

HACKER  
ATTACK AND DEFENSE

# 黑客攻防

## 从入门到精通

九天科技◎编著

实战  
秘笈版

知识  
丰富

图文  
并茂

案例  
丰富

- 涵盖了黑客攻防知识点，PC端的攻防策略、无线攻防、移动端攻防、手机钱包等内容
- 注重操作，图文并茂，在介绍案例的过程中，每一个操作均有对应的图片示例
- 把知识点融于系统的案例实训中，结合经典案例进行讲解和拓展

微信  
扫一扫  
轻松  
看视  
频



书中关键知识点视频演示，不仅可在PC端播放，还可随时在手机端观看，实现即扫即看

中国铁道出版社  
CHINA RAILWAY PUBLISHING HOUSE

# 黑客攻防

## 从入门到精通

九天科技◎编著

实战  
秘笈版

中国铁道出版社  
CHINA RAILWAY PUBLISHING HOUSE

## 内 容 简 介

本书从黑客“攻”、“防”两个不同的角度出发,深入介绍了黑客经常使用的入侵手段和工具,以及防御黑客攻击所必须掌握的方法、工具和技巧等知识。本书共分为12章,主要内容包括:黑客攻防入门必修,构建虚拟测试环境,黑客常用的DOS命令,黑客攻击目标的扫描与嗅探,远程入侵与控制黑客攻防实战,系统漏洞黑客攻防实战,系统安全黑客攻防实战,账户与密码黑客攻防实战,QQ与电子邮件黑客攻防实战,木马与病毒黑客攻防实战,无线网络及智能手机安全防御,以及网络支付安全防御实战。

本书适合想了解并掌握黑客攻防技术的初学者,以及对黑客攻防与网络安全维护感兴趣的读者学习使用,也可作为IT从业人员、网络安全从业人员及网络管理员的参考用书。

### 图书在版编目(CIP)数据

黑客攻防从入门到精通:实战秘笈版/九天科技编著. —北京:  
中国铁道出版社, 2017. 9  
ISBN 978-7-113-23320-4

I. ①黑… II. ①九… III. ①黑客—网络防御 IV.  
①TP393.081

中国版本图书馆CIP数据核字(2017)第142721号

书 名: 黑客攻防从入门到精通(实战秘笈版)  
作 者: 九天科技 编著

策 划: 苏 茜  
责任编辑: 张 丹  
责任印制: 赵星辰

读者热线电话: 010-63560056

封面设计: **MXK** DESIGN  
STUDIO

出版发行: 中国铁道出版社(北京市西城区右安门西街8号 邮政编码: 100054)  
印 刷: 北京鑫正大印刷有限公司  
版 次: 2017年9月第1版 2017年9月第1次印刷  
开 本: 787mm×1092mm 1/16 印张: 18.75 字数: 597千  
书 号: ISBN 978-7-113-23320-4  
定 价: 49.80元

版权所有 侵权必究

凡购买铁道版图书,如有印制质量问题,请与本社读者服务部联系调换。电话:(010) 51873174

打击盗版举报电话:(010) 51873659

# 前言

## PREFACE

目前网上支付、购物、投资、理财等已经成为人们日常消费生活的重要内容，财产的安全性也越来越受到人们的关注。如果账户、密码被黑客截取，将会带来非常大的经济损失。因此黑客攻击已经成为威胁网络安全的重大隐患之一。随着网络的大范围普及、黑客工具的迅速传播，黑客只需使用简单的工具就能对一些疏于防范的电脑或移动终端进行攻击，并在受侵的电脑或终端中为所欲为。当发现自己的密码被盗、资料被修改或删除、硬盘变成一片空白时再想进行补救，为时已晚。

虽然黑客的攻击手段越来越“高明”，但防御黑客攻击的方法也在不断增强，如果您对黑客攻击和防御还比较陌生，还不了解常用黑客工具的使用方法，对木马程序和远程监控一无所知，不懂无线网络、智能手机与网络支付安全防御，并且经常受到电脑病毒和木马的侵袭，等等。那么请您静下心来阅读本书，它将带您进入变幻莫测的黑客世界。

### 内容导读



本书旨在帮助读者清晰地了解黑客入侵的攻击方式，进而制订出完善的防御方案，同时从另一个完全不同的角度全面解读黑客攻防，深入洞察防御的死角，组织更为严密的防御体系，以应对层出不穷的黑客入侵挑战。

### 主要特色



本书由业内资深信息安全专家精心策划编写，其主要特色如下：

#### ● 从零开始，无师自通

无论您是否在从事电脑行业工作，无论您是否接触过网络，无论您以前是否了解黑客攻防技术，都能从本书中找到适合自己的起始点，开启黑客攻防的学习历程。

#### ● 侧重实战，案例演绎

本书侧重实战技能，摒弃晦涩难懂的技术理论，基于实际案例的分析和操作指导，让读者学习起来更加轻松，操作起来有章可循。

#### ● 图文并茂，易学易用

采用图文结合的方式使读者在学习过程中能够直观、清晰地看到案例操作的过程及效果，以便更快速地理解和掌握。颠覆“看”书的传统观念，变成一本能“操作”、能“上手”的图书。

