介绍 `Ipconfig` 命令使用到的一些常用参数，用户必须熟练掌握这些参数。

- ❶ `Ipconfig /all`: 显示本机 TCP/IP 配置的详细信息。
- ❷ `Ipconfig /release`: DHCP 客户端手工释放 IP 地址。
- ❸ `Ipconfig /renew`: DHCP 客户端手工向服务器刷新请求。
- ❹ `Ipconfig /flushdns`: 清除本地 DNS 缓存内容。
- ❺ `Ipconfig /displaydns`: 显示本地 DNS 内容。
- ❻ `Ipconfig /registerdns`: DNS 客户端手工向服务器进行注册。
- ❼ `Ipconfig /showclassid`: 显示网络适配器的 DHCP 类别信息。
- ❽ `Ipconfig /setclassid`: 设置网络适配器的 DHCP 类别。
- ❾ `Ipconfig /renew "Local Area Connection"`: 更新本地连接适配器的由 DHCP 分配 IP 地址的配置。
- ❿ `Ipconfig /showclassid Local*`: 显示名称以 Local 开头的所有适配器的 DHCP 类别 ID。
- ⓫ `Ipconfig /setclassid "Local Area Connection" TEST`: 将本地连接适配器的 DHCP 类别 ID 设置为 TEST。

2. 参数说明

下面介绍有关 `Ipconfig` 命令参数的详细作用和显示信息。

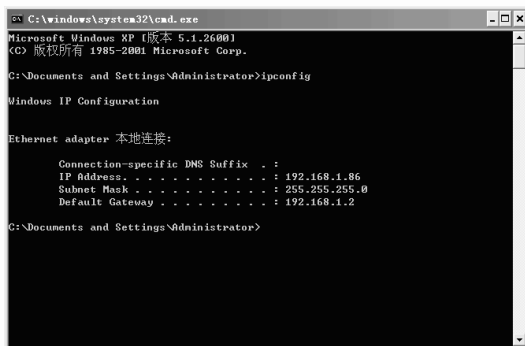
- ❶ `/all`: 显示所有网络适配器(网卡、拨号连接等)的完整 TCP/IP 配置信息。与不带参数的用法相比,它的信息更全更多,如 IP 是否动态分配、显示网卡的物理地址等。
- ❷ `/batch 文件名`: 将 `Ipconfig` 所显示信息以文本方式写入指定文件。此参数

可用来备份本机的网络配置。

- ❸ `/release_all` 和 `/release N`: 释放全部(或指定)适配器的由 DHCP 分配的动态 IP 地址。此参数适用于 IP 地址非静态分配的网卡,通常和 `renew` 参数结合使用。
- ❹ `ipconfig /renew_all` 或 `ipconfig /renew N`: 为全部(或指定)适配器重新分配 IP 地址。此参数同样仅适用于 IP 地址非静态分配的网卡,通常和上文的 `release` 参数结合使用。

3. Ipconfig 命令应用

在入侵目标主机后,可以使用 `Ipconfig` 命令查看所有网卡的 TCP/IP 配置,例如在命令提示符窗口中输入 `Ipconfig` 命令,按下 Enter 键,即可查看所有网卡的 IPv6 地址或 IPv4 地址、子网掩码和默认网关等信息。



此外,输入 `Ipconfig /batch bak-netcfg` 命令可以将有关网络配置的信息备份到文件 `bak-netcfg` 中。

```
C:\windows\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : 
    IP Address . . . . . : 192.168.1.86
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.2

C:\Documents and Settings\Administrator>ipconfig /batch bak-netcfg

Error: unrecognized or incomplete command line.

USAGE:
    ipconfig [/? | /all | /renew [adapter] | /release [adapter] |
    /flushdns | /displaydns | /registerdns |
    /showclassid adapter | /setclassid adapter {classid} ]
```

输入 `Ipconfig /release 1` 命令去除网卡(适配器 1)的动态 IP 地址。输入 `Ipconfig /renew 1` 命令, 可以为网卡重新动态分配 IP 地址。

3.2.8 Netstat 命令

Netstat 在前面章节中也有提到过, 它是一个监控 TCP/IP 网络的非常有用的工具, 它可以显示路由表、实际的网络连接以及每一个网络接口设备的状态信息。Netstat 用于显示与 IP、TCP、UDP 和 ICMP 协议相关的统计数据, 一般用于检验本机各端口的网络连接情况。

1. Netstat 命令选项

Netstat 命令相关的选项主要有以下几种。

- netstat -s:** 能够按照各个协议分别显示其统计数据。如果应用程序(如 IE 浏览器)运行速度比较慢, 或者不能显示 Web 页之类的数据, 那么用户就可以用本选项来查看所显示的信息。需要仔细查看统计数据的各行, 找出出错关键字, 进而确定问题所在。
- netstat -e:** 用于显示关于以太网的统计数据。它列出的项目包括传送的数据包的总字节数、错误数、删除数、数据包的数量和广播的数量。这些统计数据既有发送的数据包数量, 也有接收的数据包数量。这个选项可以用来统计一些基本的网络流量。

- netstat -r:** 可以显示关于路由表的信息, 类似于后面将要讲的使用 `route print` 命令时看到的信息。除了显示有效路由外, 还显示当前有效的连接。
- netstat -a:** 本选项显示一个所有的有效连接信息列表, 包括已建立的连接 (ESTABLISHED), 也包括监听连接请求 (LISTENING) 的那些连接。
- netstat -n:** 显示所有已经建立的有效连接。

