

摆脱黑客攻击的 150 招秘籍

现如今网络用户越来越多，由于其用户在线时间长、速度快，因此成为黑客们的攻击目标。现在网上出现了各种越来越详细的“IP地址库”，要知道某系用户的IP是非常容易的事情。要怎么保卫自己的网络安全呢？不妨看看以下方法。

- 黑客常用攻击方法
- 摆脱黑客攻击策略 1——铸造本机堡垒
- 摆脱黑客攻击策略 2——黑客常用系统运行命令
- 摆脱黑客攻击策略 3——黑客常用命令行命令

1.1 黑客常用攻击方法

黑客的攻击方法有多种，常见的有网络欺骗攻击、口令猜解攻击、缓冲区溢出攻击、恶意代码攻击等。使用这些方法中的一种，或结合各种攻击方法，都可使黑客达到不可告人的目的。本章主要介绍黑客常用的攻击方法，包括攻击的原理和相关实战。

1. 口令猜解攻击

口令是目前防止黑客入侵系统的主要方法之一，因此，获取合法用户的账号和口令已经成为黑客攻击的重要手段之一，如猜解系统账户口令、压缩文件口令等。

(1) 攻击原理

由于网络上的用户一般都习惯采用自己姓名的汉语拼音或生日数字作为密码，这就为黑客进行口令猜解提供了突破口。

针对这一现象，进行口令猜测攻击的原理是：通过一些专门的软件，攻击者可以自动地从电脑字典中取出一个单词或一组数字，作为用户的口令输入给远端的主机，申请进入系统。如果密码有误，会自动就按序取出下一个单词或数字组，再一次进行同样的尝试，这样一直循环下去，直到字典中的单词试完为止。这个破译过程是由计算机程序来自动完成，因此，几个小时就可以把字典的所有单词或数字组都试一遍，这样对于那些用英语单词、姓氏拼音或生日作为密码的口令，很容易会被猜解出来。

(2) 攻击实战

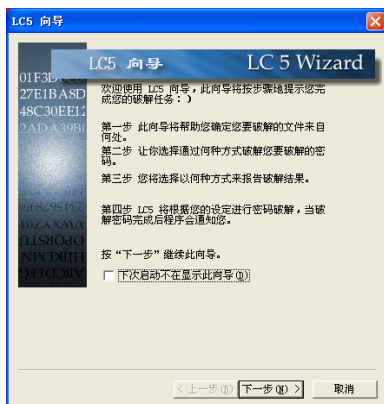
由口令猜测的原理可以知道，进行口令猜解时，需要使用一些必要的密码破解软件，下面以几个常用的软件为例，来模拟一下黑客是如何进行口令猜测攻击的。

1. 使用 LC5 破解计算机密码

LC5，全称为 L0phtCrack5.02，它是 L0phtCrack 组织开发的 Windows 平台口令审核的程序，提供了审核 Windows 账号的功能，以提高系统的安全性。但是，LC5 却被一些黑客用来破解 Windows 用户口令，因为 LC5 可以从本地系统、其他文件系统、系统备份中获得 SAM 文件，从而破解出口令。

使用 LC5 破解密码的具体操作步骤如下。

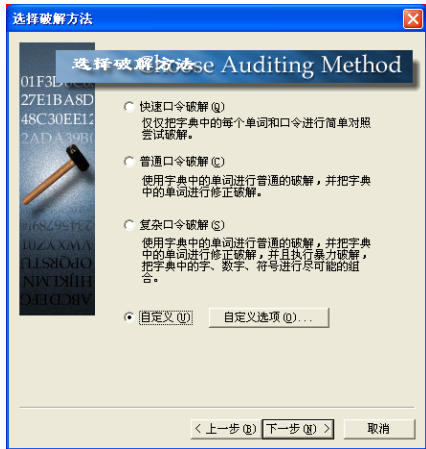
❶ 下载并安装 LC5 后，双击桌面上的【LC5】图标，打开【LC5 向导】对话框。



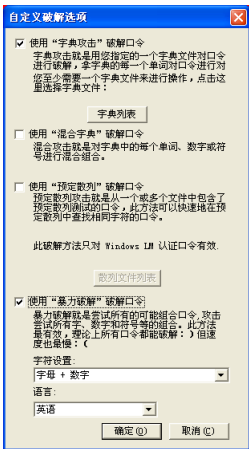
② 单击【下一步】按钮，打开【取得加密口令】对话框，在其中选择相应的单选按钮，来设置导入加密口令的方法，这里选择【从本地计算机导入】单选按钮。



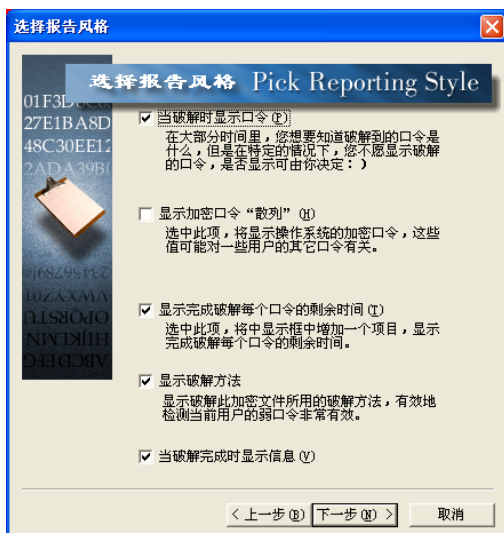
③ 单击【下一步】按钮，打开【选择破解方法】对话框。LC5 提供了快速口令破解、普通口令破解、复杂口令破解以及自定义等 4 种破解方式。



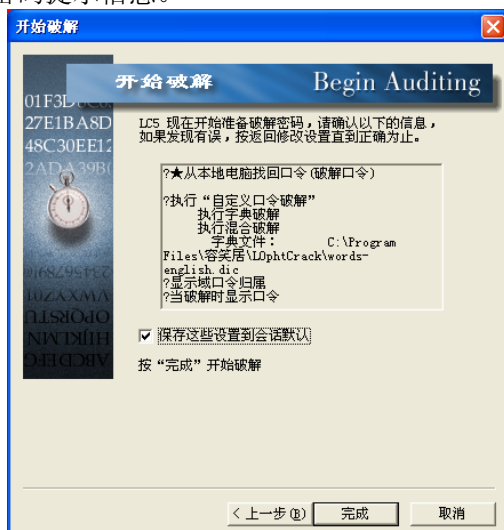
④ 这里选择【自定义】单选按钮，然后单击【自定义选项】按钮，打开【自定义破解选项】对话框。LC5 提供了字典攻击、混合字典、预定散列以及暴力破解等 4 种自定义破解方式，这里选择【使用“字典攻击”破解】复选框。



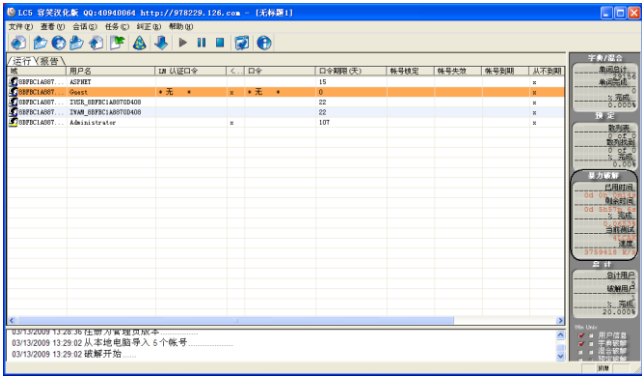
⑤ 单击【确定】按钮，返回【选择破解方法】对话框。再单击【下一步】按钮，打开【选择报告风格】对话框，在其中选择自己所需的报告风格。



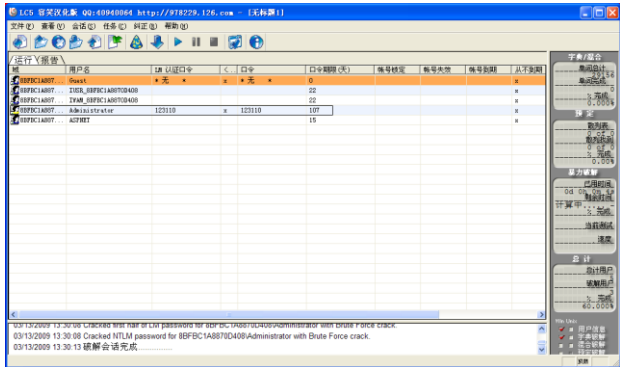
⑥ 单击【下一步】按钮，打开【开始破解】对话框，在其中可以看到提示准备破解密码提示信息。



⑦ 单击【完成】按钮，打开【LC5】主窗口，开始破解密码，在其中可以看到本地计算机中所有的账户名称以及其属性。



⑨ 待破解完成后，在【LC5】主窗口的【口令】列中，看到破解出来的账户口令。



提示：LC5 是一款比较常用的密码破解工具，其使用过程非常方便，但是当遇到密码比较复杂的情况时，破解密码可能会需要很多时间。

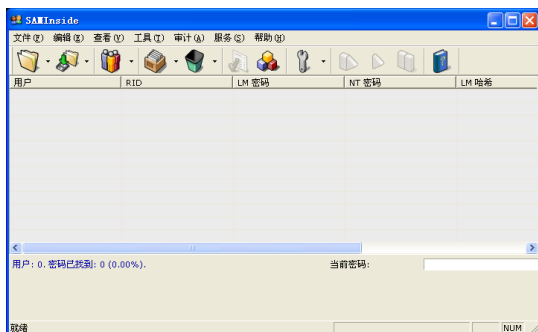
2. 使用 SAMInside 破解 Administrator 的密码


SAMInside 是一款功能强大的口令猜测的软件，即使用 Syskey 加密过的密码，使用 SAMInside 依然可以破解。此外，该软件还支持暴力破解、模糊破解、字典攻击、多台电脑分布式破解等多种破解方式，破解密码的速度可以达到每秒几百万，

这里以 SAMInside-v2.6.0 汉化版为例来介绍如何破解计算机的密码，其具体的操作步骤如下。

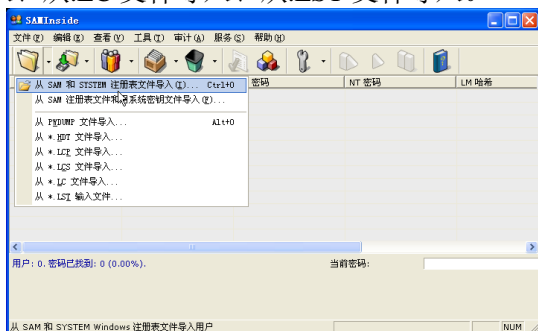
第 1 步：SAMInside 功能介绍


① 下载并解压缩 SAMInside-v2.6.0 软件包后，双击 SAMInside.exe 程序，打开【SAMInside】主窗口。



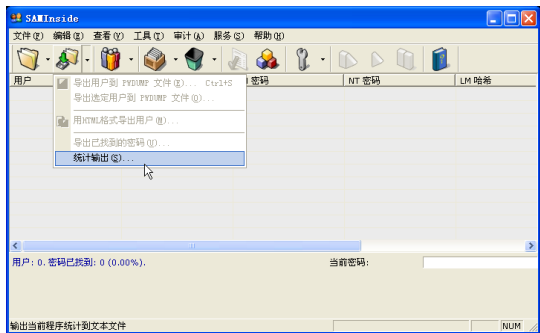
② 单击工具栏中的【导入】按钮，在弹出的快捷菜单中可以看出该软件提供了 8 种导入方式。


