



黑客入门

七种武器攻防 一百零八招

工欲善其事 必先利其器

中国第一黑客团队——鹰派联盟权威推荐

十八般武艺 黑客绝技高招

【工具·应用篇】

仲治国 编著

超值光盘

价值128元大礼包

华夏黑客同盟视频

远程控制及防范工具

扫描与反扫描工具

加密与解密工具

挑战黑客

孔雀翎

扫描与反扫描

碧玉刀

加密与解密

离别钩

日志与检测

长生剑

控制与反控制

霸王枪

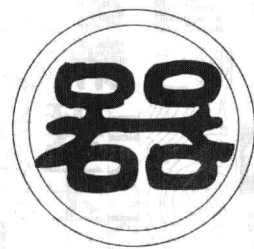
围剿间谍软件

拳头

黑客工具箱

多情环

账号盗取与防范



新手入门

黑客

工具·应用篇

七种武器攻防 一百零八招

编著 仲港国

山东电子音像出版社出版

内 容 提 要

《黑客七种武器攻防一百零八招》是一本为广大电脑爱好者定制的黑客入门指导图书，内容涵盖了当今互联网黑客应用的各大领域，并以古龙的《七种武器》为参考为读者归纳了七大板块内容，它们是：孔雀翎——扫描与反扫描、碧玉刀——加密与解密、长生剑——控制与反控制、多情环——账号盗取与安全防范、霸王枪——暴力攻击与恶意绑架、离别钩——安全防范与入侵检测、拳头——黑客工具箱。各大板块既各自成章，又相互关联，涉及黑客攻防的各个方面。

全书采用全程图解、攻防兼备的形式，即便是初学入门的读者也能够随学随用、即查即知，最终成为一名网络安全高手。

正所谓江湖道，十八般武艺样样精通；黑客道，一百零八招式式克敌。只要你掌握黑客入门一百零八招，就能潇潇洒洒走江湖。

多媒体教学光盘运行说明

运行环境：Windows 98/Me/2000/XP/2003；

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

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

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

书 名：黑客七种武器攻防一百零八招

编 著：仲治国

执行编辑：李 勇 何 磊

封面设计：刘学敏

责任编辑：李 萍

监 制：时均建

出版单位：山东电子音像出版社

地 址：济南市胜利大街39号

邮政编码：250001

电 话：(0531)82060055-7616

发 行：山东电子音像出版社

经 销：各地新华书店、报刊亭

C D 生产：北京中联光碟有限公司

文本印刷：重庆联谊印务有限公司

开本规格：787mm × 1092mm 1/16 20.5印张 250千字

版 本 号：ISBN 7-89491-638-2

版 次：2006年6月第1版 2006年6月第1次印刷

定 价：28.00元(1CD+配套书)

Preface

序

黑客道

计谋层出，胸藏攻防先见之明

谈笑之间，指点网络诡诈真伪

“黑客道”系列图书自2005年推出以来，得到了很多读者的喜爱和好评，多次荣登全国图书畅销排行榜，图书历经多次加印，累计销量达到10万余册，创下黑客类图书的多个NO.1：

第一套兵法战术与电脑安全相结合的黑客类图书

第一套古典风格的电脑应用图书

第一套将古代兵法完美演绎的黑客实战宝典

……

一名技艺高超的黑客无非体现在以下两方面：其一是娴熟的黑客工具应用，其二是独到的谋略技巧施展。“黑客道”系列图书正是从以上两个方面的黑客攻防必备技能进行展开。该系列图书共两本：

《黑客攻防三十六计》（谋略·技巧篇）是以我国最负盛名的神奇兵书《三十六计》为模式，从三十六个方面详尽地进行了实战式的黑客入侵与防御演练，将古代兵法韬略在黑客攻击防范中体现得淋漓尽致！

《黑客七种武器攻防一百零八招》（工具·应用篇）是源自武侠巨匠古龙大师的扛鼎之作《七种武器》，并结合当前黑客最流行的一百零八种工具，进行了具体详细的讲解。

网络就是战场，安全就是用兵。

战场上硝烟弥漫，鲜血进溅；网络中尔虞我诈，明争暗斗！

你想踏入黑客这块令人热血沸腾、神秘莫测的领域吗？

正所谓兵来将挡，水来土掩。只要我们抱着“勿恃敌之不来，恃吾有以待之”的精神，必能将各种危机化解于无形！熟读兵书三百遍，不会用兵也能防。

应读者的要求，今年我们对“黑客道”系列图书进行了全新改版：增加了最近一年内新出现的各种黑客技术和黑客工具的使用，新版“黑客道”将给大家更加实用的黑客应用与黑客技巧，让你轻松迈入黑客之门，有效防范黑客攻击。

