1.1 什么是黑客

黑客原指那些热衷于电脑，并懂得一些编程知识的电脑爱好者。由于系统、网络和软件不可避免地存在某些安全漏洞，黑客的目的就是为了找出并弥补这些漏洞。

1.1.1 黑客简介

黑客(Hacker)是热衷研究、撰写程序的专才，必须具备乐于追根究底、穷究问题的特质。

1. 认识黑客

在黑客圈中，hacker 一词无疑是带有正面意义的，例如 system hacker 是熟悉操作系统的设计与维护；password hacker 是精于找出使用者的密码；如果是 computer hacker，则是通晓计算机系统，熟练操作计算机的高手。

黑客基本上是一项业余嗜好，通常是出于自己的兴趣，而非为了赚钱或工作需要。根据开放原始码计划创始人 Eric Raymond 对此字的解释，hacker 与 cracker 是分属两个不同世界的族群，基本差异在于，hacker 是有建设性的，而 cracker 则专门搞破坏。

知识点滴

hacker 原意是指用斧头砍柴的工人，最早被引进计算机圈则可追溯自 1960 年。加州柏克莱大学计算机教授 Brian Harvey 在考证此字时曾写到：当时在麻省理工学院中(MIT)的学生通常分成两派，一是 tool，意指成绩优秀的学生；另一则是所谓的 hacker，也就是成绩一般，但却热衷于其他研究且精力充沛喜欢搞课外活动的学生。

2. 黑客与电脑的关系

- 黑客与电脑开始并没有什么关联。不过当时黑客也区分等级，就如同 tool 用成绩比高下一样。真正一流黑客并非整天不学无术，而是会热衷追求某种特殊嗜好，比如研究电话、铁道(模型或者真的)、科幻小说，无线电或者是计算机。因此后来才有所谓的 computer hacker 出现，意指计算机高手。

对一个黑客来说，学会入侵和破解是必要的，但最主要的还是编程，毕竟使用工具是体现别人的思路，而程序是自己的想法。而对于一个骇客来说，他们只追求入侵的快感，不在乎技术，他们普遍不懂得编程，更不知道入侵的具体细节。

1.1.2 黑客必须了解的网络知识

作为一个最基本的黑客，必须了解相关的网络知识，例如 IP 地址、端口和服务等。

1. IP 地址

IP 地址就是一个网络上的地址，在外网上的 IP 地址都是唯一的，就像身份证号码一样，给每台进入网络的电脑一个身份证号码。但是对于大部分用户来说，IP 地址并不是固定的，在重新连接到互联网时，IP 地址可能会被重新分配。如果申请了固定的 IP 地址，可以便于其他电脑找到它，并提供服务。

一般的 IP 地址的格式为：a.b.c.d(0<=a，b，c，d<=255)，该格式为点分 10 进制，例如 218.242.161.231，IP 地址的标准形式是二进制形式，例如 212.13.123.52 的二进制 11010100000000001101011101100110100 ..... 由 192.168 开头的是局域网的 IP 地址，127.0.0.1 是用来检测网络的自己的 IP 地址，也就是说任何一台电脑不管是否连接到互联网上，127.0.0.1 对应于本地的 IP 地址。

2. 端口

电脑上有很多的端口(65535 个)，但是这些端口大部分都是关闭的，每个网络连接都要用一个端口，就好比一根线把两个电脑连起来，插座就是端口。有些端口有它们特定的用途，例如网页服务器要开 80 端口，FTP 服务器要开 21 端口。

有关电脑中常用端口的功能如下表所示。

端　口	功　能
21 端口	ftp 下载
23--telnet 端口	远程登录，入侵后可以留下后门木马
79--finger 端口	可以知道用户信息
80--http 端口	HTTP 服务器
110--pop 端口	接收电子邮件
139(445)--netbios 端口	共享，远程登录
135--RPC 端口	远程溢出的大洞的端口
3389--win2000 端口	超级终端

黑客在入侵成功后，就要为自己运行木马，打开一个端口，为自己以后回来留后门。

3. 服务

服务就是 service，例如 HTTP 服务器就要安装 World Wide Web Publishing 服务。服务实质是为他人提供服务的程序，这个程序会在开机时自动加载，同时打开端口等待对方连接并向对方提供服务。可以在入侵对方机器后，启动或安装一些服务，例如 SUCH AS 远程桌面、TELNET 等，这些服务都是 Microsoft 提供的，所以不用担心被杀毒软件发现。在开了一些远程管理的服务后，攻击者就可以很方便地回到被侵入过的主机了。

4. 网络协议

网络协议就是一套双方约定好的通信协议。网络协议具有特定的约定来达成连接。

网络协议分为多种，作为一名合格的黑客，必须对以下两种网络协议有深刻的了解。

- 面向连接的 TCP 协议：TCP 是 Transmission Control Protocol 的缩写，“面向连接”就是在正式通信前必须要与对方建立起连接。例如打电话，必须等线路接通了才能相互通话。TCP 传输控制协议是基于连接的协议，也就是说，在正式收发数据前，必须和对方建立可靠的连接。一个 TCP 连接必须要经过三次“对话”才能建立起来。TCP 协议能为应用程序提供可靠的通信连接，使一台计算机发出的字节流无差错地发往网络上的其他计算机，对可靠性要求高的数据通信系统往往使用 TCP 协议传输数据。
- 面向非连接的 UDP 协议：面向非连接就是在正式通信前不必与对方先建立连接，不管对方状态就直接发送。这与手机短信非常相似，在发短信时，只需要输入对方手机号即可。UDP(User Data Protocol)用户数据报协议是与 TCP 相对应的协议。它是面向非连接的协议，它不与对方建立连接，而是直接就把数据包发送过去。UDP 协议是面向非连接的协议，没有建立连接的过程。正因为 UDP 协议没有连接的过程，所以它的通信效果高；但也正因为如此，它的可靠性不如 TCP 协议高。