从上到下分别是：从 SAM 和 SYATEM 文件导入、从 SAM 和 SYSKEY 文件导入、从 PWDUMP 文件导入、从.HDT 文件导入、从.LCP 文件导入、从.LCS 文件导入、从.LC 文件导入、从.LST 文件导入。



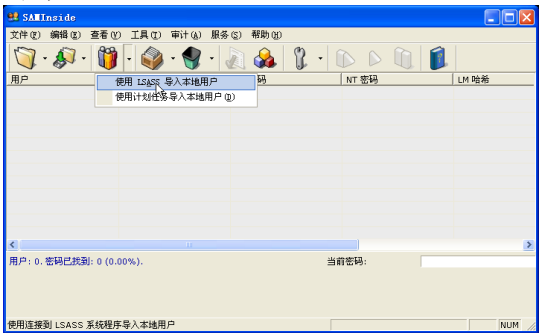
③ 如果想把账户导出到指定的文件中，则可单击工具栏【导出】按钮，在弹出的快捷菜单中选择相应的导出方式即可。


SAMInside 提供了导出 PWDUMP 文件中的用户、导出 PWDUMP 文件中选定的用户、导出已猜解的密码、导出统计表等多种导出方式。

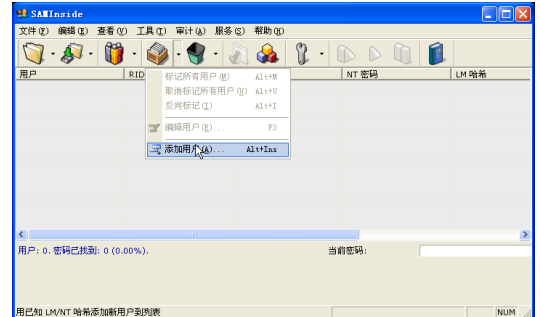


④ 如果想破解本地计算机密码，则可单击工具栏的第三个【导入】按钮，在弹出的快捷菜单中相应的菜单项即可。

如果选择【LSASS 导入要破解的内容】菜单项，则可快速导入本地账户；如果选择【从本地电脑使用计划任务导入破解内容】菜单项，则需要等进行等候才可导入。

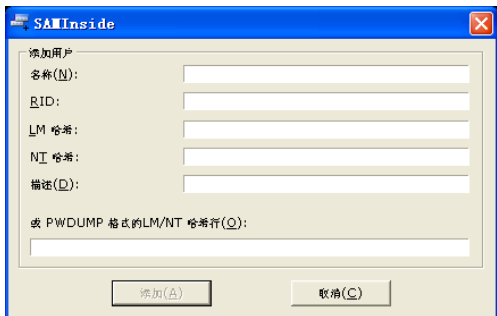



⑤ 单击工具栏的按钮，则可进行【标记所有用户】、【取消标记所有用户】、【反向标记】、【编辑用户】和【添加用户】等操作。

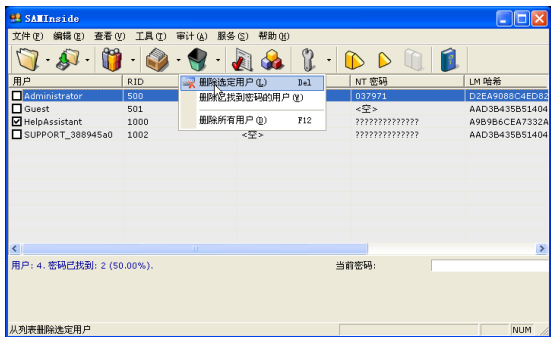



⑥ 在弹出的快捷菜单中选择【添加账户】菜单项，打开【SAMInside】对话框。在其中可以设置新添加账户的信息，还可以在相应位置输入 LM

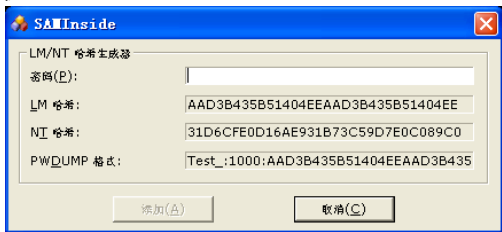
和 NT 的哈希值 (hash)。




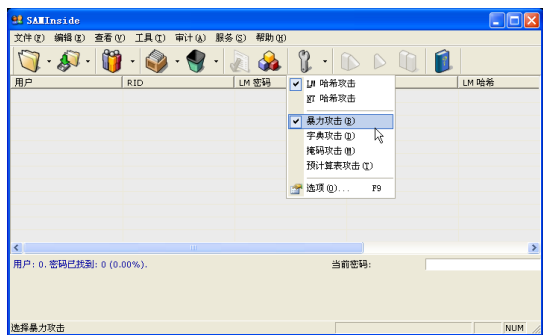
⑦ 单击工具栏的【删除】按钮，在弹出的快捷菜单中选择相应的选项即可进行删除选择的账户、删除已经创建了密码的账户、删除所有的账户等操作。



⑧ 单击工具栏按钮，打开【生成器】窗口，从中可以分别看出 LM 和 NT 的哈希值。




⑨ SAMInside 提供了 LM 哈希攻击、NT 哈希攻击、暴力攻击、掩码攻击、字典攻击、预计算式攻击等多种攻击方式。单击工具栏中的【攻击】按钮，在弹出的快捷菜单中选择相应的方式即可。

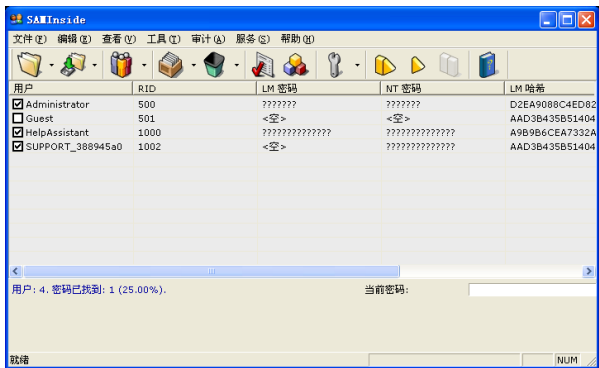



提示：如果密码前 3 位是数字，后 2 位是字母，中间有 3 位不详，此时需要设置一下以增加破解速度，这种破解方式就是掩码攻击。

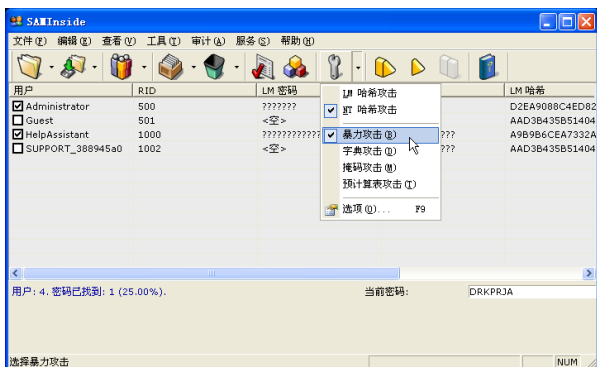
⑩ 单击工具栏中的  按钮或  按钮，即可恢复密码，当然，黑客们会利用该菜单猜解目标口令。而  按钮的作用是停止猜解。

第 2 步：使用 SAMInside 破解本地计算机账户 Administrator 的密码

① 在【SAMInside】主窗口中击工具栏的第三个按钮 ，在弹出的快捷菜单中【LSASS 导入要破解的内容】菜单项，即可自动读入本机的用户账户信息。





② 选中【Administrator】账户，单击工具栏中的【攻击】按钮 ，在弹出的快捷菜单中选择【NT 哈希攻击】和【暴力攻击方式】菜单项。



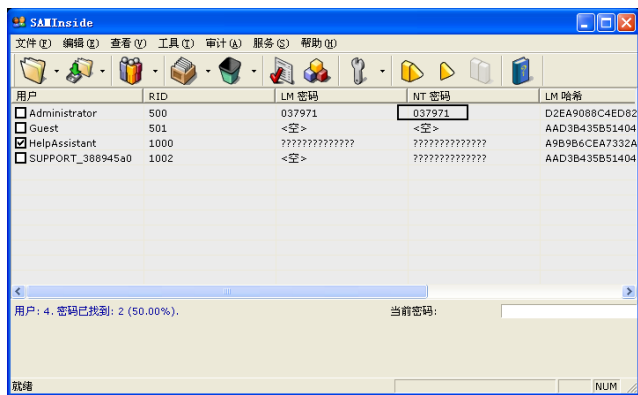
③ 选择【选项】选项，打开【Options】对话框，在其中勾选【0…9】复选框并选择 7 位的密码个数上限。



④ 单击【OK】按钮，返回到【SAMInside】主窗口中。单击工具栏中的  按钮或  按钮，即可开始猜解密码，待猜解完毕后，将弹出【暴力攻击完成】提示框。



⑤ 单击【确定】按钮，返回到【SAMInside】主窗口中，在其中可以看到猜解出的密码。



提示：猜解的过程往往需要一段时间，需要耐心等待，另外，用户还可以根据自己的需要选择其他的攻击方式。

2. 恶意代码攻击

恶意代码是一段没有作用却会带来危害的代码，恶意代码攻击一般是通过强行修改用户操作系统的注册表设置、系统实用配置程序、恶意删除硬盘文件、格式化硬盘文件来破坏计算机系统。用户一旦遭受到恶意代码的攻击，就会使计算机不完全受用户的控制，使系统遭受不同程序的破坏。

(1) 攻击原理

恶意代码攻击主要是通过插在网页中代码的形式，来修改浏览者的注册表，IE 浏览器等，从而破坏目标主机的系统。常见的攻击方式有禁用注册表、修改 IE 首页、修改 IE 标题栏、系统启动时弹出对话框、查看“源文件”菜单被禁用、部分菜单被禁止等。

下面分别介绍一下其攻击的原理

(1) 禁用注册表

这是由于注册表 HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Policies\System 下的 DWORD 值“DisableRegistryTools”被修改为“1”的缘故，将其键值恢复为“0”即可恢复注册表的使用。

(2) 修改 IE 主页

有些 IE 被修改了起始页后，即使设置“使用默认页”仍然无效，这是由于 IE 起始页的默认页也被篡改了。具体表现在注册表项：HKEY_LOCAL_MACHINE\Software\Microsoft\InternetExplorer\Main\Default_Page_URL 中的“Default_Page_URL”子键的键值被修改了。

(3) 修改 IE 标题栏

在系统默认状态下，是由应用程序本身来提供标题栏的信息，但也允许用户自行在注册表项目中填加信息，正是因为这一点，一些恶意的网站就将串值 Window Title 下的键值改为其网站名或更多的广告信息，从而达到改变浏览者 IE 标题栏的目的。

具体来说就是更改注册表如下项目。

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\Window Title

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Window Title

(4) 系统启动时弹出对话框

受到更改的注册表项目为：
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon。

在其下被建立了字符串“LegalNoticeCaption”和“LegalNoticeText”，其中“Legal Notice Caption”是提示框的标题，“LegalNoticeText”是提示框的文本内容。利用这两个键值，使得用户每次登录到 Windows 桌面前都出现一个提示窗口，显示那些网页的广告信息。

(5) 查看“源文件”菜单被禁用

在 IE 窗口中选择【查看】>【源文件】菜单项，发现【源文件】子菜单已经被禁用。这是由于恶意网页病毒修改了注册表，具体的位置为：

① 在注册表 HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer 下建立子键“Restrictions”，然后在“Restrictions”下面建立两个 DWORD 值：“NoViewSource”和“NoBrowserContextMenu”，并为这两个 DWORD 值赋值为“1”。