2. Netstat 命令应用

要查看本机电脑上网时各端口与外部之间的所有连接情况信息, 只需在命令提示符窗口中输入 Netstat 命令, 按下 Enter 键即可。

```
C:\windows\system32\cmd.exe
C:\Documents and Settings\Administrator>netstat

Active Connections

Proto Local Address Foreign Address State
TCP china-20f6b5d2d:1828 localhost:18888 ESTABLISHED
TCP china-20f6b5d2d:2425 localhost:2426 ESTABLISHED
TCP china-20f6b5d2d:2426 localhost:2425 ESTABLISHED
TCP china-20f6b5d2d:2427 localhost:2428 ESTABLISHED
TCP china-20f6b5d2d:2428 localhost:2427 ESTABLISHED
TCP china-20f6b5d2d:18888 localhost:1828 ESTABLISHED
TCP china-20f6b5d2d:5903 211.155.228.24:http ESTABLISHED
TCP china-20f6b5d2d:6966 121.10.120.174:9877 CLOSE_WAIT
TCP china-20f6b5d2d:8081 218.2.247.83:http ESTABLISHED
TCP china-20f6b5d2d:9464 58.49.59.17:http ESTABLISHED
TCP china-20f6b5d2d:9465 58.49.59.17:http ESTABLISHED
TCP china-20f6b5d2d:9466 58.49.59.17:http ESTABLISHED
TCP china-20f6b5d2d:9467 58.49.59.17:http ESTABLISHED
TCP china-20f6b5d2d:9472 58.49.59.17:http ESTABLISHED
TCP china-20f6b5d2d:9473 58.49.59.17:http ESTABLISHED
TCP china-20f6b5d2d:9474 58.49.59.17:http ESTABLISHED
TCP china-20f6b5d2d:9475 58.49.59.17:http ESTABLISHED
TCP china-20f6b5d2d:9480 58.49.59.17:http ESTABLISHED
TCP china-20f6b5d2d:9481 58.49.59.17:http ESTABLISHED
TCP china-20f6b5d2d:9482 58.49.59.17:http ESTABLISHED
```

如果要检查共享服务端口的 137、138 和 139 端口开放情况, 输入 `Netstat -ao` 命令, 然后按下 Enter 键即可。

```
C:\windows\system32\cmd.exe
C:\Documents and Settings\Administrator>netstat -ao

Active Connections

Proto Local Address Foreign Address State PID
TCP china-20f6b5d2d:smtp china-20f6b5d2d:0 LISTENING 1368
TCP china-20f6b5d2d:http china-20f6b5d2d:0 LISTENING 1368
TCP china-20f6b5d2d:81 china-20f6b5d2d:0 LISTENING 1728
TCP china-20f6b5d2d:pppoe china-20f6b5d2d:0 LISTENING 824
TCP china-20f6b5d2d:http china-20f6b5d2d:0 LISTENING 1368
TCP china-20f6b5d2d:microsoft-ds china-20f6b5d2d:0 LISTENING 4
TCP china-20f6b5d2d:1826 china-20f6b5d2d:0 LISTENING 1368
TCP china-20f6b5d2d:8137 china-20f6b5d2d:0 LISTENING 34408
TCP china-20f6b5d2d:18086 china-20f6b5d2d:0 LISTENING 2256
TCP china-20f6b5d2d:18087 china-20f6b5d2d:0 LISTENING 2256
TCP china-20f6b5d2d:18088 china-20f6b5d2d:0 LISTENING 2256
TCP china-20f6b5d2d:12034 china-20f6b5d2d:0 LISTENING 6400
TCP china-20f6b5d2d:18080 china-20f6b5d2d:0 LISTENING 2256
TCP china-20f6b5d2d:1826 localhost:18888 ESTABLISHED 2336
TCP china-20f6b5d2d:1832 china-20f6b5d2d:0 LISTENING 3324
TCP china-20f6b5d2d:2425 localhost:2426 ESTABLISHED 18088
TCP china-20f6b5d2d:2426 localhost:2425 ESTABLISHED 18088
TCP china-20f6b5d2d:2427 localhost:2428 ESTABLISHED 18088
TCP china-20f6b5d2d:2428 localhost:2427 ESTABLISHED 18088
```

在反馈的信息中可以查看到 NetBIOS-ns、NetBIOS-dgm、NetBIOS-ssn 信息, 分别代表了

137、138 和 139 端口进程开放情况。

3.2.9 Ping 命令

Ping (Packet Internet Grope), 因特网包探索器, 用于测试网络连接量的程序。Ping 发送一个 ICMP 回声请求消息给目的地并报告是否收到所希望的 ICMP 回声应答。

1. Ping 命令参数

Ping 命令的语法为:

Ping [-t] [-a] [-n Count] [-l Size] [-f] [-I TTL] [-v TOS] [-r Count] [-s Count] [{-j HostList | -k HostList}] [-w Timeout] [TargetName]。

下面详细介绍了有关 Ping 命令的参数作用。

- t: 不断使用 Ping 命令发送回响请求信息到目标主机。按下 Ctrl+C 键可以中断并退出 Ping。
- a: 指定对目标主机 IP 地址进行反向名称解析, 如果解析成功, Ping 将显示主机名。例如输入命令 Ping -a 192.168.1.86, 得到下图所示的 NetBIOS 名称, 其中 china-20f6b5d2d 就是目标主机名称。

```
C:\windows\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping -t
IP address must be specified.

C:\Documents and Settings\Administrator>ping -a 192.168.1.86

Pinging china-20f6b5d2d [192.168.1.86] with 32 bytes of data:

Reply from 192.168.1.86: bytes=32 time<1ms TTL=128
Reply from 192.168.1.86: bytes=32 time<1ms TTL=128
Reply from 192.168.1.86: bytes=32 time<1ms TTL=128
Reply from 192.168.1.86: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.86:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>
```

