

电脑应用
疑难解析与技巧系列

黑客攻防

疑难解析与技巧800例

华师傅资讯 编著

讲解黑客攻防原理让黑客无处遁形

识破黑客的各种攻击伎俩

用事实说话

真实地重现黑客攻防实战场面

知己知彼百战不殆

保护网络安全保护个人隐私

放心地享受网络生活

附赠光盘以多媒体教程来帮助学习

附赠光盘中披露黑客攻防常用武器

附赠光盘中收录了其他的实用案例

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

电脑应用
疑难解析与技巧系列

黑客攻防

疑难解析与技巧800例

华师傅资讯 编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 提 要

本书是指导初学者快速掌握黑客攻防操作和应用的入门书籍。书中详细地介绍了初学者必须掌握的基本知识、使用方法和操作步骤,并对初学者在学习过程中经常遇到的问题进行了专家级的指导,以免初学者在起步的过程中走弯路。

本书内容丰富、全面,图文并茂,深入浅出,以图解的方式对每一个入侵步骤都进行了详细的分析,以推测入侵者的入侵目的;对入侵过程中常见的问题进行了必要的说明与解答;并对一些常见的入侵手段进行了比较与分析,以方便读者了解入侵者常用的方式、方法,保障网络安全。本书适合于网络技术爱好者、网络系统管理员阅读,也可作为相关专业学生的参考书。

图书在版编目(CIP)数据

黑客攻防疑难解析与技巧 800 例/华师傅资讯编著.

北京:中国铁道出版社,2008.6

(电脑应用疑难解析与技巧)

ISBN 978-7-113-08959-7

I. 黑… II. 华… III. 计算机网络—安全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字(2008)第 079943 号

书 名: 黑客攻防疑难解析与技巧 800 例

作 者: 华师傅资讯 编著

策划编辑: 严晓舟 郑 双

责任编辑: 苏 茜

编辑部电话: (010) 63583215

封面设计: 付 巍

封面制作: 白 雪

责任校对: 高 爽

责任印制: 李 佳

出版发行: 中国铁道出版社(北京市宣武区右安门西街 8 号 邮政编码: 100054)

印 刷: 北京新魏印刷厂

版 次: 2008 年 9 月第 1 版

2008 年 9 月第 1 次印刷

开 本: 787mm×1092mm 1/16 印张: 16.5 字数: 369 千

印 数: 5 000 册

书 号: ISBN 978-7-113-08959-7/TP·2915

定 价: 29.00 元(附赠光盘)

版权所有 侵权必究

凡购买铁道版的图书,如有缺页、倒页、脱页者,请与本社计算机图书批销部调换。

前言

随着计算机网络技术的发展,黑客与网络安全逐渐成为人们关注的热点。怎样认识黑客与防范黑客,保证系统与网络的安全,导致了黑客与反黑客的较量。黑客,或因为“欲望”、“好奇”,或其他原因,经常神出鬼没于黑暗和光明交接的缝隙,利用各种千奇百怪的入侵软件,自由出入于大大小小的公私领域,在用户疏于防范的时候突然现身,叫人防不胜防!如何在网络中生存,成为每个网络使用者必备的基本认识。

在当今这个科技发达的时代,网络在人们的工作、生活和学习中起着重要作用,但目前大多数用户的网络安全知识还很匮乏,在遇到别有用心者的入侵时不知道该如何应对。本书的主要目的就是让读者在尽可能短的时间内,了解黑客入侵原理、常用工具以及攻击方式,并在熟悉基本网络安全知识的前提下,掌握基本的反黑知识、工具和防范技巧,从而揭开黑客的神秘面纱,让广大用户对网络安全高度重视起来,从而采取相关的方法来制定相应的自救措施,“害人之心不要有,防人之心不可无”,也是这个道理。

本书从“攻”、“防”两个不同的角度,通过现实中的入侵实例,并结合作者的心得体会,图文并茂地再现了网络入侵与防御的全过程。本书从内容和层次上可以分为13章:第1章介绍黑客的入侵命令,培养用户最基本的黑客攻防技能;第2~3章讲解针对Windows 98/Me/NT/2000/XP操作系统的黑客攻击方式和防范技巧;第4章讲解木马的工作原理以及黑客如何利用木马入侵计算机,培养用户封杀木马的技能;第5章针对国人最常用的即时聊天工具——QQ软件,讲解黑客如何盗取号码、QQ尾巴病毒的发作原理、破解本地加密聊天记录等,分析黑客入侵QQ的原理并提出解决办法;第6~7章讲解黑客如何入侵系统、邮件、网站及网吧,从而增强用户的防范意识;第8~10章讲解如何破解系统、邮箱、程序、文档的密码,从而使用工具进行反入侵;第11~12章讲解综合防范技能,封堵黑客可能利用的系统漏洞和端口;第13章讲解系统被黑客破坏的情况和如何快速恢复注册表和系统。

本书附带一张精心开发的专业级多媒体教学光盘。它采用了语音讲解、情景式教学、详细的图文对照和真实的情景演示等方式,紧密结合书中的内容对各个知识点进行了深入的讲解,以便于读者快速地对书中的知识点进行消化。同时,本书所涉及的软件全部保存在光盘中,利于读者获取和使用,由于篇幅的缘故,更多的案例不能收录到本书正文中,为此,我们将更多的相关内容和案例附在光盘中,以便于读者随时查阅。

本书由华师傅资讯编著,张燕、吴万军、王利、水淼、张亮、周鹏、李立明、束庆丰、杨杰、朱静、年夫兰、唐国祥、李平、王春燕、尹瑜、刘琢、黄海、冯玉川、吴燕群、潘天、胡平、汪玲、张德友、朱小怀、丁霞共同精心编写而成,由于编者水平有限,书中难免有疏漏和不妥之处,希望广大读者批评指正,联系邮箱:fl05888339@163.com。