② 在注册表 HKEY_USERS\DEFAULT\Software\Policies\Microsoft\Internet Explorer\Restrictions 下，将两个 DWORD 值：“NoViewSource”和“NoBrowserContextMenu”的键值都改为了“1”。

通过上面这些键值的修改就达到了在 IE 中使鼠标右键失效，使【查看】菜单项中的【源文件】子菜单实现被禁用的目的。

(2) 攻击实战

曾经风靡一时的“万花谷”病毒就是一个比较有代表性的恶意代码病毒，该病毒是在一个叫“万花谷”的网站上传出的，利用 Java 最新技术进行破坏系统。该病毒的破坏特征表现在如下几个方面。

① 用户不能正常使用 Windows 系统的 DOS 功能程序。

② 用户不能正常退出 Windows 系统。

③ 开始菜单上的“关闭系统”、“运行”等栏目被屏蔽，防止用户重新以 DOS 方式启动，关闭 DOS 命令、关闭 REGEDIT 命令等。

④ 将 IE 的浏览器的首页和收藏夹中都加入了含有该有害网页代码的网络地址。

如果用户不小心进入该网站，则网页显示的将是一个有光效滤镜的网页，随着鼠标的移动，会造成光线照在网页图片的不同地方的效果，光效一共有 4 种。

将 IE 的首页通过系统注册表项：
HKEY_LOCAL_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Start Page 设置成为“on888.xxx.xxx.com/”，就能达到破坏目标主机的目的。

3. 缓冲区溢出攻击

缓冲区溢出攻击是利用缓冲区溢出漏洞所进行的攻击行为。缓冲区溢出是一种非常普遍、非常危险的漏洞，在各种操作系统、应用软件中广泛存在，利用缓冲区溢出攻击，可以导致程序运行失败、系统无故关机、重新启动等后果。更为严重的是，利用缓冲区溢出攻击可以执行非授权指令，甚至可以取得系统特权，从而进行各种非法操作。

(1) 攻击原理

缓冲区是内存中存放数据的地方，操作系统所使用的缓冲区又被称为堆栈，在各个操作进程之间，指令被临时存储在堆栈当中，当然堆栈也会出现缓冲区溢出。缓冲区溢出是指当计算机程序向缓冲区内填充的数据位数超过了缓冲区本身的容量，从而造成数据的溢出。溢出的数据会覆盖在合法数据上，这就为缓冲区溢出埋下了安全隐患。

黑客正是利用这一安全隐患，将精心设置的病毒数据溢出覆盖在合法的数据上，一旦溢出数据被编译执行后，“黑客”或病毒就有可能获取系统的控制权，这就是缓冲区溢出攻击的原理。

造成缓冲区溢出的原因是程序中没有仔细检查用户输入的参数。例如下面一段代码。example1.c

```
void func1(char *input) {  
    char buffer[16];  
    strcpy(buffer, input);  
}
```

其中 strcpy() 将直接把 input 中的内容 copy 到 buffer 中，这样，只要 input 的长度大于 16，就会造成 buffer 的溢出，使程序运行出错。

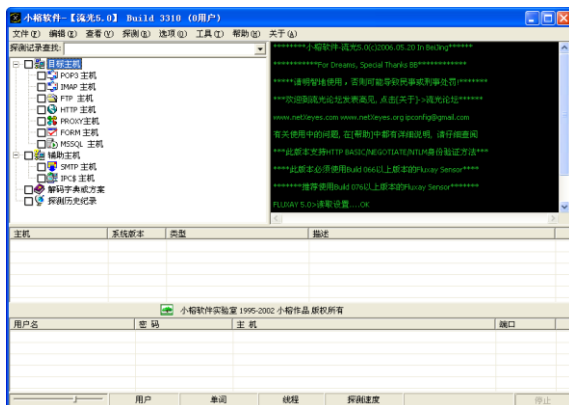
(2) 攻击实战

为了进一步了解缓冲区溢出攻击的原理，下面介绍几个利用缓冲区溢出攻击的实例，来演示一下其攻击的过程。

1. IDA 和 IDQ 扩展漏洞攻击

实施 IDA 和 IDQ 扩展溢出漏洞攻击需要借助于流光和 Snake IIS 溢出两种工具，实施漏洞攻击的具体操作步骤如下。

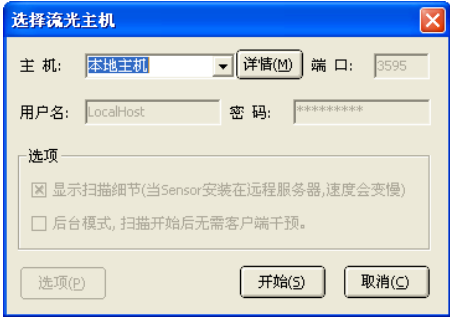
① 下载并安装流光软件后，双击桌面上的【流光】图标，进入流光主界面。



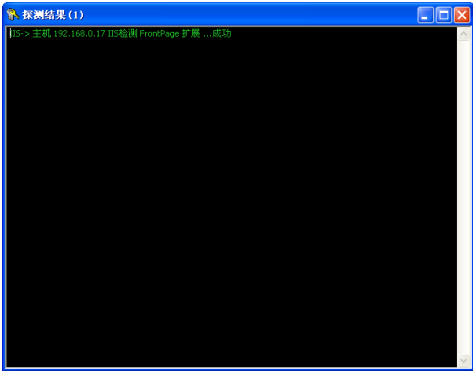
② 选择【探测】>【高级扫描工具】菜单项，打开【高级扫描设置】对话框，并设置扫描的 IP 地址范围和检测范围。



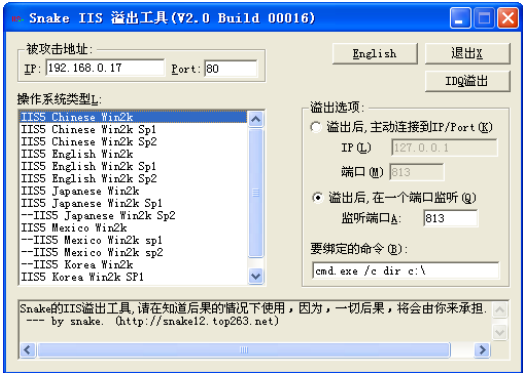
③ 设置完毕后，单击【确定】按钮完成设置操作，弹出【选择流光主机】对话框。



④ 单击【开始】按钮，系统即可自动进行检测，并把最终结果显示出来。



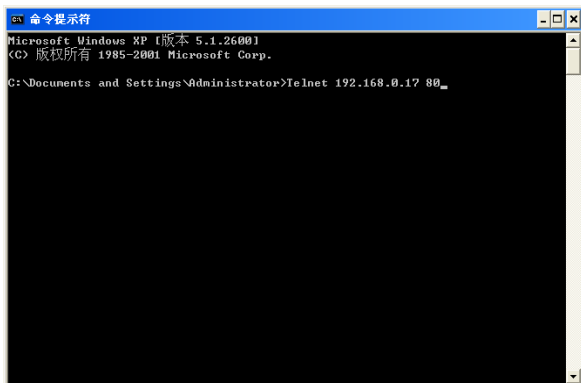
⑤ 运行 Snake IIS 溢出工具，进入其界面，并在【IP】和【Port】文本框中输入被攻击的 IP 地址和端口号，接着选择操作系统类型，然后选择 cmd.exe 绑定端口。



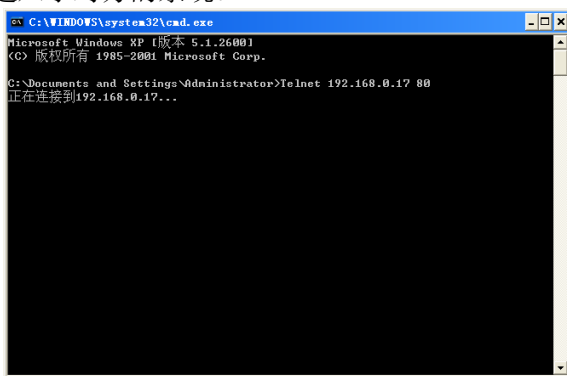
⑥ 单击【IDQ 溢出】按钮，如果溢出攻击成功，将会出现如下图的提示。



⑦ 运用终端工具 Telnet，在 DOS 命令行下输入“Telnet 192.168.0.17 80”。



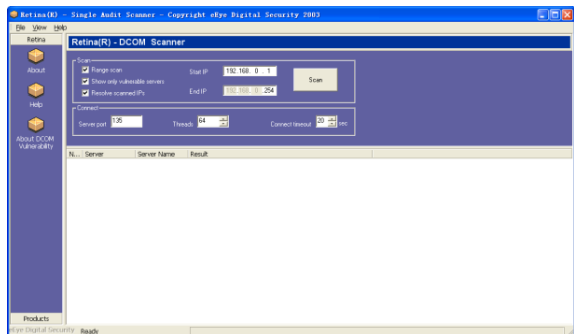
⑧ 输入完毕后，按回车键，如果出现“C: \WINNT\system32”提示符，表示已经进入了对方的系统。



2. RPC 溢出漏洞攻击

攻击者利用这个漏洞，发送特殊形式的请求到远程机器上的 135 端口，成功攻击之后就可以随意在远程计算机上执行任何指令。实现 RPC 漏洞攻击的具体操作步骤如下。

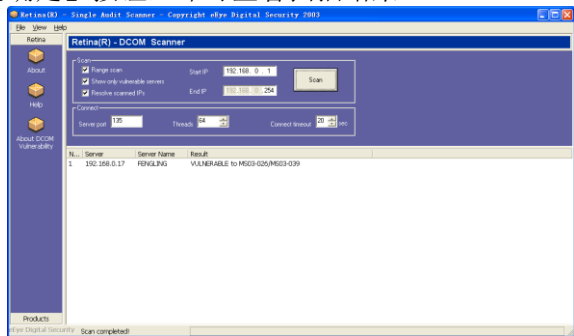
① 运行漏洞扫描工具“retinarpdcom.exe”，即可进入其界面，并设置要扫描的 IP 段。



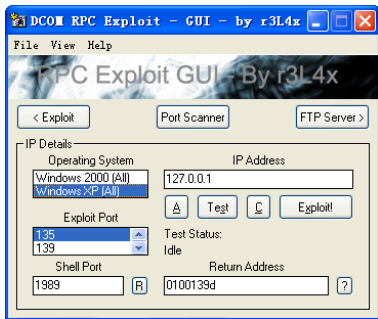
② 单击【Scan】按钮，即可对设置的 IP 范围进行漏洞的扫描工作，扫描完成后会弹出扫描完毕的提示。