- n Count: 指定发送回响请求消息的次数, 默认值为 4。可以自己定义发送的个数, 对衡量网络速度很有帮助, 例如测试发送 50 个数据包的返

回的平均时间为多少, 最快时间为多少, 最慢时间为多少, 就可以输入命令 Ping -n 50 192.168.1.86。

- l Size: 在默认情况下, ping 发送的数据包大小为 32byt, 用户可以自定义它的大小, 但有一个大小的限制, 就是最大只能发送 65500byt。虽然大小被限制, 但该参数配合其他参数以后危害依然非常大。
- f: 一般情况下发送的数据包都会通过路由分段再发送给对方, 加上该参数以后路由就不会再分段处理。
- i TTL: 指定发送回响请求消息的 IP 标题中的 TTL 字段值。默认值是主机的默认 TTL 值, 对于 Windows 系统来说, 该值一般是 128, TTL 的最大值为 225。
- v TOS: 指定发送回响请求消息的 IP 标题中将【服务类型】字段设置为 TOS 指定的值, 默认值为 0。
- r Count: 一般情况下发送的数据包是通过一个个路由才到达对方的, 通过该参数就可以设定想探测经过的路由的个数, 但这里限制在 9 个, 也就是说只能跟踪到 9 个路由, 如果想探测更多, 可以通过其他命令实现。

```
C:\windows\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping -n 1 -r 9 192.168.1.86

Pinging 192.168.1.86 with 32 bytes of data:

Reply from 192.168.1.86: bytes=32 time<1ms TTL=128
    Route: 192.168.1.86

Ping statistics for 192.168.1.86:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>
```

- s Count: 指定 IP 标题中的【Internet 时间戳】选项用于记录每一个跃点的

01章

02章

03章

04章

05章

06章

07章

08章

回响请求消息和响应的回响应答消息的到达时间。Count 的最小值必须为 1, 最大值为 4。

- -j Path: 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 3。
- -k HostList: 利用 computer-list 指定计算机列表的路由数据包。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: 指定超时时间, 单位为毫秒。
- TargetName: 指定目的端, 可以是 IP 地址, 也可以是主机名。

2. Ping 命令各类反馈信息

在使用 Ping 命令时, 通常会反馈 Request timed out、Destination host Unreachable 等信息, 下面详细介绍使用 Ping 命令后反馈的主要信息说明。

- Request timed out: 对方已关机; 对方与自己不在同一网段内, 通过路由也无法找到对方; 设置了 ICMP 数据包过滤; 错误设置 IP 地址。
- Destination host Unreachable: 对方与本机不在同一网段内, 而本机又未设置默认的路由, 例如上例中 A 机中未设定默认的路由, 运行 Ping 命令就会出现 Destination host Unreachable。

知识点滴

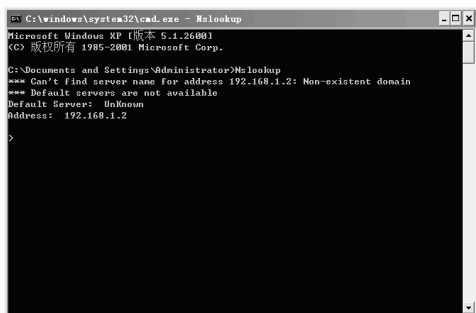
destination host unreachable 和 time out 的区别在于如果所经过的路由器的路由表中具有到达目标的路由, 而目标因为其他原因不可到达, 这时候会显示 time out, 如果路由表中连到达目标的路由都没有, 那就会显示

destination host unreachable。

- Bad IP address: 没有连接到 DNS 服务器, 所以无法解析这个 IP 地址, 也可能是 IP 地址不存在。
- Source quench received: 表示对方或中途的服务器繁忙无法回应。
- Unknown host(不知名主机): 该远程主机的名字不能被域名服务器(DNS)转换成 IP 地址。故障原因可能是域名服务器有故障, 或者名字不正确, 或者网络管理员的系统与远程主机之间的通信线路有故障。
- No answer(无响应): 说明本地系统有一条通向中心主机的路由, 但却接收不到它发给该中心主机的任何信息。故障原因可能是中心主机没有工作、本地或中心主机网络配置不正确、本地或中心的路由器没有工作、通信线路有故障、中心主机存在路由选择问题。
- no rout to host: 网卡工作不正常。
- transmit failed,error code: 10043 网卡驱动不正常。
- unknown host name: DNS 配置错误。

3.2.10 Nslookup 命令

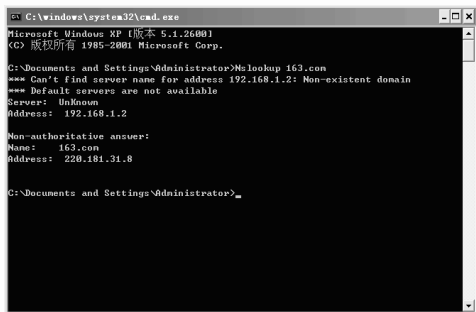
Nslookup 命令可以用来监测网络中 DNS 服务器是否能正确实现域名解析。在命令提示符窗口中输入 Nslookup 命令, 按下 Enter 键, 反馈信息如下图所示。