黑客其实就是这么简单，防范黑客其实根本就不难，只是大家没有涉足而已！

最后，衷心地祝愿广大读者能够通过这套书快速掌握黑客知识：学黑客绝技高招，做网络安全卫士！

编者

2006年6月

●黑客攻防视频教程

(华夏黑客同盟网站授权)

- 1.利用IRM彻底保护Office文档
- 2.局域网二级代理及查找
- 3.进程管理Process Explorer
- 4.简单教你恢复文件关联
- 5.Windows下架设Apache服务器1
- 6.Windows下架设Apache服务器2
- 7.批处理保护你的CMD
- 8.代理服务器技术详解
- 9.Ipsec防范DDos攻击
- 10.加强服务器安全
- 11.Xscan使用教学
- 12.认识计算机病毒

●黑客工具软件

1.《木马防线2005+》(电脑报专用版)

木马防线2005+是安天实验室开发的一款功能强大的个人信息安全产品,具备高效木马查杀、系统安全管理、网络保护等功能。它采用全新的高速智能检测引擎(SVE),能够完全查杀国内外流行的75,000余种木马、后门、蠕虫、间谍软件、广告软件、黑客工具、色情拨号程序等,尤其对各类未知有害程序具有极高的检出率。

2.《私人磁盘》(电脑报专用版)

“私人磁盘”可以通过创建私人磁盘文件的方式将各个磁盘分区中的剩余空间从该分区中分离出来,作为私人磁盘的空间来源,并虚构一个磁盘分区供用户使用,只要实际的磁盘空间足够,就可以无限地向这个虚拟磁盘分区中放入文件,操作完成后,将“私人磁盘”软件关闭,存放在私人磁盘中的文件将会自动加密。

3.《熊猫入侵防护个人版》(电脑报专用版)

熊猫入侵防护个人版基于“专门针对未知病毒和攻击而设计”的智能识别技术,即是通过采用“行为分析技术”鉴别文件是否具有危险性或攻击性,即使那些诸如冲击波、震荡波之流的未知病毒亦能够有效隔离。该技术改变了传统杀毒软件所使用的“响应式”技术(被动查杀),转而通过对程序行为的主动跟踪和分析,从而判断是否为病毒或攻击并对之相应做出防范措施。

4.安全扫描工具

微点主动防御软件
局域网查看工具
木马克星
X-Scan
SuperScan
RegShot
Real Spy Monitor
ProtectX
Network Scanner
File Monitor
MBSA

5.加密解密工具

绝对隐私
多功能密码破解软件
Wps Password Recovery
Word Key
WinGuard Pro
SecurStar DriveCrypt
PhotoEncrypt
Lock it Easy
File & Folder Protector
Dekart Private Disk
ZIP Password Recovery

6.远程控制工具

屏幕间谍
WinVMC
WinShell
URLY Warning
QuickIP
Net Tools X

特别提示:光盘中收录了鹰派联盟主题曲《黑夜的力量》供读者欣赏。

第一篇

孔雀翎——扫描与反扫描

第1招 使用X-scan查本机隐患	2
一、用X-scan查看本机IP地址	2
二、添加IP地址	2
三、开始扫描	3
四、高级设置	4
第2招 妙用流光扫描主机漏洞	6
一、认识流光	6
二、批量主机扫描	7
三、指定漏洞扫描	10
第3招 LANNSS扫描局域网安全隐患	11
一、扫描局域网内计算机的安全漏洞	11
二、查看扫描结果	14
第4招 Windows系统安全检测	15
一、MBSA 特色功能	15
二、安装设置MBSA	15
三、检测单台计算机	16
四、检测多台计算机	17
第5招 用诺顿网络安全特警在线扫描	18
一、登录网站扫描	18
二、查看检测结果	20
第6招 RPC漏洞扫描器	21
一、RPC漏洞带来的危险	21
二、深入浅出RPC	21
三、扫描RPC漏洞	22
第7招 WebDAVScan漏洞扫描器	23
一、WebDAV漏洞解析	23
二、扫描WebDAV漏洞	23
三、解决方法	24
第8招 SQL安全扫描器Hscan	24
一、SQL漏洞危险的由来	25
二、黑客入侵解析	25
第9招 用ProtectX防御扫描器追踪	26
一、ProtectX实用组件解析	26
二、防御扫描器攻击	27