③ 单击【确定】按钮，即可查看扫描结果。

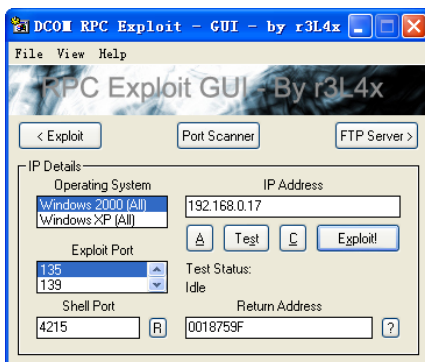


④ 运行漏洞工具 RPC GUI v2-r3L4x，进入其界面。

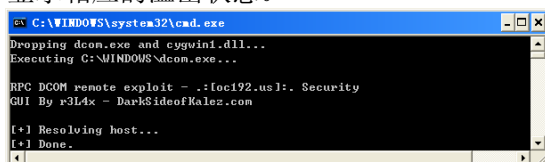


⑤ 在该界面中设置被攻击者的操作系统，并选择攻击端口，并输入

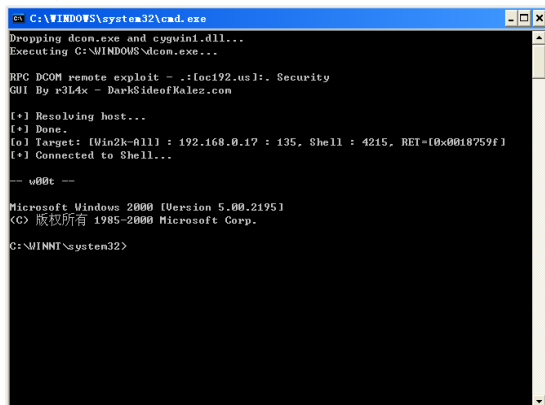
攻击目标的 IP 地址。



⑥ 单击【Exploit!】按钮，即可开始溢出攻击，溢出开始后会弹出一个命令窗口，显示相应的溢出状态。



⑦ 溢出状态出现“Connect to shell”提示，就表明溢出攻击成功。



提示：溢出完毕后出现一个命令提示符状态，也就是经常提到的 Shell，在其中可以随意操作对方硬盘中的文件，添加账户、提升权限等操作。

4. 网络欺骗攻击

网络欺骗的技术主要有：HONEYPOT 和分布式 HONEYPOT、欺骗

空间技术等，常见的攻击方式有 IP 欺骗、ARP 欺骗、DNS 欺骗、Web 欺骗、电子邮件欺骗、源路由欺骗等多种方式。

(1) 攻击原理

网络欺骗就是黑客使目标主机用户相信信息资源存在有价值，当然这些资源是伪造的，将用户引向带有病毒或恶意代码的资源，实施网络欺骗可显著提高入侵的成功率。欺骗能够成功的关键是在受攻击者和其他 Web 服务器之间，建立起攻击者的 Web 服务器，这种攻击方法在安全问题中被称为“来自中间的攻击”。

要想网络欺骗攻击成功，就必须建立起中间 Web 服务器，黑客经常通过改变 URL 链接地址、填写表单等方法建立中间 Web 服务器，从而实现网络欺骗。

1. 通过改变地址

攻击者先改写 Web 网页中的所有 URL 链接地址，这样其就不会指向真正的 Web 服务器，而是指向了攻击者自己的 Web 服务器。比如攻击者所处的 Web 服务器是 xxx.yyy，攻击者通过在所有链接前增加 http://www.xxx.yyy 来改写 URL。

如此一来，当用户点击任何一个链接，都会直接进入攻击者的服务器，而不会进入真正的 URL。如果用户由此依次进入其他网页，将永远不会摆脱掉受攻击的可能。

2. 通过填写表单

由于表单的确定信息被编码到 URL 中后，其内容再以 HTML 形式返回，那么，即使前面的 URL 被黑客篡改了，表单的确定信息依然还会传送给指定的 URL，从表面上看，填写的信息和正常的表单一样。但是，这些提交的信息被送到了攻击者的服务器，从而实现网络欺骗。

(2) 攻击实战

下面以网络钓鱼为例，来讲述一下网络欺骗的具体的攻击实战。网络钓鱼是通过大量发送声称来自于银行或其他知名机构的欺骗性垃圾邮件，意图引诱收信人给出敏感信息（如用户名、口令、帐号 ID、ATM PIN 码或信用卡详细信息）的一种攻击方式。

网络钓鱼攻击技术有很多，比较常见的有向用户发送电子邮件、建立假冒的网上银行和网上证券等。下面列出了几种较为常见攻击技术。

(1) 黑客向用户发送电子邮件，采用虚假信息引诱用户。黑客以垃圾邮件的形式发送大量的欺诈性邮件，如中奖、顾问、对账等极具诱惑性的内容，引诱用户在邮件中填入自己的金融账号和密码，或以各种紧迫的理由要求收件人登录某网页提交用户名、密码、身份证号、信用卡号等信息，继而盗窃用户资金。

比如：今年 2 月份发现的一种骗取美邦银行（Smith Barney）用户的账号和密码的“网络钓鱼”电子邮件，该邮件利用了 IE 的图片映射地址欺骗漏洞，并精心设计脚本程序，用一个显示假地址的弹出窗口遮挡住 IE 浏览器的地址栏，使用户无法看到此网站的真实地址。当用户使用未打补丁的 Outlook 打开此邮件时，状态栏显示的链接是虚假的。当用户点击链接时，实际连接的是钓鱼网站。该网站页面酷似 Smith Barney 银行网站的登录界面，而用户一旦输入了自己的账号密码，则个人账号信息就会被黑客窃取。

(2) 通过建立假冒的网上银行、网上证券等网站，来骗取用户的账号密码。犯罪分子建立起与真正的网上银行系统、网上证券交易平台域名和网页内容都极为相似的网站，引诱用户输入账号密码等信息，进而通过真正的网上银行、网上证券系统或者伪造银行储蓄卡、证券交易卡盗窃资金。

如曾经出现过的某假冒银行网站，网址为 <http://www.1cbc.com.cn/>，而真正银行网站是 <http://www.icbc.com.cn/>，犯罪分子利用数字 1 和字母 i 非常相近的特点企图蒙蔽粗心的用户。如下图所示即为一个银行钓鱼网站。



(3) 利用虚假的电子商务进行诈骗。这种欺骗行为往往通过建立电子商务网站，或在比较知名、大型的电子商务网站上发布虚假的商品销售信息，犯罪分子在收到受害人的购物汇款后就销声匿迹。

(4) 利用木马和黑客技术等手段窃取用户信息后实施盗窃活动。木马制作者通过发送邮件或在网站中隐藏木马等方式大肆传播木马程序，

当感染木马的用户进行网上交易时，木马程序即以键盘记录的方式获取用户账号和密码，并发送给指定邮箱，用户资金将受到严重威胁。

比如木马“证券大盗”，可以通过屏幕快照将用户的网页登录界面保存为图片，并发送给指定邮箱。黑客通过对照图片中鼠标的点击位置，就很有可能破译出用户的账号和密码，从而突破软键盘密码保护技术，严重威胁股民网上证券交易的安全。

(5) 利用用户弱口令等漏洞破解、猜测用户账号和密码。不法分子利用部分用户贪图方便设置弱口令的漏洞，对银行卡密码进行破解。

实际上，不法分子在实施网络诈骗的犯罪活动过程中，经常采取以上几种手法交织、配合进行，还有的通过手机短信、QQ 和 msn 等工具进行各种各样的“网络钓鱼”的不法活动。

1.2 摆脱黑客攻击策略 1——铸造本机堡垒

5. 取消文件夹隐藏共享

在“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanmanworkstation\parameters”，新建一个名为“AutoShareWks”的双字节值，并将其值设为“0”，然后重新启动电脑，这样共享就取消了。

6. 拒绝恶意代码

运行IE浏览器，点击“工具→Internet选项→安全→自定义级别”，将安全级别定义为“安全级-高”，对“ActiveX控件和插件”中第2、3项设置为“禁用”，其它项设置为“提示”，之后点击“确定”。这样设置后，当你使用IE浏览网页时，就能有效避免恶意网页中恶意代码的攻击。

7. 封死黑客的“后门”

俗话说“无风不起浪”，既然黑客能进入，那说明系统一定存在为他们打开的“后门”，只要堵住这个后门，让黑客无处下手，便无后顾之忧！

8. 封死黑客的“后门”之——删掉不必要的协议

对于服务器和主机来说，一般只安装TCP/IP协议就够了。鼠标右击“网络邻居”，选择“属性”，再鼠标右击“本地连接”，选择“属性”，卸载不必要的协议。其中NETBIOS是很多安全缺陷的根源，对于不需要提供文件和打印共享的主机，还可以将绑定在TCP/IP协议的NETBIOS关闭，避免针对NETBIOS的攻击。选择“TCP/IP协议/属性/高级”，进入“高级TCP/IP设置”对话框，选择“WINS”标签，勾选“禁用TCP/IP上的NETBIOS”一项，关闭NETBIOS。

9. 封死黑客的“后门”之——关闭“文件和打印机共享”

文件和打印共享应该是一个非常有用的功能，但在不需要它的时候，也是黑客入侵的很好的安全漏洞。所以在没有必要“文件和打印共享”的情况下，我们可以将它关闭。用鼠标右击“网络邻居”，选择“属性”，然后单击“文件和打印共享”按钮，将弹出的“文件和打印共享”对话框中的两个复选框中的钩去掉即可。

虽然“文件和打印共享”关闭了，但是还不能确保安全，还要修改注册表，禁止它人更改“文件和打印共享”。打开注册表编辑器，选择“HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionPoliciesNetWork”主键，在该主键下新建DWORD类型的键值，键值名为“NoFileSharingControl”，键值设为“1”表示禁止这项功能，从而达到禁止更改“文件和打印共享”的目的；键值为“0”表示允许这项功能。这样在“网络邻居”的“属性”对话框中“文件和打印共享”就不复存在了。

10. 封死黑客的“后门”之——把Guest账号禁用

有很多入侵都是通过这个账号进一步获得管理员密码或者权限的。如果不想把自己的计算机给别人当玩具，那还是禁止的好。打开控制面板，双击“用户和密码”，单击“高级”选项卡，再单击“高级”按钮，弹出本地用户和组窗口。在Guest账号上面点击右键，选择属性，在“常规”页中选中“账户已停用”。另外，将Administrator账号改名可以防止黑客知道自己的管理员账号，这会在很大程度上保证计算机安全。

11. 封死黑客的“后门”之——禁止建立空连接

在默认的情况下，任何用户都可以通过空连接连上服务器，枚举账号并猜测密码。因此，我们必须禁止建立空连接。

在注册表“HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA”将DWORD值“RestrictAnonymous”的键值改为“1”即可。

12. 封死黑客的“后门”之——及时为系统打上补丁

建议大家给自己的系统打上补丁，微软那些没完没了的补丁还是很有用的。这些系统漏洞都是黑客们最乐于使用的最好后门。

13. 封死黑客的“后门”之——隐藏IP地址

黑客经常利用一些网络探测技术来查看我们的主机信息，主要目的就是得到网络中主机的IP地址。IP地址在网络安全上是一个很重要的概念，如果攻击者知道了你的IP地址，等于为他的攻击准备好了目标，他可以向这个IP发动各种进攻，如DoS(拒绝服务)攻击、Flood溢出攻击等。隐藏IP地址的主要方法是使用代理服务器。

与直接连接到Internet相比，使用代理服务器能保护上网用户的IP地址，从而保障上网安全。代理服务器的原理是在客户机（用户上网的计算机）和远程服务器（如用户想访问远端WWW服务器）之间架设一个“中转站”，当客户机向远程服务器提出服务要求后，代理服务器首先截取用户的请求，然后代理服务器将服务请求转交远程服务器，从而实现客户机和远程服务器之间的联系。很显然，使用代理服务器后，其它用户只能探测到代理服务器的IP地址而不是用户的IP地址，这就实现了隐藏用户IP地址的目的，保障了用户上网安全。提供免费代理服务器的网站有很多，你也可以自己用代理猎手等工具来查找。