1.1.3 黑客需要掌握的基本技能

下面介绍作为一名初级黑客所必须掌握的

基本技能，帮助用户揭开黑客的神秘面纱，更好地学习黑客攻防知识。

1. 有一定的英文基础

学习英文对于黑客来说非常重要，因为现在大多数资料和教程都是英文版本，而且有关黑客的新闻也是从国外过来的，一个漏洞从发现到出现中文介绍，需要大约一个星期的时间，在这段时间内网络管理员就已经有足够的时间修补漏洞了，所以当我们看到中文介绍时，这个漏洞可能早就已经不存在了。因此学习黑客从一开始就要尽量阅读英文资料、使用英文软件、并且及时关注国外著名的网络安全网站。

2. 学习基本软件的使用

这里所指的基本软件是指两个内容：一个是日常使用的各种电脑常用命令，例如 ftp、ping、net 命令等；另一方面还要学会有关黑客工具的使用，这主要包括端口扫描器、漏洞扫描器、信息截获工具和密码破解工具等。因为这些软件品种多，功能各不相同。

3. 初步了解网络协议和工作原理

所谓初步了解就是按照自己的方式去理解网络的工作原理，因为协议涉及的知识多且复杂，所以如果在一开始就进行深入研究，势必会大大挫伤学习积极性。建议用户初步了解有关 tcp/ip 协议，尤其是浏览网页时，网络是如何传递信息、客户端浏览器如何申请“握手信息”、服务器端如何“应答握手信息”并“接受请求”等内容。

4. 有一定的编程基础

不要求用户对编程语言或脚本进行深入的学习，只要能够看懂有关语言、知道程序执行结果即可。建议用户初步学习 C 语言、asp 和 cgi 脚本语言，另外对于 htm 超文本语言和 php、java 等有一定了解即可，主要学习这些语言中的“变量”和“数组”部分，因为语言之间存在内在联系，所以只要熟练掌握其中一门，其他语言也可以了解。

5. 熟悉网络应用程序

网络应用程序包括各种服务器软件后台程序，例如 wuftp、Apache 等服务器后台；还有网上流行的各种论坛、电子社区。有条件的学习者最好将自己的电脑做成服务器，然后安装并运行一些论坛代码，经过一番尝试之后，将会感性地弄清楚网络工作原理，这比依靠理论学习要容易许多，能够达到事半功倍的效果。

1.2 黑客攻击的特点

要想更好地保护网络不受黑客的攻击，就必须对黑客的攻击方法、攻击原理、攻击过程有深入和详细的了解，只有这样才能更有效、更具有针对性地进行主动防护。下面介绍有关黑客攻击的特点，来研究如何对黑客攻击行为进行检测与防御。

1.2.1 反攻击技术核心问题

攻击技术(入侵检测技术)的核心问题是如何截获所有的网络信息。目前主要是通过两种途径来获取信息，一种是通过网络侦听的途径(如 Sniffer，Vpacket 等程序)来获取所有的网络信息(数据包信息，网络流量信息、网络状态信息、网络管理信息等)，这既是黑客进行攻击的必然途径，也是进行反攻击的必要途径；另一种是通过对操作系统和应用程序的系统日志进行分析，来发现入侵行为和系统潜在的安全漏洞。

1.2.2 黑客主要攻击方式

黑客对网络的攻击方式是多种多样的，一般来讲，攻击大多利用系统配置的缺陷、操作系统的安全漏洞或通信协议的安全漏洞。

有关黑客的主要攻击方式可以归纳为以下几种。

1. 拒绝服务攻击

一般情况下，拒绝服务攻击是通过使被攻击对象(通常是工作站或重要服务器)的系统关键资源过载，从而使被攻击对象停止部分或全部服务。目前已知的拒绝服务攻击就有几百种，它是最基本的入侵攻击手段，也是最难对付的入侵攻击之一，典型示例有 SYN Flood 攻击、Ping Flood 攻击、Land 攻击、WinNuke 攻击等。

2. 非授权访问尝试

非授权方式尝试是攻击者对被保护文件进行读、写或执行的尝试，也包括为获得被保护访问权限所做的尝试。

3. 预探测攻击

预探测攻击是在连续的非授权访问尝试过程中，攻击者为了获得网络内部的信息及网络周围的信息，通常使用这种攻击尝试，典型示例包括 SATAN 扫描、端口扫描和 IP 地址半途扫描等。

4. 可疑活动

可疑活动通常是指定义的“标准”网络通信范畴之外的活动，也可以指网络上不希望有的活动，例如 IP Unknown Protocol 和 Duplicate IP Address 事件等。

5. 协议解码

协议解码可用于以上任何一种黑客主要的攻击方式中，网络或安全管理员需要进行解码工作，并获得相应的结果，解码后的协议信息可能表明期望的活动，例如 FTU User 和 Portmapper Proxy 等解码方式。

6. 系统代理攻击

系统代理攻击通常是针对单个主机发起的，而并非整个网络，通过 RealSecure 系统代理可以对它们进行监视。

1.2.3 黑客攻击的流程

一般来说，黑客对电脑进行攻击的步骤大致相同，主要包括以下几步。

1. 扫描漏洞

目前大多数电脑安装的是 Windows 操作系统，Windows 操作系统的稳定性和安全性随着其版本的提升而得到不断的提高，但难免会出现这样或那样的安全隐患，这些安全隐患就是漏洞。黑客通过其专业的研究发现了这些漏洞，于是使用病毒和木马通过这些漏洞攻击和破坏电脑。

