

丛书累计销量**40**万册

快速掌握 知识技巧 一应俱全

书盘结合 互动教学 视频讲解

生动有趣 全彩印刷 易看易学



新手学

黑客攻防入门

新鲜版

华诚科技
编著



全彩印刷版



视频教学



机械工业出版社
China Machine Press



新手学

黑客攻防入门

华诚科技 编著



机械工业出版社
China Machine Press

无论您是普通的计算机爱好者、企业员工，还是公务员，互联网已经和我们的生活、工作和学习紧密地联系到了一起，并且发挥的作用越来越大。然而，黑客的存在却让互联网中的每一台计算机都随时处于危险的边缘。

本书是指导初学者学习黑客攻防的入门书籍，书中详细地介绍了黑客经常使用的入侵手段和工具，把黑客入侵的整个过程展现在读者面前。同时讲解防御这些攻击时读者必须掌握的基础知识、使用方法和操作步骤，帮助读者在起步的过程中走弯路。本书共分为 13 章，分别介绍了黑客攻防基础知识、黑客入侵的前奏——嗅探与扫描、病毒木马的植入与清除、远程控制技术、网络攻击与欺骗技术、黑客隐匿与追踪技术、漏洞攻防实战、网页攻防实战、邮件攻防实战、QQ 攻防实战、局域网攻防实战、系统清理与安全性能提升、系统安全防护技术等内容。

本书中加入“温馨提示”配套讲解，在每章的最后以问答的形式列举了在与黑客攻防实战中遇到的与本章内容相关的问题。

本书特别适合学习黑客攻防的入门级用户，无论是个人计算机爱好者、企业技术人员，还是政府机构人员。本书也可作为计算机维护与管理人员或大专院校师生的技术参考书籍。

封底无防伪标均为盗版

版权所有，侵权必究

本书法律顾问 北京市展达律师事务所

图书在版编目 (CIP) 数据

黑客攻防入门 / 华诚科技编著. —北京: 机械工业出版社, 2012.11
(新手易学)

ISBN 978-7-111-39808-0

I. 黑… II. 华… III. 计算机网络—安全技术 IV. TP393.08

中国版本图书馆CIP数据核字 (2012) 第221914号

机械工业出版社 (北京市西城区百万庄大街 22 号 邮政编码 100037)

责任编辑: 陈佳媛

中国电影出版社印刷厂印刷

2013 年 1 月第 1 版第 1 次印刷

147mm×210mm·7.125 印张

标准书号: ISBN 978-7-111-39808-0

ISBN 978-7-89433-658-3 (光盘)

定价: 39.00 元 (附光盘)

凡购本书, 如有缺页、倒页、脱页, 由本社发行部调换

客服热线: (010) 88378991; 88361066

购书热线: (010) 68326294; 88379649; 68995259

投稿热线: (010) 88379604

读者信箱: hzsj@hzbook.com

前言

随着互联网技术的飞速发展，人们在享受网络带来的方便与快捷的同时，殊不知看不见的网络的另一端或许正有黑客在窥视自己的电脑。我们的数据、账户、敏感信息无不处于危险的边缘。为了防止电脑因被黑客入侵而造成不可挽回的损失，我们必须了解黑客常用的入侵方式及相应的防范措施。随着系统的升级换代，黑客的入侵手段也会发生微妙的变化，本书就是为了满足用户了解黑客最新的入侵方式及学习相应的防范措施这方面的需求而编写的。

主要内容

本书包括：黑客攻防基础知识、黑客入侵的前奏——嗅探与扫描、病毒木马的植入与清除、远程控制技术、网络攻击与欺骗技术、黑客隐匿与追踪技术、漏洞攻防实战、网页攻防实战、邮件攻防实战、QQ 攻防实战、局域网攻防实战、系统清理与安全性能提升、系统安全防御技术等。

