

# 《防黑档案》

## 图书基本信息

书名：《防黑档案》

13位ISBN编号：9787121011252

10位ISBN编号：7121011255

出版时间：2005-5

出版社：第1版(2005年5月1日)

作者：郭鑫

页数：275

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：[www.tushu000.com](http://www.tushu000.com)

# 《防黑档案》

## 内容概要

本书为畅销书《防黑档案》的升级版，由业内知名黑客“东言飘云”编写，对第一版的内容进行了全面的调整和完善，删掉了部分过时的内容，增加了近期最新出现的网络漏洞及攻防技术。本书最大程度地沿袭了第一版优秀的畅销书特质，以精辟的语言深入浅出地讲解了在日常的网络生活中广大网友经常会遇到的一些安全性问题，包括即时通信工作、Mail、Web、病毒、系统安全、后门木马、黑客工具、数据库注入等攻防技术，以及当前的热点加密解密技术。本书旨在让读者快速形成正确的网络安全观念，并掌握维护与防范的技巧，能够从容应对来自网络的形形色色的威胁，从而更大程度地享受网络带给我们的巨大乐趣。附书光盘内容为网络攻防视频演示文件。本书既可作为从事网络安全工作人员的参考资料，也可作为网络爱好者充实自己的学习和辅导用书。