第 10 招 网页安全扫描器	28
一、网页漏洞扫描	28
二、查看网页安全漏洞	29
第 11 招 玩转 NC 监控与扫描功能	30
一、监听本地计算机端口数据	30
二、监听远程计算机端口信息	31
三、将 NC 作为扫描器使用	32
第 12 招 用 RegShot 监控注册表修改	32
一、认识 RegShot	32
二、注册表的监控	33
第 13 招 文件操作监控大师	36
一、捕获事件	36
二、事件的识别	36
三、存储数据	37
第 14 招 还有什么我不知道——Real Spy Monitor	37
一、添加使用密码	38
二、设置弹出热键	38
三、监控浏览过的网站	39
四、键盘输入内容监控	40
五、程序执行情况监控	41
第 15 招 局域网监控大师 LanSee	41
一、搜索计算机	42
二、搜索共享资源	42
三、检查端口连接状态	43

第二篇

碧玉刀——加密与解密

第 16 招 使用 WordKey 恢复 Word 密码	45
一、创建加密文件	45
二、使用 WordKey 解密	46
第 17 招 用“密码查看器”找出密码	47
一、软件介绍	47
二、密码恢复实战	47
第 18 招 Excel 与 WPS 密码攻防	48
一、轻松查看 Excel 文档密码	48
二、WPS 密码攻防	48

第 19 招 “多功能密码破解软件” 恢复密码	49
一、工具介绍	49
二、密码恢复实战	49
第 20 招 暴力破解压缩文件密码	50
一、WinZIP 压缩文件的破解	50
二、WinRAR 压缩文件的破解	51
三、让压缩文件无懈可击	51
第 21 招 syskey 双重加密与解除	52
一、syskey 双重加密方法	53
二、轻松解除 syskey 加密	54
三、防范方法	55
第 22 招 轻松找回 Windows XP 管理员密码	55
一、清除管理员密码	55
二、借助工具从 SAM 文件中查看密码	56
三、使用工具修改管理员密码	56
四、用好密码重设盘	57
第 23 招 文件分割巧加密	58
一、分割文件	58
二、合并文件	58
第 24 招 与众不同的分时段加密	59
一、特色功能	59
二、管理加密用户	59
三、加密文件夹	60
四、设置自解密时间	61
五、激活加密功能	61
第 25 招 公用电脑上的隐私保护神	61
一、认识“绝对隐私”	62
二、文件加密与解密	62
三、目录加密与解密	63
四、方便好用的编辑功能	63
五、“绝对隐私”个性设置	64
第 26 招 图片加密好帮手	64
一、新建一个档案文件	64
二、导入图片	65
三、解密文件	65
第 27 招 生成自解密文件的“机器宏加密”	66
一、加密文件	66
二、解密文件	66
第 28 招 用 WinGuard 锁定应用程序	67
一、设置密码	67
二、设置要限制的程序	68

目录

三、文件文件夹加密	68
四、锁定其他选项	69
第 29 招 军用级硬盘加密	70
一、创建虚拟磁盘空间	70
二、加密数据文件	72
三、在虚拟磁盘中创建“虚拟磁盘”	73
第 30 招 为你的 U 盘加把锁	74
一、加密整个 U 盘	74
二、部分数据加密	75
三、密码解除	76
第 31 招 虚拟磁盘加密隐藏你的隐私	76
一、创建虚拟加密磁盘	76
二、虚拟磁盘的使用	78
第 32 招 “私人磁盘”隐藏大文件	79
一、认识“私人磁盘”	79
二、大文件的隐藏	80

第三篇

长生剑——控制与反控制

第 33 招 妙用“冰河陷阱”防冰河	82
一、冰河陷阱简介	82
二、清除冰河木马	83
三、诱骗黑客	84
第 34 招 木马克星	86
一、检测木马	87
二、激活防火墙	87
三、强大的扫描功能	88
第 35 招 使用 SuperScan 监控端口	89
一、认识 SuperScan	89
二、监控端口	90
第 36 招 用 WinVNC 体验远程控制	91
一、配置服务器	92
二、客户端连接	92