本书从保障计算机系统和数据的安全实际需要出发,分析黑客常用的攻击方式和手段,其目的是让更多的读者认识和了解黑客,从而防范黑客,而不是让读者利用黑客技术和手段去攻击别人的计算机系统。因此,最后我们特别声明:利用本书所传授的技术或利用本书光盘中的黑客软件所引起的一切法律和社会后果,由具体行为人负责。

编者

2008年5月

目 录

第 1 章 剖析黑客入侵命令 1

1-1 ping 命令有哪些功能 2

1-2 ping 命令返回信息的含义是什么 3

1-3 如何判断目标主机的操作系统
类型 3

1-4 怎样测试网卡是否工作正常 4

1-5 如何测试网络协议是否工作正常 5

1-6 如何测试网络连接情况 5

1-7 如何测试网关 6

1-8 怎样比较测试数据包的大小对
反应时间的影响 7

1-9 如何长时间测试网络连接 7

1-10 如何获取网站服务器 IP 地址 7

1-11 如何自定义数据包检测服务器的
返回时间 8

1-12 如何自定义数据包大小检测
服务器返回时间 8

1-13 如何测试 host 文件 8

1-14 黑客如何破坏网络通信 9

1-15 ipconfig 命令有什么功能 9

1-16 如何显示本机 IP 地址 9

1-17 如何显示 TCP/IP 配置详细信息 9

1-18 如何释放 IP 地址 10

1-19 如何更新动态 IP 地址 10

1-20 什么是网卡 MAC 地址 10

1-21 如何实现 IP 和 MAC 绑定 11

1-22 在局域网如何隐身 11

1-23 如何搞定系统服务 12

1-24 如何实现 IPC\$ 连接 13

1-25 如何管理用户账户 14

1-26 如何管理网络 15

1-27 如何管理共享资源 17

1-28 如何查看网络连接 17

1-29 如何显示系统进程信息 18

1-30 如何终止系统进程 19

1-31 如何获取 NetBIOS 信息 19

1-32 at 命令为何不能使用 20

1-33 at 命令有哪些高级用法 21

1-34 如何远程复制文件 22

1-35 如何判别系统类型 22

1-36 如何远程管理信箱 23

1-37 如何配置 Telnet 23

1-38 如何实现上传下载 24

1-39 如何跟踪路由数据包 24

1-40 doskey 命令有哪些特殊功能 25

1-41 黑客如何使用 echo 命令黑网页 25

1-42 如何一次执行多个命令 25

1-43 如何快速修改文件扩展名关联 26

1-44 如何更改网络配置 26

1-45 如何实现网络配置备份和还原 27

1-46 如何快速编辑注册表 28

1-47 如何诊断 DNS 故障 29

1-48 如何关闭计算机 29

第 2 章 Windows 9x 攻防实战 31

2-1 黑客如何入侵 Windows 9x 32

2-2 如何解决 NetBIOS 隐患 32

2-3 如何设置共享资源密码 33

2-4 如何使用设备名称解析漏洞
进行攻击 34

2-5 怎样防止蓝屏攻击 34

2-6 如何利用扩展名存在的缓冲
溢出漏洞 35

2-7 怎么利用漏洞绕过登录验证 36

2-8 UPnP 漏洞为什么导致系统遭受
多种攻击 37

2-9 什么是 Cookies 漏洞 37

2-10	如何绕过屏保密码进入系统.....	38	3-16	如何实战 RPC 漏洞.....	60
2-11	怎样利用 IP 冲突绕过屏保密码.....	39	3-17	如何拒绝 RPC 攻击.....	61
2-12	黑客如何破解.pwl 文件.....	39	3-18	如何进行 DDoS 攻击.....	62
2-13	如何防止匿名登录.....	40	3-19	快速修改远程计算机注册表.....	62
2-14	怎样让 Windows 98 拥有两个 IP 地址.....	41	3-20	如何禁止枚举账号防攻击.....	63
2-15	如何限制用户使用指定程序.....	41	3-21	如何让黑客一无所获.....	64
2-16	如何在注册表中查找密码.....	41	3-22	如何安全指派用户权利.....	64
2-17	如何用“系统策略编辑器” 消除共享隐患.....	42	3-23	如何用“组策略”控制用户 访问共享.....	65
2-18	如何打造 Windows 9x 口令 审核策略.....	43	3-24	黑客如何实施远程关机.....	66
2-19	怎样限制“控制面板”.....	44	3-25	如何禁用 ping 命令.....	66
2-20	如何隐藏系统资源.....	44	3-26	如何进行 EFS 加密.....	67
2-21	如何备份注册表.....	45	3-27	如何备份密钥.....	68
2-22	如何预防网页恶意代码.....	45	第 4 章 牧马记.....	69	
2-23	如何屏蔽恶意网站.....	46	4-1	木马类型有哪些.....	70
第 3 章 Windows NT/2000/XP			4-2	系统为什么会中木马.....	70
攻防实战.....	49		4-3	木马会通过哪些自运行程序 加载.....	70
3-1	黑客如何实施 139 入侵.....	50	4-4	木马藏匿于注册表中何处.....	71
3-2	如何防范 139 入侵.....	50	4-5	黑客如何使用“冰河”入侵 计算机.....	72
3-3	黑客如何开启 3389 端口.....	51	4-6	如何使用“冰河”陷阱.....	73
3-4	如何实施 IPC 入侵.....	51	4-7	黑客如何使用“灰鸽子”进行 入侵.....	73
3-5	黑客如何通过软件实施 IPC 入侵.....	52	4-8	黑客如何使用“黑洞”进行 入侵.....	74
3-6	黑客如何通过工具实施 IPC 入侵.....	53	4-9	黑客如何使用“蓝色火焰” 入侵.....	75
3-7	怎样防范 IPC 入侵.....	54	4-10	黑客如何使用后门.....	76
3-8	黑客如何让系统崩溃.....	55	4-11	黑客如何使用“木牛”入侵.....	76
3-9	黑客如何利用 Unicode 漏洞入侵.....	55	4-12	黑客如何使用“隐型木牛”.....	77
3-10	如何预防 Unicode 漏洞入侵.....	56	4-13	黑客如何使用 WNC 入侵.....	78
3-11	黑客如何利用 IDA 和 IDQ 扩展溢出漏洞入侵.....	57	4-14	rmtSvc 如何运行.....	79
3-12	printer 溢出漏洞攻防战.....	57	4-15	黑客如何实现脚本入侵.....	80
3-13	黑客如何通过 FrontPage 服务器 扩展漏洞黑网页.....	58	4-16	黑客使用脚本入侵有哪些技巧.....	81
3-14	黑客如何通过 WebDAV 漏洞 入侵网页服务器.....	59	4-17	黑客如何使用 Falling Star 入侵.....	82
3-15	如何堵住 ICMP 漏洞.....	59	4-18	黑客怎样实现 Falling Star 反弹连接.....	83
			4-19	如何进行 DMRC 的优化配置.....	83