14. 关闭不必要的端口

黑客在入侵时常常会扫描你的计算机端口，如果安装了端口监视程序（比如Netwatch），该监视程序则会有警告提示。如果遇到这种入侵，可用工具软件关闭用不到的端口，比如，用“Norton Internet Security”关闭用来提供网页服务的80和443端口，其他一些不常用的端口也可关闭。

15. 更换管理员账户

Administrator账户拥有最高的系统权限，一旦该账户被人利用，后果不堪设想。黑客入侵的常用手段之一就是试图获得Administrator账户的密码，所以我们

要重新配置Administrator账号。

首先是为Administrator账户设置一个强大复杂的密码，然后重命名Administrator账户，再创建一个没有管理员权限的Administrator账户欺骗入侵者。这样一来，入侵者就很难搞清哪个账户真正拥有管理员权限，也就在一定程度上减少了危险性。

16. 杜绝Guest账户的入侵

Guest账户即所谓的来宾账户，它可以访问计算机，但受到限制。不幸的是，Guest也为黑客入侵打开了方便之门！网上有很多文章中都介绍过如何利用Guest用户得到管理员权限的方法，所以要杜绝基于Guest账户的系统入侵。

禁用或彻底删除Guest账户是最好的办法，但在某些必须使用到Guest账户的情况下，就需要通过其它途径来做好防御工作了。首先要给Guest设一个强壮的密码，然后详细设置Guest账户对物理路径的访问权限。举例来说，如果你要防止Guest用户可以访问tool文件夹，可以右击该文件夹，在弹出菜单中选择“安全”标签，从中可看到可以访问此文件夹的所有用户。删除管理员之外的所有用户即可。或者在权限中为相应的用户设定权限，比方说只能“列出文件夹目录”和“读取”等，这样就安全多了。

17. 安装必要的安全软件

我们还应在电脑中安装并使用必要的防黑软件，杀毒软件和防火墙都是必备的。在网上时打开它们，这样即便有黑客进攻我们的安全也是有保证的。

18. 防范木马程序之一——来路不明的文件先体检

在下载文件时先放到自己新建的文件夹里，再用杀毒软件来检测，起到提前预防的作用。

19. 防范木马程序之一——删除可疑程序

将注册表里的 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 下的所有以

“Run”为前缀的可疑程序全部删除即可。

20. 不要回陌生人的邮件

有些黑客可能会冒充某些正规网站的名义，然后编个冠冕堂皇的理由寄一封信给你要求你输入上网的用户名称与密码，如果按下“确定”，你的帐号和密码就进了黑客的邮箱。所以不要随便回陌生人的邮件，即使他说得再动听再诱人也不上当。

21. 做好IE的安全设置

ActiveX控件和 Applets有较强的功能，但也存在被人利用的隐患，网页中的恶意代码往往就是利用这些控件编写的小程序，只要打开网页就会被运行。所以要避免恶意网页的攻击只有禁止这些恶意代码的运行。IE对此提供了多种选择，具体设置步骤是：“工具”→“Internet选项”→“安全”→“自定义级别”，建议您将ActiveX控件与相关选项禁用。谨慎些总没有错！

另外，在IE的安全性设定中我们只能设定Internet、本地Intranet、受信任的站点、受限制的站点。不过，微软在这里隐藏了“我的电脑”的安全性设定，通过修改注册表把该选项打开，可以使我们在对待ActiveX控件和 Applets时有更多的选择，并对本地电脑安全产生更大的影响。

在

HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet\Settings\Zones0值右边窗口中找到DWORD值“Flags”，默认键值为十六进制的21(十进制33)，双击“Flags”，在弹出的对话框中将它的键值改为“1”即可，关闭注册表编辑器。无需重新启动电脑，重新打开IE，再次点击“工具→Internet选项→安全”标签，你就会看到多了一个“我的电脑”图标，在这里你可以设定它的安全等级。将它的安全等级设定高些，这样的防范更严密。

22. 禁止使用注册表编辑器

在 HKEY_CURRENT_USER\Software\Microsoft\Windows\Current-Version\Policies\System\DisableRegistryTools下新建一个双字节(REG_DWORD)值项，并修改其值为1。

23. 禁止用户使用“任务管理器”

在 HKEY _ CURRENT _ USER\Software\Microsoft\ Windows\Current-Version\Policies\System\DisableTaskMgr下新建一个双字节(REG__DWORD)值项,并修改其值为1。

24. 禁止运行命令解释器和批处理文件

在 HKEY _ CURRENT _ USER\Software\Policies\Microsoft\Windows\System\DisableCMD下新建一个双字节(REG__DWORD)值项,并修改其值为2。

25. 禁用光盘自动运行

在 HKEY _ CURRENT _ USER\Software\Microsoft\Windows\Current-Version\Policies\Explorer子键下新建二进制键值NoDriveTypeAutoRun,并设置该键值为b5, 00, 00, 00。

26. 禁用“开始”菜单中“程序”上的水平线

在 HKEY _ CURRENT _ USER\Software\Microsoft\Windows\Current-Version\Policies\Explorer子键下新建dword键值EditLevel,并设置该键值为1。

27. 禁用单击“从这里开始”动画箭头

在 HKEY _ CURRENT _ USER\Software\Microsoft\Windows\Current-Version\Policies\Explorer子键下新建二进制键值NoStartBanner,并设置该键值为01, 00, 00, 00。

28. 禁用“开始”菜单中的“收藏夹”

在 HKEY _ CURRENT _ USER\Software\Microsoft\Windows\Current-Version\Policies\Explorer子键下新建dword键值NoFavoritesMenu,并设置该键值为1。

29. 禁用“开始”菜单中的“文档”

在 HKEY _ CURRENT _ USER\Software\Microsoft\Windows\Current-Version\Policies\Explorer子键下新建dword键值NoRecentDocsMenu, 并设置该键值为1。

30. 禁用“开始”菜单中的“查找”

在 HKEY _ CURRENT _ USER\Software\Microsoft\Windows\Current-Version\Policies\Explorer子键下新建dword键值NoFind, 并设置该键值为1。

31. 禁用“开始”菜单中的“运行”

在 HKEY _ CURRENT _ USER\Software\Microsoft\Windows\Current-Version\Policies\Explorer子键下新建dword键值NoRun, 并设置该键值为1。

32. 禁用“开始”菜单中的“注销”

在 HKEY _ CURRENT _ USER\Software\Microsoft\Windows\Current-Version\Policies\Explorer子键下新建dword键值NoLogOff, 并设置该键值为1。

33. 禁用“开始”菜单中的“关闭”

在 HKEY _ CURRENT _ USER\Software\Microsoft\Windows\Current-Version\Policies\Explorer子键下新建dword键值NoClose, 并设置该键值为1。

34. 不保存新近打开的文档历史记录

在 HKEY _ CURRENT _ USER\Software\Microsoft\Windows\Current-Version\Policies\Explorer子键下新建二进制键值NoRecentDocsHistory, 并设置该键值为01, 00, 00, 00。

35. 禁用“网上邻居”图标

在 HKEY _ CURRENT _ USER\Software\Microsoft\Windows\Current-

Version\Policies\Explorer子键下新建dword键值NoNetHood，并设置该键值为1。

36. 禁用IE浏览器图标

在 HKEY _ CURRENT _ USER\Software\Microsoft\Windows\Current-Version\Policies\Explorer子键下新建dword键值NoInternetIcon，并设置该键值为1。

37. 禁用退出时保存设置(锁定桌面)

在 HKEY _ CURRENT _ USER\Software\Microsoft\Windows\Current-Version\Policies\Explorer子键下新建dword键值NoSaveSettings，并设置该键值为1。

38. 禁用所有驱动器

在 HKEY _ CURRENT _ USER\Software\Microsoft\Windows\Current-Version\Policies\Explorer子键下新建二进制键值NoDrives，并设置该键值为ff ff ff。

39. 禁用显示属性中的“Web”选项卡

在 HKEY _ CURRENT _ USER\Software\Microsoft\Windows\Current-Version\Policies\Explorer子键下新建dword键值NoActiveDesktop，并设置该键值为1。

40. 禁止在“开始”菜单中拖放快捷菜单

在 HKEY _ CURRENT _ USER\Software\Microsoft\Windows\Current-Version\Policies\Explorer子键下新建dword键值NoChangeStartMenu，并设置该键值为1。

41. 禁用右键快捷菜单

在 HKEY _ CURRENT _ USER\Software\Microsoft\Windows\Current-Version\Policies\Explorer子键下新建dword键值NoViewContextMenu，并设置该键值为1。

42. 禁用任务栏的快捷菜单

在 HKEY _ CURRENT _ USER\Software\Microsoft\Windows\Current-Version\Policies\Explorer子键下新建dword键值NoTrayContextMenu，并设置该键值为1。

43. 禁用桌面上的所有图标选项

在 HKEY _ CURRENT _ USER\Software\Microsoft\Windows\Current-Version\Policies\Explorer子键下新建dword键值NoDesktop，并设置该键值为1。

44. 在打印机文件夹中禁用“添加打印机”

在 HKEY _ CURRENT _ USER\Software\Microsoft\Windows\Current-Version\Policies\Explorer子键下新建dword键值NoAddPrinter，并设置该键值为1。

45. 在打印机文件夹中禁用“删除打印机”

在 HKEY _ CURRENT _ USER\Software\Microsoft\Windows\Current-Version\Policies\Explorer子键下新建dword键值NoDeletePrinter，并设置该键值为1。

46. 禁用“设置”中的“任务栏属性和开始菜单”

在 HKEY _ CURRENT _ USER\Software\Microsoft\Windows\Current-Version\Policies\Explorer子键下新建dword键值NoSetTaskbar，并设置该键值为1。

47. 禁用“设置”菜单中的“文件夹选项”

在 HKEY _ CURRENT _ USER\Software\Microsoft\Windows\Current-Version\Policies\Explorer子键下新建dword键值NofolderOptions，并设置该键值为1。

48. 禁用“设置”菜单中的“活动桌面”

在 HKEY _ CURRENT _ USER\Software\Microsoft\Windows\Current-Version\Policies\Explorer子键下新建dword键值NoSetActiveDesktop，并设置该键值为1。

49. 禁用“设置”菜单中的“Windows Update”选项

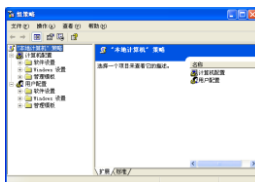
在 HKEY _ CURRENT _ USER\Software\Microsoft\Windows\Current-Version\Policies\Explorer子键下新建dword键值NoWindowsUpdate，并设置该键值为1。