2. 试探漏洞

在了解了目标主机的漏洞和弱点之后，黑客就能使用缓冲区溢出和测试用户帐号和密码等，达到对其进行试探性攻击的目的。

3. 取得权限与提升权限

如果试探出了可以利用的漏洞，那就意味着黑客获得了攻击该目标主机的初步权限，只要能登录目标主机，那么提升权限将变得易如反掌，借助木马等程序可以更顺利地达到目的。在某些情况下，黑客在取得权限与提升权限时会采用破坏目标电脑操作系统的方法来实现。

4. 木马入侵

木马是一种能窃取用户存储在电脑中的帐

户、密码等信息的应用程序。黑客通过木马程序可以轻易地入侵并控制用户电脑，并在用户不知情的状况下通过用户的电脑进行各种破坏活动。在日常生活中经常出现的 QQ 号码被盗的情况，一般就是黑客通过木马进行窃取的。

5. 建立后门与清理痕迹

为了达到长期控制目标主机的目的，黑客在取得管理员权限之后会立刻在其中建立后门，这样就可以随时登录该主机。为了避免被目标主机的管理员发觉，在完成入侵之后需要清除其中的系统日志文件、应用程序日志文件和防火墙的日志文件等，清理完毕即可从目标主机中退出。至此，一次完整的黑客攻击便完成了。

1.3 黑客攻击的入口——端口

前文已经对端口进行了介绍。可以把端口看成电脑与外界网络连接的一扇门，在某种意义上说，端口掌控着网络连接大权，因此也是黑客攻击的入口。

1.3.1 端口的分类

在 Windows 系统的端口分配中，按照端口号可以划分为已知端口、注册端口和动态端口 3 类。

1. 已知端口

已知端口是指端口号在 0~1023 之间的端口。这些端口号一般固定分配给一些服务，例如前面提到的 21 端口分配给 FTP 服务，80 端口分配给 HTTP 服务等。

2. 注册端口

注册端口是指端口号在 1024~49151 之间的端口。注册端口在大多数系统是上可以由普通用户进程或普通用户所执行的程序使用，也就是这些端口号通常不固定分配给某个服务，只要运行的程序向系统提出访问网络需求，系统就会分配一个端口号给该服务使用。

3. 动态端口

动态端口是指端口号在 49152~65535 之间的端口。这些端口不为服务分配端口，但在实际操作时，电脑通常从 1024 端口号起就分配动态端口。因此，从 1024 端口开始，也可以一并归纳为动态端口。

动态端口常常被病毒木马程序所利用，例如大名鼎鼎的冰河木马默认连接端口是 7626，Netspy 的连接端口为 7306。

1.3.2 开启和关闭端口

在 Windows 系统中，可以使用自带的 Netstat 命令查看网络状况。

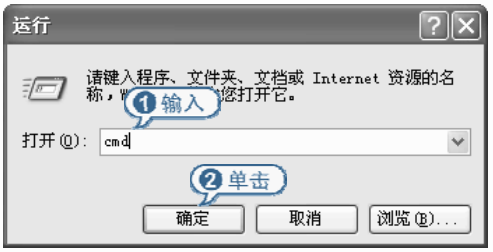
Netstat 命令的格式为：netstat[-a][-e][-n][-o][-s][-p protocol][-r][interval]其中[-a]参数的含义是显示所有连接和监听的端口；[-n]参数的含义是以数字格式显示地址和端口号。下面通过实例来介绍使用 Netstat 命令查看本地电脑开放的端口信息。

【例 1-1】使用 Netstat 命令查看本地电脑开放的端口信息。

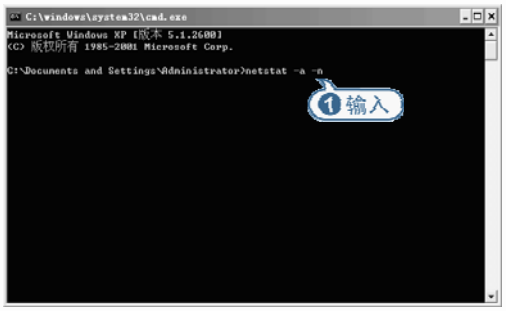
☑ 教学视频 ☐ 源文件

01 单击【开始】按钮，在弹出的快捷菜单中选择【运行】命令，打开【运行】对话框。

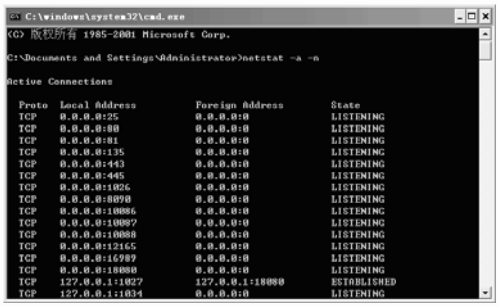
02 在【运行】文本框中输入命令 cmd，然后单击【确定】按钮，打开命令提示符窗口。



03 在命令提示符状态下输入 netstat –a –n。



04 按下 Enter 键，即可以数字形式显示 TCP 和 UDP 连接的端口号以及状态。



高手点拨

在命令提示符窗口显示的端口信息列表中，Active Connections 指本机的活动连接；Proto 指使用的协议名称；Local Address 指本机 IP 地址和正在使用的端口号；Foreign Address 指连接某个端口的远程主机和 IP 地址以及端口号；State 指当前 TCP 连接状态；LISTENING 指该端口是开放的并且正在监听等待连接。

