

#### 图书基本信息

书名：<<Linux黑客大曝光(Linux安全机密与解决方案)>>

13位ISBN编号：9787302058762

10位ISBN编号：7302058768

出版时间：2002-10-1

出版时间：清华大学出版社

作者：Brian Hatch,George Kurtz,James Lee

页数：554

字数：661

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：<http://www.tushu007.com>

## 内容概要

全书以step-by-step的方式详细讨论了黑客的攻击方法，其中包括黑客收集信息、确定目标、提升权限、获得控制、架设后门和掩盖踪迹的方法；并述及各个Linux发布版本的安全特点及其细节，包括RedHat Linux，SuSE，Debian和Slackware。

全书注重案例分析，讲解了很多具体攻击的过程，更重要的是对几乎所有讨论过的攻击手段都提供了相应的对策。

本书是安全漏洞的宝典，是负责Linux安全保障工作的网络管理员和系统管理员的必读之书，也可作为信息管理员以及对计算机和网络安全感兴趣的人员的重要参考书。

## 作者简介

Brian Hatch——Onsight公司 ( <http://www.onsight.com> ) 的首席黑客，他是一位Unix/Linux和网络安全顾问。

他的客户遍及各主要银行、制药公司、教育机构，以及加利福尼亚主要的Web浏览器开发商和幸存的网络公司。

Hatch先生通过Onsight向各个企业讲授安全、Unix和程序

书籍目录

前言

第1部分 锁定Linux目标

第1章 Linux安全问题概述 3

1.1 黑客为什么想成为root用户 4

1.2 开放源代码运动 5

1.3 Linux用户 7

1.3.1 /etc/passwd 7

1.3.2 为用户分配权限 10

1.3.3 其他安全性控制 21

1.4 小结 23

第2章 预防措施与从入侵中恢复 25

2.1 预防措施 26

2.1.1 弱点扫描程序 26

2.1.2 扫描检测器 31

2.1.3 加固系统 34

2.1.4 日志文件分析 37

2.1.5 文件系统完整性检查 47

2.2 从黑客攻击中恢复 60

2.2.1 如何知道系统何时被黑 61

2.2.2 被入侵后应采取的措施 63

2.3 小结 68

第3章 对机器和网络踩点 69

3.1 在线搜索 70

3.2 whois数据库 73

3.3 ping扫射 78

3.4 DNS问题 81

3.4.1 DNS查找举例 82

3.4.2 DNS查询的安全问题 83

3.4.3 DNSSEC 88

3.5 traceroutes 89

3.6 端口扫描 91

3.7 操作系统检测 101

3.7.1 主动协议栈指纹 103

3.7.2 被动协议栈指纹 107

3.8 枚举RPC服务 109

3.9 通过NFS的文件共享 112

3.10 简单网络管理协议 (SNMP) 115

3.11 网络漏洞扫描程序 119

3.12 小结 127

第2部分 由外入内

第4章 社交工程、特洛伊木马和其他黑客伎俩 131

4.1 社交工程 (Social Engineering) 132

4.1.1 社交工程种类 133

4.1.2 怎样避免遭受社交工程攻击 137

4.1.3 黑客的家庭作业 138

- 4.2 特洛伊木马 139
- 4.3 病毒和蠕虫 148
  - 4.3.1 病毒和蠕虫的传播方式 149
  - 4.3.2 病毒和Linux 149
  - 4.3.3 蠕虫和Linux 150
- 4.4 IRC后门 154
- 4.5 小结 155
- 第5章 物理攻击 157
  - 5.1 攻击办公室 158
  - 5.2 启动权限是root权限 165
  - 5.3 加密文件系统 175
  - 5.4 小结 176
- 第6章 网络攻击 179
  - 6.1 使用网络 180
    - 6.1.1 TCP/IP网络 180
    - 6.1.2 公共电话网络 186
    - 6.1.3 默认或有害的配置 187
    - 6.1.4 NFS加载 187
    - 6.1.5 Netscape 默认配置 189
    - 6.1.6 Squid 189
    - 6.1.7 X Windows 系统 190
  - 6.2 默认口令 192
  - 6.3 嗅探网络信息 194
    - 6.3.1 嗅探器的工作方式 194
    - 6.3.2 常见的嗅探器 195
  - 6.4 口令猜测 198
  - 6.5 漏洞 201
    - 6.5.1 缓冲区溢出 201
    - 6.5.2 服务漏洞 202
    - 6.5.3 脚本漏洞 203
  - 6.6 不必要的服务 204
    - 6.6.1 使用Netstat 205
    - 6.6.2 使用Lsof 207
    - 6.6.3 使用Nmap识别服务 208
    - 6.6.4 关闭服务 209
  - 6.7 小结 211
- 第7章 恶意使用网络 213
  - 7.1 DNS攻击 214
  - 7.2 路由问题 219
  - 7.3 高级嗅探和会话劫持 222
    - 7.3.1 Hunt 223
    - 7.3.2 Dsniff 228
    - 7.3.3 中间人攻击 229
  - 7.4 拒绝服务攻击 234
    - 7.4.1 潮涌 (Flood) 235
    - 7.4.2 TCP/IP攻击 239
  - 7.5 滥用信任关系 241