黑客可以通过反馈的信息探测目标网站绑定的 IP 地址数量，找准攻击 IP 地址范围。

Nslookup 命令有许多子命令可以使用，例如 ls 命令可以列出域名系统(DNS)域的信息。如果要默认将查询类型更改为主机信息，并将超时时间更改为 30 秒，输入命令 Nslookup -querytype=hinfo -timeout=30 即可。

使用 Nslookup 命令最简单的用法是查询网站域名对应的 IP 地址，包括 A 记录、MX 记录、NS 记录、CHAME 记录等。在命令提示符窗口中输入要查询的网站 IP 地址，例如 Nslookup 163.com，然后按下 Enter 键，即可显示 163.com 这个域名的相关信息。

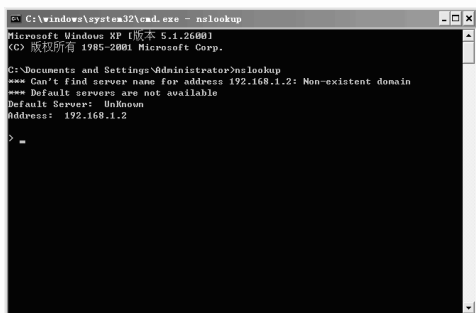


在实际应用中，黑客都是预先知道攻击网站使用的 IP 地址群，然后确定攻击的范围。下面以查询 www.sina.com.cn 网站为例，使用 Nslookup 命令查询 IP 地址列表。

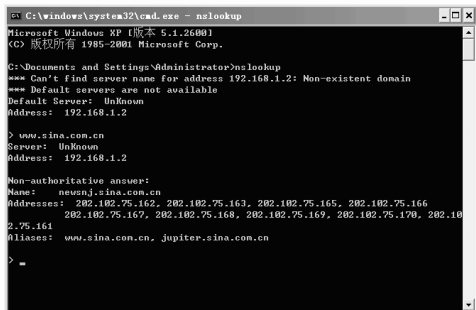
【例 3-6】 使用 Nslookup 命令查询 IP 地址列表。

☒ 教学视频 ☐ 源文件

01 打开命令提示符窗口，输入 Nslookup 命令，然后按下 Enter 键得到反馈信息。



02 输入查询的网站域名地址 www.sina.com.cn，然后按下 Enter 键，在反馈信息中可以获取 IP 地址列表。



获得 IP 地址列表是非常重要的，入侵者可以在多台服务器中尝试入侵。

3.2.11 Net 命令

Net 命令是功能强大的以命令行方式执行的工具。它包含了管理网络环境、服务、用户、登录等重要管理功能。使用它可以轻松地管理本地或者远程计算机的网络环境，以及各种服务程序的运行和配置。使用它还可以进行用户管理和登陆管理等。Net 命令是黑客最常用的命令之一。

Net 命令应用的范围非常广泛，下面主要介绍有关网络安全方面的命令。

1. Net computer 命令

Net computer 命令可以从域数据库中添加或删除计算机，所有计算机的添加和删除都会

转发到主域控制器。该命令语法为：`net computer \\computername {/add | /del}`，其中各参数的作用如下。

- `\\computername`：指定要从域中添加或删除的计算机名。
- `/add`：将特定的计算机添加到域中。
- `/del`：从域中删除指定的计算机。

2. Net file 命令

`Net file` 命令可以显示某服务器上所有打开的共享文件名及锁定文件数。该命令也可以关闭个别文件并取消文件锁定。该命令语法为 `net file [id [/close]]`，其中各参数作用如下。

- `id`：指定文件的标识号。
- `/close`：关闭打开的文件并释放锁定记录。请从共享文件的服务器中键入该命令。

3. Net session 命令

`Net session` 命令可以列出或断开本地计算机和与之连接的客户端的会话。该命令语法为 `net session [\\computername] [/delete]`，其中各参数作用如下。

- `\\computername`：标识要列出或断开会话的计算机。
- `/delete`：结束与 `\\computername` 计算机会话并关闭本次会话期间计算机的所有打开文件。如果省略 `\\computername` 参数，将取消与本地计算机的所有会话。

4. Net share 命令

`Net share` 命令用于创建、删除或显示共享资源。该命令语法为：

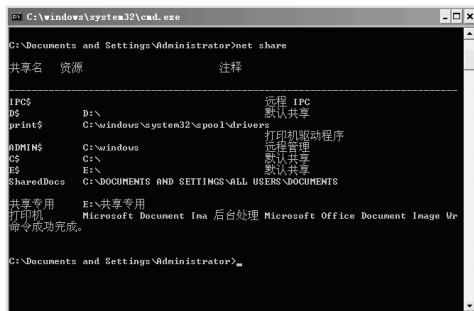
`Net share [sharename]`

`Net share [shareName=Drive:Path [{/users: Number | /unlimited}}] [/remark: "Text"] [/cache: {manua | automatic | no}]`

`Net share [{ShareName | Drive:Path}]/delete]`
该命令各参数的作用如下。

- `ShareName`：指定共享资源的网络名称，输入带参数 `ShareName` 的 `Net share` 命令仅显示有关该共享的信息。
- `Drive:Path`：指定共享目录绝对路径。
- `/user:Number`：设置可以同时访问共享资源的用户数。
- `/unlimited`：指定可以同时访问共享资源数量不受限制的用户。
- `/remark:"Text"`：添加关于资源的描述性注释，给外部内容加上引号。
- `/cache>manual`：启用带手动重新集成的脱机客户端缓存。
- `/cache:automatic`：启用带自动重新集成的脱机客户端缓存。
- `/cache:documents`：启用共享文档中的自动缓存。
- `/cache:programs`：启用文档和程序的自动缓存。
- `/cache:no`：禁用缓存。
- `/delete`：停止共享资源。