#### ● 传授经验，私房秘笈

在本书中穿插了大量黑客攻防提示与技巧，且在每章最后均设有“高手私房秘笈”版块，真正帮助读者解决在学习和工作中遇到的各种难题。

## ● 视听视频，模拟课堂

为了增加读者的学习渠道，增强读者的学习兴趣，本书配有超大容量多媒体视听教学视频，读者可以跟着其提供的语音视频进行实战演练，并能快速应用于实际工作中。

### 视频说明



本书随书配有交互式、600 分钟超长播放的多媒体视听教学视频，它是与图书完美结合的视听课堂，让您像看电视一样轻松、直观地进行学习。

如何获取视频教程：

1. “扫一扫”封面上的二维码，在打开的界面上单击本书所对应的下载文件；
2. 选择保存路径后开始下载；

备注：读者只需解压一个文件，即可免费得到全部视频内容。

视频下载地址：<http://www.crphdm.com/2017/0620/13570.shtml>



微信扫一扫  
轻松看视频

视频中超值赠送由本社出版的《全图解电脑软硬件维修实用大全》和《全图解电脑组装与维修实用大全》的视频教程，超大容量，物超所值。

### 适用读者



本书适用面广，适合以下读者学习使用：

- (1) 没有任何电脑黑客攻防知识的初学者；
- (2) 对电脑黑客攻防技术有些了解但不精通的学习者；
- (3) 网络安全从业人员以及网络管理员；
- (4) 大、中专院校的在校学生和社会电脑安全培训机构的学员；
- (5) 想在短时间内掌握电脑安全实用技能的读者朋友。

### 售后服务



如果读者在使用本书的过程中遇到问题或者有好的意见或建议，可以通过发送电子邮件（E-mail: 9335404@qq.com）或者在线 QQ: 843688388 联系我们，我们将及时予以回复，并尽最大努力提供学习上的指导与帮助。

### 特别提醒：

根据国家有关法律规定，任何入侵和窃取他人系统和文件的做法都是违法的，希望读者不要使用本书介绍的黑客技术攻击他人电脑，否则后果自负，特此声明！

编者

2017 年 5 月

## 第 1 章 黑客攻防入门必修

|                         |   |
|-------------------------|---|
| 1.1 黑客揭秘 .....          | 2 |
| 1.1.1 黑客的由来 .....       | 2 |
| 1.1.2 黑客的组成 .....       | 2 |
| 1.1.3 黑客的主要行为 .....     | 3 |
| 1.1.4 黑客术语 .....        | 4 |
| 1. 肉鸡 .....             | 4 |
| 2. 木马 .....             | 4 |
| 3. 网页木马 .....           | 4 |
| 4. 挂马 .....             | 4 |
| 5. 后门 .....             | 4 |
| 6. 端口 .....             | 4 |
| 7. rootkit .....        | 4 |
| 8. IPC\$ .....          | 5 |
| 9. 弱口令 .....            | 5 |
| 10. 默认共享 .....          | 5 |
| 11. 溢出 .....            | 5 |
| 12. shell .....         | 5 |
| 13. WebShell .....      | 5 |
| 14. 注入 .....            | 5 |
| 15. 注入点 .....           | 5 |
| 16. 内网 .....            | 6 |
| 17. 外网 .....            | 6 |
| 18. 免杀 .....            | 6 |
| 19. 加壳 .....            | 6 |
| 20. 花指令 .....           | 6 |
| 21. 嗅探器 (Sniffer) ..... | 6 |
| 22. 蜜罐 .....            | 6 |
| 23. 服务端/客户端 .....       | 6 |
| 1.1.5 黑客攻击的流程 .....     | 6 |
| 1. 扫描漏洞 .....           | 6 |
| 2. 试探漏洞 .....           | 7 |
| 3. 取得权限与提升权限 .....      | 7 |
| 4. 木马入侵 .....           | 7 |
| 5. 建立后门与清理痕迹 .....      | 7 |
| 1.2 认识网络协议 .....        | 7 |
| 1.2.1 TCP/IP 协议 .....   | 7 |
| 1.2.2 IP 协议 .....       | 8 |

|                                   |    |
|-----------------------------------|----|
| 1. IP 地址的基本格式 .....               | 8  |
| 2. IP 地址的分类 .....                 | 9  |
| 1.2.3 TCP 协议 .....                | 10 |
| 1.2.4 UDP 协议 .....                | 11 |
| 1.2.5 ARP 协议 .....                | 11 |
| 1.2.6 ICMP 协议 .....               | 12 |
| 1.3 黑客攻击的入口——端口 .....             | 13 |
| 1.3.1 端口的分类 .....                 | 13 |
| 1. 按端口号分布划分 .....                 | 13 |
| 2. 按通信服务方式划分 .....                | 13 |
| 1.3.2 使用命令查看系统的<br>开放端口 .....     | 14 |
| 1. LISTENING .....                | 15 |
| 2. SYN_SENT (客户端状态) .....         | 15 |
| 3. SYN_RCVD (服务器端状态) .....        | 16 |
| 4. ESTABLISHED .....              | 16 |
| 5. FIN-WAIT-1 .....               | 16 |
| 6. FIN-WAIT-2 .....               | 16 |
| 7. CLOSE-WAIT .....               | 16 |
| 8. CLOSING .....                  | 16 |
| 9. LAST-ACK .....                 | 16 |
| 10. TIME-WAIT .....               | 16 |
| 11. CLOSED .....                  | 17 |
| 1.3.3 使用资源监视器查看系统<br>端口使用情况 ..... | 17 |
| 1.3.4 使用工具软件查看电脑<br>端口 .....      | 17 |
| 1.3.5 关闭不必要的端口 .....              | 18 |
| 1.3.6 限制端口访问 .....                | 19 |
| 1.4 木马藏匿的首选地——系统<br>进程 .....      | 24 |
| 1.4.1 认识系统进程 .....                | 24 |
| 1.4.2 关闭与重建进程 .....               | 25 |
| 1.4.3 使用进程查看工具 .....              | 26 |