4-20	DMRC 有哪些操纵技巧.....	84	5-11	如何加密聊天记录.....	102
4-21	黑客如何使用 20CN 远程控制 计算机.....	85	5-12	黑客怎样识破 QQ 隐身好友	102
4-22	黑客如何利用 winShadow 控制计算机.....	86	5-13	黑客如何破解 QQ 本地密码	103
4-23	如何实现木马的查、堵、杀.....	87	5-14	黑客如何实现在线盗取 QQ 密码.....	104
4-24	阻断恶意病毒攻击有哪 三大要素.....	88	5-15	黑客如何应用“QQ 机器人” 在线破解.....	104
4-25	如何使用“木马克星”防护 计算机.....	88	5-16	黑客如何使用“QQ 砸门机”	105
4-26	如何使用“绿鹰 PC 万能精灵” 防木马.....	89	5-17	如何清除“QQ 黑暗精灵”	105
4-27	如何使用 Trojan Remover 清除 木马.....	90	5-18	为什么公司的 QQ 被封闭.....	106
4-28	黑客如何使用 WinRAR 捆绑 木马.....	90	5-19	如何使用 Socks Online 冲破 代理封锁.....	107
4-29	黑客如何使用 IExpress 捆绑 木马.....	91	5-20	如何使用 CCProxy 冲破代理的 封锁.....	108
4-30	黑客如何制作网页木马.....	93	5-21	如何防范最新 GOP 攻击	109
4-31	黑客如何利用 HTA 漏洞制作 网页木马.....	93	5-22	如何斩断“QQ 尾巴”	110
4-32	黑客如何使用 Vbs 蠕虫制造机.....	93	5-23	抵御消息病毒的手段有哪些	110
第 5 章	QQ 主题乐园	95	5-24	QQ 安全的防范措施包括哪些	111
5-1	黑客如何获取好友的 IP 地址	96	5-25	如何防范木马记录键盘信息	112
5-2	黑客如何通过防火墙获取 好友的 IP 地址	96	5-26	黑客经常使用的攻击手段 有哪些.....	112
5-3	黑客如何使用专用工具查询 好友的 IP	97	5-27	如何隐藏 QQ.....	112
5-4	黑客如何从 QQ 通信端口获取 信息.....	97	5-28	维护 QQ 安全的工具有哪些	113
5-5	黑客如何利用 QQ 获取好友的 主机信息.....	98	第 6 章	炸弹里的秘密.....	115
5-6	黑客如何发起 QQ 消息攻击.....	99	6-1	什么是网络炸弹	116
5-7	黑客如何盗取 QQ 密码.....	99	6-2	什么是 IP 炸弹.....	116
5-8	黑客如何使用工具窃取密码.....	100	6-3	黑客如何使用 IP Hacker	116
5-9	黑客如何获取好友的 QQ 名单及 聊天记录.....	101	6-4	黑客如何使用命令重启远程 计算机.....	117
5-10	黑客如何破解本地 QQ 好友 名单.....	101	6-5	反击 IP 炸弹的工具有哪些.....	118
			6-6	如何在线反击 IP 炸弹.....	118
			6-7	为什么会出现信使骚扰	119
			6-8	什么是电子邮件炸弹	120
			6-9	黑客使用什么工具轰炸 电子邮件.....	120
			6-10	黑客如何使用“E-mail 杀手”	120
			6-11	黑客如何实现邮件的批量 发送.....	121

6-12	黑客如何使用“KaBoom!” 发送邮件.....	121
6-13	黑客如何通过网页制造邮件 炸弹.....	122
6-14	如何防止邮件连环炸弹.....	123
6-15	如何使用“亿虎 E-mail 群发大师”.....	123
6-16	清理垃圾邮件的工具包括 哪些.....	124
6-17	如何防范邮件炸弹.....	125
6-18	为什么浏览网页会中网页 炸弹.....	126
6-19	为什么 IE 不断闪烁, 然后 死机.....	126
6-20	为什么网页总是抖动.....	127
6-21	黑客如何制作网页恶作剧.....	127
6-22	为什么移动鼠标会中网页 炸弹.....	128
6-23	为什么浏览网页后注册表 编辑器被禁止.....	129
6-24	为什么使用网页即可显示 浏览者的硬盘内容.....	129
6-25	手机炸弹游戏包括哪些.....	130
6-26	如何使用“懒人短消息 攻击器”.....	131
6-27	黑客如何实现手机的规模 轰炸.....	131
第 7 章 黑客网吧在线		133
7-1	如何突破网吧的下载限制.....	134
7-2	如何突破网吧的本地硬盘.....	134
7-3	如何使用软件破解网吧限制.....	134
7-4	如何在线编辑注册表.....	135
7-5	如何利用在线工具破解网吧 管理软件.....	135
7-6	黑客如何使用“网吧幽灵”.....	136
7-7	黑客如何进行网吧 IP 冲突 攻击.....	136
7-8	如何破解 IP 和 MAC 的捆绑.....	137
7-9	黑客为什么能够任意执行 硬盘文件.....	138