在命令提示符窗口中输入命令 `Net share`，按下 `Enter` 键，可以显示本地电脑上的共享资源信息。



如果要使用共享名 `DataShare` 作为本机电脑中的 `e:\共享专用` 目录并包括注释，输入命令 `Net Share DataShare=e:\共享专用 \remark: "For department123."`，然后按下 `Enter` 键即可。

5. Net Start/Stop 命令

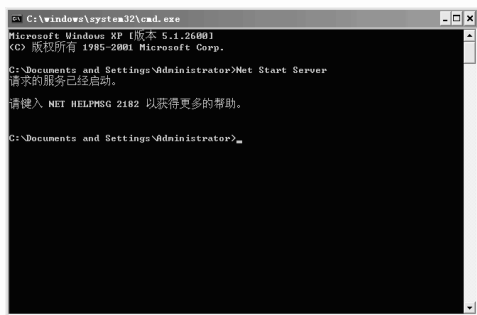
Net Start/Stop 命令用于启动、停止网络服务，黑客常使用该命令管理添加的服务，例如启动一个木马服务等。

Net Start/Stop 命令语法为：

net start service

net stop service

其中参数 Service 表示启动或停止的服务，例如输入命令 Net Start Server，按下 Enter 键即可启动 Server 服务。



下面列出了使用 Net Start/Stop 命令启动和关闭的常用服务。

- Net start Alerter: 启动警报器服务。警报器服务发送警告消息。
- Net start Client Service for NetWare: 启动 NetWare 客户服务。该命令只有在安装了 NetWare 客户服务的情况下才能在 Windows 2000 Professional 上使用。
- Net start ClipBook Serve: 启动剪贴簿服务器服务。
- Net start Computer Browser: 启动计算机浏览器服务。
- Net start DHCP Client: 启动 DHCP 客户服务。该命令只有在安装了 TCP/IP 协议之后才可用。
- Net start Directory Replicator: 启动目录复制程序服务。目录复制程序服务将指定的文件复制到指定服务器上。

- Net start Eventlog: 启动事件日志服务，该服务将事件记录在本地电脑。
- Net start File Server for Macintosh: 启动 Macintosh 文件服务，允许 Macintosh 计算机使用共享文件。
- Net start Net Logon: 启动网络登录服务。网络登录服务验证登录请求。
- Net start Network DDE: 启动网络 DDE 服务。
- Net start Schedule: 启动计划服务。计划服务使计算机可以使用 at 命令在指定时间启动程序。
- Net start Server: 启动服务器服务。服务器服务使计算机可以共享网络上的资源。
- Net start Simple TCP/IP Services: 启动简单 TCP/IP 服务服务。该命令只有在安装了 TCP/IP 和简单 TCP/IP 服务后才可以使

- Net start Workstation: 启动工作站服务。工作站服务使计算机可以连接并使用网络资源。
- Net start Telnet: 启动 telnet 服务，打开 23 端口，有的情况下需先运行 NTLM.exe。
- net start msftpsvc: 打开 FTP 服务

6. Net time 命令

Net time 命令可以使得本机电脑的时钟与另一个电脑或域的时钟同步。如果在没有 /set 选项的情况下使用，则显示另一个计算机或域的时间。

Net time 命令语法为：

net time [[\\computername | /domain[:domain-name] | /rtdomain[:domainname]]] [/set]

net time [[\\computername] [/querysnpt] |

[/setsntp[:ntp server list]]

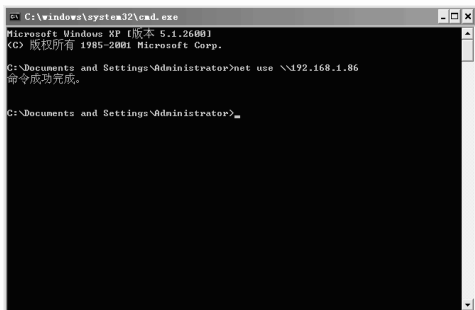
其中各参数的作用如下。

- `\\computername`: 指定要检查或与之同步的服务器的名称。
- `/domain[:domainname]`: 指定要同步时间的域。
- `/rtsdomain[:domainname]`: 指定要与之同步的可信时间服务器所在的域。
- `set`: 使计算机的时钟与指定的计算机或域的时间同步。
- `/querysnTP`: 显示当前为本地计算机或 `\\computername` 所指定的计算机配置的网络时间协议(NTP)服务器名称。
- `/setsntp[:ntp server list]`: 指定本地计算机所使用的 NTP 时间服务器的列表。该列表可以包含 IP 地址或 DNS 名称, 用空格分开。如果要使用多个时间服务器, 该列表必须用引号引起来。

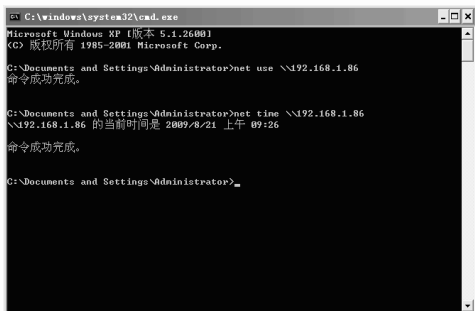
【例 3-7】使用 Net time 命令获取远程主机的系统时间。

☒ 教学视频 ☐ 源文件

01 打开命令提示符窗口, 输入命令 Net use \\192.168.1.86, 然后按下 Enter 键, 当显示“命令成功完成”文本内容, 表示登录到远程主机中。