高手点拨

如果本机的 7626 端口已经开放并且正在监听等待连接(LISTENING 状态)，那么极有可能已经感染了冰河木马。为谨慎起见，必须马上断开网络，使用杀毒软件查杀病毒。

1. 关闭端口

默认情况下，有许多端口是不安全的。为了保证系统的安全性，可以关闭这些端口。下面通过实例介绍关闭端口的方法。

【例 1-2】关闭系统中无用的端口。

教学视频 源文件

01 打开【控制面板】窗口，双击【管理工具】图标，打开【管理工具】窗口。

02 双击【服务】图标打开【服务】窗口。

03 在【服务】窗口右侧的窗格中双击 Remote Procedure Call(RPC)服务，打开【Remote Procedure Call(RPC)的属性】对话框。单击【停止】按钮，可以停止服务。

2. 开启端口

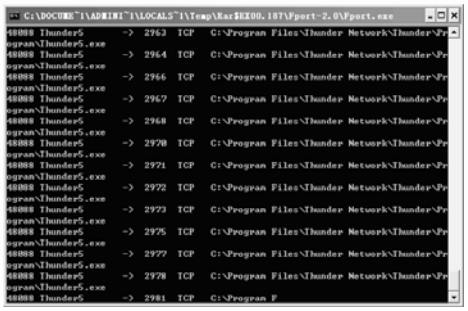
如果要开启某个端口，双击该端口，例如自动更新端口，打开【自动更新的属性】对话框，然后单击【启动】按钮，即可开启端口。

1.3.3 使用 fport 工具

使用 fport 工具可以查看当前系统打开的 TCP/IP 和 UDP 端口信息，还可以查看与端口对应的软件路径和进程名称等。

双击 Fport.exe 应用程序即可运行 fport。

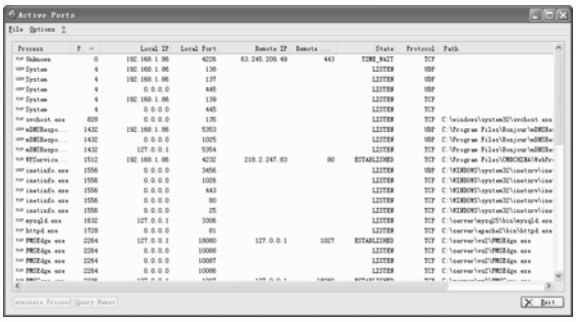
运行 fport 后，会自动打开命令提示符窗口，fport 工具会自动扫描本地电脑开放的端口和使用该端口相应的应用程序。



1.3.4 使用 Active Ports 工具

使用 Active Port 软件同样可以查看端口信息，而且相对命令提示符窗口而言，使用 Active Port 软件可以更为轻松且更加清晰地显示端口信息。

安装好 Active Port 软件后，单击【开始】按钮  ，在弹出的【开始】菜单中选择【所有程序】|Active Ports|Active Ports 命令，启动 Active Ports 工具软件。



在打开的 Active Ports 窗口中可以查看当前系统所开放的端口以及这些端口所对应的应用程序。

1.4 木马藏身之处——系统进程

进程是指在系统中正在运行的一个应用程序，它是木马程序主要的藏身地。下面介绍有关系统进程的基础知识以及一些基本操作。

1.4.1 认识系统进程

进程是指在系统中正在运行的一个应用程序；线程是系统分配处理器时间资源的基本单元，或者说进程之内独立执行的一个单元。对于操作系统而言，其调度单元是线程。一个进程至少包括一个线程，通常将该线程称为主线

程。一个进程从主线程的执行开始进而创建一个或多个附加线程，就是所谓基于多线程的多任务。

这里的进程是指一系列进程，这些进程是由它们所运行的可执行程序实例来识别的，这就是进程选项卡中的第一列给出了映射名称的原因。请注意，这里并没有进程名称列。进程并不拥有独立于其所归属实例的映射名称。

1.4.2 基本系统进程列表

进程是系统运行的基本条件，有了这些进程，系统才能正常运行。下表中列出了一些最基本的系统进程。

进　程	功　能
csrss.exe	子系统服务器进程
winlogon.exe	管理用户登录
services.exe	包含很多系统服务
lsass.exe	管理 IP 安全策略以及启动 ISAKMP/Oakley(IKE)和 IP 安全驱动程序
svchost.exe	包含很多系统服务
Explorer.exe	资源管理器
internat.exe	托盘区的拼音图标
mstask.exe	允许程序在指定时间运行
regsvc.exe	允许远程注册表操作
winmgmt.exe	提供系统管理信息
inetinfo.exe	通过 Internet 信息服务的管理单元提供 FTP 连接和管理
tlntsvr.exe	允许远程用户登录到系统并且使用命令行运行控制台程序
tftpd.exe	实现 TFTP Internet 标准。该标准不要求用户名和密码。远程安装服务的一部分

(续表)

进　程	功　能
termsrv.exe	提供多会话环境允许客户端设备访问虚拟的 Windows 2000 Professional 桌面会话以及运行在服务器上的基于 Windows 的程序
ups.exe	管理连接到计算机的不间断电源(UPS)
ismserv.exe	允许在 Windows Advanced Server 站点间发送和接收消息
ntfrs.exe	在多个服务器间维护文件目录内容的文件同步
locator.exe	注册客户端许可证
locator.exe	管理 RPC 名称服务数据库
dfssvc.exe	管理分布于局域网或广域网的逻辑卷
faxsvc.exe	帮助用户发送和接收传真。
mnmsrvc.exe	允许有权限的用户使用 NetMeeting 远程访问 Windows 桌面
netdde.exe	提供动态数据交换(DDE)的网络传输和安全特性
smlogsvc.exe	配置性能日志和警报
RsEng.exe	协调用来储存不常用数据的服务和管理工具
RsFsa.exe	管理远程储存的文件的操作
grovel.exe	扫描零备份存储(SIS)卷上的重复文件，并且将重复文件指向一个数据存储点，以节省磁盘空间
snmptrap.exe	接收由本地或远程 SNMP 代理程序产生的陷阱消息，然后将消息传递到运行在本机上 SNMP 管理程序

