内容提要

《黑客攻防三十六计》是“黑客道”系列图书中的“谋略技巧篇”，从初、中级安全技术爱好者的角度，以《三十六计》的计谋名称为引，以《三十六计》的谋略精髓为线，从三十六个方面详尽地讲解了目前主流的黑客入侵与对抗技术。在每一计中还介绍了一个相关的历史故事，以便读者们能够更加容易地理解这36条谋略，进而可以轻松地把这些计谋运用在复杂多变的安全攻防之中。

初、中级电脑用户可以将本手册作为入门的参考读物，资深的网络管理员也可以将本手册作为案头必备的安全技术手册进行查阅。

多媒体教学光盘运行说明

运行环境： Windows 98/Me/2000/XP/2003；

操作说明： 光盘放入光驱后会自动运行，也可以打开光盘目录，运行hacker36.exe文件即可；

光盘内容： 图书配套软件以及精彩黑客攻防视频教学（参见“多媒体教学光盘目录”页）。

警告：文中涉及到的黑客攻防相关内容，仅供读者学习之用，如用于非法用途，后果自负！

书　　名：黑客攻防三十六计
编　　著：庄礼杰　仲治国
执行编辑：李　勇　何　磊
封面设计：刘学敏
责任编辑：李　萍
监　　制：时均建
出版单位：山东电子音像出版社
地　　址：济南市胜利大街39号
邮政编码：250001
电　　话：(0531)82060055-7616
发　　行：山东电子音像出版社
经　　销：各地新华书店、报刊亭
CD生产：北京中联光碟有限公司
文本印刷：重庆联谊印务有限公司
开本规格：787mm × 1092mm　1/16　19印张　350千字
版 本 号：ISBN 7-89491-637-4
版　　次：2006年6月第1版　2006年6月第1次印刷
定　　价：28.00元(1CD+配套书)

目录

开战计篇

（多媒体光盘中收录了图书配套软件和黑客攻防精彩视频，请读者配合使用。）

目录

胜战计篇

谋

黑客道

并战计篇

并战计篇是处于劣势下运用的计谋，共有六计，分别为：偷梁换柱、指桑骂槐、假痴不癫、上屋抽梯、树上开花、反客为主。

上屋抽梯——端口过滤与禁止
偷梁换柱——恶意进程追踪与清除
指桑骂槐——危险 dll 文件揭秘
假痴不癫——共享资源攻防实战
树上开花——RSO 漏洞攻防实战
反客为主——DDoS 攻击与防范

第一计 上屋抽梯

端口过滤与禁止

“上屋抽梯”通常有两种解释：一种是断敌人后路，这个比较好理解，就是当敌人进了包围圈后，将敌人彻底消灭；另外一种是断自己后路，这个有些破釜沉舟的意思。历史上比较有名的典故就是三国时期的刘琦引诱诸葛亮“上屋”，“抽梯”求其指点出路的故事。总之，安放梯子，有很大学问，对性贪之敌，则以利诱之；对情骄之敌，则以示我方之弱以惑之；对莽撞无谋之敌，则设下埋伏以使其中计。总之，要根据情况，巧妙地安放梯子，致敌中计。

在本计的网络安全应用中，“上屋抽梯”用于彻底而有效地设置端口过滤和禁止，颇有些将网络防范中端口设置所有招数都使出的感觉。

一、什么是端口

首先，需要明白的一点是，我们这里所说的端口，不是计算机硬件的I/O端口，而是软件形式上的概念。在Windows的端口分配中，端口号可以分为三个范围：“已知端口”、“注册端口”以及“动态和/或专用端口”。

- “已知端口”是从 0 到 1023 的端口。
- “注册端口”是从 1024 到 49151 的端口。
- “动态和/或专用端口”是从 49152 到 65535 的端口。

“已知端口”由 IANA 分配，并且在大多数系统中只能由系统（或根）进程或有特权的用户所执行的程序使用。

什么是IANA？

Internet Assigned Numbers Authority，Internet号分配机构。负责对IP地址分配规划以及对TCP/UDP公共服务的端口定义。国际互联网代理成员管理局（IANA）是在国际互联网中使用的IP 地址、域名和许多其他参数的管理机构。IP地址、自治系统成员以及许多顶级和二级域名分配的日常职责由国际互联网注册中心（IR）和地区注册中心承担。