7-10	黑客如何获取网吧的聊天 记录.....	138
7-11	网吧服务器为什么会崩溃.....	138
7-12	如何使用“网络法官”.....	139
7-13	黑客如何窃取网络游戏密码.....	140
7-14	如何防止网吧中账号的丢失.....	141
7-15	如何获取网络用户信息.....	141
第 8 章 密码的破解		143
8-1	如何使用 debug 命令破解 CMOS 密码.....	144
8-2	如何使用 copy 命令破解 CMOS 密码.....	144
8-3	硬件破解 CMOS 密码的方法有 哪些.....	145
8-4	黑客如何破解 Windows 2000/XP 的登录密码.....	145
8-5	把 Windows XP 密码放在 磁盘中.....	146
8-6	如何给 Windows 2000/XP 加上 双保险.....	146
8-7	如何破解 Windows 9x/Me 屏保密码.....	148
8-8	如何破译 Windows 9x 共享 密码.....	148
8-9	黑客如何破解 IE 分级审理 口令.....	149
8-10	如何使用 Agelx 星号密码 还原器.....	149
8-11	如何使用星号密码查看器.....	150
8-12	如何使用 XP 星号密码查看器.....	150
8-13	如何使用 PartitionMagic 隐藏 硬盘分区.....	150
8-14	如何破解 EFS 加密.....	151
8-15	如何破解 WinZip 加密的 压缩文件.....	151
8-16	破解 WinRAR 加密的压缩 文件.....	152
8-17	如何使用 WinRAR 打造 永不破解的加密文件.....	153

8-18 如何使用 AOEPR 暴力破解 OE 密码.....	153	9-15 如何快速架设 FTP 服务器	175
8-19 Word 文档是怎样被破解的.....	154	9-16 如何实现 3389 主机与本地 主机的文件交换.....	175
8-20 如何暴力破解 Web 邮箱	154	9-17 黑客如何使用 UPX Graphical 加壳木马.....	176
8-21 如何使用 Password Door 为 程序设置密码.....	155	9-18 木马避免查杀的手段有哪些	176
8-22 如何使用 PrivateEXE 实现 应用程序的加密.....	156	9-19 如何使用代理服务器上上网	177
8-23 如何使用 Access Administrator 保护文件安全.....	156	9-20 如何使用 Windows 2000 日志 系统.....	178
8-24 如何使用 ASP 加密解密	157	9-21 如何使用 Windows XP 日志	179
8-25 如何将 EXE 文件进行伪装.....	157	9-22 如何从 FTP 日志中找到黑客的 踪迹.....	180
8-26 黑客如何使用 Cain 提取缓存 密码.....	158	9-23 如何备份系统日志	180
8-27 黑客如何使用 Cain 进行暴力 破解	159	9-24 黑客入侵后如何清除日志	181
8-28 如何铸就安全的 Windows 9x 登录口令	159	9-25 黑客如何伪造日志	181
第 9 章 从入侵到反入侵.....	163	9-26 如何查看黑客入侵时的端口 信息.....	182
9-1 入侵的本质是什么.....	164	9-27 如何实现端口的实时监测 管理.....	182
9-2 黑客入侵的一般步骤有哪些.....	164	9-28 如何监视莫名程序	183
9-3 黑客是如何搜索目标主机 信息的	165	9-29 如何诱捕黑客	184
9-4 黑客常用的攻击方法有哪些.....	165	9-30 如何实现网络的嗅探	185
9-5 病毒攻击手段包括哪些.....	166	9-31 如何使用 Sniffer Pro 监听 Telnet.....	185
9-6 黑客如何实现 DDoS 攻击.....	167	9-32 如何使用 X-Sniffer 捕获密码.....	186
9-7 黑客如何实现 Telnet 入侵.....	168	9-33 如何使用 Sniffem 监视 数据包.....	187
9-8 黑客如何逃避 Telnet 的 NTLM 认证	169	第 10 章 网络特种兵	189
9-9 如何使用网络注册表清除 NTLM.....	170	10-1 什么是代理服务器	190
9-10 黑客如何使用 BITS 入侵、 控制目标主机.....	170	10-2 代理服务器有哪些分类	190
9-11 黑客如何发现网络服务器 漏洞	171	10-3 如何快速获取代理服务器	191
9-12 黑客如何入侵 Real 流服务器.....	172	10-4 在 IE 中如何设置代理服务器	191
9-13 如何入侵 3389 目标主机.....	173	10-5 如何在 QQ 设置代理服务器.....	192
9-14 黑客如何使用 TFTP 实现 远程文件的上传下载.....	174	10-6 如何在 FTP 设置代理服务器	193
		10-7 使用代理服务器有哪些注意 事项.....	193
		10-8 压缩软件有什么安全漏洞	194
		10-9 如何防止计算机长时间 连接服务器.....	194