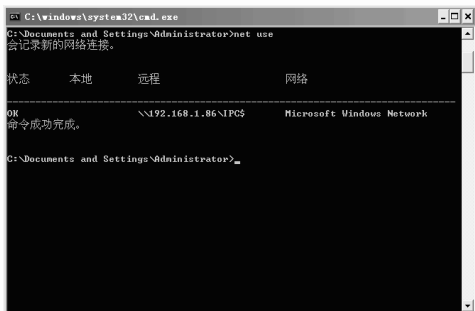


02 输入命令 Net time \\192.168.1.86, 按下 Enter 键, 即可获取远程主机系统时间。



7. Net use 命令

Net use 命令常用于连接/断开远程主机, 或者显示有关远程主机的连接信息。在无参数的情况下使用该命令可以检索网络连接列表。



Net use 命令的语法为:

```
Net use [devicename | *] [\\computername\sharename[\\volume] [password | *]] [/USER:[domainname\username] [/USER:[dotteddomainname\username] [/USER:[username@dotted domainname] [/SMARTCARD] [/SAVECRED] [/DELETE] [/PERSISTENT:{YES|NO}]] NETUSE {devicename | *} [password*] /HOMENETUSE [/PERSISTENT:{YES | NO}]
```

该命令各参数的作用如下。

- `Devicename`: 指定一个名字以便与资源相连接, 或者指定要切断的设备。
- `\\computername`: 指定控制共享资源的计算机的名字。如果计算机名中包含有空字符, 就要将双反斜线(\\)和计算机名一起用引号(" ")括起来。计算机名可以有 1~15 个字符。

- ❶ \sharename: 共享资源的网络名字。
- ❷ \volume: 指定一个服务器上的 NetWare 卷。用户必须安装 Netware 的客户服务(Windows 工作站)或者 Netware 的网关服务(Windows 服务器)并使之与 NetWare 服务器相连。
- ❸ Password: 访问共享资源所需要的密码。* 进行密码提示。当在密码提示符号下输入密码时, 密码不会显示。
- ❹ /USER: 指定连接时的一个不同的用户名。
- ❺ Domainname: 指定另外一个域。如果缺省域, 就会使用当前登录的域。
- ❻ Username: 指定登录的用户名。
- ❼ /SMARTCARD: 指定连接使用在智能卡上的凭据。
- ❽ /SAVECRED: 指定保留用户名和密码。此开关被忽略, 除非命令提示输入用户名和密码。

- ❾ /HOME: 将用户与其主目录相连。
- ❿ /DELETE: 取消一个网络连接, 并且从永久连接列表中删除该连接。
- ⓫ /PERSISTENT: 控制对永久网络连接的使用。默认值是最近使用的设置。

8. Net view 命令

Net view 命令用于显示一个计算机上共享资源的列表。当不带选项使用本命令时, 它就会显示当前域或工作组中计算机的列表。该命令语法为: Net view [[computername [/cache]] /domain[:domainname]]或 Net view /network:nw [[computername], 其中各参数的作用如下。

- ❶ \\Computername: 指定希望查看其共享资源的目标计算机。

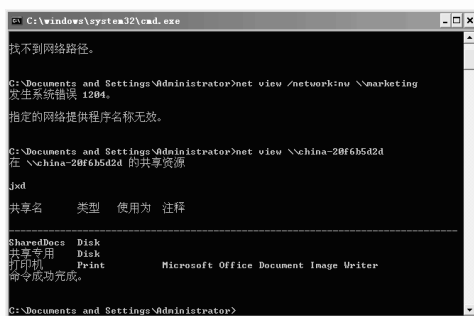
- ❷ /domain[:domainname]: 指定要查看其可用计算机的域或工作组。如果省略 DomainName, /domain 将显示网络上的所有域或工作组名。

- ❸ /network:nw: 显示 NetWare 网络上所有可用的服务器。如果指定计算机名, /network:nw 将通过 NetWare 网络显示该计算机上的可用资源。也可以指定添加到系统中的其他网络。

下面是使用 Net view 命令的常用范例。

- ❶ net view \\production: 查看由 \\Production 计算机共享的资源列表。
- ❷ net view /network:nw \\marketing: 查看 NetWare 服务器\\Marketing 上的可用资源。
- ❸ net view /domain:sales: 查看 sale 域或工作组中的计算机列表。
- ❹ net view /network:nw: 查看 NetWare 网络中的所有服务器:

要查看计算机中的共享资源列表, 只需要输入命令 net view \\china-20f6b5d2d, 然后按下 Enter 键即可。



9. Net User 命令

Net User 命令用于增加/创建/改动用户帐户。该命令语法为:

```
net user <username> [password or *] [/add]
[options] [/domain]

net user <username> /delete /domain
```

各参数的作用如下。

- **username:** 帐户名。
- **password:** 分配或改变密码。*进行密码提示。
- **/domain:** 在一个域中执行。
- **/add:** 创建一个帐户。
- **/delete:** 删除一个帐户。
- **Options:** 指定 Net User 命令可以使用的参数。