“注册端口”由 IANA 列出，并且在大多数系统上可以由普通用户进程或普通用户所执行的程序使用。

IANA 会注册这些端口的使用情况，从而向社区提供方便。为了尽可能利用这些端口，UDP 使用了同样的端口分配。"注册端口"的范围为1024~49151。

由此我们可以知道，在系统间发送数据包都是通过系统的各种端口进行的，也就是说，系统拥有很多端口。

二、端口的安全设置

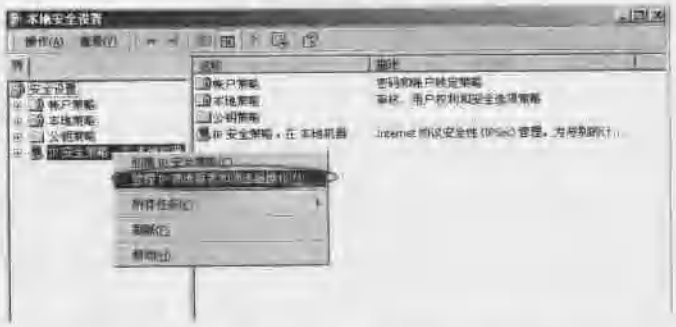
现在让我们来以Windows 2000 Server 系统为平台，以IPsec阻止对135端口的访问为例，进行端口的访问设置。

1. 创建 IP 筛选器和筛选器操作

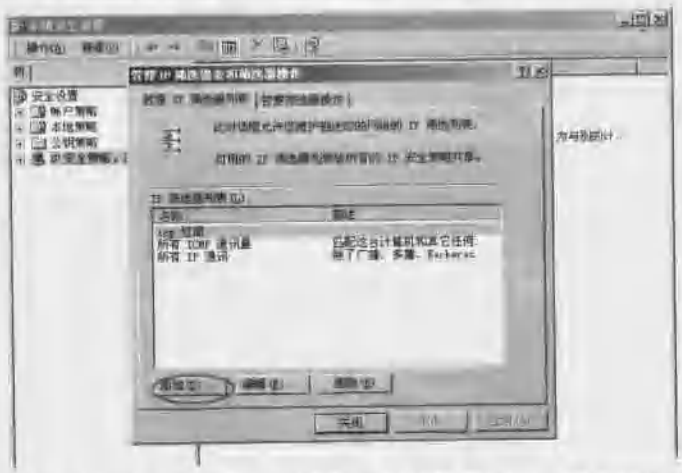
（1）依次点击"开始→程序→管理工具→本地安全策略"；

（2）右击"IP 安全策略，在本地机器"，选择"管理 IP 筛选器表和筛选器操作"，启动管理 IP 筛选器表和筛选器操作对话框；

（3）这里要先创建一个 IP 筛选器和相关操作才能够建立一个相应的 IPsec 安全策略；



（4）在"管理 IP 筛选器表"中，按"添加"按钮建立新的 IP 筛选器；

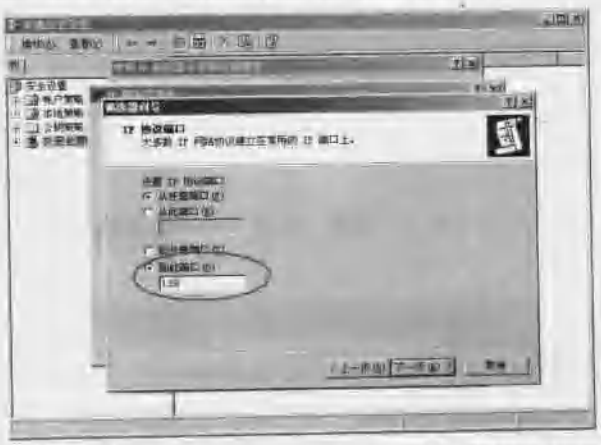


（5）在 IP 筛选器列表对话框内，填上"135"，描述随便填写，单击右侧的"添加..."按钮；

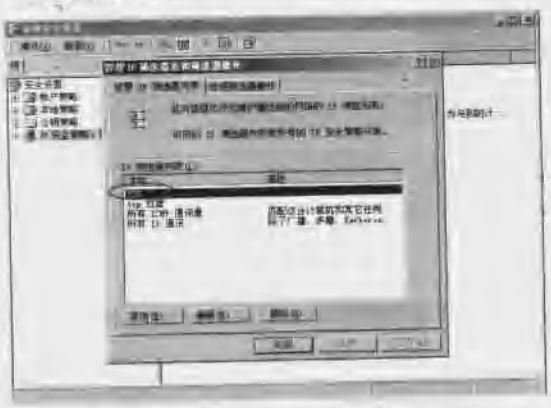
（6）跳过向导欢迎对话框后单击“下一步”按钮，在IP通信源页面中，源地址选“任何IP地址”，因为我们要阻止传入的访问。设置完毕点击“下一步”按钮继续；