(续表)

进　程	功　能
UtilMan.exe	从一个窗口中启动和配置辅助工具
msiexec.exe	依据 .MSI 文件中包含的命令来安装、修复以及删除软件

1.4.3　打开系统进程

打开系统进程可以查看哪些进程是正常的，哪些是系统必需的进程。按下 Ctrl+Shift+Del 键，打开【Windows 任务管理器】窗口，单击【进程】选项卡，即可显示当前系统正在运行的进程。

通常情况下，smss.exe、csrss.exe、winlogon.exe、services.exe、lsass.exe、svchost.exe、spoolsv.exe、explorer.exe、SystemIdleProcess 这些都是系统正常的进程。

1.4.4　关闭和新建系统进程

对于熟悉系统进程的用户来说，查看进程可以快速判断出系统是否存在安全隐患。

1. 关闭进程

在【Windows 任务管理器】窗口的【进程】选项卡的进程列表中，选中相应的进程，然后单击右下角的【结束进程】按钮，即可关闭该进程。

在关闭有些进程时要注意，例如关闭 Explorer.exe 进程，该进程是 Windows 资源管理器，用于管理 Windows 图形壳，包括【开始】菜单、任务栏、桌面和文件管理，关闭该进程会导致 Windows 图形界面无法使用。

高手点拨

Explorer.exe 进程也可能是 w32.codered 和 w32.mydoom.b@mm 病毒。该病毒通过电子邮件附件传播。

2. 新建进程

打开【Windows 任务管理器】窗口，选择【文件】|【新建任务(运行...)】命令，打开【创建新任务】对话框，然后在【打开】文本框中输入 Explorer.exe 进程，单击【确定】按钮，即可新建 Explorer.exe 进程。

3. 在 DOS 下查看进程

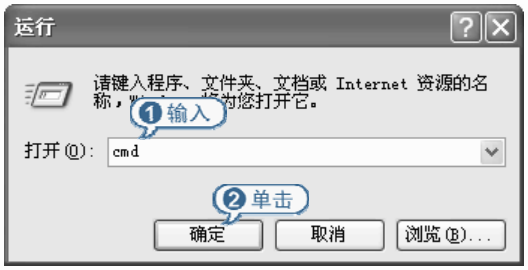
如果无法进入桌面环境时，可以在 DOS 下查看进程。

【例 1-3】在 DOS 下查看系统进程。

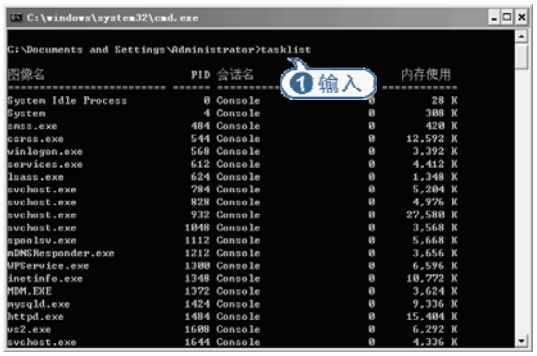
教学视频　源文件

01 单击【开始】按钮，在弹出的【开始】菜单中选择【运行】命令，打开【运行】对话框。

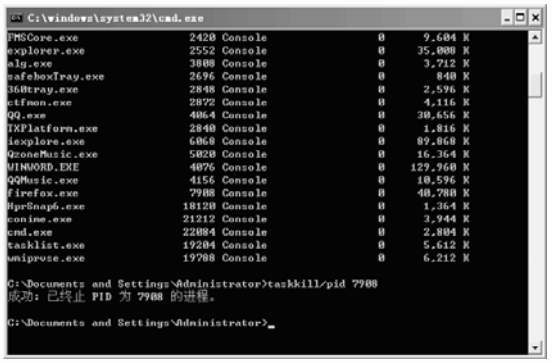
02 在【运行】文本框中输入 cmd，单击【确定】按钮，打开命令提示符窗口。



03 输入 tasklist 命令，按下 Enter 键，即可显示当前系统中的所有进程。



04 如果要结束当前系统进程，例如关闭 firefox.exe 进程，该进程的 PID 为 7908，输入命令 taskkill/pid 7908，然后按下 Enter 键，即可终止该进程。