10-10	如何防止远程修改注册表.....	195	11-19	如何快速断开/接通网络	211
10-11	怎样使用文件的安全 访问权限	195	11-20	如何查看“天网防火墙”的 日志	211
10-12	如何屏蔽 ActiveX 控件以 防攻击	196	11-21	如何使用“KFW 防火墙” 防御黑客攻击	211
10-13	如何隐藏服务器名称.....	197	11-22	如何利用 KFW 应用程序跟踪 功能	212
10-14	如何使用屏保防止注册表被 锁定	197	11-23	如何利用 KFW 数据包内容 记录功能	212
10-15	怎样快速黑掉 ADSL 用户	198	11-24	如何阻止网站弹出广告	212
第 11 章	安全防范	201	11-25	如何通过修改注册表防范 恶意网站的攻击	213
11-1	防火墙的工作原理是什么	202	11-26	如何使用 IE 在线修复	214
11-2	防火墙有哪些类型	202	11-27	如何使用“铁盾 IE 保护器”	214
11-3	如何查看“安全中心”组件	202	11-28	如何使用“金山毒霸 IE 修复 工具”	215
11-4	如何启用“Windows 防火墙”	203	11-29	如何隐藏上网痕迹	216
11-5	如何处理“Windows 防火墙” 的安全警报	203	11-30	如何防止网页攻击	217
11-6	如何设置防火墙中允许运行的 程序	204	11-31	如何预防脚本攻击	218
11-7	如何设置防火墙的端口	204	11-32	如何防止黑客 Telnet 入侵	219
11-8	如何对“Windows 防火墙” 进行高级设置	205	11-33	如何禁止拨号连接	219
11-9	“诺顿个人安全防火墙”有何 特点	206	11-34	如何预防其他用户管理局域网 计算机	220
11-10	如何设置“诺顿个人防火墙” 选项	206	11-35	如何修改 Terminal Server 默认端口	220
11-11	如何进行“诺顿个人防火墙”的 更新	207	11-36	如何修改规则防止黑客 入侵	221
11-12	如何使用 NIS2007 进行系统的 全面扫描	207	11-37	如何使用“木马辅助查找器” 预防木马	222
11-13	如何设置 NIS2007 防护	208	11-38	如何创建隐藏账户	223
11-14	如何检测病毒、间谍软件和 其他风险程序	208	11-39	如何防止感染邮件病毒	224
11-15	如何分析、查看自动防护 通知	209	11-40	如何使用 A-Lock 加密邮件	224
11-16	“天网防火墙”有何特点	210	11-41	如何保护 OE 通信簿安全	226
11-17	如何定义应用程序规则	210	11-42	如何为 OE 设置 SSL 邮件 加密功能	226
11-18	如何设置“天网防火墙”的 IP 规则	210	11-43	如何更新 Windows Update 漏洞补丁	227
第 12 章	安全漏洞与端口检查	229	12-1	什么是安全漏洞	230

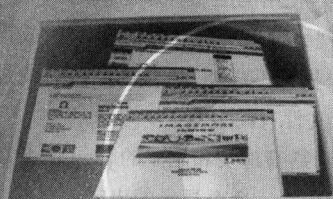
12-2 如何使用 SSS 软件检测安全漏洞	230	第 13 章 系统备份与恢复	241
12-3 如何使用 MBSA 检查计算机的系统安全	231	13-1 为什么要备份注册表	242
12-4 如何使用 NMap 扫描系统安全漏洞	233	13-2 如何利用编辑器备份注册表	242
12-5 什么是计算机端口	235	13-3 如何利用工具备份注册表	242
12-6 如何监视计算机端口	236	13-4 如何使用 Ghost 备份系统	243
12-7 如何在线检测计算机端口	237	13-5 如何使用 Ghost 恢复系统	247
		13-6 如何使用 “一键 Ghost”	249

Chapter 1

1

剖析黑客入侵命令

黑客世界，风云变幻！黑客王国，谁与争锋！
黑客不断敲打着键盘，输入一系列神秘的指令，随着计算机屏幕信息的不断刷新，一个网站可能就这样被黑客入侵了。我们一定很想知道：究竟是什么命令让黑客如虎添翼，有如神助？要揭开黑客的神秘面纱，进入变幻莫测的黑客风云世界，我们先得轻松玩转一些入侵命令。为了了解黑客，我们就从学习各种常用的网络命令开始。



命令	功能
ping	测试网络连通性
tracert	跟踪数据包的路径
nslookup	查询DNS记录
dig	域名系统查询工具
whois	查询域名注册信息
dig	域名系统查询工具
nslookup	域名系统查询工具
whois	查询域名注册信息

1-1 ping 命令有哪些功能

菜鸟提问：

听说 Windows 系统自带一个功能强大的网络命令：**ping**。利用 **ping** 命令可以测试 TCP/IP 协议是否正常工作、测试网络是否畅通。请问 **ping** 命令有哪些功能？

理论点拨：

ping 是测试网络连接状况以及信息包发送和接收状况非常有用的工具，是网络测试最常用的命令。**ping** 向目标主机（地址）发送一个数据包，要求目标主机收到后给予答复，从而判断网络的响应时间和本机是否与目标主机（地址）连通。

实战解决：

单击“开始”→“运行”菜单命令，在打开的“运行”对话框中输入 **cmd**，单击“确定”按钮，可以打开命令提示符窗口，在命令提示符窗口的提示符后输入 **ping** 命令，按【Enter】键，可以显示 **ping** 命令的帮助信息，如图 1-1 所示。

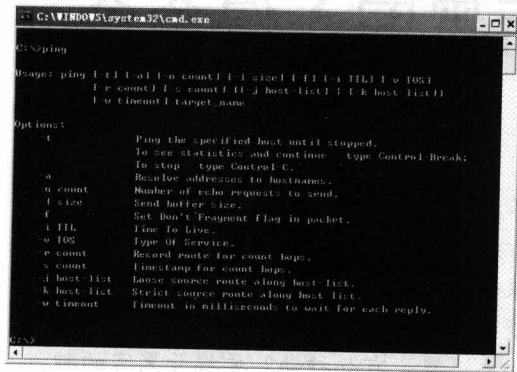


图 1-1

ping 命令有很多功能，在使用 **ping** 命令时，使用不同的参数，可以进行不同的测试。表 1-1 对 **ping** 命令的各项参数的功能进行了说明。

表 1-1 ping 命令参数及功能

ping 命令参数	功 能
-t	校验与指定计算机的连接，直到用户中断
-a	将地址解析为计算机名
-n count	发送由 count 指定数量的 ECHO 报文，默认值为 4

续表

Ping 命令参数	功 能
-l size	发送包字节的大小，默认值为 32
-f	在包中发送“不分段”标志。该包将不被路由上的网关分段
-i ttl	将“生存时间”字段设置为 ttl 指定的数值
-v tos	将“服务类型”字段设置为 tos 指定的数值
-r count	在“记录路由”字段中记录发出报文和返回报文的由数量。指定的 count 值最小可以是 1，最大可以是 9
-s count	指定由 count 指定转发次数的时间
-j host-list	经过由 computer-list 指定的计算机列表的路由报文。中间网关可能分隔连续的计算机（松散的路由）。允许的最大 IP 地址数目是 9
-k host-list	经过由 computer-list 指定的计算机列表的路由报文。中间网关可能分隔连续的计算机。允许的最大 IP 地址数目是 9
-w timeout	以毫秒为单位指定超时间隔
destination-list	指定要校验连接的远程计算机