（7）在IP通信目标页面中目标地址选“我的IP地址”，在下一步出现的IP协议类型页面选择“TCP”并点击“下一步”按钮；

（8）在IP协议端口页面，选择“到此端口”并设置为“135”，其他不变；



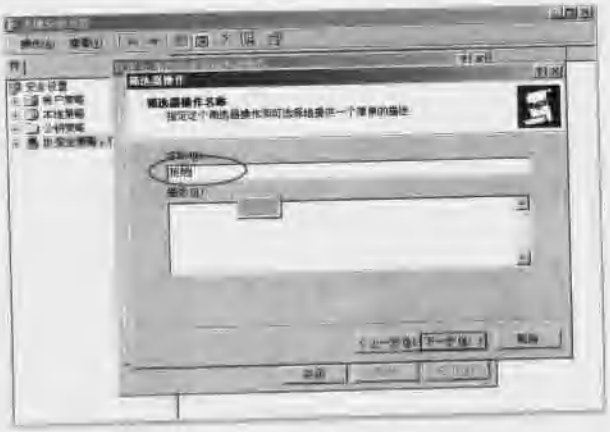
（9）余下的步骤请选择默认状态，当向导设置完成并关闭IP筛选器列表对话框后，可以发现135IP筛选器出现在IP筛选器列表中；



（10）现在点击切换到“管理筛选器操作”选项卡设置界面，创建一个拒绝操作；

（11）单击“添加”按钮，启动“筛选器操作向导”，并跳过欢迎页面；

（12）在筛选器操作名称页面填写名称，这儿填写“拒绝”。在筛选器操作常规选项页面将行为设置为“阻止”；

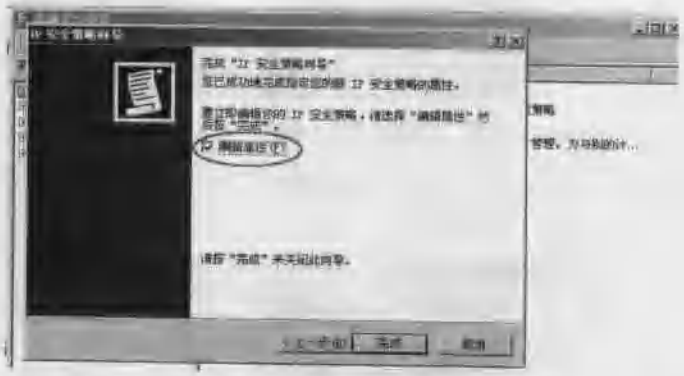


(13) 完成设置后，关闭“管理IP筛选器表和筛选器操作”对话框；

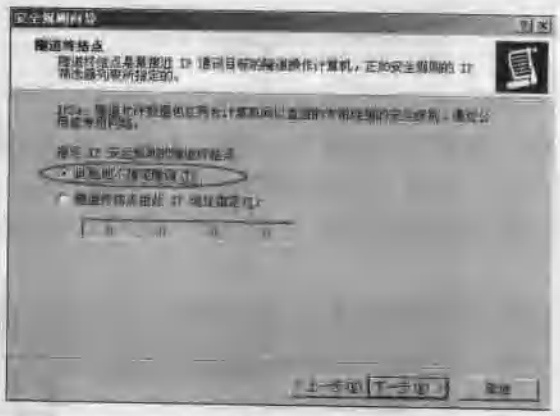
(14) 在IP安全策略名称页面填写合适的IP安全策略名称，这儿我们可以填写“拒绝对135端口的访问”，描述可以随便填写，在安全通信要求页面不选择“激活默认响应规则”，最后完成设置即可。