本书特色

简单易懂——从新手的角度出发，按部就班地将黑客入侵的步骤和方法娓娓道来，使读者不仅可以轻松掌握有关网络安全知识，还可在

不知不觉中快速提升网络安全防范的实战技巧。

内容丰富多彩——在书中包含了“温馨提示”和“新手提升”等内容，在讲解相关操作的同时，补充了其他相关知识点。

新手常见问题——在每章的最后都有“新手常见问题”内容，对新手在学习黑客相关知识和对黑客入侵进行防御时遇到的常见问题进行了总结，并给出了相应的解答。

读者对象

本书内容全面、讲解充分，融入了作者的实际学习和操作心得，可以作为计算机新手防御黑客的自学参考书籍，也可作为企业、政府用户在使用计算机过程中保护计算机不受黑客入侵以及了解自己不足的一本书。

希望本书对广大读者朋友有所帮助。由于时间仓促，作者水平有限，书中难免存在疏漏和不足之处，欢迎各位读者朋友批评指正，并提出宝贵意见。

更多精彩图书和丰富资讯可访问 www.epubhome.com。

编者

2012年8月

目 录

前言

第1章 黑客攻防基础知识	1
1.1 认识黑客	2
1.2 网络攻击基础——认识网络协议	3
1.2.1 网络连接标准接口——TCP/IP协议	3
1.2.2 ARP欺骗攻击必知——ARP协议	3
1.2.3 洪水攻击必知——ICMP协议	4
1.3 黑客必经的两道门——IP地址与端口	5
1.3.1 IP地址与端口概述	5
1.3.2 设置IP地址	7
1.3.3 查看端口	9
1.3.4 关闭端口	9
1.4 认识系统进程	11
1.4.1 系统进程概述	11
1.4.2 关闭与新建系统进程	12
1.5 黑客常用的DOS命令	14
1.5.1 使用ping命令查看网络连接	14
1.5.2 使用netstat命令检测当前端口	15
1.5.3 使用ipconfig命令查看TCP/IP配置	17
1.5.4 使用net命令管理网络环境	17

- | | |
|------------------------|----|
| 1. 成为一名黑客需要满足哪些条件? | 19 |
| 2. 什么是SMTP协议? | 19 |
| 3. 能否利用“任务管理器”窗口来实现关机? | 19 |
| 4. 如何使用telnet命令进行远程登录? | 19 |

第2章 黑客入侵的前奏——嗅探与扫描 21

- | | | | |
|-------------------------|----|----------------------|----|
| 2.1 搭建虚拟环境 | 22 | 数据包 | 26 |
| 2.1.1 在VMware上新建虚拟机 | 22 | 2.2.2 使用影音神探监测网络 | 30 |
| 2.1.2 在VMware虚拟机中安装操作系统 | 24 | 2.3 黑客扫描端口必备的工具 | 31 |
| 2.2 黑客常用的嗅探工具 | 25 | 2.3.1 端口扫描的原理 | 31 |
| 2.2.1 使用Sniffer Pro截获 | | 2.3.2 使用X-Scan扫描器 | 32 |
| | | 2.3.3 使用SuperScan扫描器 | 35 |

- | | |
|------------------------------|----|
| 1. 如何在VMware中安装VMware Tools? | 37 |
| 2. 如何获取局域网中目标主机的IP地址? | 37 |
| 3. 能否根据IP地址查看其地理位置? | 38 |
| 4. 防范嗅探的常用方式有哪些? | 38 |

第3章 病毒木马的植入与清除 39

- | | | | |
|---------------|----|---------------------|----|
| 3.1 木马的概念 | 40 | 3.4 了解冰河木马的工作原理 | 48 |
| 3.1.1 木马工作原理 | 40 | 3.5 防范计算机木马与病毒的常见措施 | 55 |
| 3.1.2 常见木马分类 | 41 | 3.5.1 防范木马入侵的常见措施 | 56 |
| 3.2 认识病毒 | 42 | 3.5.2 防范计算机病毒的常用技巧 | 56 |
| 3.2.1 病毒概述 | 42 | | |
| 3.2.2 病毒的工作原理 | 45 | | |
| 3.3 捆绑木马的制作方法 | 45 | | |