### 高手私房秘笈

秘笈 1 更改 IP 地址

秘笈 2 使用进程查看命令 tasklist



## 第2章

### 构建虚拟测试环境

|                             |    |
|-----------------------------|----|
| 2.1 使用 VMware 虚拟系统 .....    | 33 |
| 2.1.1 安装 VMware 虚拟机软件 ..... | 33 |
| 2.1.2 创建虚拟机 .....           | 34 |
| 2.1.3 在虚拟机中安装操作系统 .....     | 37 |
| 2.2 使用系统自带虚拟机 .....         | 42 |
| 2.2.1 启用 Hyper-V 功能 .....   | 42 |
| 2.2.2 创建虚拟机 .....           | 43 |
| 2.2.3 设置虚拟网卡 .....          | 45 |
| 2.2.4 安装虚拟机操作系统 .....       | 47 |

#### 高手私房秘笈

- 秘笈 1 WMware Workstation 与 Hyper-V 不兼容
- 秘笈 2 设置从 U 盘启动 Vmware 虚拟机

## 第3章

### 黑客常用的 DOS 命令

|                                    |    |
|------------------------------------|----|
| 3.1 初识 DOS .....                   | 54 |
| 3.1.1 DOS 系统特征 .....               | 54 |
| 1. DOS 操作特征 .....                  | 54 |
| 2. 文件与目录 .....                     | 54 |
| 3.1.2 认识 Windows 系统中的<br>命令行 ..... | 55 |
| 1. 打开“命令提示符”窗口 .....               | 55 |
| 2. 编辑命令行 .....                     | 56 |
| 3.2 DOS 基本命令 .....                 | 57 |
| 3.2.1 cd 命令 .....                  | 57 |
| 3.2.2 dir 与 tree 命令 .....          | 58 |
| 3.2.3 subst 命令 .....               | 60 |
| 3.2.4 attrib 命令 .....              | 60 |
| 3.2.5 md 和 rd 命令 .....             | 60 |
| 3.2.6 move 命令 .....                | 61 |
| 3.2.7 ren 命令 .....                 | 61 |

|                                    |    |
|------------------------------------|----|
| 3.2.8 type 命令 .....                | 61 |
| 3.2.9 copy 命令 .....                | 62 |
| 1. 复制文件 .....                      | 62 |
| 2. 合并文件 .....                      | 62 |
| 3. 追加信息 .....                      | 64 |
| 4. 批量更改扩展名 .....                   | 64 |
| 3.2.10 xcopy 命令 .....              | 64 |
| 3.2.11 del 命令 .....                | 65 |
| 3.2.12 more 命令 .....               | 65 |
| 3.2.13 cipher 命令 .....             | 66 |
| 1. 加密和解密文件 .....                   | 66 |
| 2. 备份加密证书 .....                    | 67 |
| 3.2.14 find 和 findstr 命令 .....     | 67 |
| 3.3 黑客常用的 DOS 命令 .....             | 68 |
| 3.3.1 查看网络配置的 ipconfig<br>命令 ..... | 68 |
| 3.3.2 测试物理网络的 ping 命令 .....        | 68 |
| 3.3.3 查看网络连接的 netstat<br>命令 .....  | 71 |
| 3.3.4 跃点追踪 tracert 命令 .....        | 71 |
| 3.3.5 传输协议 ftp 命令 .....            | 72 |
| 3.3.6 用户和工作组 net 命令 .....          | 74 |
| 1. net user 命令 .....               | 74 |
| 2. net localgroup 命令 .....         | 75 |
| 3.3.7 多功能网络 net 命令 .....           | 76 |
| 1. net view 命令 .....               | 76 |
| 2. net share 命令 .....              | 77 |
| 3. net use 命令 .....                | 78 |
| 4. 使用 net 命令管理服务 .....             | 79 |

#### 高手私房秘笈

- 秘笈 1 使用外部命令
- 秘笈 2 创建批处理文件

## 第4章

### 黑客攻击目标的扫描与嗅探

|                           |    |
|---------------------------|----|
| 4.1 搜集攻击目标的重要信息 .....     | 83 |
| 4.1.1 确定入侵目标的 IP 地址 ..... | 83 |