2. 创建IP安全策略

右击“IP安全策略，在本地机器”，选择“创建IP安全策略”，启动IP安全策略向导，跳过欢迎页面。

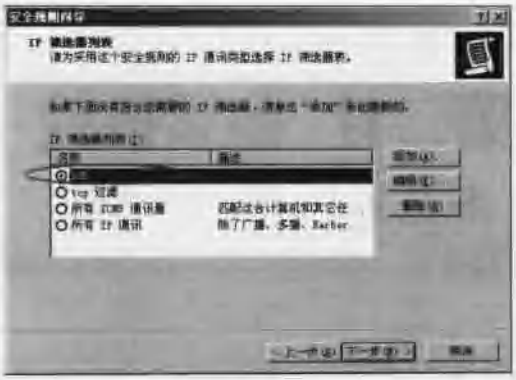


在“拒绝对135端口的访问属性”对话框中进行设置，首先设置规则：单击下面的“添加...”按钮，启动安全规则向导并跳过其欢迎页面，在下一步的隧道终结点页面选择默认的“此规则不指定隧道”。



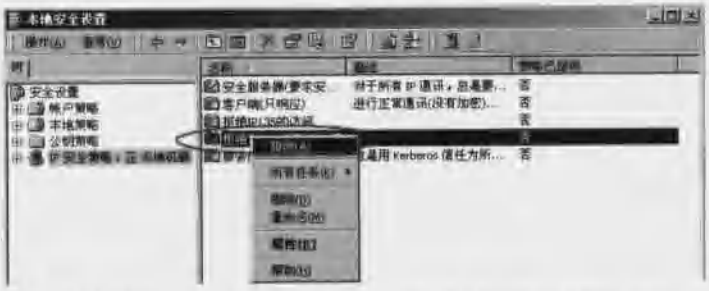
接着在下一步的网络类型页面，选择默认的“所有网络连接”。在身份验证方法页面，选择默认的“Windows 2000默认值(Kerberos V5 协议)”。在IP筛选器列表页面选择我们刚才建立的“135”筛选器。

在筛选器操作页面，选择我们刚才建立的“拒绝”操作。稍后按照提示将可完成设置并关闭“拒绝对135端口的访问属性”对话框。



3. 指派和应用 IPsec 安全策略

默认情况下，任何IPsec安全策略都未被指派，首先我们要对新建立的安全策略进行指派。在本地安全策略MMC中，右击我们刚刚建立的“拒绝对135端口的访问属性”安全策略，选择“指派”。



接着，需要使用“secedit /refreshpolicy machine_policy”命令立即刷新组策略。刷新完成后，安全设置就结束了。

第二计 偷梁换柱

恶意进程追踪与清除

“偷梁换柱”指用偷换的办法，暗中改换事物的本质和内容，以达蒙混欺骗的目的。“偷天换日”、“偷龙转凤”、“调包计”等都是同样的意思。此计归于“并战计”中，本意是乘友军作战不利，借机兼并他的主力为己方所用。此计中包含尔虞我诈、乘机控制别人的谋略，所以颇有些小人的意味在内。我国名著《红楼梦》第九十七回中即有：“偏偏凤姐想出一条偷梁换柱之计”，……只跟宝玉说娶林姑娘，待入了洞房，才知道娶回来的竟是宝姑娘。

在本计的网络安全应用中，“偷梁换柱”是指一些恶意程序在进驻本机后，总是会在进程列表中添加自己的进程，将正常的系统进程更改为自己的进程。这种可恶的行径该如何查究？在本计中，就将与读者们探讨这个问题。

一、进程概述

在系统中如果需要打开一个软件，系统便会在后台加载相应的进程，进程是系统或应用程序的一次动态执行，我们可以简单地理解为它是操作系统当前运行的执行程序。在系统当前运行的执行程序里包括系统管理计算机个体和完成各种操作所必需的程序以及用户开启、执行的额外程序，当然也包括用户不知道的，自动运行的非法程序等等。进程控制着程序的各个方面，起到非常重要的作用，正是它具有这种特性，所以它也经常受到“侵犯”，比如有些病毒就伪装成为系统进程搞破坏。

说到进程就不能不说说线程，Windows 操作系统能同时运行几个程序，独立运行的程序又称之为进程。对于同一个程序，又可以分成若干个独立的执行流，我们称之为线程，线程提供了多任务处理的能力。用进程和线程的观点来研究软件是当今普遍采用的方法，进程和线程概念的出现，对提高软件的并行性有着重要的意义。现在的应用软件无一不是多线程多任务处理，包括木马和病毒亦是如此。

