

《黑客攻防实战入门》

图书基本信息

书名：《黑客攻防实战入门》

13位ISBN编号：9787121127021

10位ISBN编号：7121127024

出版时间：2011-4

出版社：电子工业

作者：邓吉

页数：320

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

《黑客攻防实战入门》

内容概要

《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。

《黑客攻防实战入门》

作者简介

邓吉，原国内著名黑客组织成员，著有《黑客攻防实战入门》，《黑客攻防实战详解》，《黑客攻防实战进阶》，《黑客攻防实战编程》，《网络安全攻防实战》。2000—2004年就读于大连理工大学电子系，目前从事网络安全解决方案与嵌入式产品方面的研发工作。

书籍目录

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 搜索引擎	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

章节摘录

版权页：插图：《孙子兵法》云：“知己知彼，百战不殆。”在网络这个没有硝烟的战场上，入侵者在入侵之前都会想方设法收集尽可能多的信息，甚至是网络管理员的私人邮箱和住宅电话。入侵者始终坚信着这样一个信条：“无论目标网络的规模有多大、安全指数有多高，只要是人类参与设计的网络就必然存在着人为因素，而任何人为因素都有可能网络设计的缺陷。”入侵者很清楚，自己的任务就是去发掘这些被常人忽略的缺陷。事实也证明，入侵者获得的信息越多，他们发现的漏洞也就越多，侵入网络的可能性就越大。成熟的入侵者犹如经验丰富的猎豹，他们花费在信息收集上的时间往往是最多的，而真正的入侵只需一刹那。信息收集、筛选、分析、再收集、再筛选、再分析是入侵者最重要、最枯燥的工作。网络中的计算机也就是在这个阶段被入侵者一览无余的。不妨举个简单的例子来说明信息收集对入侵者的重要性。前些天，笔者偶然在论坛上看见一个网管询问“如何去掉某服务器的默认密码”的帖子，从中可以知道该管理员所管辖网络的脆弱之处，甚至可以根据该网管的技术水平来推断该网络的总体安全指数。如果这个帖子被那些“感兴趣”的人发现，该服务器的命运就可想而知了。可见，仅仅是一个小小的帖子就极有可能导致该服务器，甚至整个网络崩溃。然而在如此浩渺的网络海洋中，如何在不可计量的信息中找到这张帖子也是一门技术。那么，入侵者在正式入侵之前都要收集哪些信息，又是如何收集的呢？

《黑客攻防实战入门》

编辑推荐

《黑客攻防实战入门(第3版)》揭示了：入侵者如何实现信息的收集；入侵者如何通过获取的信息打开目标服务器的切入点(基于身份验证、漏洞、木马的入侵)；入侵者如何实现入侵即远程连接；入侵者入侵后如何执行各种任务；入侵者如何留下后门以便再次进入系统；入侵者如何清除系统日志防止目标服务器发现入侵痕迹；入侵者如何实现从信息扫描到入侵过程中的隐身保护。

《黑客攻防实战入门》

精彩短评

- 1、不错，就是没有一层塑料包装暖，害的书差点就弄脏了
- 2、课程要求参考书，很不错，但是感觉技术方面讲的差不多啊
- 3、很实用的入门黑客教材!
- 4、都什麼年代了，還說1.4.1 x-scan1.4.2 流光fluxay1.4.3 x-way這些過時的東西。

《黑客攻防实战入门》

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