了解了 Net User 命令的语法和参数后,下面通过实例介绍使用 Net User 命令建立一个普通新用户的方法。

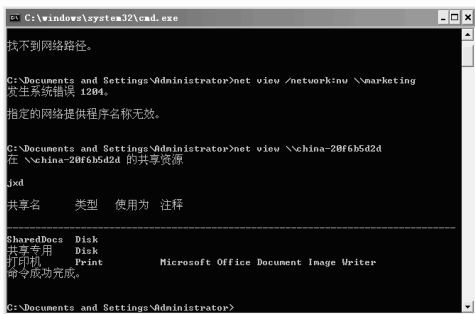
【例 3-8】使用 Net user 命令创建一个普通用户。

☒ 教学视频 ☐ 源文件

01 打开命令提示符窗口,输入命令 net user john 123 /add。

02 在该段命令中 john 是创建的用户名,123 是该用户密码。

03 按下 Enter 键,显示“命令成功完成”文本内容,表示成功创建一个名为 John,密码为 123 的普通用户。



10. Net Localgroup 命令

Net Localgroup 命令用于添加、显示或修改本地组。使用不带参数的 net localgroup 命令可以显示服务器和计算机本地组的名称。

Net Localgroup 命令语法为:

```
net localgroup [GroupName [/comment:  
"Text"]] [/domain]
```

```
net localgroup [GroupName{/add [/com  
ment:"Text"]] [/delete] [/domain]]
```

```
net localgroup [GroupNameName[ ...]]{/add |  
/delete} [/domain]]
```

其中各参数作用如下。

- **GroupName:** 指定要添加、扩展或删除的本地组的名称。使用不带其他参数的 net localgroup Group Name 显示本地组中的用户或全局组列表。
- **/comment:" Text ":** 为新建或已经存在的组添加注释。注释最多可以包含 256 个字符。
- **/domain:** 在当前域的主域控制器上执行操作。否则,操作将在本地计算机上执行。
- **Name [...]:** 列出要从本地组中添加或删除的一个或多个用户名或组名。
- **/add:** 向本地组中添加全局组名称或者用户名。必须在使用此命令将用户或全局组添加到本地组之前先为其建立帐户。
- **/delete:** 从本地计算机组中删除组名或用户名。
- **net help Command:** 显示指定 net 命令的帮助。

下面列出了使用 net localgroup 的常用命令和作用。

- **net localgroup:** 显示本地服务器上所有本地组的列表。
- **net localgroup exec /add:** 可以将本地组 Exec 添加到本地用户帐户数据库。
- **net localgroup exec /add /domain:** 可以将本地组 Exec 添加到域用户帐户数据库。
- **net localgroup exec stevev sales\ralphr jennyt /add:** 可以将现有用户帐户

stevev、ralphr(来自 Sales 域)和 jennyt 添加到本地计算机上的 Exec 本地组。

net localgroup exec stevev ralphr jennyt /add /domain: 可以将现有用户帐户 stevev、ralphr 和 jennyt 添加到域中的

Exec 本地组。

net localgroup exec /comment:"The executive staff.": 显示 Exec 本地组中的用户。

3.3 批处理应用

使用批处理，可以自动执行大量的 DOS 命令，进而能够帮助黑客大大提高攻击效率。下面将介绍有关批处理的应用。

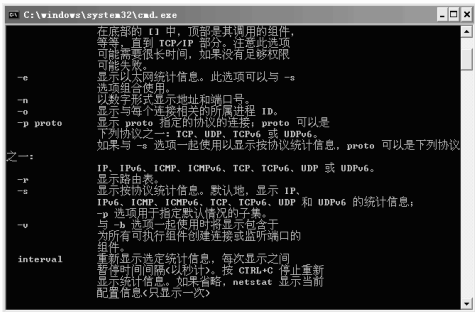
3.3.1 检查指定端口开放状态

网络程序的运行必须开启网络端口，木马程序也不例外。通过检查系统中是否开放了某个木马程序使用的端口，可以判断出系统中中了相应的木马程序。

启动【记事本】应用程序，输入如下内容。

```
@echo off
Echo 正在检查系统中是否存在木马
Netstat -a -n >jc.txt
Find jc.txt "7614">nul
If %errorlevel%==0 (
Echo.
Echo 系统中存在木马
Goto end
)
Echo.
Echo 系统中未发现木马
:end
Del /q jc.txt>nul
```

保存文件为 dd.bat，打开命令提示符窗口，切换到批处理文件所在路径，输入 dd.bat，按下 Enter 键，执行命令。



3.3.2 关闭默认共享

关闭默认共享一般是使用编写注册表文件的方法来实现的。下面通过实例介绍如何在批处理文件中实现注册表文件的创建、调用和关闭，实现关闭默认共享操作。

【例 3-9】使用批处理文件关闭默认共享。

教学视频 源文件

01 启动【记事本】应用程序，输入如下内容。

```
@echo off
Echo Windows Registry Editor Version
5.00 ?dk.reg
Echo 正在关闭默认共享
Echo
[HEKY_LOCAL_MACHINE\SYSTEM\CurrentC
ontrolSet\Services\lanmanserver\parame
ters]>>dk.reg
Echo
```

01章

02章

03章

04章

05章

06章

07章

08章

```
"AutoShareServer"=dword:00000000>>dk.reg
Echo
"AutoShareWks"=dword:00000000??dk.reg
Echo
Echo 正在关闭共享
Echo.
Echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]>>dk.reg
Echo
"restrictanonymouse"=dword:00000001>>dk.reg
Echo 已经关闭共享
```

```
Echo.
Regedit/s dk.reg
Del/q/f dk.reg>nul
Echo.
```