- 7.6 实施出口过滤 244
- 7.7 小结 246
- 第3部分 本地用户攻击
- 第8章 提升用户权限 249
  - 8.1 用户和权限 250
  - 8.2 可信路径和特洛伊木马 252
  - 8.3 口令存储和使用 255
  - 8.4 组成员 259
    - 8.4.1 特殊用途组和设备访问 260
    - 8.4.2 wheel组 261
  - 8.5 SUDO 262
  - 8.6 setuserid程序 267
  - 8.7 针对编程错误的攻击 274
    - 8.7.1 硬链接和符号链接 276
    - 8.7.2 输入验证 283
  - 8.8 小结 285
- 第9章 口令破解 287
  - 9.1 Linux上口令的工作方式 288
    - 9.1.1 /etc/passwd 288
    - 9.1.2 Linux加密算法 290
  - 9.2 口令破解程序 293
    - 9.2.1 其他破解程序 302
    - 9.2.2 字典的有效性 303
  - 9.3 阴影口令和/etc/shadow 304
    - 9.3.1 阴影口令说明 304
    - 9.3.2 阴影口令命令组 307
  - 9.4 Apache口令文件 308
  - 9.5 Pluggable Authentication Modules 309
  - 9.6 口令保护 310
  - 9.7 小结 319
- 第10章 黑客保持通道的方法 321
  - 10.1 基于主机的认证和用户访问 322
  - 10.2 使用远程命令的无口令远程访问 330
  - 10.3 使用Ssh的无口令登录 333
  - 10.4 可从网络访问的root shell 336
  - 10.5 木马化的系统程序 345
    - 10.5.1 踪迹隐藏 346
    - 10.5.2 后门 352
  - 10.6 入侵内核 360
  - 10.7 rootkit 371
  - 10.8 小结 374
- 第4部分 服务器安全问题
- 第11章 邮件和FTP安全性 379
  - 11.1 MAIL安全性 380
    - 11.1.1 MTA 381
    - 11.1.2 邮件服务器漏洞 383
  - 11.2 文件传输协议 (FTP) 402

- 11.2.1 FTP协议 402
- 11.2.2 FTP会话范例 403
- 11.2.3 主动FTP模式 404
- 11.2.4 被动FTP模式 405
- 11.2.5 通过第三方FTP服务器进行端口扫描 409
- 11.2.6 启用第三方FTP 418
- 11.2.7 不安全的有状态FTP防火墙规则 422
- 11.2.8 匿名FTP问题 425
- 11.3 小结 426
- 11.3.1 邮件服务器 426
- 11.3.2 FTP 427
- 第12章 Web服务和动态页面 429
- 12.1 生成HTTP请求 430
- 12.2 Apache Web服务器 438
- 12.3 CGI程序问题 452
- 12.4 其他Linux Web服务器 470
- 12.5 小结 471
- 第13章 访问控制和防火墙 473
- 13.1 inetd和xinetd概述 474
- 13.1.1 inetd 474
- 13.1.2 xinetd 476
- 13.2 防火墙：内核级访问控制 490
- 13.2.1 防火墙类型 490
- 13.2.2 Linux包过滤 492
- 13.2.3 阻塞特定的网络访问 494
- 13.2.4 防火墙策略 497
- 13.2.5 防火墙产品 500
- 13.3 小结 501
- 第5部分 附录
- 附录A 保持你的程序为最新版本 505
- A.1 Red Hat的RPM 506
- A.2 Debian 的DPKG和APT 508
- A.3 Slackware包 511
- 附录B 关闭不必要的服务 513
- B.1 运行级别 514
- B.2 关闭特定服务 515
- B.2.1 Red Hat 516
- B.2.2 SuSE 517
- B.2.3 Inetd网络服务 520
- 附录C 在线资源 521
- C.1 开发商邮件列表 522
- C.2 其他安全问题邮件列表 522
- C.3 安全问题和黑客Web站点 523
- C.4 新闻组 524
- C.5 Linux黑客大曝光Web站点 524
- 附录D 案例研究 525
- D.1 案例研究A 526

- D.1.1 背景 526
- D.1.2 侦察 527
- D.1.3 尝试登录 528
- D.1.4 寻找另一扇门 529
- D.1.5 驱逐入侵者 530
- D.2 案例研究B 531
  - D.2.1 锁定目标 532
  - D.2.2 勘探网络 533
  - D.2.3 进入 533
  - D.2.4 进入服务器机房 533
  - D.2.5 侵入监控主机 534
  - D.2.6 研究被侵入的主机 534
  - D.2.7 嗅探网络 537
  - D.2.8 监视日志 538
  - D.2.9 关闭嗅探 539
  - D.2.10 现在, 到哪里去 539
  - D.2.11 追逐 540
  - D.2.12 离开, 但并非永远 540
- D.3 案例研究C 540
  - D.3.1 扫描机器 541
  - D.3.2 探测sendmail 542
  - D.3.3 探测Web服务器 542
  - D.3.4 查找CGI程序 544
  - D.3.5 攻击CGI程序 544
  - D.3.6 隐藏踪迹 547
  - D.3.7 创建持久连接 549
  - D.3.8 防火墙冲突 550
  - D.3.9 从本地帐号入侵 551
  - D.3.10 扫描其他网络服务, 发现目标 552
  - D.3.11 攻击FTP服务器 553
  - D.3.12 把问题打包 554

#### 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:<http://www.tushu007.com>