|                            |     |                                |     |
|----------------------------|-----|--------------------------------|-----|
| 4.1.2 查看入侵目标所属位置.....      | 83  | 5.1.1 IPC\$入侵与防范.....          | 106 |
| 4.1.3 网站 ICP 备案查询.....     | 84  | 1. 什么是 IPC\$入侵.....            | 106 |
| 4.2 认识扫描器.....             | 85  | 2. IPC\$入侵方式.....              | 106 |
| 4.2.1 扫描器的工作原理.....        | 85  | 3. 创建后门账号.....                 | 107 |
| 4.2.2 扫描器的作用.....          | 85  | 4. IPC\$入侵防范.....              | 108 |
| 4.3 端口扫描器的应用.....          | 85  | 5.1.2 Telnet 入侵.....           | 111 |
| 4.3.1 SuperScan 扫描器.....   | 85  | 5.2 通过注册表入侵.....               | 113 |
| 1. SuperScan 的功能.....      | 86  | 5.2.1 开启远程注册表服务.....           | 113 |
| 2. 使用 SuperScan 扫描信息.....  | 86  | 5.2.2 修改注册表实现远程监控.....         | 114 |
| 4.3.2 Nmap 扫描器.....        | 88  | 5.3 远程桌面控制.....                | 115 |
| 1. Nmap 简介.....            | 88  | 5.3.1 Windows 10 远程协助.....     | 115 |
| 2. Nmap 的安装.....           | 88  | 1. 开启远程桌面连接.....               | 115 |
| 3. 使用 Nmap 扫描信息.....       | 89  | 2. 远程操作电脑.....                 | 116 |
| 4.4 多功能扫描器的应用.....         | 90  | 5.3.2 Windows 10 远程关机.....     | 117 |
| 4.4.1 流光扫描器.....           | 90  | 5.4 使用网络执法官.....               | 118 |
| 1. 探测开放端口.....             | 91  | 5.4.1 网络执法官的功能.....            | 118 |
| 2. 探测目标主机的 IPC\$用户列表.....  | 92  | 1. 实时记录上线用户并<br>存档备查.....      | 118 |
| 4.4.2 SSS 扫描器.....         | 93  | 2. 自动侦测未登记主机接入<br>并报警.....     | 118 |
| 1. 设置功能选项参数.....           | 93  | 3. 限定各主机的 IP, 防止 IP<br>盗用..... | 118 |
| 2. 定制扫描任务.....             | 94  | 4. 限定各主机的连接时段.....             | 118 |
| 3. 扫描系统漏洞.....             | 96  | 5.4.2 认识网络执法官操作界面.....         | 119 |
| 4.4.3 X-Scan 扫描器.....      | 97  | 5.4.3 网络执法官的应用.....            | 120 |
| 4.5 网络嗅探工具的应用.....         | 99  | 5.5 使用远程控制软件.....              | 122 |
| 4.5.1 认识嗅探的原理.....         | 99  | 5.5.1 TeamViewer 的功能.....      | 122 |
| 4.5.2 嗅探利器 SmartSniff..... | 99  | 5.5.2 TeamViewer 的使用.....      | 122 |
| 4.5.3 网络数据包嗅探专家.....       | 100 |                                |     |
| 4.5.4 影音神探.....            | 101 |                                |     |

### 高手私房秘笈

- 秘笈 1 使用局域网查看工具  
秘笈 2 使用命令行下的嗅探器  
WinDump

### 高手私房秘笈

- 秘笈 1 使用聚生网管  
秘笈 2 使用 QQ 远程控制异地电脑

## 第 5 章 远程入侵与控制黑客攻防实战

### 5.1 基于认证入侵..... 106

## 第 6 章 系统漏洞黑客攻防实战

|                    |     |
|--------------------|-----|
| 6.1 认识系统漏洞.....    | 128 |
| 6.1.1 系统漏洞是什么..... | 128 |



|       |                                   |     |
|-------|-----------------------------------|-----|
| 6.1.2 | 系统漏洞产生的原因 .....                   | 128 |
| 6.2   | Windows 7 系统存在的漏洞 .....           | 128 |
| 6.3   | Windows 10 系统存在的漏洞 .....          | 129 |
| 6.3.1 | Adobe Flash Player 漏洞 .....       | 130 |
| 6.3.2 | IE 漏洞 .....                       | 130 |
| 6.3.3 | Microsoft Windows SMB 服务器漏洞 ..... | 131 |
| 6.3.4 | 浏览器远程内存损坏漏洞 .....                 | 132 |
| 6.3.5 | Microsoft Office 内存损坏漏洞 .....     | 132 |
| 6.3.6 | 系统恶意软件防护引擎漏洞 .....                | 132 |
| 6.3.7 | 手动安装更新和扫描恶意软件 .....               | 133 |
| 6.4   | 系统漏洞的监测与修复 .....                  | 135 |
| 6.4.1 | 使用系统自动更新功能 .....                  | 135 |
| 6.4.2 | 使用 360 安全卫士 .....                 | 136 |
| 1.    | 安装 360 安全卫士 .....                 | 136 |
| 2.    | 修复系统漏洞 .....                      | 136 |
| 6.4.3 | 使用驱动精灵修复系统漏洞 .....                | 137 |

高手私房秘笈

- 秘笈 1 系统漏洞补丁管理
- 秘笈 2 关闭 Windows 更新

第 7 章  
系统安全黑客攻防实战

|       |                       |     |
|-------|-----------------------|-----|
| 7.1   | 为系统加密 .....           | 142 |
| 7.1.1 | 设置 CMOS 开机密码 .....    | 142 |
| 7.1.2 | 设置账户密码 .....          | 143 |
| 7.1.3 | 创建密码重置盘 .....         | 144 |
| 7.1.4 | 设置 Windows 启动密码 ..... | 145 |
| 7.2   | 系统安全设置 .....          | 146 |
| 7.2.1 | 设置账户安全策略 .....        | 146 |