02 保存文件为 dd.bat。

03 打开命令提示符窗口，切换到批处理文件所在路径，输入 dd.bat，按下 Enter 键，执行命令。

3.4 上机练习

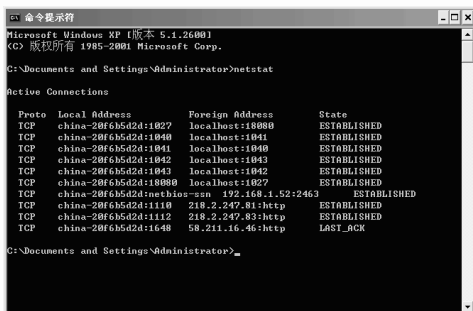
本章上机练习包括使用 DOS 命令获取对方的 IP 地址以及使用批处理文件处理垃圾文件，用户通过练习可以巩固本章知识。

3.4.1 通过 QQ 获取对方 IP 地址

【例 3-10】使用 Netstat 命令，通过 QQ 获取对方 IP 地址。

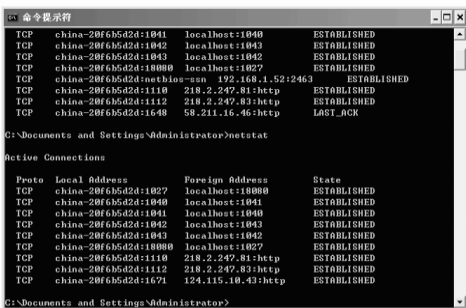
☒ 教学视频 ☐ 源文件

01 登录 QQ，打开命令提示符窗口，输入 Netstat 命令，按下 Enter 键。



02 通过 QQ 给欲查看 IP 地址的 QQ 好友发送一个文件。

03 当好友接收文件时，在命令提示符窗口中输入命令 netstat，按下 Enter 键，查看反馈信息，其中新的 IP 地址就是对方的 IP 地址。



3.4.2 清理垃圾文件

【例 3-11】使用批处理文件清除垃圾文件。

☒ 教学视频 ☐ 源文件

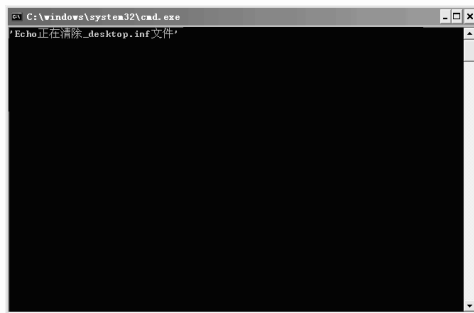
01 启动【记事本】应用程序，输入以下内容。

```
@echo off
Echo 正在清除 _desktop.inf 文件
Del c:\_desktop.ini/f/s/q/a
```

```
Del d:\_desktop.ini/f/s/q/a
Del e:\_desktop.ini/f/s/q/a
Echo 清除完毕
Echo.&pause
```

02 保存文件为 dd.bat。

03 打开命令提示符窗口，切换到批处理文件所在路径，输入 dd.bat，按下 Enter 键，执行操作。



3.5 高手解答

问与答

问：如何有效地防止黑客使用 Ping 命令判断目标主机？

答：通过 Ping 和 Tracert 程序就能判断目标主机类型，Ping 最主要的用处就是检测目标主机是否能连通。Tracert 利用 ICMP 数据包和 IP 数据包头部中的 TTL 值，防止数据包不断在 IP 互联网上永不终止地循环。许多入侵者首先会 Ping 一下你的机器，如看到 TTL 值为 128 就认为系统为 Windows NT/2000；如果 TTL 值为 32 则认为目标主机操作系统为 Windows 98；如果 TTL 值为 255/64 就认为是 UNIX/Linux 操作系统。既然入侵者相信 TTL 值所反映出来的结果，那么只要修改 TTL 值，入侵者就无法入侵电脑了。

首先启动【记事本】应用程序，输入如下内容。

```
@echo REGEDIT4>>ChangeTTL.reg
@echo.>>ChangeTTL.reg
@echo
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters]
>>ChangeTTL.reg
@echo "DefaultTTL"="dword:000000">>ChangeTTL.reg
@REGEDIT /S/C ChangeTTL.reg
```

在上面的命令中，echo 是 DOS 下的回显命令，如果想看到程序执行过程，请将“@”去掉。“>>”产生的内容将追加到它后面的文件即 ChangeTTL.reg 中。而“DefaultTTL”=dword: 000000ff”则是用来设置系统默认 TTL 值的，如果你想将自己的操作系统的 TTL 值改为其他操作系统的 ICMP 回显应答值，请改变“DefaultTTL”的键值，要注意将对应操作系统的 TTL 值改为十六进制才可以。这样，当入侵者 Ping 你的机器时，他得到的就是一个假的 TTL 值，这个假的 TTL 值就会误导对方，使入侵者的判断出现失误，因为针对不同的操作系统的入侵方法并不一样，所以用这个方法欺骗对方，可以让他摸不着头脑！

01章

02章

03章

04章

05章

06章

07章

08章



保存文件为 `dd.bat`，双击这个文件，操作系统的默认 TTL 值就会被修改为 `ff`，即 10 进制的 255，也就是操作系统人为改为 UNIX 系统了。同时，在该文件所在的文件夹会生成一个名为 `hangeTTL.reg` 的注册表文件。如果想运行完这个批处理文件而不产生 `ChangeTTL.reg` 文件，可以在此批处理文件的最后一行加上 `deltree/Y ChangeTTL.reg`，就可以无须确认自动删除 `ChangeTTL.reg` 文件。