1. 理解线程

进程是应用程序的执行实例，每个进程是由私有的虚拟地址空间、代码、数据和其他系统资源组成。进程在运行时创建的资源随着进程的终止而死亡。线程的基本思想很简单，它是一个独立的执行流，是进程内部的一个独立的执行单元，相当于一个子程序。单独一个执行程序运行时，默认运行包含一个主线程，主线程以函数地址的形式（如main或WinMain函数）提供程序的启动点。当主线程终止时，进程也随之终止，但根据需要，应用程序又可以分解成许多

独立执行地线程，每个线程并行的运行在同一进程中。

一个进程中的所有线程都在该进程的虚拟地址空间中，使用该进程的全局变量和系统资源。操作系统给每个线程分配不同的CPU时间片，在某一个时刻，CPU只执行一个时间片内的线程，多个时间片中的相应线程在CPU内轮流执行，由于每个时间片时间很短，所以对用户来说，仿佛各个线程在计算机中是并行处理的。操作系统根据线程的优先级来安排CPU的时间，优先级高的线程优先运行，优先级低的线程则继续等待。

线程被分为两种：用户界面线程和工作线程（又称为后台线程）。用户界面线程通常用来处理用户的输入并响应各种事件和消息，其实，应用程序的主执行线程CWinAPP对象就是一个用户界面线程，当应用程序启动时自动创建和启动，同样它的终止也意味着该程序的结束和进程的终止。工作线程用来执行程序的后台处理任务，比如计算、调度、对串口的读写操作等，它和用户界面线程的区别是它不用从CwinThread类派生来创建，对它来说最重要的是如何实现工作线程任务的运行控制函数。工作线程和用户界面线程启动时要调用同一个函数的不同版本；最后需要读者明白的是，一个进程中的所有线程共享它们父进程的变量（每个进程还可以启动几个线程，比如每下载一个文件可以单独开一个线程），但同时每个线程可以拥有自己的变量。

二、正常的进程列表

虽然，从安全的角度上我们应该抱着“怀疑一切”的态度进行系统管理，但是这种怀疑也是应该建立在一定的基础上的。以管理系统进程为例，我们不能看到一个进程就怀疑一下，那我们自己就要累死了。正确的方法是多看一些如下表所示的有关于正常进程的名称列表，加深自己对进程的印象，熟悉哪些进程可能被病毒或木马改头换面，熟悉那些进程不会出现这种情况。这样一来，管理进程的操作就会轻松很多了。

进程名称	系统进程	后台程序	描述
alg.exe	是	是	用于处理Windows网络连接共享和网络连接防火墙
ccmexec.exe	是	是	SMS操作系统服务，对系统的正常运行非常重要
clisvcl.exe	是	是	该进程调用SMSS进程检测计算机上的软件
Csrss.exe	是	是	该进程管理Windows图形相关任务，容易被病毒感染
dfssvc.exe	是	是	服务器版Windows的DFS分布式文件系统服务
dotnetfx.exe	是	否	升级到.net技术的一个进程，不是纯粹的系统进程
fast.exe	是	是	用于用户账号的快速切换，不是纯粹的系统进程
iexplore.exe	是	否	Internet Explorer浏览器进程
loadwc.exe	是	是	Internet Explorer浏览器的一部分
lsass.exe	是	是	系统进程，用于本地安全和登录策略。容易被感染
mmc.exe	是	否	Windows管理控制程序，显示管理插件的控制面板
msconfig.exe	是	是	用于帮助编辑和管理配置文件，如Win.ini等启动项
msiexec.exe	是	否	Windows Installer的一部分，对系统正常运行非常重要