|        |                           |     |
|--------|---------------------------|-----|
| 1.     | 禁止显示上次登录的用户名 .....        | 146 |
| 2.     | 防止“账号克隆” .....            | 146 |
| 3.     | 使用账户锁定策略 .....            | 147 |
| 4.     | 设置 Administrator 账户 ..... | 148 |
| 7.2.2  | 设置用户账户控制 .....            | 151 |
| 7.2.3  | 加密文件 .....                | 151 |
| 7.2.4  | 彻底隐藏文件 .....              | 153 |
| 7.2.5  | 彻底删除文件 .....              | 154 |
| 7.2.6  | 清除页面文件 .....              | 155 |
| 7.2.7  | 清除程序和文档使用痕迹 .....         | 156 |
| 7.2.8  | 清除搜索记录 .....              | 156 |
| 7.2.9  | 清除系统日志 .....              | 157 |
| 7.2.10 | 禁止运行注册表文件 .....           | 157 |
| 7.2.11 | 禁止远程修改注册表 .....           | 158 |
| 7.2.12 | 清除 Word 文档隐私信息 .....      | 159 |
| 7.2.13 | 修改 TTL 值迷惑黑客 .....        | 160 |
| 7.2.14 | 设置 ARP 缓存生存时间 .....       | 160 |
| 7.2.15 | 防范 ICMP 重定向报文攻击 .....     | 160 |
| 7.2.16 | 配置 Windows 防火墙 .....      | 161 |
| 7.2.17 | 隐藏共享文件夹 .....             | 164 |

高手私房秘笈

- 秘笈 1 使用 PowerTool 维护系统安全
- 秘笈 2 恢复误删数据

第 8 章  
账户与密码黑客攻防实战

|       |                         |     |
|-------|-------------------------|-----|
| 8.1   | 常用文件加密 .....            | 169 |
| 8.1.1 | 为 Word 文档加密 .....       | 169 |
| 1.    | 限制文档编辑 .....            | 169 |
| 2.    | 加密文档 .....              | 170 |
| 8.1.2 | 为 Excel 表格加密 .....      | 170 |
| 8.1.3 | 为 WPS Office 文档加密 ..... | 172 |
| 8.1.4 | 为电子邮件加密 .....           | 173 |
| 8.1.5 | 为压缩文件加密 .....           | 173 |
| 8.1.6 | 为 PDF 文档加密 .....        | 174 |

|                       |     |
|-----------------------|-----|
| 8.2 使用加密软件加密 .....    | 176 |
| 8.2.1 文件夹卫士 .....     | 176 |
| 1. 加密文件夹 .....        | 176 |
| 2. 隐藏文件夹 .....        | 177 |
| 3. 解除限制 .....         | 178 |
| 8.2.2 文本文件专用加密器 ..... | 178 |
| 8.2.3 终极程序加密器 .....   | 180 |
| 8.2.4 万能加密器 .....     | 181 |
| 1. 加密文件 .....         | 181 |
| 2. 编译 EXE 文件 .....    | 182 |
| 3. 嵌入与分割文件 .....      | 183 |
| 4. 伪装文件目录 .....       | 184 |

### 高手私房秘笈

秘笈 1 使用注册表隐藏磁盘

秘笈 2 使用图片加密器加密图片

## 第 9 章

### QQ 与电子邮件黑客攻防实战

|                                        |     |
|----------------------------------------|-----|
| 9.1 黑客攻击 QQ 常用的方式 .....                | 189 |
| 9.1.1 向指定 QQ 发送炸弹 .....                | 189 |
| 1. 向好友频繁发送信息 .....                     | 189 |
| 2. 频繁发送身份认证请求 .....                    | 189 |
| 9.1.2 破解本地 QQ 的密码 .....                | 190 |
| 9.2 盗取 QQ 密码——QQExplorer<br>在线盗号 ..... | 190 |
| 9.3 黑客远程攻击——QQ 细胞<br>发送器 .....         | 191 |
| 9.4 查看聊天记录——暗夜 QQ<br>聊天记录查看器 .....     | 192 |
| 9.5 对 QQ 进行保护 .....                    | 193 |
| 9.5.1 设置 QQ 密码保护 .....                 | 193 |
| 9.5.2 QQ 聊天安全 .....                    | 194 |
| 9.5.3 删除 QQ 消息 .....                   | 196 |
| 9.5.4 备份与还原 QQ 聊天消息 .....              | 197 |
| 9.5.5 防范 IP 地址被探测 .....                | 198 |
| 1. 升级 QQ 软件 .....                      | 198 |
| 2. 限制文件传送 .....                        | 198 |
| 3. 安装防火墙 .....                         | 198 |
| 4. 使用代理 .....                          | 198 |
| 9.6 认识电子邮件病毒 .....                     | 199 |
| 9.7 认识电子邮件炸弹 .....                     | 200 |
| 9.7.1 电子邮件炸弹的定义和<br>危害 .....           | 200 |
| 9.7.2 电子邮件炸弹的制作 .....                  | 201 |
| 9.8 破解电子邮件密码 .....                     | 202 |
| 9.8.1 使用“流光” .....                     | 202 |
| 9.8.2 使用“溯雪 Web 密码<br>探测器” .....       | 203 |
| 9.8.3 使用“黑雨”软件暴力<br>破解 .....           | 205 |
| 9.8.4 使用“流影”破解邮箱<br>密码 .....           | 205 |
| 9.9 防范电子邮件攻击 .....                     | 206 |
| 9.9.1 邮箱保护措施 .....                     | 207 |
| 1. 使用备用邮箱 .....                        | 207 |
| 2. 保护邮箱密码 .....                        | 207 |
| 9.9.2 找回邮箱密码 .....                     | 207 |
| 9.9.3 防止炸弹攻击 .....                     | 209 |
| 1. 邮件地址保密 .....                        | 209 |
| 2. 隐藏邮件地址 .....                        | 209 |
| 3. 使用垃圾邮件拦截工具 .....                    | 209 |
| 4. 谨慎使用“自动回复”功能 .....                  | 209 |
| 5. 指定邮件过滤规则 .....                      | 209 |
| 6. 限制接收邮件大小 .....                      | 209 |
| 7. 使用转信功能 .....                        | 209 |
| 8. 拒绝 Cookie 信息 .....                  | 210 |
| 9.10 Outlook 防范电子邮件病毒 .....            | 210 |
| 1. 设置邮件格式 .....                        | 210 |
| 2. 隐藏邮件文件夹 .....                       | 210 |
| 3. 利用 Outlook 2016 过滤器<br>功能 .....     | 212 |
| 4. 启用 Outlook 2016 自动<br>删除功能 .....    | 213 |