1.4.5 查看进程起始程序

通过查看进程起始程序，可以判断哪些进程是恶意进程。

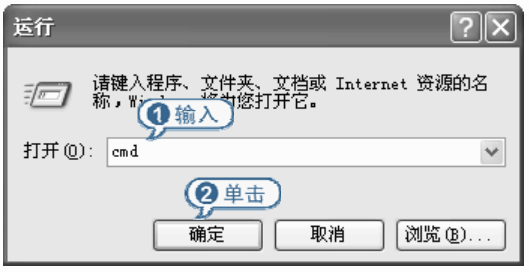
下面通过实例，以查看 Svchost 进程为例，来介绍查看进行起始程序的方法。

【例 1-4】查看系统进程起始程序。

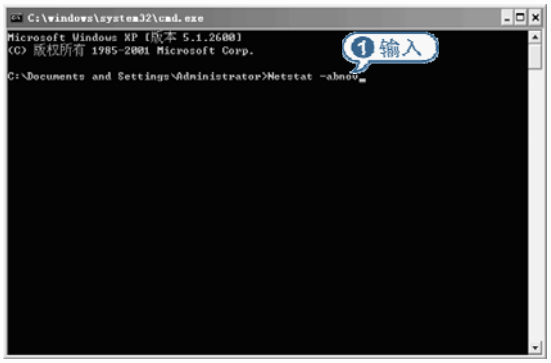
教学视频 源文件

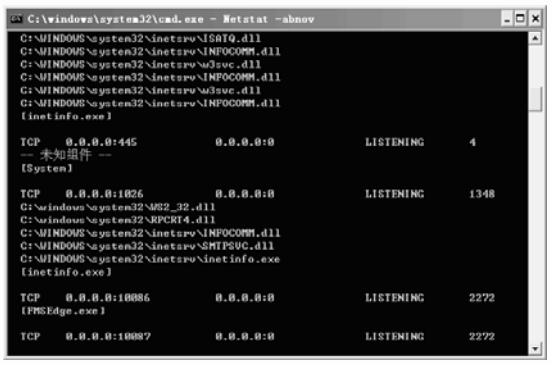
01 单击【开始】按钮 开始，在弹出的【开始】菜单中选择【运行】命令，打开【运行】对话框。

02 在【运行】文本框中输入 cmd，单击【确定】按钮，打开命令提示符窗口。



03 在命令提示符窗口中输入 Netstat –abnov 命令，然后按下 Enter 键，即可在反馈的进程信息中查看每个进程的起始程序或文件列表。可以根据相关知识来判断是否为病毒或木马发起程序。





1.4.6 查看隐藏进程

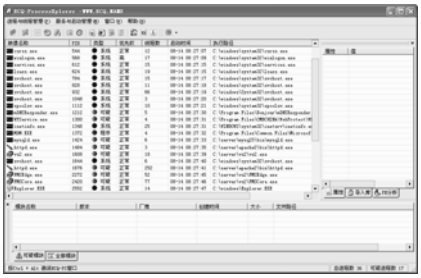
在【Windows 任务管理器】窗口中并不能显示一些隐藏的进程，而这些隐藏的系统进程很可能是病毒木马程序。下面通过实例介绍使用软件查看隐藏进程的方法。

【例 1-5】使用【隐藏进程管理工具】查看隐藏的系统进程。

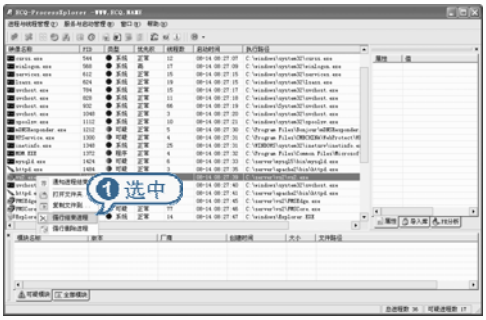
教学视频 源文件

01 启动【隐藏进程管理工具】程序。

02 在打开的窗口中可以查看当前系统中的所有进程。



03 窗口中的每个进程都显示了 PID、类型、优先权、线程数、启动时间和执行路径等信息。对于提示为【可疑】的进程，可以查看具体的文件路径，如果确认为恶意程序时，可以右击该进程，在弹出的快捷菜单中选择【强行结束进程】命令，强行关闭该进程。



知识点滴

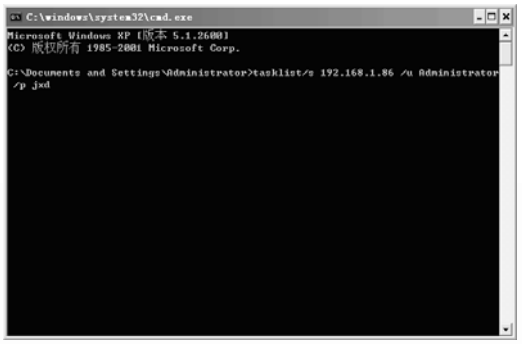
有关隐藏进程管理工具的其他功能，用户可以自行进行操作，这里就不再介绍了。

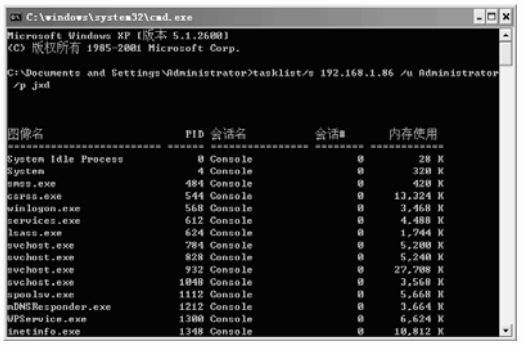
1.4.7 查看远程进程

查看远程电脑的进程是黑客必须掌握的技巧，在命令提示符窗口中输入命令即可查看远程电脑的进程。

打开命令提示符窗口，输入 tasklist/s IP 地址 /u Administrator /p 帐户密码。

打开命令提示符窗口，然后输入 takslist/s 192.168.1.86 /u Administrator /p jxd，然后按下 Enter 键，稍等片刻后，即可反馈 192.168.1.86 这个 IP 地址的远程电脑进程列表信息，其中的 jxd 是远程电脑的 Adminitrator 帐户密码，如果未设置密码可以直接输入 takslist/s 192.168.1.86 /u Administrator。





1.4.8 查杀病毒进程

在实际操作时，可能无法在【Windows 任务管理器】窗口中删除某个可疑进程，此时可以在命令提示符窗口中输入 taskkill/im 进程名命令关闭某个进程，例如输入 taskkill/im firefox.exe 命令，可以关闭 firefox.exe 进程。