当用户不能通过某一应用程序访问远程主机时，可进行如下之一的操作和判断。

(1) 如果网络管理员对该远程主机使用 **ping** 命令进行联机检查，结果成功；接着，在用户端对远程主机执行 **ping** 命令，结果也成功，则说明网络故障可能是由用户使用的应用程序造成的。

(2) 如果网络管理员的 **ping** 命令执行成功而用户的 **ping** 命令执行不成功，则故障原因可能是用户端的网络配置文件有问题。

(3) 如果网络管理员和用户的 **ping** 命令都失败了，这时可注意 **ping** 命令显示的出错信息，这种出错信息通常分为三种情况：

- **unknown host**（不知名主机）：这种出错信息的意思是该远程主机的名字不能被命名服务器转换成 IP 地址。网络故障可能为命名服务器有故障，或者其名字不正确，或者网络管理员的系统与远程主机之间的通信线路有故障。

- network unreachable (网络不能到达): 这时本地系统没有到达远程系统的路由, 可用 netstat -rn 检查路由表来确定路由配置情况。
- no answer (无响应): 远程系统没有响应。这种故障说明本地系统有一条到达远程主机的路由, 但却接受不到它发给该远程主机的任何分组报文。这种故障可能是: 远程主机没有工作, 或者本地或远程主机网络配置不正确, 或者本地或远程的路由器没有工作、或者通信线路有故障, 或者远程主机存在路由选择问题。

1-2 ping 命令返回信息的含义是什么

菜鸟提问:

当用户在使用 ping 命令时, 比如: ping www.163.com, 程序就会返回一连串的英文提示信息, 这些信息的含义是什么?

理论点拨:

简单地说, ping 就是一个测试程序, 按照默认设置, Windows 上运行的 ping 命令发送 4 个 ICMP (网间控制报文协议) 回送请求。如果一切正常, 每个 32 字节数据, 应能得到 4 个回送应答。

实战解决:

在命令提示符窗口的提示符后输入 ping www.163.com, 按【Enter】键后, 可以显示如图 1-2 所示的信息。

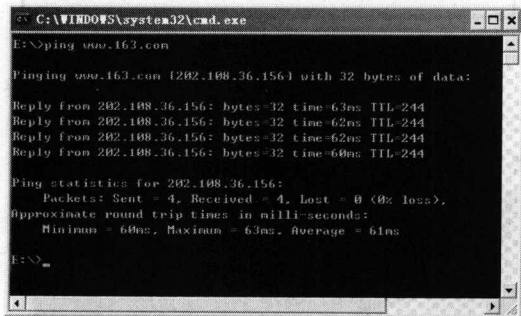


图 1-2

下面我们就来对返回信息一一进行解释:

(1) ping www.163.com [202.108.36.156] with 32 bytes of data:

正在将 32 字节数据 (Windows 默认, 但可改变) 发送到远程服务器 www.163.com, 其后的数字 202.108.36.156 就是该服务器的 IP 地址, 所以有时也可用来实现域名与 IP 地址的转换功能。

(2) Reply from 202.108.36.156: bytes=32 time=63ms TTL=244

本地主机已收到回送信息, 具体为: 32 字节, 共用 63ms, TTL 为 244。TTL (Time To Live) 是存在时间值。

(3) ping statistics for 202.108.36.156:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 60ms, Maximum = 63ms, Average = 61ms

对照解释如下:

ping 202.108.36.156 总的信息如下:

数据包个数: 发送 4 个数据包 (系统默认设置, 每次 ping 时向服务器端发送 4 个数据包), 共收到 4 个, 共丢失 0 个, 占总数的 0%。

发送时间总的概括: 最快回收时间为 60ms, 最慢回收时间为 63ms, 平均为 61ms。

1-3 如何判断目标主机的操作系统类型

菜鸟提问:

要入侵远程计算机, 首先必须判断计算机的操作系统类型, 如何使用 ping 命令判断远程计算机的操作系统类型呢?

理论点拨:

ping 命令能够以毫秒为单位显示发送回请求到回送应答之间的时间量。如果应答时间短, 表示数据包不必通过太多的路由器或网络, 连接速度会比较快。ping 还能显示 TTL (Time To Live 存在时间) 值, 可以通过 TTL 值推算一下数据包已经通过了多少个路由器, 即源地点 TTL 起始值 (就是比返回 TTL 略大的一个 2 的乘方数) 减去返回时 TTL 值。例如: 返回 TTL 值为 119, 那么可以推算数据报离开源地址的 TTL 起始值为 128, 所以源地点到目标地点要通过 9 个路由器网段 (128-119); 如果返回

TTL 值为 246, TTL 起始值就是 256, 源地点到目标地点要通过 10 个路由器网段, 所以可以根据 Ping 命令返回的 TTL 值就可以判断远程计算机的操作系统类型。

实战解决:

如果要判断远程计算机 220.170.241.90 的操作系统类型, 可以在命令提示符窗口的提示符后运行 ping 220.170.240.90 命令, 返回如图 1-3 所示的信息。

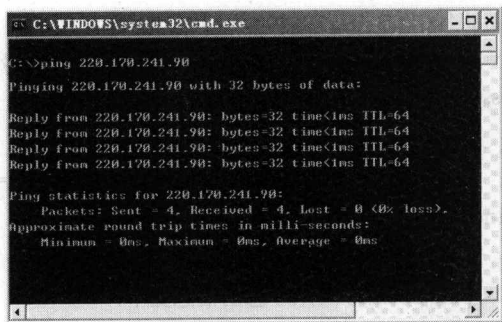


图 1-3

不同的操作系统的主机设置的 TTL 值是不同的, 所以利用这个 TTL 值可以帮助识别操作系统类型。一般 Windows 9x/Me 的 ICMP 回显应答的 TTL 值为 32; Windows NT/2000 操作系统 ICMP 回显应答的 TTL 值为 128; Linux Kernel 2.2.x/2.4.x 操作系统的 TTL 值为 64 (有的时候使用 ping Windows XP 命令, 其 TTL 值是 64 或者 128); 一般 UNIX 及类 UNIX 操作系统的 TTL 值为 255。