高手私房秘笈

秘笈 1 设置 QQ 邮箱独立密码

秘笈 2 加密邮件

## 第 10 章

### 木马与病毒黑客攻防实战

|                       |     |
|-----------------------|-----|
| 10.1 认识木马 .....       | 218 |
| 10.1.1 木马及其结构 .....   | 218 |
| 10.1.2 木马的分类 .....    | 219 |
| 1. 破坏型 .....          | 219 |
| 2. 密码发送型 .....        | 219 |
| 3. 远程访问型 .....        | 219 |
| 4. 键盘记录型 .....        | 219 |
| 5. DOS 攻击型 .....      | 219 |
| 6. 代理木马 .....         | 220 |
| 7. FTP 木马 .....       | 220 |
| 8. 程序杀手木马 .....       | 220 |
| 9. 反弹端口型木马 .....      | 220 |
| 10.1.3 木马的特点 .....    | 220 |
| 1. 隐蔽性 .....          | 220 |
| 2. 潜伏性 .....          | 221 |
| 3. 自动运行性 .....        | 221 |
| 4. 欺骗性 .....          | 221 |
| 5. 自动恢复性 .....        | 221 |
| 6. 自动打开特别端口 .....     | 221 |
| 7. 通用性 .....          | 221 |
| 10.1.4 木马的入侵和启动 ..... | 221 |
| 1. 木马的入侵方式 .....      | 221 |
| 2. 木马的启动方式 .....      | 222 |
| 10.1.5 木马的伪装手段 .....  | 223 |
| 1. 图标伪装 .....         | 223 |
| 2. 名称伪装 .....         | 223 |
| 3. 捆绑文件 .....         | 223 |
| 4. 出错提示 .....         | 223 |
| 5. 定制端口 .....         | 223 |
| 6. 自我销毁 .....         | 223 |
| 7. 伪装成应用程序扩展组件 .....  | 224 |
| 8. 网页伪装 .....         | 224 |
| 9. 邮件附件 .....         | 224 |

|                                   |     |
|-----------------------------------|-----|
| 10.2 木马的制作 .....                  | 224 |
| 10.2.1 捆绑木马 .....                 | 224 |
| 10.2.2 自解压木马 .....                | 226 |
| 1. 自解压木马的制作 .....                 | 226 |
| 2. 自解压木马的查杀 .....                 | 227 |
| 10.2.3 CHM 电子书木马 .....            | 228 |
| 1. CHM 电子书木马的制作 .....             | 228 |
| 2. CHM 电子书木马的查杀 .....             | 230 |
| 10.3 “广外女生”木马的应用 .....            | 230 |
| 10.3.1 “广外女生”木马的使用 .....          | 230 |
| 10.3.2 “广外女生”木马的清除 .....          | 232 |
| 10.4 “新鬼影”木马的清除 .....             | 232 |
| 10.4.1 认识“新鬼影”木马 .....            | 232 |
| 10.4.2 清除“新鬼影”木马 .....            | 232 |
| 10.5 木马的清除与防范 .....               | 233 |
| 10.5.1 使用木马清道夫清除木马 .....          | 233 |
| 1. 进行多方位扫描 .....                  | 234 |
| 2. 可疑模块探测 .....                   | 236 |
| 3. 木马清道夫防火墙 .....                 | 237 |
| 10.5.2 使用木马克星 Ipmor<br>清除木马 ..... | 238 |
| 10.5.3 使用金山贝壳木马专杀<br>清除木马 .....   | 238 |
| 10.5.4 手动查杀系统中的隐藏<br>木马 .....     | 239 |
| 10.5.5 常见木马防范措施 .....             | 240 |
| 1. 关闭易攻击端口 .....                  | 240 |
| 2. 良好的电脑日常使用习惯 .....              | 241 |
| 10.6 认识电脑病毒 .....                 | 242 |
| 10.6.1 电脑病毒的特征 .....              | 242 |
| 1. 繁殖性 .....                      | 242 |
| 2. 破坏性 .....                      | 242 |
| 3. 传染性 .....                      | 242 |
| 4. 潜伏性 .....                      | 242 |
| 5. 隐蔽性 .....                      | 243 |
| 6. 可触发性 .....                     | 243 |

|                             |     |
|-----------------------------|-----|
| 10.6.2 电脑病毒常见的传播途径          | 243 |
| 10.6.3 电脑中毒后的常见症状           | 243 |
| 10.7 制作简单病毒                 | 244 |
| 10.8 预防和查杀电脑病毒              | 246 |
| 10.8.1 掌握防范病毒的常用措施          | 246 |
| 10.8.2 使用杀毒软件查杀病毒           | 247 |
| 1. 使用金山毒霸查杀病毒               | 247 |
| 2. 使用 360 安全卫士查杀病毒          | 248 |
| 3. 使用卡巴斯基查杀病毒               | 250 |
| 4. 使用 Norton AntiVirus 查杀病毒 | 252 |