- | | |
|---------------------|----|
| 1. 木马的伪装手段有哪些? | 57 |
| 2. 计算机中木马后的症状有哪些? | 58 |
| 3. “熊猫烧香”是一类什么样的病毒? | 58 |
| 4. 清除病毒木马的常用软件有哪些? | 58 |

第4章 远程控制技术 59

- | | | | |
|-------------------|----|-------------------------|----|
| 4.1 利用QQ实现远程协助 | 60 | 监控工具 | 62 |
| 4.1.1 让好友操控自己的计算机 | 60 | 4.2.1 使用“远程控制任我行”实现远程控制 | 62 |
| 4.1.2 远程操控好友的计算机 | 61 | 4.2.2 使用“网络法官”实时监控局域网 | 67 |
| 4.2 认识其他常见的远程 | | | |

- | | |
|----------------------|----|
| 1. 远程控制的原理是什么? | 72 |
| 2. 常见的远程控制类别有哪些? | 72 |
| 3. 如何利用注册表实现远程监控? | 72 |
| 4. 系统中存在与远程控制相关的服务吗? | 73 |

第5章 网络攻击与欺骗技术 74

- | | | | |
|------------------------|----|----------------------|----|
| 5.1 网络攻击概述 | 75 | 模拟ARP欺骗 | 79 |
| 5.1.1 黑客常用的网络攻击方式 | 75 | 5.2.3 使用防火墙防御ARP攻击 | 81 |
| 5.1.2 防范网络攻击的措施 | 76 | 5.3 DNS欺骗攻击 | 84 |
| 5.2 ARP欺骗攻击 | 78 | 5.3.1 DNS欺骗攻击的原理 | 84 |
| 5.2.1 ARP欺骗攻击原理 | 78 | 5.3.2 使用网络守护神防御DNS攻击 | 84 |
| 5.2.2 使用WinArpAttacker | | | |

- | | |
|------------------|----|
| 1. IP欺骗攻击是怎么一回事? | 86 |
| 2. DDoS攻击是怎么一回事? | 86 |
| 3. 如何防范IP欺骗工具? | 87 |
| 4. 如何防范DDoS攻击? | 87 |

第6章 黑客隐藏与追踪技术 88

- | | | | |
|------------------------------|----|------------------------------|-----|
| 6.1 入侵隐藏技术 | 89 | 6.3 黑客追踪工具 | 97 |
| 6.1.1 跳板技术概述 | 89 | 6.3.1 使用NeoTrace Pro
追踪工具 | 97 |
| 6.1.2 代理服务器概述 | 90 | 6.3.2 使用IP搜索客 | 99 |
| 6.2 跳板与代理服务器的
使用与防范 | 91 | 6.4 清除自己留下的痕迹 | 100 |
| 6.2.1 利用“代理猎手”
找代理 | 91 | 6.4.1 手动清除系统日志 | 101 |
| 6.2.2 使用SocksCap32
设置动态代理 | 94 | 6.4.2 使用拟处理清除
系统日志 | 102 |

- | | |
|---------------------|-----|
| 1. 什么是端口重定向? | 102 |
| 2. 什么是Windows事件日志? | 103 |
| 3. 如何防范黑客的远程跳板代理攻击? | 103 |
| 4. IP追踪的原理是什么? | 103 |

第7章 漏洞攻防实战 104

- | | | | |
|-------------------|-----|----------------------|-----|
| 7.1 漏洞攻击基础 | 105 | 实施入侵 | 107 |
| 7.1.1 常见的系统漏洞 | 105 | 7.2.2 SAM数据库漏洞
入侵 | 108 |
| 7.1.2 常见的网站漏洞 | 106 | 7.3 认识黑客常用的注入
工具 | 109 |
| 7.2 常见漏洞入侵实例 | 107 | | |
| 7.2.1 利用Unicode漏洞 | | | |

7.3.1 使用啊D注入工具	109	留下后门	114
7.3.2 使用NBSI注入工具	111	7.5 查漏补缺, 防范漏洞入侵	115
7.4 黑客开启后门的常用工具	113	7.5.1 安装补丁	115
7.4.1 后门概述	113	7.5.2 常用的防范措施	116
7.4.2 用Shift后门生成器			