1.3 摆脱黑客攻击策略 2——黑客常用系统运行命令

使用方法：单击【开始】按钮，然后选择【运行】命令，在弹出的【运行】对话框中输入命令，即可运行相应的程序。



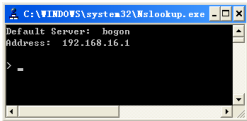
50. 组策略命令——gpedit.msc



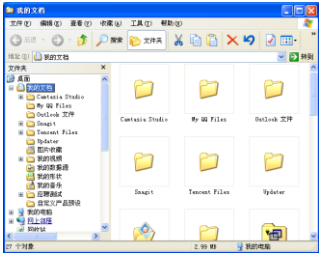
51. 录音机命令—sndrec32



52. IP地址侦测器命令—Nslookup



53. 打开资源管理器—explorer



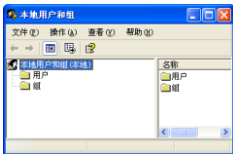
54. 注销命令—logoff



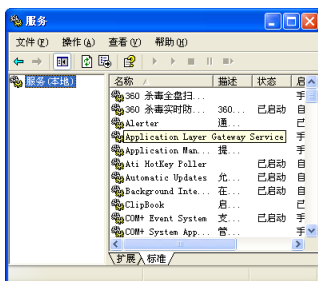
55. 60秒倒计时关机命令—tsshtutdn



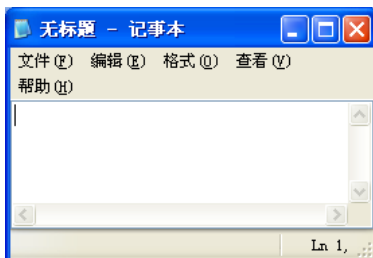
56. 本地用户和组—lusrmgr.msc



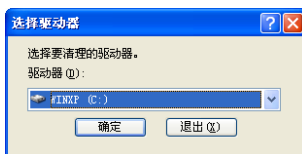
57. 本地服务设置—services.msc



58. 打开记事本—notepad



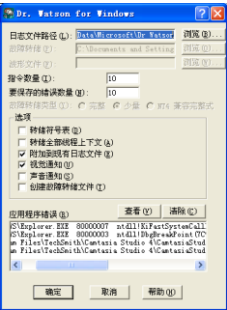
59. 垃圾整理—cleanmgr



60. 计算机管理—compmgmt.msc



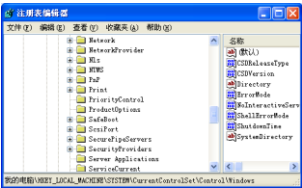
61. 启动netmeeting—conf



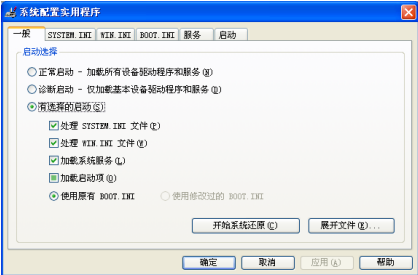
70. 检查DirectX信息—dxdiag



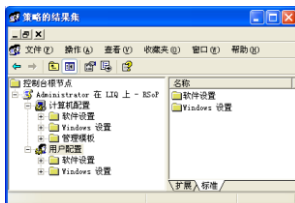
71. 注册表编辑器—regedt32



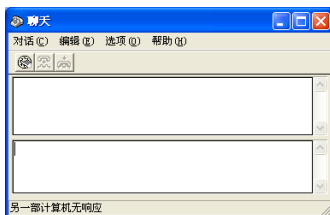
72. 系统配置实用程序—msconfig.exe



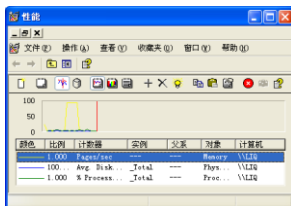
73. 组策略结果集—rsop.msc



74. Windows XP自带局域网聊天—winchat



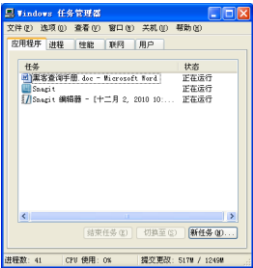
75. 计算机性能监测程序—perfmon.msc



76. 检查Windows版本—winver



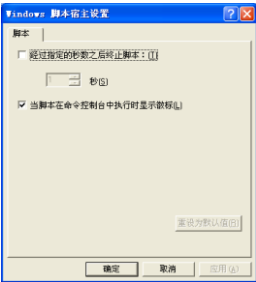
77. 任务管理器—taskmgr



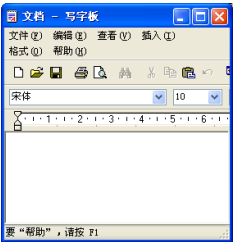
78. 打开Windows管理体系结构(WMI) — wmicgmt.msc



79. Windows脚本宿主设置—wscript



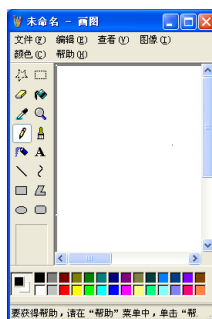
80. 写字板—write



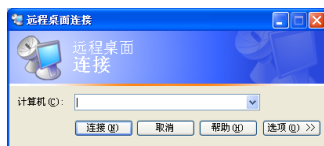
81. 简易Windows Media Player— mplayer2



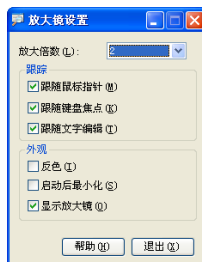
82. 画图板—mspaint



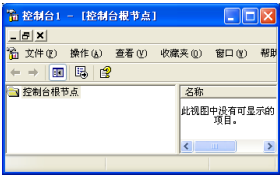
83. 远程桌面连接—mstsc



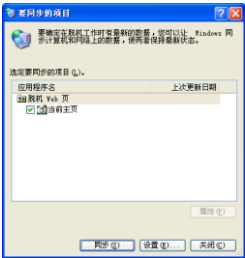
84. 放大镜实用程序—magnify



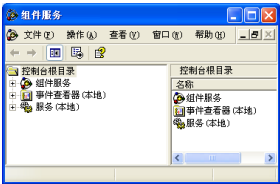
85. 打开控制台—mmc



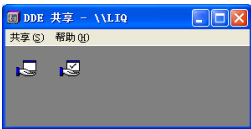
86. 同步命令—mobsync



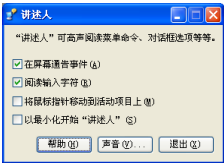
87. 打开系统组件服务—dcomcnfg



88. ddeshare—打开DDE共享设置



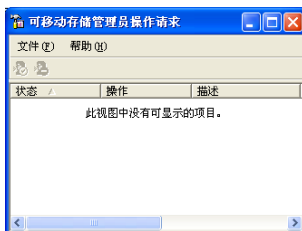
89. narrator—屏幕“讲述人”



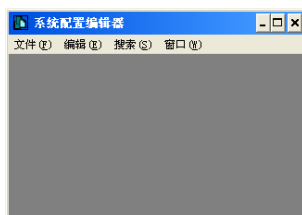
90. ntmsmgr.msc—移动存储管理器



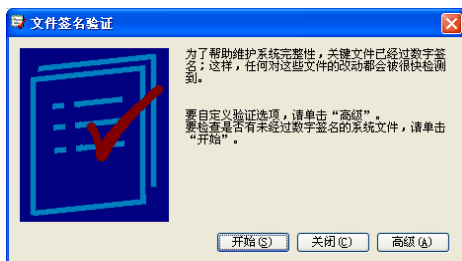
91. ntmsoprq.msc—可移动存储管理员操作请求



92. sysedit—系统配置编辑器



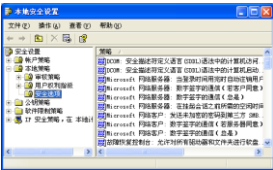
93. sigverif—文件签名验证程序



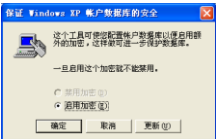
94. shrpwbw—创建共享文件夹



95. secpol.msc—本地安全策略



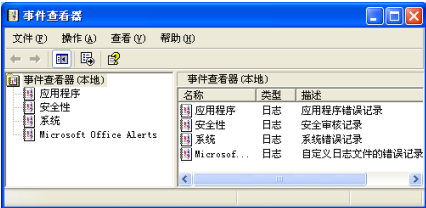
96. syskey—加密系统账户数据库



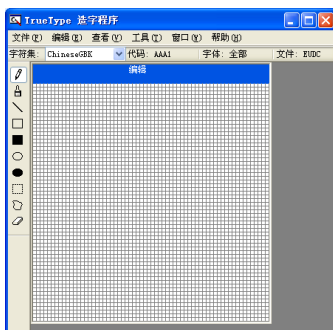
97. sndvol32—音量控制程序



98. eventvwr—事件查看器



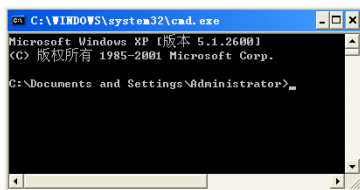
99. eudcedit—造字程序



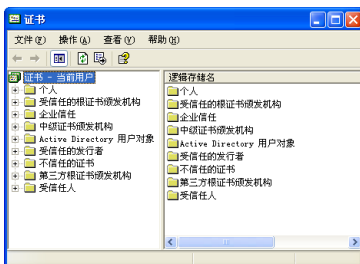
100. packager—对象包装程序



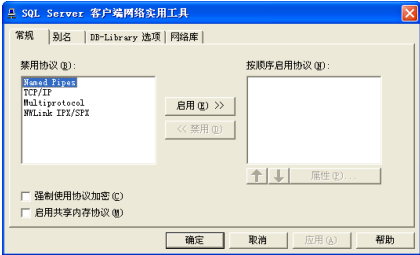
101. cmd.exe—CMD命令提示符



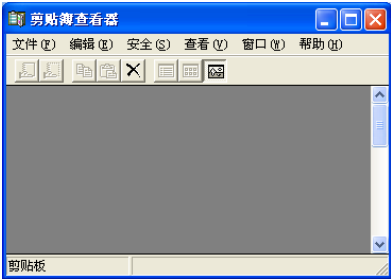
102. certmgr.msc—证书管理实用程序



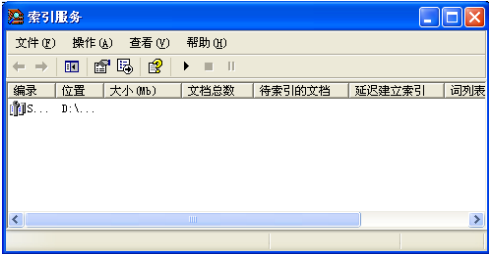
103. cliconfg—SQL Server 客户端网络实用程序



104. clipbrd—剪贴簿查看器



105. ciadv.msc—索引服务程序



106. osk—打开屏幕键盘



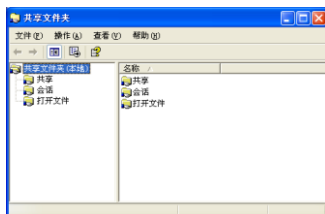
107. odbcad32—ODBC数据源管理器



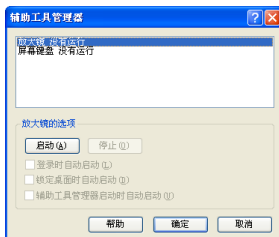
108. iexpress—自解压文件创建器



109. fsmgmt.msc—共享文件夹管理器



110. utilman—辅助工具管理器



1.4 摆脱黑客攻击策略 3——黑客常用命令行命令

111. ASSOC

格式：[.ext[=[fileType]]]

参数说明：

参数	说明
ext	指定跟文件类型关联的文件扩展名
fileType	指定跟文件扩展名关联的文件类型

使用说明：

键入 ASSOC 而不带参数，显示当前文件关联。如果只用文件扩展名调用 ASSOC，则显示那个文件扩展名的当前文件关联。如果不为文件类型指定任何参数，该命令会删除文件扩展名的关联。

112. AT

功能：安排在特定日期和时间运行命令与程序，要使用 AT 命令，计划服务必须已在运行中。

格式：AT [[\computername] [[id] [/DELETE] | /DELETE [/YES]]AT [[\computername] time [/INTERACTIVE][/EVERY:date[,...]] /NEXT:date[,...]] "command"

参数说明：

参数	说明
\\computername	指定远程计算机。 如果省略这个参数，会计划在本地计算机上运行命令
id	指定给已计划命令的识别号
/delete	删除某个已计划的命令。如果省略id，计算机上所有已计划的命令都会被删除
/yes	不需要进一步确认时，跟删除所有作业的命令一起使用
time	指定运行命令的时间
/interactive	允许作业在运行时与当时登录的用户桌面进行交互
/every:date[,...]	每个月或每个星期在指定的日期运行命令。如果省略日期，则默认为在每月的本日运行
/next:date[,...]	指定在下一个指定日期（如下周四）运行命令。如果省略日期，则默认为在每月的本日运行
"command"	准备运行的 Windows NT 命令或批处理程序

113. ATTRIB

功能：显示或更改文件属性。

格式：ATTRIB [+R | -R] [+A | -A] [+S | -S] [+H | -H] [[drive:] [path] filename] [/S [/D]]

参数说明：

参数	说明
----	----

参数	说明
+	设置属性
-	清除属性
R	只读文件属性
A	存档文件属性
H	隐藏文件属性
[drive:][path][filename]	指定要处理的文件属性
/S	处理当前文件夹及其子文件夹中的匹配文件
/D	也处理文件夹
S	系统文件属性

114. CACLS

功能：显示或者修改文件的访问控制表（ACL）。

格式：CACLS filename [/T] [/E] [/C] [/G user:perm] [/R user [...]] [/P user:perm [...]] [/D user [...]]

