

黑客攻防实战入门



[黑客攻防实战入门_下载链接1](#)

著者:邓吉

出版者:电子工业出版社

出版时间:2011-4

装帧:

isbn:9787121127021

《黑客攻防实战入门(第3版)》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。《黑客攻防实战入门(第3版)》共分为8章，系统地介绍了入侵的全部过程，以及相应的防御措施和方法。其中包括信息的收集与扫描、本地入侵、木马圈套、远程控制、web攻击、路由器盗用、入侵无线网、qq攻防技术。《黑客攻防实战入门(第3版)》用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，保卫网络安全。

《黑客攻防实战入门(第3版)》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学习资料和参考资料。

作者介绍:

目录: 第1章 信息收集与扫描 1

1.1 网站信息收集 2

1.1.1 相关知识 2

1.1.2 信息收集 6

1.1.3 网站注册信息收集 12

1.1.4 结构探测 17

1.1.5 收索引擎 22

1.2 资源扫描器 25

1.2.1 共享资源简介 25

1.2.2 共享资源扫描器 26

1.2.3 利用共享资源入侵 29

1.2.4 ftp资源扫描器 31

1.2.5 安全解决方案 31

1.2.6 常见问题与解答 32

1.3 端口扫描器 32

1.3.1 网络基础知识 32

1.3.2 端口扫描原理 36

1.3.3 端口扫描应用 37

1.3.4 操作系统识别 40

1.3.5 常见问题与解答 41

1.4 综合扫描器 41

1.4.1 x-scan 41

1.4.2 流光fluxay 46

1.4.3 x-way 50

1.4.4 nmap 52

1.4.5 扫描器综合性能比较 58

1.4.6 常见问题与解答 58

1.5 小结 60

第2章 本地入侵 61

2.1 基础知识 61

2.2 盘载操作系统简介 62

2.3 erd commander 62

2.3.1 erd commander简介 62

2.3.2 利用erd commander进行入侵的实例 62

2.4 windows 69

2.4.1 windows pe简介 69

2.4.2 利用windows pe入侵本地主机的3个实例 69

2.5 安全解决方案 76

2.6 本章小结	76
第3章 木马圈套	77
3.1 木马的工作原理	78
3.1.1 木马是如何工作的	78
3.1.2 木马的隐藏	79
3.1.3 木马是如何启动的	80
3.1.4 黑客如何欺骗用户运行木马	83
3.2 木马的种类	84
3.3 木马的演变	86
3.4 第二代木马	87
3.4.1 冰河	87
3.4.2 广外女生	94
3.5 第三代与第四代木马	98
3.5.1 木马连接方式	98
3.5.2 第三代木马——灰鸽子	100
3.5.3 第四代木马	106
3.5.4 常见问题与解答	113
3.6 木马防杀技术	113
3.7 种植木马	118
3.7.1 修改图标	118
3.7.2 文件合并	118
3.7.3 文件夹木马	121
3.7.4 安全解决方案	124
3.7.5 常见问题与解答	125
3.8 常见木马的手动清除	125
3.8.1 冰河木马的清除	125
3.8.2 shareqq木马的清除	126
3.8.3 bladerunner木马的清除	126
3.8.4 广外女生的清除	126
3.8.5 brainspy木马的清除	127
3.8.6 funnyflash木马的清除	127
3.8.7 qq密码侦探特别版木马的清除	128
3.8.8 iethief木马的清除	128
3.8.9 qeyes潜伏者的清除	128
3.8.10 蓝色火焰的清除	128
3.8.11 back construction木马的清除	129
3.9 小结	129
第4章 远程控制	130
4.1 dameware入侵实例	130
4.1.1 dameware简介	130
4.1.2 dameware的安装	131
4.1.3 dameware的使用	131
4.2 radmin入侵实例	146
4.2.1 radmin简介	146
4.2.2 radmin的安装	146
4.2.3 radmin的使用	147
4.3 vnc入侵实例	150
4.3.1 vnc简介	150
4.3.2 vnc的安装	150
4.4 其他远程控制软件	153
4.5 小结	154
第5章 web攻击	155
5.1 web欺骗攻击	155
5.1.1 网络钓鱼	155

5.1.2 基于页面的web欺骗	163
5.1.3 基于程序的web欺骗	167
5.2 sql 注入	172
5.2.1 测试环境的搭建	172
5.2.2 一个简单的实例	176
5.2.3 用浏览器直接提交数据	181
5.2.4 注入漏洞的利用	184
5.2.5 注入漏洞的高级利用	189
5.2.6 对very-zone sql注入漏洞的利用	196
5.2.7 对动易商城2006 sql注入漏洞的利用	200
5.2.8 使用工具进行sql注入	206
5.2.9 对sql注入漏洞的防御	211
5.3 跨站脚本攻击	213
5.3.1 跨站的来源	214
5.3.2 简单留言本的跨站漏洞	215
5.3.3 跨站漏洞的利用	217
5.3.4 未雨绸缪——对跨站漏洞预防和防御	225
5.4 web后门及加密隐藏	227
5.4.1 什么是web后门	227
5.4.2 web后门免杀	228
5.4.3 web后门的隐藏	229
5.5 web权限提升	234
5.5.1 系统漏洞提权	234
5.5.2 第三方软件权限提权	236
5.5.3 配置不当提升系统权限（陷阱式提权）	241
5.6 小结	248
第6章 盗用路由器	249
6.1 路由器介绍	249
6.1.1 什么是路由器	249
6.1.2 路由器与集线器、交换机的区别	250
6.1.3 路由器的种类	251
6.2 adsl家庭路由	252
6.2.1 默认口令入侵	252
6.2.2 通过adsl路由器入侵内网	256
6.3 入侵 cisco 路由器	260
6.3.1 cisco路由器基础	260
6.3.2 snmp配置缺陷入侵cisco路由器	267
6.4 小结	275
第7章 入侵无线网	276
7.1 无线威胁概述	276
7.1.1 无线网络基本知识	276
7.1.2 什么是无线威胁	277
7.2 无线广播 ssid	279
7.3 wi-fi功能漏洞	281
7.4 比较wep与wpa	282
7.5 无线网络配置实例	286
7.6 leap	291
7.7 攻陷wep	293
7.8 小结	299
第8章 qq攻防	300
8.1 qq漏洞简介	300
8.2 盗取qq号码	301
8.2.1 “广外幽灵”盗qq	301
8.2.2 “qqexplorer”盗qq	304

8.2.3 “挖掘鸡” 306
8.2.4 其他号码盗窃程序 307
8.3 如何保护qq密码 308
8.4 小结 311
附录A 端口一览表 312
· · · · · (收起)

[黑客攻防实战入门_下载链接1](#)

标签

黑客

安全

评论

[黑客攻防实战入门_下载链接1](#)

书评

[黑客攻防实战入门_下载链接1](#)