1. 为什么Windows系统会存在漏洞?	117
2. 什么是IPC \$ 漏洞?	117
3. 如何使用Windows Update安装系统补丁?	118
4. “360安全卫士”为系统安装的补丁文件是从哪儿来的?	118

第8章 网页攻防实战

119

8.1 网页攻击概述	120	8.2.3 网页恶意代码攻击的形式	125
8.1.1 网页攻击的危害	120	8.3 网页恶意代码的修复与防范	129
8.1.2 网页攻击的防范措施	121	8.3.1 网页恶意代码修复	129
8.2 网页恶意代码概述	124	8.3.2 网页恶意代码防范	130
8.2.1 认识网页恶意代码	124		
8.2.2 网页恶意代码的特点和分类	124		

1. 网页恶意代码的传播方式有哪些?	131
2. 如何避免再次遭到同一网站恶意代码攻击?	132
3. 为何IE浏览器经常遭到攻击?	133
4. 除了IE浏览器外, 还有哪些安全性较高的第三方浏览器?	133

第9章 邮件攻防实战

134

- | | | | |
|-------------------------|-----|---------------------|-----|
| 9.1 邮件炸弹实战 | 135 | 9.2.1 黑雨 | 140 |
| 9.1.1 认识邮件炸弹 | 135 | 9.2.2 流光 | 142 |
| 9.1.2 使用亿虎Email
群发大师 | 135 | 9.3 做好电子邮箱的防御
措施 | 144 |
| 9.1.3 邮件炸弹防范 | 138 | 9.3.1 安全登录电子邮箱 | 144 |
| 9.2 黑客获取邮箱密码的
常用工具 | 140 | 9.3.2 找回被盗的电子
邮箱 | 145 |

新手常见问题

- | | |
|----------------------|-----|
| 1. 邮件攻击的主要方式有哪些? | 146 |
| 2. 邮件攻击具有哪些危害性? | 146 |
| 3. 如何为邮箱设置不易被破解的密码? | 146 |
| 4. 能否在邮箱中设置拒绝陌生人的邮件? | 147 |

第10章 QQ攻防实战

148

- | | | | |
|------------------------|-----|----------------------|-----|
| 10.1 黑客常用的QQ盗号
工具 | 149 | 10.2.1 风云QQ尾巴
生成器 | 159 |
| 10.1.1 QQ简单盗 | 149 | 10.2.2 QQ细胞发送器 | 160 |
| 10.1.2 阿拉QQ密码
潜伏者 | 151 | 10.2.3 飘叶千夫指 | 161 |
| 10.1.3 盗Q黑侠 | 153 | 10.2.4 QQ狙击手 | 162 |
| 10.1.4 QQ密码掠夺者 | 154 | 10.3 QQ安全防范 | 164 |
| 10.1.5 QQ眼睛 | 156 | 10.3.1 QQ密码防盗专家 | 165 |
| 10.2 黑客常用的QQ信息
攻击工具 | 158 | 10.3.2 防范QQ信息攻击 | 166 |
| | | 10.3.3 申请QQ密码保护 | 167 |

- | | |
|------------------------------|-----|
| 1. 能够使用手机号码绑定QQ号码吗? | 168 |
| 2. 如何彻底删除QQ登录信息? | 168 |
| 3. 安装了其他杀毒软件后, 还需要安装QQ电脑管家吗? | 169 |
| 4. QQ被盗后如何找回? | 169 |

第11章 局域网攻防实战

170

- | | | | |
|--------------------|-----|------------------------|-----|
| 11.1 局域网监听的原理与防范 | 171 | 11.3.1 使用LanSee查看局域网信息 | 179 |
| 11.1.1 局域网监听的原理 | 171 | 11.3.2 使用局域网终结者 | 182 |
| 11.1.2 局域网监听的检测与防范 | 172 | 11.3.3 使用网络剪刀手netcut | 183 |
| 11.2 实现局域网挂马 | 174 | 11.3.4 局域网攻击防范措施 | 184 |
| 11.2.1 端口映射概述 | 174 | 11.4 提高无线局域网的安全系数 | 186 |
| 11.2.2 在局域网中挂马 | 175 | | |
| 11.3 局域网攻击与防范 | 179 | | |