### 高手私房秘笈

秘笈 1 使用 Trojan Remover 查杀木马

秘笈 2 恢复被 360 安全卫士误删的木马

## 第 11 章

### 无线网络及智能手机安全防御

|                     |     |
|---------------------|-----|
| 11.1 无线路由器基本设置      | 256 |
| 11.1.1 无线路由器参数设置    | 256 |
| 11.1.2 搜索无线信号连接上网   | 257 |
| 11.1.3 无线路由安全设置     | 258 |
| 1. 定期修改密码           | 258 |
| 2. 禁用 DHCP 功能       | 258 |
| 3. 无线加密             | 258 |
| 4. 关闭 SSID 广播       | 259 |
| 11.2 Wi-Fi 密码手机破解技术 | 260 |
| 11.3 平板电脑的病毒攻防技术    | 261 |
| 11.3.1 黑客攻击平板电脑的手法  | 261 |
| 1. 系统漏洞问题           | 261 |
| 2. 病毒攻击             | 261 |
| 3. 密码安全问题           | 261 |
| 11.3.2 iPad 防黑技术    | 262 |

|                    |     |
|--------------------|-----|
| 1. 保持物理安全          | 262 |
| 2. 及时升级系统          | 262 |
| 3. 不要“越狱”          | 262 |
| 4. 开启自动锁屏及密码功能     | 262 |
| 5. 不要加入不熟悉的无线网络    | 262 |
| 6. 在不需要时关闭蓝牙       | 263 |
| 7. 关闭地点设置          | 263 |
| 8. 上网浏览器的设置        | 263 |
| 9. 电子邮件的设置         | 263 |
| 10. 使用设置软件         | 263 |
| 11.4 智能手机的病毒攻防技术   | 263 |
| 11.4.1 黑客攻击智能手机的手法 | 263 |
| 11.4.2 常见手机病毒      | 264 |
| 1. 安卓吸费王           | 264 |
| 2. 短信窃贼            | 264 |
| 3. 短信大盗            | 264 |
| 4. X 卧底            | 264 |
| 5. 安卓窃听猫           | 264 |
| 6. 电话吸费军团          | 265 |
| 7. 电话杀手            | 265 |
| 8. 跟踪隐形人           | 265 |
| 9. 联网杀手            | 265 |
| 10. 阿基德锁           | 265 |
| 11.4.3 智能手机的防护策略   | 265 |
| 11.4.4 智能手机的防黑技术   | 266 |
| 1. 遵章守纪            | 266 |
| 2. 严防病毒            | 266 |
| 3. 技术防范            | 266 |
| 4. 自我保护            | 266 |
| 11.4.5 使用 360 手机卫士 | 266 |
| 1. 智能手机杀毒          | 266 |
| 2. 对骚扰电话或垃圾短信进行拦截  | 269 |

### 高手私房秘笈

秘笈 1 查看手机的 MAC 地址

秘笈 2 设置无线 MAC 地址过滤



## 第 12 章 网络支付安全防御实战

|                            |     |
|----------------------------|-----|
| 12.1 防御黑客入侵支付宝 .....       | 274 |
| 12.1.1 “支付大盗”木马的攻击手法 ..... | 274 |
| 12.1.2 保障支付宝账户安全 .....     | 275 |
| 1. 定期修改登录密码 .....          | 275 |
| 2. 定期修改安全保护问题 .....        | 276 |
| 12.1.3 保障支付宝资金安全 .....     | 277 |
| 1. 定期修改支付密码 .....          | 277 |
| 2. 使用数字证书 .....            | 278 |
| 12.2 防御黑客入侵网银 .....        | 280 |
| 12.2.1 定期修改登录密码 .....      | 280 |
| 12.2.2 修改预留验证信息 .....      | 281 |
| 12.2.3 使用小 e 安全检测控件 .....  | 281 |
| 12.3 网络游戏账号安全防范 .....      | 283 |
| 12.3.1 网络游戏常见盗号技术 .....    | 283 |
| 1. 键盘记录器 .....             | 283 |
| 2. 消息跟踪器 .....             | 283 |
| 3. 内存扫描器 .....             | 283 |
| 4. 网络数据监听器 .....           | 283 |
| 12.3.2 网络游戏账号安全机制 .....    | 283 |
| 1. 加密卡 .....               | 283 |
| 2. 网站防毒扫描、阻挡木马植入程序 .....   | 283 |
| 3. 装备绑定系统 .....            | 283 |
| 4. 虚拟键盘 .....              | 284 |
| 5. 游戏内仓库锁 .....            | 284 |

### 高手私房秘笈

- 秘笈 1 使用支付宝自助服务
- 秘笈 2 无线支付安全设置

以下拓展内容，请扫描二维码阅读 PDF 文件



扫一扫，  
看 PDF 文件

## 附录 A 系统的备份与还原

|                         |     |
|-------------------------|-----|
| 附录 A.1 操作系统的备份与还原 ..... | 288 |
| 附录 A.2 制作系统应急启动盘 .....  | 297 |