目录

第 37 招 用 TFTP 实现上传下载	93
一、安装 TFTP 服务	93
二、使用 TFTP 服务	95
三、防范 TFTP 入侵	96
第 38 招 使用 WinShell 实现远程控制	96
一、WinShell 简介	96
二、配置服务器端	96
第 39 招 使用 QuickIP 进行多点控制	99
一、QuickIP 功能介绍	99
二、设置 QuickIP 服务端	100
三、设置 QuickIP 客户端	101
四、远程控制	102
第 40 招 巧用屏幕间谍定时抓屏	104
一、屏幕截图	104
二、设置抓取时间间隔	105
第 41 招 实战命令行下的远程控制 PsExec	107
一、进入 Telnet 操作状态	107
二、执行本地程序	108
三、启动远程服务	108
第 42 招 用灰鸽子通过局域网进行远程管理	108
一、灰鸽子简介	108
二、灰鸽子远程管理	109
三、卸载灰鸽子	111
第 43 招 感受 Serv-U 的远程控制	113
一、服务器配置	113
二、工作站配置	114
第 44 招 用 URLy Warning 监控远程信息	115
一、URLy Warning 简介	115
二、URLy Warning 远程监控	115
第 45 招 用 Simple Bind 自制远程控制程序	116
一、合并 EXE 文件	116
二、修改合并后的 EXE 文件图标	117
第 46 招 远程控制好帮手 PcAnywhere	117
一、PcAnywhere 的安装	118
二、PcAnywhere 的基本设置	118
三、使用 PcAnywhere 进行远程控制	119

第四篇



多情环——账号盗取与安全防范

第47招 防范“啊拉QQ大盗”盗取QQ	123
一、邮箱收信	123
二、网站收信	124
三、“啊拉QQ大盗”防范方法	125
第48招 QQ密码保护的克星——QQ密保大盗	127
一、木马客户端制作	127
二、轻松盗取QQ密码	128
三、轻松突破密码保护	128
四、巧用QQ申诉信息“夺取”QQ号	129
第49招 当心“QQ掠夺者”盗取QQ	130
一、认识QQ掠夺者	130
二、QQ盗取曝光	130
三、防范QQ掠夺者	132
第50招 防范“QQ破密使者”盗取QQ	132
一、本地破解	132
二、防范QQ破密使者	133
第51招 在线破解QQ揭秘	134
一、在线破解	134
二、QQExplorer在线破解及其防范	134
第52招 解读“密码使者”截获QQ	135
一、初识“密码使者”	135
二、“密码使者”作案剖析	135
三、应对措施	136
第53招 来自“QQ枪手”的攻击	137
一、QQ枪手简介	137
二、QQ枪手盗号探密	137
第54招 “QQ机器人”盗号也疯狂	138
一、安装运行QQ机器人	138
二、配置QQ机器人	138
第55招 防范“OICQ密码轻松盗”监听	139
一、曝光盗号方法	140
二、防范OICQ密码轻松盗的监听	140
第56招 识破“QQ密码保护”的骗局	141
一、认识“QQ密码反保精灵”	141

二、“QQ 密码反保精灵”骗术曝光	141
三、防范 QQ 密码保护的骗术	141
第 57 招 全面武装打造安全 QQ	142
一、妙用磁盘读写权限彻底封杀 QQ 广告	142
二、为 QQ 硬盘设置密码	142
三、为 QQ 通讯录设置密码	143
四、看好你的 Q 币	144
第 58 招 用“防盗专家”为 QQ 保驾护航	144
一、认识防盗专家	144
二、自动关闭 QQ 广告	145
三、取回密码	145
四、内核修改	146
五、病毒查杀	146
六、无敌外挂	146
七、其他功能	147
第 59 招 伸向 MSN 的黑手——MSN Messenger Hack	147
一、认识 MSN Messenger Hack	147
二、MSN 盗取揭秘	147
三、防范 MSN Messenger Hack	149
第 60 招 MSN 密码查看帮凶——MessenPass	149
一、MessenPass 简介	149
二、查看 MSN 密码解析	149
三、防范 MessenPass	150
第 61 招 防范 E 话通靓号被盗	150
一、解读 E 话通号码被盗	150
二、防范 E 话通靓号被盗	152
第 62 招 联众密码也受伤	152
一、当心“联众密码监听器”的监听	152
二、找回丢失的联众密码	153
第 63 招 防范“传奇密码邮差”	153
一、传奇密码盗取方式揭秘	153
二、警惕“传奇密码邮差”	154
三、拒绝传奇盗号	154
第 64 招 揪出内鬼——密码监听器	155
一、“密码监听器”盗号披露	156
二、找出“卧底”拒绝监听	158