- | | |
|----------------------------------|-----|
| 1. 广播风暴是局域网攻击中的一种吗? | 188 |
| 2. 入侵无线局域网的常用手段有哪些? | 188 |
| 3. 除了使用LanSee外, 还有其他的局域网信息查看工具吗? | 188 |
| 4. 能否隐藏无线局域网对应的SSID标识? | 189 |

第12章 系统清理与安全性能提升

190

- | | | | |
|-------------------|-----|--------------------------------|-----|
| 12.1 清除流氓软件 | 191 | 12.2 使用防护间谍软件 | 193 |
| 12.1.1 使用超级兔子清理 | 191 | 12.2.1 使用Windows Defender反间谍软件 | 193 |
| 12.1.2 使用瑞星安全助手清理 | 192 | | |

12.2.2	使用“间谍克星” 反间谍软件	195	12.4	注册表编辑器使用防范	200
12.3	更改组策略	196	12.4.1	禁止访问和编辑 注册表	200
12.3.1	禁止访问指定程序	196	12.4.2	关闭默认共享 保证系统安全	201
12.3.2	禁止从远端关闭 计算机	197	12.4.3	关闭远程注册表 管理服务	203
12.3.3	设置控制面板 显示项目	198			

1.	间谍软件与流氓软件有什么区别?	203
2.	如何为计算机设置开机密码	204
3.	如何为指定账户设置登录密码?	204
4.	能否让计算机认可高安全系数的密码?	204

第13章 系统安全防御技术

205

13.1	防火墙技术	206	13.2.1	使用文件加解密 系统加密文件	209
13.1.1	开启Windows 防火墙	206	13.2.2	Windows EFS加密	210
13.1.2	瑞星防火墙的 应用	207	13.3	使用FinalData恢复 被删除的数据	211
13.2	文件加密技术	208			

1.	防火墙的原理是什么?	213
2.	加密与解密的原理是什么?	213
3.	黑客破解密码的常用工具有哪些?	214
4.	能否恢复从回收站中删除的数据?	214

黑客攻防基础知识

要点导航

- 认识黑客
- 认识常见的网络协议
- IP地址与端口
- 认识系统进程
- 黑客常用的DOS命令

黑客往往会被认为是神秘的、不可琢磨的、难以接近的一类人，他们利用自己熟练的技术使得互联网的安全频频告急，甚至还会使得人们随时在担心自己的系统被黑客入侵。其实，黑客也有高手和菜鸟之分，只要用户了解了黑客的基本手段，一般的黑客是无法入侵您的计算机的。而对于黑客高手来说，可能您的计算机没有让他入侵的价值，所以您不用太担心。

本章将主要介绍什么是黑客，常见的网络协议有哪些，认识IP地址、端口和系统进程以及黑客常用的DOS命令等知识。



1.1 认识黑客

“黑客”是由英文hacker直接音译过来的，可将黑客简单地理解为破坏者。黑客一般都是利用系统或者软件的漏洞入侵用户计算机的。当用户进行了一些较为危险的操作时，就会给黑客创造入侵的机会。

关键词 黑客、骇客、入侵
难度 ★☆☆☆☆

“黑客”一词，原意是指计算机技术水平超高的专家，尤其是指程序设计人员，但到了今天，“黑客”一词已被用于泛指那些专门利用计算机网络搞破坏或恶作剧的家伙，而对这些人正确的英文叫法是cracker，译为“骇客”。黑客与骇客的主要区别是黑客们修补相关漏洞，而骇客们却会抓住这些漏洞对其他计算机进行入侵。

在网络发展初期，网络有关的立法还不够健全，黑客在法律的漏洞下可以为所欲为。目前，世界各国法律的发展速度还是落后于互联网的发展速度，在黑客活动转入地下以后，其攻击的隐蔽性更强，使当前法律和技术缺乏针对网络犯罪卓有成效的法纪和跟踪手段，无规范的黑客活动已经成为网络安全的重要威胁。