mstinit.exe	是	是	用于管理杀毒软件和磁盘碎片整理
ntoskrnl.exe	是	是	在你计算机反复启动的情况下出现，可能被病毒感染
pstores.exe	是	是	用于应用程序储存，如IE储存机密数据
regsvc.exe	是	是	用于远程计算机访问本地注册表
rpcss.exe	是	是	用于本地计算机的远程程序调用服务
rundll32.exe	是	是	用于在内存中运行dll文件，容易被病毒感染
savedump.exe	是	是	用于NT内存储存，该进程会写内存内容到页面文件
services.exe	是	是	用于管理启动和停止服务
spool32.exe	是	是	Windows打印任务控制程序，用以打印机就绪
srvany.exe	是	是	用于将一个程序注册为一个服务
System Idle Process	否	是	不是一个进程，用于显示CPU可用资源百分比情况
taskmgr.exe	是	是	显示系统中正在运行的进程，用Ctrl+Alt+Del打开
tlntsvr.exe	是	否	属于微软Telnet程序的一部分
winmgmt.exe	是	是	用于系统管理员创建Windows管理脚本
wmiexe.exe	是	是	用于让用户访问基本系统信息
wpabaln.exe	是	是	微软Windows操作系统监听精灵程序
wuauboot.exe	是	是	用于管理Windows自动更新
wucrtupd.exe	是	是	用于检测Windows的更新
actmovie.exe	是	是	用于支持显示卡运行一些屏幕保护和微软程序
ASPNET_WP.exe	是	是	涉及Microsoft asp.net技术的程序运行所必须的进程
cidaemon.exe	是	是	是一个索引服务，为了让你更加快速的查找文件
cmd.exe	是	否	微软Windows系统的命令行程序
ctfmon.exe	是	是	用于选择文字输入程序和Office语言条
dllhost.exe	是	是	用于管理dll应用
dumprep.exe	是	是	记录出现错误的程序信息并发送相关错误信息到微软
grpconv.exe	是	是	用于转换Windows 3.1的文件夹格式至高版本Windows
scanregw.exe	是	是	用于检测Windows注册表并会用正确的覆盖错误的
smss.exe	是	是	管理子系统和操作系统的对话，容易被感染
spoolss.exe	是	是	用于将打印机任务发送到本地打印机
svchost.exe	是	是	用于执行dll文件，容易被感染
systray.exe	是	是	用于显示信息，例如日期和时间
taskmon.exe	是	是	用于监视硬件资源对计算机的维护任务
userinit.exe	是	是	关键进程，用于管理不同的启动顺序
winoa386.mod	是	否	用于控制32位的Windows环境下提供DOS命令行
wmiprvse.exe	是	是	用于通过WinMgmt.exe程序处理WMI操作

wscntfy.exe	是	否	Windows 安全相关策略的一部分
wuauclt.exe	是	是	Windows 自动升级管理程序，会不断在线检测
agentsvr.exe	是	是	是一个 ActiveX 插件，用于多媒体程序
btwdins.exe	是	是	是为了微软 Windows 操作系统支持蓝牙技术的进程
cisvc.exe	是	是	用于监测 CIDAEMON.exe 内存使用状态
ddhelp.exe	是	否	DirectX 的一部分，用于对 Windows 3D 显示卡加速
dos4gw.exe	是	否	DOS 操作系统在 32 位操作系统上的扩展壳
explorer.exe	是	否	用于管理 shell、开始菜单、任务栏、桌面和文件管理
hidserv.exe	是	是	用于支持 Windows 操作系统的 USB 多媒体设备
inetinfo.exe	是	是	用于支持微软 Windows IIS 网络服务
launch32.exe	是	否	储存管理服务的远程部署与安装程序
logonui.exe	是	是	用于显示微软 Windows XP 系统用户切换界面
mapisp32.exe	是	是	用于调用 MAPI 消息的程序
mprexe.exe	是	是	用于计算机使用多个网络协议和网卡与路由的连接
msgsrv32.exe	是	是	是一个 32 位的消息服务
mstask.exe	是	是	Windows 计划任务程序
netdde.exe	是	是	微软 Windows 的网络动态数据 Exchange 服务
pchschd.exe	是	是	用于监视分析系统硬件使用
rdpclip.exe	是	否	用于从服务器到本地拷贝粘贴文件
rnaapp.exe	是	是	Win98/Me 操作系统的进程，用于进行拨号网络连接
sapisvr.exe	是	否	用于语音识别支持
scardsvr.exe	是	是	用于认证本地系统的简单型的安全卡
snmp.exe	是	是	用于局域网 LAN 和局域网基础配置
spoolsv.exe	是	是	用于将 Windows 打印机任务发送给本地打印机
tcpsvcs.exe	是	是	用于计算机使用专用的 TCP/IP 网络服务
winlogon.exe	是	是	用于处理你系统的登录和登录过程
wowexec.exe	是	否	用于支持 16 位进程
wuaclt.exe	是	是	用于系统自动检测你计算机上软件更新

三、查看、关闭和重建进程

对于一些安全高手来说，查看系统进程有无异常，可以快速判断出系统是否存在安全隐患。那么，安全高手们都是怎样查看系统进程的呢？对于该关闭的进程如何禁用？禁用后如何新建此进程？在本小节中将以 Explorer.exe 进程为例，谈谈如何查看、关闭和重建进程的方法。