根据 TTL 值来判断操作系统类型, 有时也不一定正确, 因为不排除人为修改 TTL 值而达到欺骗的效果。

1-4 怎样测试网卡是否工作正常

网卡是连网的关键部件, 如果网卡损坏或网卡的驱动程序发生错误, 则不可能进行连网。在 Windows XP 下, 一般通过如下步骤查看网卡驱动是否正常。

第 1 步: 在桌面上右击“我的电脑”图标, 在弹出的快捷菜单中选择“属性”命令, 打开“系统属性”对话框, 如图 1-4 所示。

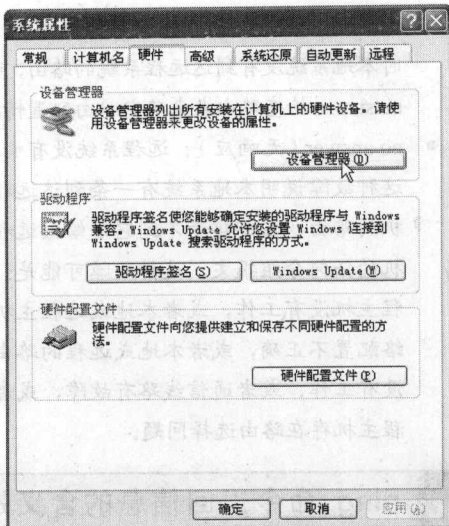


图 1-4

第 2 步: 切换到“硬件”选项卡, 单击“设备管理器”按钮, 即可打开如图 1-5 所示的“设备管理器”窗口, 如果在“网络适配器”区域出现红色的叉号或黄色的感叹号, 即表示网卡的驱动存在故障, 需要重新安装网卡驱动程序。

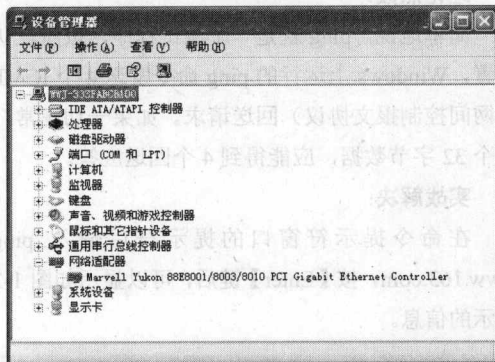


图 1-5

而在命令提示符环境下, 可以使用 ping 127.0.0.1 命令快速测试网卡是否正常工作, 如果出现如图 1-6 所示的信息即可判断出是网卡故障。

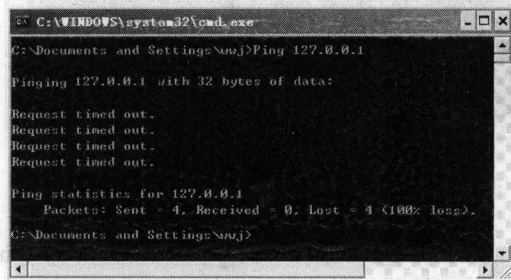


图 1-6

重新安装网卡的驱动程序,使“设备管理器”中的“网络适配器”区域中不存在红色的叉号或黄色的感叹号,再次使用 ping 127.0.0.1 命令测试网卡,出现如图 1-7 所示的信息时,即表示网卡工作正常。