第五篇

目录

霸王枪——暴力攻击与恶意绑架

第 65 招 IP 炸弹工具 IP Hacker	160
一、防范攻击 Windows 98	161
二、防范攻击 Windows NT	161
第 66 招 Ping 攻击的安全防范	162
一、Ping 命令详解	162
二、防范被人 Ping	164
第 67 招 RPC 溢出工具	165
一、漏洞描述	165
二、入侵实战	166
三、防范方法	168
第 68 招 Messenger 溢出工具	169
一、漏洞简介	169
二、漏洞扫描	170
三、溢出方法	171
四、漏洞修补方法	172
第 69 招 Windows logon 溢出工具体验	173
一、漏洞初识	173
二、远程溢出	173
三、漏洞防范	174
第 70 招 Google Toolbar 解除恶意绑架	175
一、Google Toolbar 简介	175
二、解除恶意绑架	175
第 71 招 防暴专家 AtGuard	177
一、AtGuard 简介	178
二、AtGuard 的个性化设置	178
第 72 招 浏览器绑架克星 Hijack This	182
一、系统检测	182
二、编号识别	183
第 73 招 微软反间谍高手	184
一、初识反间谍软件利器	184
二、手动扫描查杀间谍软件	184
三、设置定时自动扫描	186
四、开启实时监控	186
五、四款特色安全工具	188
第 74 招 Spybot-Search & Destroy 清除间谍	189
一、使用 Spybot-Search & Destroy 清除间谍软件	189
二、用 Spybot 恢复误删除的文件	190

目录

三、设置 Spybot 对间谍软件免疫	191
四、用 Spybot 查找启动项中的间谍	191
第 75 招 间谍杀手 Ad-aware	192
一、软件更新	192
二、使用 Ad-aware 全面扫描系统	192
三、使用 Ad-aware 快速清除任务	193
第 76 招 用 Spy Sweeper 铲除间谍软件	194
一、软件安装	194
二、铲除间谍软件实战	194
第 77 招 根除流氓软件	196
一、认识“流氓软件”及其分类	196
二、使用超级兔子魔法设置清除流氓软件	197
三、用瑞星“卡卡安全助手”根除“流氓软件”	198
第 78 招 清理“流氓软件”中的浏览器插件	202
一、使用 Windows XP SP2 插件管理功能	202
二、IE 插件管理专家	203
第 79 招 防范“流氓软件”	203
一、及时更新补丁程序	203
二、禁用 ActiveX 脚本	204
三、加入受限站点	204
四、修改 HOSTS 文件	204
五、设置网页安全扫描	205
六、修改注册表	205

第六篇

离别钩——安全分析与入侵检测

第 80 招 天网防火墙	207
一、天网防火墙初步应用	207
二、天网安全设置	207
三、检查并修复系统漏洞	210
第 81 招 上传文件检测之思易 ASP 木马追捕	211
一、思易 ASP 木马追捕简介	211
二、检测网页木马	211
第 82 招 单机版入侵检测系统 NID	213
一、NID 简介	213
二、NID 基本设置	213
三、NID 规则设置与使用	214