以 Windows XP 为例，在桌面环境中按下组合键“Ctrl+Shift+Esc”键打开“Windows 任务管理器”窗口后，单击切换到“进程”选项卡后，从中就可以看到进程列表了。

以关闭Explorer.exe为例，只需选中此进程并单击右下角的“结束进程”即可关闭此进程了。

在关闭此进程后，桌面将消失并只剩一个Windows任务管理器窗口存在。因为桌面的消失，所以屏幕中的鼠标操作将不被响应。

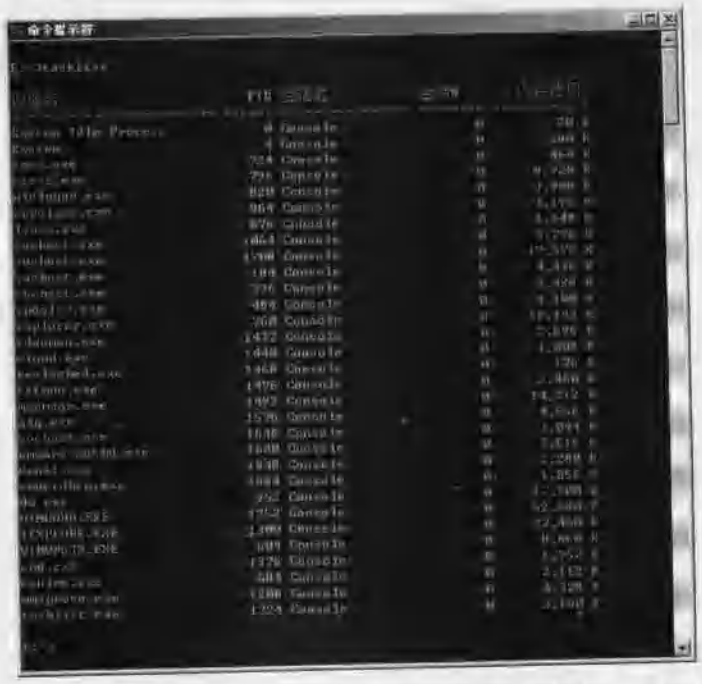
那么，如何新建此进程呢？因为Windows任务管理器窗口还是存在的，此窗口本身支持鼠标操作，所以可以按如下方法执行新建Explorer.exe进程的操作：

（1）在“Windows任务管理器”窗口中，依次单击“文件→新建任务（运行…）”菜单。

（2）在打开的“创建新任务”对话框中，输入“Explorer.exe”进程名称并单击“确定”按钮继续。

（3）稍后，桌面环境中恢复，桌面上的图标将显示出来，鼠标的操作也将响应。

这就是一次标准的进程查看、关闭和重建的过程。接着，再来看看DOS下如何查看进程，这个方法学会了对于无法进入桌面环境时非常有用。方法很简单：在弹出的"命令提示符"窗口中输入"tasklist"命令并按Enter键，在随即得到的如下图所示反馈信息中，就可以看到本机的所有进程了。



从上图中可以看出，本机的进程显示结果由五部分组成：图像名（进程名）、PID、会话名、会话#、内存使用。此时，如果要关闭某个进程，可以使用如下方法：

如要终止本机的"QQ.exe"进程，就应该首先使用Tasklist命令查找它的PID。通过上图中可以看到系统显示本机"QQ.exe"进程的PID值为"952"，此时就可以运行：

Taskkill /pid 952

从而将QQ.exe进程终止。

四、隐藏进程和远程进程

除了我们可以看得见的进程外，还有一些隐藏进程和远程进程是需要我们使用不同方法进行管理的。

1. 隐藏进程

查看隐藏进程有很多方法，我们推荐大家搜索下载"隐藏进程管理工具"来完成对隐藏进程的管理。

（1）下载完成后需要解压；

（2）运行其中的"ECO-PS.exe"文件，在打开的窗口中可以看到系统中所有的进程列表。

（3）在每个进程后面，可以看到此程序的线程有多少个，它主要关联的程序名和路径是什么，它是否为可疑程序等等；

（4）对于提示为“可疑”的进程，在查看具体的文件路径后，当确认为是恶意程序时，可以选中此进程并单击鼠标右键，在弹出的快捷菜单中选择“强行结束进程”；

（5）将此程序与Windows任务管理器中的进程列表对比时，明显可以感觉到程序中的进程数要多得多。