参数说明：

参数	说明
filename	显示 ACL
/T	更改当前目录及其所有子目录中指定文件的 ACL
/E	编辑 ACL 而不替换
/C	在出现拒绝访问错误时继续
/G user:perm	赋予指定用户访问权限。Perm 可以是R（读取）、W（写入）、C（更改）、F（完全控制）
/R user	撤销指定用户的访问权限（仅在与 /E 一起使用时合法）
/P user:perm	替换指定用户的访问Perm可以是N（无）、R（读取）、W（写入）、C（更改）、F（完全控制）
/D user	拒绝指定用户的访问。在命令中可以使用通配符指定多个文件，也可以在命令中指定多个用户

115. CALL

功能：从批处理程序调用另一个批处理程序。

格式：CALL [drive:][path]filename [batch-parameters]

使用说明：batch-parameters 用于指定批处理程序所需的命令行信息。如果命令扩展名被启用，CALL 会发生改变。

116. CD

功能：显示当前目录名或改变当前目录。

使用说明：

CD：显示当前目录名。

CD\：返回根目录。

CD..：返回上一级目录。

CD temp：如果当前的目录下有temp文件夹，则更改当前的目录为temp。

117. CHKDSK

功能：检查磁盘并显示状态报告。
格式：CHKDSK [volume[[path]filename]] [/F] [/V] [/R] [/X] [/I] [/C] [/L:size]
参数说明：

参数	说明
volume	指定驱动器（后面跟一个冒号）、装入点或卷名
filename	仅用于 FAT/FAT32，指定要检查是否有碎片的文件
/F	修复磁盘上的错误
/V	在 FAT/FAT32 上显示磁盘上每个文件的完整路径和名称。在 NTFS 上，如果有清除消息，将其显示
/R	查找不正确的扇区并恢复可读信息（隐含/F）。
/L:size	仅用于 NTFS，用于将日志文件大小改成指定的KB 数。如果没有指定大小，则显示当前的大小
/X	如果必要，强制卷先卸下。卷的所有打开的句柄就会无效（隐含/F）
/I	仅用于 NTFS 对索引项进行强度较小的检查
/C	仅用于 NTFS 跳过文件夹结构的循环检查

/I 和 /C 命令行开关跳过卷的某些检查，减少运行CHKDSK所需的时间。

118. CLS

功能：清除屏幕。

119. CMD

功能：启动 Windows XP 命令解释程序一个新的实例。
格式：CMD [/A | /U] [/Q] [/D] [/E:ON | /E:OFF] [/F:ON | /F:OFF] [/V:ON | /V:OFF] [/S] [/C | /K] string]
参数说明：

参数	说明
/C	执行字符串指定的命令，然后中断
/K	执行字符串指定的命令但保留
/S	在 /C 或 /K 后修改字符串处理（见下）
/Q	关闭回应
/D	从注册表中停用执行 AutoRun 命令（见下）
/A	使向内部管道或文件命令的输出成为 ANSI
/U	使向内部管道或文件命令的输出成为 Unicode
/T:fg	设置前景/背景颜色（详细信息请见 COLOR /?）
/E:ON	启用命令扩展（见下）
/E:OFF	停用命令扩展（见下）
/F:ON	启用文件和目录名称完成字符（见下）
/F:OFF	停用文件和目录名称完成字符（见下）
/V:ON	将 ! 作为定界符启动延缓环境变量扩展。
/V:OFF	停用延缓的环境扩展

120. COLOR

功能：设置默认控制台的前景和背景颜色。

格式：COLOR [attr]

参数说明：

颜色属性由2个十六进制数字指定，第1个为背景色，第2个则为前景色，每个数字可以为以下任何值之一。如“COLOR 07”表示设置背景色为黑色，设置前景色（文字颜色）为白色。

参数	说明
0	黑色
1	蓝色
2	绿色
3	湖蓝色
4	红色
5	紫色
6	黄色
7	白色
8	灰色
9	淡蓝色
A	淡绿色
B	淡淡绿色
C	淡红色
D	淡紫色
E	淡黄色
F	亮白色

121. COMP

功能：比较两个文件或两个文件集的内容。

格式：COMP [data1] [data2] [/D] [/A] [/L] [/N=number] [/C] [/OFF[LINE]]

参数说明：

参数	说明
data1	指定要比较的第一个文件的位置和名称
data2	指定要比较的第二个文件的位置和名称
/D	用十进制格式显示不同处
/A	用 ASCII 字符显示不同处
/L	显示不同的行数
/N=number	只比较每个文件中第一个指定的行数
/C	比较文件时不区分 ASCII 字母的大小写
/OFF[LINE]	不要跳过带有脱机属性集的文件

注意：如果要比较文件集，在 data1 和 data2 参数中使用通配符。

122. CONVERT

摆脱黑客攻击的 150 招秘籍

功能：将 FAT 卷转换成 NTFS。
格式：CONVERT volume /FS:NTFS [/V] [/CvtArea:filename] [/NoSecurity] [/X]
参数说明：

参数	说明
volume	指定驱动器号（后面跟一个冒号）、装载点或卷名
/FS:NTFS	指定要被转换成 NTFS 的卷
/V	指定 Convert 应该用详述模式运行
/CvtArea:filename	将根目录中的一个接续文件指定为NTFS 系统文件的占位符
/NoSecurity	指定每个人都可以访问转换的文件和目录的安全设置
/X	如果必要，先强行卸载卷。该卷的所有打开的句柄则无效

123. COPY

功能：将一份或多份文件复制到另一个位置。
格式：COPY [/D] [/V] [/N] [/Y | /-Y] [/Z] [/A | /B] source [/A | /B][+ source [/A | /B] [+ ...]] [destination
[/A | /B]]
参数说明：

参数	说明
source	指定要复制的文件
/A	表示一个 ASCII 文本文件
/B	表示一个二进制文件
/D	允许解密要创建的目标文件
destination	为新文件指定目录和/或文件名
/V	验证新文件写入是否正确
/N	复制带有非 8dot3 名称的文件时，尽可能使用短文件名的提示
/Y	使用确认是否要改写现有目标文件的提示
/Z	用可重新启动模式复制已联网的文件

124. DATE

功能：显示或设置日期。
格式：DATE [/T | date]

125. DEL

功能：删除一个或数个文件。
格式：DEL [/P] [/F] [/S] [/Q] [/A[:[attributes]]] names
ERASE [/P] [/F] [/S] [/Q] [/A[:[attributes]]] names
参数说明：

参数	说明
names	指定一个或数个文件或目录列表。通配符可被用来删除多个文件。如果指定了一个目录，目录中的所有文件都会被删除
/P	删除每一个文件之前提示确认
/F	强制删除只读文件
/S	从所有子目录中删除指定文件

参数	说明
/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	R: 只读文件 S: 系统文件 H: 隐藏文件 A: 存档文件 -: 表示“否”的前缀

126. DIR

功能：显示目录中的文件和子目录列表。

格式：DIR [drive:][path][filename] [/A[:attributes]] [/B] [/C] [/D] [/L] [/N]/O[:sortorder]] [/P] [/Q] [/S] [/T[:timefield]] [/W] [/X] [/4][drive:][path] [filename]

参数说明：

参数	说明
/A: attributes	显示具有指定属性的文件 D: 目录 R: 只读文件 H: 隐藏文件 A: 准备存档的文件 S: 系统文件 -: 表示“否”的前缀
/B	使用空格式（没有标题信息或摘要）
/C	在文件大小中显示千位数分隔符，这是默认值，用 /-C来停用分隔符显示
/D	跟宽式相同，但文件是按栏分类列出的
/L	用小写列出文件目录
/N	新的长列表格式，其中文件名在最右边
/O	用分类顺序列出文件和目录
sortorder	N: 按名称（字母顺序） S: 按大小（从小到大） E: 按扩展名（字母顺序） D: 按日期/时间（从先到后） G: 组目录优先 -: 颠倒顺序的前缀
/P	在每个信息屏幕后暂停
/Q	显示文件所有者
/S	显示指定目录和所有子目录中的文件
/T	控制显示或用来分类的时间字符域
timefield	C: 创建时间

参数	说明
	A: 上次访问时间 W: 上次写入的时间
/W	用宽列表格式
/X	显示为非8dot3文件名产生的短名称。格式是 /N, 短名称插在长名称前面。如果没有短名称, 在其位置则显示空白
/4	用4位数字显示年

127. ECHO

功能：显示信息，或将命令回显打开或关闭。
格式：ECHO [ON | OFF]ECHO [message]

128. EXIT

功能：退出 CMD.EXE 程序（命令翻译程序）或当前批处理脚本。
格式：EXIT [/B] [exitCode]
参数说明：

参数	说明
/B	指定要退出当前批处理脚本而不是CMD.EXE。如果从一个批处理脚本外执行，则会退出 CMD.EXE
exitCode	指定一个数字号码。如果指定了/B, 将 ERRORLEVEL设成那个数字。如果退出 CMD.EXE, 则用那个数字设置过程退出代码

129. FC

功能：比较两个文件或两个文件集并显示它们之间的不同。
格式：FC [/A] [/C] [/L] [/LBn] [/N] [/OFF[LINE]] [/T] [/U] [/W] [/nnnn][drive1:][path1]filename1
[drive2:][path2]filename2
参数说明：

参数	说明
/A	只显示每个不同处的第一行和最后一行
/B	执行二进制比较
/C	不分大小写
/L	将文件作为 ASCII 文字比较
/LBn	将连续不匹配的最大值设为指定的行数
/N	在ASCII比较上显示行数
/OFF[LINE]	不要跳过带有脱机属性集的文件
/T	不要将 Tab 扩充到空格
/U	将文件作为 Unicode 文字文件比较
/W	为了比较而压缩空白（Tab 和空格）
/nnnn	指定不匹配处后必须连续匹配的行数
[drive1:][path1]filename1	指定要比较的第一个文件或第一个文件集
[drive2:][path2]filename2	指定要比较的第二个文件或第二个文件集

130. FIND

功能：在文件中搜索字符串。

格式：FIND[/V[/C[/N[/I] [/OFF[LINE]] "string" [[drive:][path]filename[...]]