温馨提示

“红客”的词源来自于黑客，它是指维护国家利益，不去利用网络技术入侵自己国家的计算机，而是维护正义，为自己国家争光的黑客。在中国，红色有着特定的价值含义，代表正义、道德、进步、强大等。红客是一种精神，它是一种热爱祖国、坚持正义、开拓进取的精神。所以只要具备这种精神，并热爱计算机技术的人都可称为红客。红客通常会利用自己掌握的技术去维护国内网络的安全，并对外来的进攻予以还击。

1.2 网络攻击基础——认识网络协议

网络协议是指为计算机网络中进行数据交换而建立的规则、标准或约定的集合。常见的网络协议有TCP/IP协议、ARP协议、ICMP协议等。

关键词 TCP/IP、ARP、
ICMP
难度 ★☆☆☆☆

1.2.1 网络连接标准接口——TCP/IP协议

TCP/IP协议，全称是Transmission Control Protocol/Internet Protocol，中文译为传输控制协议/因特网互联协议，又叫网络通信协议。众所周知，如今计算机接入互联网后都要设置TCP/IP，因此，TCP/IP协议是互联网最基本的协议，也是国际互联网络的基础。

TCP/IP协议定义了计算机如何连入因特网，以及数据如何在它们之间传输的标准。

TCP/IP包含两层协议，TCP协议和IP协议。其中，高层的TCP协议负责收集信息或者把文件拆分成更小的数据包。发送端将这些数据包通过网络传送到接收端的TCP层，接收端的TCP层把数据包还原为原始文件，而低层的IP协议则处理每个数据包的地址部分，使得网络上的网关计算机能够识别数据包的地址并进行路由选择，让这些数据包能够正确地到达目的地。

1.2.2 ARP欺骗攻击必知——ARP协议

ARP，即地址解析协议，它能够通过已知的IP地址来获取与其对应的物理地址（MAC地址）。在TCP/IP网络环境下，每个主机都被分配了一个32bit（比特）的IP地址（如220.248.138.166），它是在网络中标识主机的一种逻辑地址，如果要成功地将报文（网络中主机之间交换与传输的数据单元）传送给目的主机，则必须知道目的主机的物理地址，此时就可以使用ARP协议将目的主机的IP地址转换为物理地址。

简单地说，ARP协议就是主机在发送报文之前，将目标主机的IP地址转换成与之对应的MAC地址的过程。谈到ARP协议就离不开ARP欺骗，本书将在第5章向读者具体介绍ARP欺骗的工作原理及防范方法。

1.2.3 洪水攻击必知——ICMP协议

ICMP，即Internet控制报文协议，它是TCP/IP协议族中的一个子协议，用于在IP主机、路由器之间传递控制消息。控制消息包括网络不通、主机是否存在、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着非常重要的作用。

ICMP在网络中提供了一致易懂的出错报告信息，它将发送的出错报文返回到发送数据的主机。ICMP唯一的功能是报告问题而不是解决问题，解决问题的任务由发送方完成。

正是这一特点使得它非常容易被用于攻击网络上的路由器和主机。例如Ping Of Death攻击，在还没有发布限制发送ICMP数据包大小的补丁之前，操作系统规定了ICMP数据包的最大尺寸不超过64KB，因此Ping Of Death根据这一规定向主机发起攻击。其攻击原理是：如果ICMP数据包的尺寸超过64KB上限时，主机出现内存分配错误，导致TCP/IP堆栈崩溃，致使主机死机。

温馨提示

洪水攻击是黑客现在比较常用的一种攻击技术，特点是实施简单，威力巨大，大多是无视防御的。最常见的洪水攻击是MAC泛洪。

MAC泛洪是指攻击者进入局域网内，将假冒的源MAC地址和目的MAC地址数据帧发送到以太网上，使得假冒的源MAC地址和目标MAC地址塞满交换机的MAC地址表，导致交换机无法正确地传送数据。