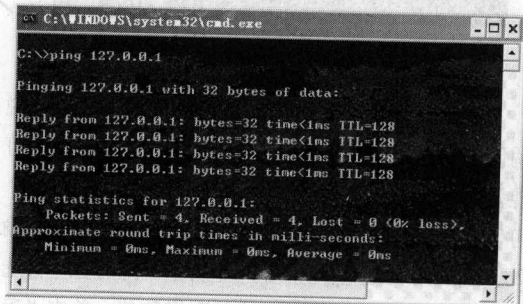


图 1-7

1-5

如何测试网络协议是否工作正常

计算机要正常连接上网络,除了本机正确安装了网卡外,还必须安装 TCP/IP 等协议,在确认网卡正常工作的情况下,可以通过以下步骤查看计算机中已安装的协议。

第1步:在桌面上右击“网上邻居”图标,在弹出的快捷菜单中选择“属性”命令,打开“网络连接”窗口,如图 1-8 所示。

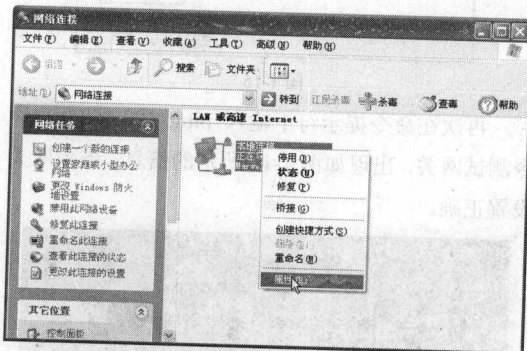


图 1-8

第2步:右击“本地连接”图标,在弹出的快捷菜单中选择“属性”命令,打开“本地连接属性”对话框,如图 1-9 所示。

在此对话框中,可以检查是否安装了 TCP/IP 等协议,也可以选中“Internet 协议 (TCP/IP)”选项,单击“属性”按钮,在打开的对话框中对协议

的属性进行配置。

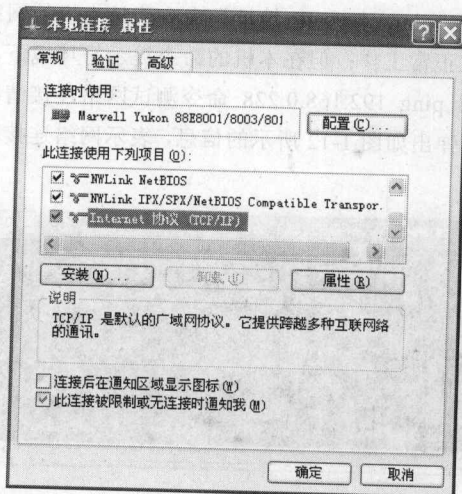


图 1-9

在命令提示符下可以使用“ping 本机 IP 地址”命令快速检测网络协议是否工作正常,出现如图 1-10 所示的界面,表示协议工作正常。

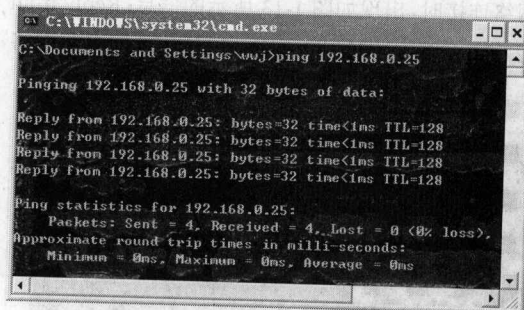


图 1-10

而出现如图 1-11 所示的界面,则表示网络协议不能正常工作,应重新安装或配置网络协议。

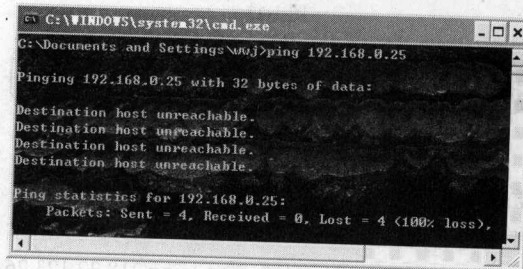


图 1-11

1-6 如何测试网络连接情况

局域网的所有计算机都无法和 IP 为 192.168.0.228 的计算机进行正常通信。事先已经使用了 ping

127.0.0.1 命令, 确认本机的网卡正常工作; 也使用了“ping 本机 IP 地址”命令确认本机的网络协议正常工作; 但在本机的命令提示符环境下, 使用 ping 192.168.0.228 命令测试网络连接情况时, 弹出如图 1-12 所示的信息, 表示网络连接不通。

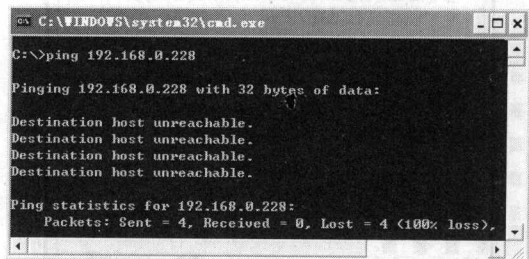


图 1-12

此故障的原因最大的可能是网络之间不通, 重新制作网线, 并确认网线的水晶头和网卡及路由器正常连接, 再一次使用 ping 192.168.0.228 命令测试网络连接时, 出现如图 1-13 所示的信息: Reply from 127.0.0.1: bytes=32 time<1ms TTL=128 即表示网络连接正常。

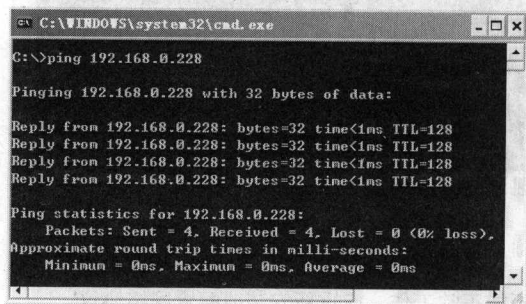


图 1-13

1-7 如何测试网关

计算机能够和局域网中的其他计算机正常通信, 但是不能访问互联网, 在命令提示符下对某一网站 www.ABCD.com 的 IP 地址 (218.22.123.26) 进行测试, 输入 ping 218.22.123.26 命令并按【Enter】键, 出现如图 1-14 所示的结果, 说明网络不通。

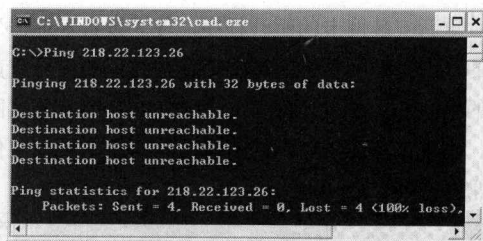


图 1-14

既然计算机能够访问局域网的其他计算机, 说明网卡和网络协议正常工作, 从故障现象分析, 可能是网关配置不当。已知网关地址为 192.168.0.1, 可以在“Internet 协议 (TCP/IP) 属性”对话框中输入正确的网关地址, 如图 1-15 所示, 同时在“首选 DNS 服务器”的空白框内输入同样数值, 单击“确定”按钮。

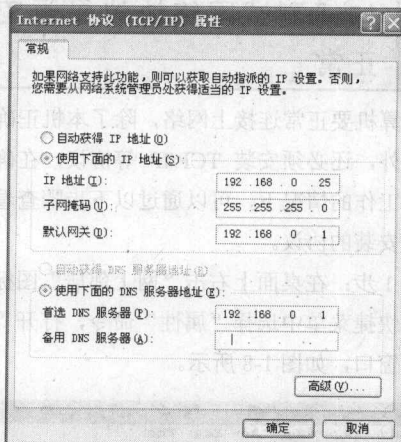


图 1-15

再次在命令提示符下输入 ping 192.168.0.1 命令测试网关, 出现如图 1-16 所示的信息, 表示网关设置正确。

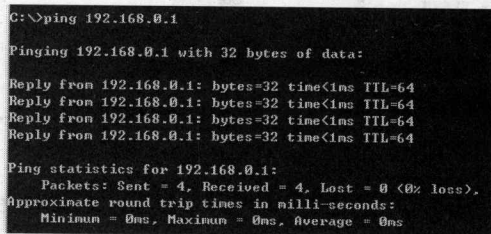


图 1-16

提示

如果无法知道网络的 IP 地址, 也可以直接对网址进行测试, 输入网址即可, 如 Ping www.ABCD.com。