参数说明：

参数	说明
/V	显示所有未包含指定字符串的行
/C	仅显示包含字符串的行数
/N	显示行号
/I	搜索字符串时忽略大小写
/OFF[LINE]	不要跳过具有脱机属性集的文件
[drive:][path]filename	指定要搜索的文件
"string"	指定要搜索的文字串

使用说明：如果没有指定路径，FIND 将搜索键入的或者由另一命令产生的文字。

131. FINDSTR

功能：在文件中寻找字符串。

格式：FINDSTR [/B] [/E] [/L] [/R] [/S] [/I] [/X] [/V] [/N] [/M] [/O] [/F:file] [/C:string] [/G:file] [/D:dir list] [/A:color attributes] [/OFF[LINE]] strings [[drive:][path]filename[...]]

参数说明：

参数	说明
/B	在一行的开始配对模式
/E	在一行的结尾配对模式
/L	按字使用搜索字符串
/R	将搜索字符串作为一般表达式使用
/S	在当前目录和所有子目录中搜索匹配文件
/I	指定搜索不分大小写
/X	打印完全匹配的行
/V	只打印不包含匹配的行
/N	在匹配的每行前打印行数
/M	如果文件含有匹配项，只打印其文件名
/O	在每个匹配行前打印字符偏移量
/P	忽略有不可打印字符的文件
/OFF[LINE]	不跳过带有脱机属性集的文件
/A:attr	指定有十六进制数字的颜色属性，请见“color /?”
/F:file	从指定文件读文件列表（/代表控制台）
/C:string	使用指定字符串作为文字搜索字符串
/G:file	从指定的文件获得搜索字符串（/代表控制台）
/D:dir	查找以分号为分隔符的目录列表
strings	要查找的文字

参数	说明
[drive:][path]filename	指定要查找的文件

132. FORMAT

功能：格式化磁盘以供 Windows XP 使用。

格式：FORMAT volume [/FS:file-system] [/V:label] [/Q] [/A:size] [/C] [/X]FORMAT volume [/V:label] [个/Q] [/F:size]FORMAT volume [/V:label] [/Q] [/T:tracks /N:sectors]FORMAT volume [/V:label] [/Q]FORMAT volume [/Q]

参数说明：

参数	说明
volume	指定驱动器（后面跟一个冒号）、装入点或卷名
/FS:filesystem	指定文件系统类型（FAT、FAT32 或 NTFS）
/V:label	指定卷标
/Q	执行快速格式化
/C	仅适于 NTFS，默认情况下，将压缩在该新建卷上创建的文件
/X	如果必要，先强制卸下卷。那时该卷所有已打开的句柄不再有效
/A:size	替代默认配置单位大小。强烈建议用户在一般状况下使用默认设置
/F:size	指定要格式化的软盘大小
/T:tracks	为磁盘指定每面磁道数
/N:sectors	指定每条磁道的扇区数

133. FTYPE

功能：显示或修改用在文件扩展名关联中的文件类型

格式：FTYPE [fileType=[openCommandString]]

参数说明：

参数	说明
fileType	指定要检查或改变的文件类型
openCommandString	指定调用这类文件时要使用的开放式命令

134. GOTO

功能：将 cmd.exe 导向到批处理程序中带标签的行。

使用说明：GOTO label中的label用于指定批处理程序中用作标签的文字字符串。标签必须单独一行，并且以冒号开头。

135. MD

功能：创建目录。

格式：MKDIR [drive:]pathMD [drive:]path

136. MORE

功能：逐屏显示输出。
格式：MORE [/E [/C] [/P] [/S] [/Tn] [+n]] < [drive:][path]filename
参数说明：

参数	说明
[drive:][path]filename	指定要逐屏显示的文件
command-name	指定要显示其输出的命令
/E	启用扩展功能
/C	显示页面前先清除屏幕
/P	扩展 FormFeed 字符
/S	将多个空白行缩成一行
/Tn	将跳格键扩展成n个空格（默认值为8），命令行开关可以出现在 MORE 环境变量中
+n	从第 n 行开始显示第一个文件
files	要显示的文件列表。用空格分开列表中的文件

137. MOVE

功能：移动文件并重命名文件和目录。
格式：MOVE [/Y/ -Y][drive:][path]filename1[,...] destination
参数说明：

参数	说明
[drive:][path]filename1	指定用户想移动的文件的位置和名称
destination	指定文件的新位置。目标可包含一个驱动器号和冒号、一个目录名或组合。如果只移动一个文件并在移动时将其重命名，用户还可以包括文件名
[drive:][path]dirname1	指定要重命名的目录
dirname	指定目录的新名称
/Y	取消确认改写一个现有目标文件的提示
/-Y	对确认改写一个现有目标文件发出提示

138. PATH

功能：显示或设置可执行文件的搜索路径。
格式：PATH [drive:]path[;...];;%PATH%

139. PRINT

功能：打印文本文件。
格式：PRINT [/D:device] [[drive:][path]filename[...]]
参数说明：
/D:device：指定打印机设备。

140. RD

功能：删除一个目录。

摆脱黑客攻击的 150 招秘籍

格式：RD [/S] [/Q] [drive:]path
参数说明：

参数	说明
/S	除目录本身外，还将删除指定目录下的所有子目录和文件。用于删除目录树
/Q	安静模式，带 /S 删除目录树时不要求确认

141. REN

功能：重命名文件。
格式：REN[drive:][path]filename1 filename2

142. REPLACE

功能：替换文件。
格式：
REPLACE [drive1:][path1]filename [drive2:][path2] [/A] [/P] [/R] [/W]
REPLACE [drive1:][path1]filename [drive2:][path2] [/P] [/R] [/S] [/W] [/U]
参数说明：

参数	说明
[drive1:][path1]filename	指定源文件
[drive2:][path2]	指定要替换文件的目录
/A	把新文件加入目标目录。不能和/S 或 /U 命令行开关搭配使用
/P	替换文件或加入源文件之前会先提示用户进行确认
/R	替换只读文件以及未受保护的文件
/S	替换目标目录中所有子目录的文件。不能与 /A 命令选项搭配使用
/W	等用户插入磁盘以后再运行
/U	只会替换或更新比源文件日期早的文件，不能与 /A 命令行开关搭配使用

143. SET

功能：显示、设置或删除 cmd.exe 环境变量。
格式：SET [variable=[string]]
参数说明：

参数	说明
variable	指定环境变量名
string	指定要指派给变量的一系列字符串

使用说明：输入不带参数的SET，则显示当前环境变量。

144. START

功能：启动另一个窗口运行指定的程序或命令。
格式：START ["title"] [/Dpath] [/I] [/MIN] [/MAX] [/SEPARATE|/SHARED]

[/LOW|/NORMAL|/HIGH|/REALTIME|/ABOVENORMAL|/BELOWNORMAL|/WAIT] [B]
[command/program] [parameters]

参数说明：

参数	说明
"title"	在窗口标题栏中显示的标题
path	起始目录
B	在不创建新窗口的情况下开始应用程序。除非启动 ^C 处理，否则该应用程序会忽略 ^C 处理，^Break 是唯一可以中断该应用程序的方式
I	新环境是传递给 cmd.exe 的原始环境，而不是当前环境
MIN	开始时窗口最小化
MAX	开始时窗口最大化
SEPARATE	在分开的空间内开始 16 位 Windows 程序
SHARED	在共享的空间内开始 16 位 Windows 程序
LOW	在 IDLE 优先级类别开始应用程序
NORMAL	在 NORMAL 优先级类别开始应用程序
HIGH	在 HIGH 优先级类别开始应用程序
REALTIME	在 REALTIME 优先级类别开始应用程序
ABOVENORMAL	在 ABOVENORMAL 优先级类别开始应用程序
BELOWNORMAL	在 BELOWNORMAL 优先级类别开始应用程序
WAIT	启动应用程序并等候它结束
command/program	用 /K 命令行开关运行 cmd.exe。这表示该窗口在命令运行后仍然存在，如果不是内部 cmd 命令或批文件，则是一个程序，并作为窗口应用程序或控制台应用程序运行
parameters	这些为传送到命令/程序的参数

145. SUBST

功能：将路径与驱动器号关联。
格式：SUBST [drive1: [drive2:]path]
SUBST drive1: /D
参数说明：

参数	说明
drive1	指定要指派路径的虚拟驱动器
[drive2:]path	指定物理驱动器和要指派给虚拟驱动器的路径
/D	删除被替换的（虚拟）驱动器

使用说明：
不加任何参数键入 SUBST，可以显示当前虚拟驱动器的清单。

146. TIME

功能：显示或设置系统时间。
格式：TIME [/T | time]

摆脱黑客攻击的 150 招秘籍

使用说明：显示当前时间设置和输入新时间的提示，请键入不带参数的 TIME。要保留现有时间，请按【Enter】键。如果命令扩展名被启用，DATE 命令会支持 /T 命令行开关；该命令行开关告诉命令只输出当前时间，但不提示输出新时间。

147. TREE

功能：以图形显示驱动器或路径的文件夹结构。

格式：TREE [drive:][path] [/F] [/A]

参数说明：

参数	说明
/F	显示每个文件夹中文件的名称
/A	使用ASCII字符，而不使用扩展字符

148. TYPE

功能：显示文本文件的内容。

格式：TYPE [drive:][path]filename

149. VER

功能：显示 Windows XP 版本。

格式：VER

150. XCOPY

功能：复制文件和目录树。

格式：XCOPY source [destination] [/A | /M] [/D[:date]] [/P] [/S /E]] [/V] [/W]/[C] [/I] [/Q] [/F] [/L] [/G] [/H] [/R] [/T] [/U]/[K] [/N] [/O] [/X] [/Y] [/Y] [/Z]/[EXCLUDE:file1[+file2][+file3]...]

参数说明：

参数	说明
source	指定要复制的文件
destination	指定新文件的位置和/或名称
/A	只复制有存档属性集的文件，但不改变属性
/M	只复制有存档属性集的文件并关闭存档属性
/D:m-d-y	复制在指定日期或指定日期以后更改的文件，如果没有提供日期，只复制那些源时间比目标时间新的文件
/EXCLUDE:file1[+file2][+file3]...	指定含有字符串的文件列表。每一个字符串必须在文件的单独行中。如果有任何字符串与要被复制的文件的绝对路径相符，那个文件将不会得到复制
/P	创建每个目标文件前提示
/S	复制目录和子目录，除了空的
/E	复制目录和子目录，包括空的，与 /S /E 相同。可以用来修改 /T
/V	验证每个新文件
/W	提示用户在复制前按键
/C	即使有错误，也继续复制

参数	说明
/I	如果目标不存在，又在复制一个以上的文件，则假定目标一定是一个目录
/Q	复制时不显示文件名
/F	复制时显示完整的源和目标文件名
/L	显示要复制的文件
/G	允许将没有经过加密的文件复制到不支持加密的目标
/H	也复制隐藏和系统文件
/R	覆盖只读文件
/T	创建目录结构，但不复制文件，不包括空目录或子目录。/T /E 包括空目录和子目录
/U	只复制已经存在于目标中的文件
/K	复制属性。一般的 Xcopy 会重置只读属性
/N	用生成的短名复制
/O	复制文件所有权和 ACL 信息
/X	复制文件审核设置（隐含 /O）
/Y	复制文件审核设置（隐含 /O），现存目标文件
/-Y	导致提示以确认改写一个现存目标文件
/Z	用重新启动模式复制网络文件