1.5 黑客攻击和网络安全相关术语

对于许多初级黑客或者即将走进黑客群体的用户来说，一些黑客术语是必须掌握的。此外，掌握一些网络安全相关术语可以帮助用户更好地了解和踏入黑客之门。

1.5.1 黑客攻击相关术语

下面详细介绍了黑客领域常见的一些专业术语。

1. 肉鸡

所谓“肉鸡”，是一种很形象的比喻，比喻那些可以随意被黑客控制的电脑，对方可以是 Windows 系统，也可以是 Unix 或 Linux 系统，可以是普通的个人电脑，也可以是大型的服务器，黑客可以像操作自己的电脑那样来操作它们，而不被对方所发觉。

2. 木马

木马就是那些表面上伪装成了正常的程序，但是当这些程序运行时，就会获取系统的整个控制权限。有很多黑客就是热衷于使用木马程序来控制别人的电脑，著名的木马程序有灰鸽子、黑洞、PcShare、特洛伊等。

3. 网页木马

网页木马表面上伪装成普通的网页文件或是将木马程序的代码直接插入到正常的网页文件中。当该页被访问时，网页木马就会利用对方系统或者浏览器的漏洞自动将配置好的木马的服务端下载到访问者的电脑上来自动执行。

4. 挂马

挂马就是在别人的网站文件里面放入网页木马或者是将代码潜入到对方正常的网页文件里，以使浏览者中木马。

5. 后门

后门是一种形象的比喻，入侵者在利用某些方法成功地控制了目标主机后，可以在对方的系统中植入特定的程序，或者是修改某些设置。这些改动表面上是很难被察觉的，但是入侵者却可以使用相应的程序或者方法来轻易地与这台电脑建立连接，重新控制这台电脑，就好象是入侵者偷偷地配了一把主人房间的钥匙，可以随时进出而不被主人发现一样。

通常大多数的特洛伊木马(Trojan Horse)程序都可以被入侵者用于制作后门(BackDoor)。

6. rootkit

rootkit 是攻击者用来隐藏自己的行踪和保留 root(根权限，可以理解成 WINDOWS 下的 system 或者管理员权限)访问权限的工具。通常，攻击者通过远程攻击的方式获得 root 访问权限，或者是先使用密码猜解(破解)的方式获得对系统的普通访问权限，进入系统后，再通过对方系统内存在的安全漏洞获得系统的 root 权限。然后，攻击者就会在对方的系统中安装 rootkit，以达到自己长久控制对方的目的，rootkit 与我们前边提到的木马和后门很类似，但远比它们要隐蔽，黑客守卫者就是很典型的 rootkit，还有国内的 ntroorkit 等都是不错的 rootkit 工具。

7. IPC

IPC 是共享命名管道的资源，它是为了让进程间通信而开放的命名管道，可以通过验证用户名和密码获得相应的权限，在远程管理计算机和查看计算机的共享资源时使用。

8. 弱口令

弱口令是指那些强度不够，容易被猜解的，类似 123.abc 这样的口令(密码)。

9. 默认共享

默认共享是 Windows 2000/XP/2003 系统开启共享服务时自动开启所有硬盘的共享，因为加了“$”符号，所以看不到共享的托手图标，也称为隐藏共享。

10. shell

Shell 指的是一种命令执行环境，比如我们按下键盘上的【开始】+R 键会打开【运行】对话框，在【运行】文本框中输入 cmd 命令可以打开用于执行命令的命令提示符窗口，这个就是 Windows 的 Shell 执行环境。

通常使用远程溢出程序成功溢出远程电脑后，获取的用于执行系统命令的环境就是对方的 shell。

11. WebShell

WebShell 就是以 asp、php、jsp 或者 cgi 等网页文件形式存在的一种命令执行环境，也可以将其称做是一种网页后门。黑客在入侵了一个网站后，通常会将这些 asp 或 php 后门文件与网站服务器 web 目录下正常的网页文件混在一起，之后就可以使用浏览器来访问这些 asp 或者 php 后门，得到一个命令执行环境，以达到控制网站服务器的目的。可以上传下载文件，查看数据库，执行任意程序命令等。国内常用的 WebShell 有海阳 ASP 木马、Phpspy、c99shell 等。

12. 溢出

溢出确切地讲，应该是“缓冲区溢出”，简单的解释就是程序对接收的输入数据没有执行有效的检测而导致错误，后果可能是造成程序崩溃或者是执行攻击者的命令。溢出大致可以分为堆溢出和栈溢出两类。

13. 注入

随着 B/S 模式应用开发的发展，使用这种模式编写程序的程序员越来越多，但是由于程序员的水平参差不齐，相当大一部分应用程序存在安全隐患。用户可以提交一段数据库查询代码，根据程序返回的结果，获得某些他想知道的数据，这个就是所谓的 SQLinjection，即：SQL 注入。

14. 注入点

注入点是可以实行注入的地方，通常是一个访问数据库的连接。根据注入点数据库的运行帐号的权限的不同，用户所得到的权限也不同。

15. 内网

内网通俗地讲就是局域网，例如网吧、校园网、公司内部网等都属于此类。查看 IP 地址，IP 地址在以下三个范围之内的所有电脑都处于内网。

- 10.0.0.0—10.255.255.255
- 172.16.0.0—172.31.255.255
- 192.168.0.0— 192.168.255.255

16. 外网

外网是直接连入 Internet(互联网)，可以与互联网上的任意一台电脑互相访问，IP 地址不是内网 IP 地址。

17. 3389、4899 肉鸡

3389 是 Windows 终端服务(Terminal Services)所默认使用的端口号，该服务是微软为了方便网络管理员远程管理及维护服务器而推出的，网络管理员可以使用远程桌面连接到网络上任意一台开启了终端服务的计算机上，成功登陆后就会象操作自己的电脑一样来操作主机了。这和远程控制软件甚至是木马程序实