第 83 招 日志分析利器 WebTrends	216
一、创建日志站点	217
二、日志报表的生成	218
三、查看日志	219
第 84 招 远程日志清除工具之 elsave	219
一、用小榕的 elsave 远程清除日志	220
二、手工清除日志法	220
第 85 招 远程维护日志之“计算机管理”功能	222
一、启动远程连接	222
二、常见日志解释	223
第 86 招 用 IIS Lock Tool 检测网站安全	225
一、IIS Lock Tool 简介	226
二、IIS Lock Tool 的基本应用	226
三、IIS Lock Tool 的高级设置	227
第 87 招 诺顿网络安全特警	230
一、配置安全特警	230
二、启用诺顿网络安全特警	231
三、程序扫描	232
四、隐私控制	233
五、在线安全检测	234
六、封锁恶意 IP	235
七、端口防范	236
第 88 招 用无处藏身检测恶意 IP	237
一、发现恶意 IP	237
二、追踪恶意 IP	237
第 89 招 免费的专业防火墙 Kerio	238
一、Kerio 基本应用	238
二、调整 Kerio 过滤机制	240
第 90 招 专业入侵检测系统 BlackICE	241
一、初识 BlackICE	241
二、BlackICE 的安装必知	242
三、BlackICE 的应用实战	242
第 91 招 经典嗅探器之 Iris	244
一、Iris 的工作原理	244
二、用 Iris 捕获数据	245
三、怎样防御 Iris 的嗅探	248
第 92 招 经典嗅探器之 NetXray	248
一、认识 NetXray	248
二、NetXray 捕获数据	249
三、NetXray 其他功能	251

第 93 招 经典嗅探器之 SpyNet Sniffer	252
一、用 SpyNet Sniffer 播放音乐或视频	252
二、用 SpyNet Sniffer 捕获下载地址	252
第 94 招 命令行下的嗅探器 WinDump	253
一、WinDump 简介	253
二、WinDump 监听网卡	254
第 95 招 看不见的网管专家 Sniffer Portable	256
一、Sniffer Portable 基本功能	256
二、安装要点与基本设置	257
三、数据捕获	259
第 96 招 用 Privacy Defender 实现安全的网际畅游	260
一、Privacy Defender 的安全演示	260
二、Privacy Defender 清除上网痕迹	260

第七篇

拳头——黑客工具箱

第 97 招 木马防线 2005 +	262
一、木马查杀傻瓜化	262
二、系统修复一键搞定	263
三、IE 插件管理工具	264
四、共享管理	264
五、端口进程管理	265
六、系统漏洞检查	266
七、安天盾防火墙	266
八、威胁预警	267
第 98 招 Windows 木马清道夫	267
一、全方位检测木马	268
二、扫描系统漏洞	268
三、探测可疑模块	269
四、监视网络连接	270
五、查看共享目录	270
第 99 招 微点主动防御软件	271
一、安全防护“多”管齐下	271
二、漏洞扫描，消除隐患	271
三、巧妙设置，自动防护	272
四、控制进程，确保安全	272
五、未知木马，照样截杀	273
六、日志管理，了然于心	274

第 100 招 攻守兼备——N.C.P.H 攻防网络入侵器	275
一、环环相扣，攻击生威	275
二、多管齐下，防守有方	278
第 101 招 多功能的菜鸟黑客工具箱	281
一、文件图标更改、捆绑	281
二、加密解密	283
三、强制破解	283
四、加壳压缩	284
五、免杀加工	284
六、扫描漏洞	285
七、记事脚本	285
八、系统控制	286
第 102 招 网络安全强大助手 Net Tools X	287
一、工具介绍	287
二、进程管理	287
三、Ping 探测	288
四、局域网安全管理	289
五、网络连接管理	290
六、地址转换	291
第 103 招 P2P 网络安全必备工具	292
一、PeerGuardian 安装设置	292
二、阻止 P2P 中的可疑连接	294
三、PeerGuardian 优化设置	296
第 104 招 U 盘安全保护神	296
一、闪存窥探者 FlashDishThief	296
二、U 盘守护者 usafer	298
第 105 招 “五妙计” 封杀 Windows 默认共享	298
一、“停止共享” 法	299
二、批处理自启动法	299
三、修改注册表法	300
四、停止服务法	300
五、卸载“文件和打印机共享” 法	301
第 106 招 妙用组策略增强 WinXP 共享资源安全	302
一、关闭简单文件共享	302
二、修改组策略指定特定用户访问	303
三、禁止非法用户访问	304
第 107 招 火眼金睛识木马——Port Reporter	305
一、安装和卸载 Port Reporter	305
二、配置 Port Reporter “捉” 木马	306
三、日志文件分析	308
四、根据端口查杀木马	309
第 108 招 看好 TCP 让黑客无机可乘	310
一、封锁向外“传播” 的 TCP 连接	310
二、监控外部恶意 TCP 连接	311