# 《防黑档案》

## 作者简介

郭鑫，网名：东方飘云；年龄：不详；全国十大黑客之一，资深网络安全顾问。

业绩：创办中国安全在线<http://www.safen.org>，并担任站长。现任瑞索讯杰信息技术有限公司，网络安全顾问。曾参与主持多个国家级项目的安全评估。

## 书籍目录

第1章 我眼中的黑客 1.1 黑客的由来 1.1.1 怎么样才是一名黑客 1.1.2 黑客的态度 1.1.3 一名黑客所需的基本技能 1.1.4 黑客守则 1.2 黑客的发展 1.2.1 黑客发展经历的四个阶段 1.2.2 黑客发展的新特点 1.2.3 黑客的行动特征 1.2.4 黑客的类型 1.2.5 黑客精神 1.2.6 黑客大事记 第2章 网络安全基础知识 2.1 认识IP地址 2.1.1 什么是IP地址 2.1.2 IP地址划分方法 2.1.3 如何查询IP地址 2.2 端口 (Port) 是什么 2.3 TCP/IP 2.3.1 TCP/IP组件的四个层次及功能 2.3.2 TCP/IP的分层 2.4 网络常用命令 2.4.1 ping 2.4.2 ipconfig 2.4.3 tracert 2.4.4 netstat 2.4.5 net 2.4.6 at 2.4.7 telnet 2.4.8 ftp 2.4.9 copy 2.4.10 set 2.4.11 echo 2.4.12 attrib 2.4.13 net start 网络名词解释 第3章 黑客常用的经典工具及使用方法 3.1 扫描工具 3.1.1 “流光” 3.1.2 ShadowSecurityScanner 3.1.3 SuperScan 3.2 木马工具 3.2.1 “冰河” 3.2.2 “网络神偷” 3.2.3 DameWare NT Utilities 3.3 网络监听工具 3.3.1 Iris 3.3.2 Xsniff 3.4 破解工具 3.4.1 L0phtcrack 3.4.2 “溯雪” 第4章 黑客大揭密——日常上网攻防篇 4.1 如何查看好友的IP 4.1.1 IPLocate 4.1.2 OICQ查IP补丁 4.2 OICQ黑客软件介绍 4.3 OICQ二人世界的陷阱 4.4 如何防止OICQ密码被盗 4.4.1 专门偷OICQ密码的木马介绍 4.4.2 OICQ防偷术 4.5 在OICQ中隐藏自己的IP 4.6 如何防范OICQ的黑客程序 4.7 聊天室攻防篇 4.7.1 聊天室炸弹攻击方法 4.7.2 聊天室防炸方法 4.8 BBS攻防篇 4.8.1 BBS漏洞 4.8.2 BBS入侵实例 4.9 网络游戏修改篇 4.9.1 网络游戏修改的一些常识 4.9.2 以“传奇”为例讲如何修改 第5章 黑客大揭密——实战Windows2000 109 5.1 Windows 2000漏洞的概述 5.2 3389输入法漏洞应用 5.3 IPC\$管道漏洞的应用 5.3.1 概述 5.3.2 入侵方法及过程 5.4 Unicode与二次解码漏洞的应用 5.4.1 漏洞原理 5.4.2 入侵方法及过程 5.5 IDA和IDQ扩展溢出漏洞的应用 5.5.1 漏洞描述 5.5.2 漏洞的应用 5.6 Printer溢出漏洞的应用 5.6.1 漏洞描述 5.6.2 漏洞的应用 5.7 SQL空密码漏洞的应用 5.7.1 漏洞概述 5.7.2 漏洞的应用 5.8 FrontPage扩展漏洞的应用 5.8.1 漏洞概述 5.8.2 漏洞的应用 5.9 DDoS拒绝服务攻击应用 5.9.1 何为DDoS 5.9.2 DDoS的检测 5.9.3 DDoS工具——UDP Flooder介绍 5.9.4 DDoS攻击的防御策略 5.10 EXPN/VRFY漏洞的应用 5.10.1 EXPN/VRFY漏洞概述 5.10.2 怎样利用EXPN/VRFY命令漏洞取得用户列表 5.11 应用程序漏洞的应用 5.11.1 何谓应用程序漏洞 5.11.2 应用程序漏洞列举及应用 5.12 用“肉鸡”做跳板 5.12.1 搜索主机 5.12.2 制作“跳板” 5.13 日志删除 5.13.1 日志讲解 5.13.2 日志删除 第6章 黑客大揭密——实战Linux/UNIX 6.1 wu-ftp 2.4.1 远程溢出漏洞的应用 6.1.1 需求 6.1.2 步骤 6.1.3 补充说明 6.2 RPC远程溢出漏洞的应用 6.2.1 漏洞描述及危害 6.2.2 攻击过程 6.3 RedHat LPD Bug溢出漏洞的应用 6.3.1 漏洞描述及危害 6.3.2 攻击步骤 6.3.3 解决方法 6.4 Sun OS远程溢出漏洞的应用 6.4.1 Sun OS简介 6.4.2 漏洞描述 6.4.3 进行攻击所需的系统和程序 6.4.4 攻击步骤 6.4.5 解决方法 6.5 FreeBSD Telnetd远程溢出漏洞的应用 6.5.1 所需工具 6.5.2 攻击步骤 6.5.3 解决办法 6.6 AIX远程溢出漏洞的应用 6.6.1 所需工具 6.6.2 攻击步骤 6.7 UNIX-Linux系统的LOG日志文件 第7章 普通用户网上防黑 7.1 木马的防范 7.1.1 特洛伊木马简介 7.1.2 特洛伊木马的原理 7.1.3 木马的入侵方式 7.1.4 木马的清除 7.1.5 注意事项 7.2 NetBIOS共享漏洞的防范 7.2.1 NetBIOS共享漏洞介绍 7.2.2 如何防范NetBIOS共享漏洞 7.3 在线病毒的防范 7.3.1 网页里的恶意代码病毒的防范 7.3.2 电子邮件中的病毒的防范 7.4 防火墙推荐 7.4.1 “天网”个人版防火墙系统环境要求 7.4.2 “天网”防火墙的功能及使用 第8章 高级用户网上防黑 8.1 IIS安全配置 8.1.1 IIS安全设置概述 8.1.2 安全配置IIS 8.2 FTP安全配置 8.2.1 FTP安全概述 8.2.2 怎样能安全地配置好FTP服务 8.3 各种日志审核配置 8.4 SMTP安全配置 8.4.1 SMTP服务概述 8.4.2 配置SMTP服务器 8.5 其他安全配置 8.5.1 定制自己的Windows 2000 Server 8.5.2 正确安装Windows 2000 Server 8.5.3 安全配置Windows 2000 Server 8.5.4 需要注意的一些事情 第9章 反黑大行动——与黑客过招 9.1 通过分析日志查找黑客 9.1.1 完整的日志有什么用处 9.1.2 怎样通过日志查找黑客 9.1.3 养成查日志的习惯 9.2 找出木马背后的黑手 9.2.1 反弹端口木马的原理 9.2.2 使用监听工具查木马 9.3 反监听——追踪黑客 9.3.1 怎样发现黑客 9.3.2 怎样防止被Sniffer 附录A 常用端口对照表 附录B 经典黑客站点推荐 附录C 经典安全站点推荐

# 《防黑档案》

## 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:[www.tushu000.com](http://www.tushu000.com)