现的功能很相似，终端服务的连接非常稳定，而且任何杀毒软件都不会查杀，所以也深受黑客喜爱。黑客在入侵了一台主机后，通常都会想办法先添加一个属于自己的后门帐号，然后再开启对方的终端服务，这样，自己就随时可以使用终端服务来控制对方了，这样的主机，通常就会被叫做 3389 肉鸡。Radmin 是一款非常优秀的远程控制软件，4899 是 Radmin 默认端口号，因此经常被黑客当作木马来使用(正是这个原因，目前的杀毒软件也对 Radmin 查杀了)。因为 Radmin 的控制功能非常强大，传输速度也比大多数木马快，而且又不被杀毒软件所查杀，所用 Radmin 管理远程电脑时使用的是空口令或者是弱口令，黑客就可以使用一些软件扫描网络上存在 Radmin 空口令或者弱口令的主机，然后就可以登录上去远程控制，这样被控制的主机通常就被称作 4899 肉鸡。

18. 免杀

免杀是通过加壳、加密、修改特征码、加花指令等技术来修改程序，使其逃过杀毒软件的查杀。

19. 加壳

加壳是利用特殊的算法，将 EXE 可执行程序或者 DLL 动态链接库文件的编码进行改变(比如实现压缩、加密)，以达到缩小文件体积或者加密程序编码，甚至是躲过杀毒软件查杀的目的。目前较常用的壳有 UPX、ASPack、PePack、PECompact、UPack、免疫 007、木马彩衣等。

20. 花指令

花指令就是几句汇编指令，让汇编语句进行一些跳转，使得杀毒软件不能正常地判断病毒文件的构造。简单来说就是杀毒软件是从头到脚按顺序来查找病毒的。如果将病毒的头和脚颠倒位置，杀毒软件就找不到病毒了。

1.5.2 网络安全相关术语

下面介绍与网络安全有关的一些专业术语，帮助用户更好地了解黑客领域的知识。

1. 服务器/客户端

最简单的网络服务形式是将若干台电脑作为客户端，使用一台电脑当作服务器，每一个客户端都具有向服务器提出请求的能力，而后由服务器应答并完成请求的动作，最后服务器会将执行结果返回给客户端电脑。例如电子邮件服务器、网站服务器、聊天室服务器等都属于这种类型。另外还有一种连接方式，它不需要服务器的支持，而是直接将两个客户端电脑进行连接，也就是说每一台电脑都既是服务器、又是客户端，它们之间具有相同的功能，对等地完成连接和信息交换工作。例如 DCC 传输协议即属于此种类型。

客户端和服务器分别是各种协议中规定的请求申请电脑和应答电脑。作为一般的上网用户，都是操作着自己的电脑(客户端)，向网络服务器发出常规请求完成诸如浏览网页、收发电子邮件等动作的，而对于黑客来说则是通过自己的电脑(客户端)对其他电脑(有可能是客户端，也有可能是服务器)进行攻击，以达到入侵、破坏、窃取信息的目的。

2. 系统与系统环境

电脑要运行必须安装操作系统，这些操作系统各自独立运行，它们有自己的文件管理、内存管理、进程管理等机制，在网络上，这些不同的操作系统既可以作为服务器、也可以作为客户端被使用者操作，它们之间通过协议来完成信息的交换工作。

不同的操作系统配合不同的应用程序就构成了系统环境，例如 Linux 系统配合 Apache 软件可以将电脑构设成一台网站服务器，其他

使用客户端的电脑可以使用浏览器来获得网站服务器上供浏览者阅读的文本信息；再比如 Windows 2000 系统配合 Ftpd 软件可以将电脑构设成一台文件服务器，通过远程 ftp 登陆可以获得系统上的各种文件资源等。

3. 加密与解密

由于网络基础设计存在问题，允许所有上网者参与信息共享，因而对某些商业、个人隐私在网络上的传送，就会暴露在众目睽睽之下，信用卡、个人电子邮件等都可以通过监听或者截获的方式获取，此时就可以通过加密处理在网络上传送的信息。

网络上经常使用的是设置个人密码、使用 DES 加密锁，这两种加密方式分别可以完成用户登录系统、网站、电子邮件信箱和保护信息包的工作，而黑客所要进行的工作，就是通过漏洞、暴力猜测、加密算法反向应用等方式获得加密档案的明文。网络上的加密方法和需要验证密码的系统层出不穷，黑客也在寻找破解这些系统的种种办法。

1.6 高手解答

问与答

问：如何进行邮箱设置，从而有效地过滤垃圾邮件？

答：以网易 163 邮箱为例，首先登录邮箱，然后单击邮箱右侧的【设置】按钮，进行邮箱设置。此时显示了【常用设置】、【邮件收发设置】和【反垃圾设置】3 个选项区域。

单击【邮件收发设置】选项卡区域中的【来信分类】链接，打开该链接窗格，可以在【名称】文本框中输入新建的来信分类名称，在【收到邮件时】选项区域中可以设置发件人、收件人或邮件主题包含的关键字，然后可以选中【拒收】单选按钮，拒收包含关键字的邮件。

单击【反垃圾设置】选项区域中的【黑名单设置】链接，打开该链接窗格，可以输入黑名单联系人的详细地址，也可以输入邮箱后缀名，例如@example.com 或@troy.com，然后单击【添加到黑名单】按钮，即可将详细的联系人名单添加到黑名单中，将不再接收黑名单中的联系人发送的邮件。