## 附录 B 网页恶意代码黑客攻防实战

|                       |     |
|-----------------------|-----|
| 附录 B.1 认识恶意代码 .....   | 308 |
| 附录 B.2 防范恶意代码 .....   | 309 |
| 附录 B.3 常见恶意代码攻防 ..... | 311 |
| 附录 B.4 IE 浏览器防护 ..... | 313 |

## 附录 C U 盘病毒黑客攻防实战

|                               |     |
|-------------------------------|-----|
| 附录 C.1 认识 U 盘病毒 .....         | 326 |
| 附录 C.2 autorun.inf 文件解析 ..... | 327 |
| 附录 C.3 U 盘病毒的防御 .....         | 329 |
| 附录 C.4 U 盘病毒的查杀 .....         | 331 |
| 附录 C.5 修复中毒 U 盘 .....         | 334 |



# 第1章

## 黑客攻防入门必修

互联网改变了人们的生活，但黑客问题也成为全世界的关注热点。在学习黑客攻防之前，首先了解一些关于黑客的基础知识，认识黑客、网络协议、端口，以及系统进程等。

### |内|容|导|航|

- 黑客揭秘
- 认识网络协议
- 黑客攻击的入口——端口
- 木马藏匿的首选地——系统进程



### 视频链接

本章知识相关的多媒体教学视频，请读者参见“教学视频\第1章”。

## 1.1 黑客揭秘

谈到网络安全，人们不自觉就会联想到黑客，人们往往会将他们同破坏网络安全、盗取用户账号、偷窃个人私密信息联系起来。其实黑客也有好坏之分，他们并不全是网络上的捣乱分子，其中也有一部分是网络上的安全卫士。下面就让我们揭开黑客的神秘面纱，让读者详细了解黑客到底是什么样的群体。

在黑客圈中，Hacker 一词早期是带有正面意义的。但到了今天，“黑客”一词已经被用于那些专门利用电脑进行破坏或入侵他人电脑者系统的人的代言词，其实对这些人正确的叫法应该是 Cracker，也有翻译成“骇客”。也正是由于这些人的出现玷污了“黑客”一词，使人们把黑客和骇客混为一谈。黑客和骇客根本的区别是：黑客修补系统漏洞，而骇客利用系统漏洞进行破坏。

### 1.1.1 黑客的由来

黑客始于 20 世纪 50 年代，最早的电脑是 1946 年在宾夕法尼亚大学出现，最早的黑客出现于麻省理工学院、贝尔实验室也有。最初的黑客一般都是一些高级技术人员，他们热衷于挑战、崇尚自由，并主张信息共享。

1994 年以来，互联网在全球的迅猛发展为人们提供了方便、自由和无限财富，政治、军事、经济、科技、教育、文化等各个方面都越来越网络化，并且逐渐成为人们生活、娱乐的一部分。可以说，信息时代的到来，使信息已成为物质和能量以外维持人类社会的第三大资源，是未来生活中的重要介质。随着电脑的普及和互联网技术的迅猛发展，黑客也随之出现。

“黑客”一词一般有以下 4 种意义：

- 一个对（某领域内的）编程语言有足够了解，可以不用经过长时间思考就能创造出有用软件的人。
- 一个试图恶意（一般是非法地）破解或破坏某个程序、系统及网络安全的人。这个意义经常对那些符合上个条件的黑客造成严重困扰，他们建议媒体将这群人称为“骇客”。
- 一个试图破解某系统，以提醒该系统所有者系统存在安全漏洞，这群人往往被称作“红客”。他们大多数是电脑安全公司的雇员，并且在完全合法的前提下攻击某系统。
- 一个通过知识或猜测而对某段程序做出（往往是好的）修改，并改变（或增强）该程序用途的人。

现在，网络上出现了越来越多的 Cracker，他们只会入侵，使用扫描器到处乱扫，用 IP 炸弹轰炸，毫无目的地入侵、破坏，他们并无益于电脑技术的发展，反而有害于网络的安全，甚至造成网络瘫痪，为人们带来巨大的经济和精神损失。

### 1.1.2 黑客的组成

今天，黑客不再像以前那样神秘，他们已经发展成网络上一个独特的群体。他们有着与常人不同的思维方法，有着自己独特的行为模式，网络上现在出现了很多由志同道合的人组织起来的黑客组织。但这些人是从什么地方来的呢？他们是什么样的人？其实除了极少数的

职业黑客以外，大多数都是业余的，而黑客其实和现实中的平常人没有两样，或许他就是一名普通的高中生。

有人曾经对黑客年龄进行过调查，黑客的主要群体是 18~30 岁之间的年轻人，大多数是男性，不过现在也有很多女性加入这个行列。他们大多数是在校学生，爱好电脑、充足的时间、好奇心强、精力旺盛等使他们步入黑客的行列。还有一些黑客有自己的事业或工作，大致分为程序员、资深安全员、安全研究员、职业间谍、安全顾问等。当然，这些人的技术和水平是刚刚入门的“小黑客”无法比拟的，不过他们也是从这里一点点地走过来的。

### 1.1.3 黑客的主要行为

“黑客”大体上分为“正”、“邪”两类，正派黑客依靠自己掌握的知识帮助系统管理员找出系统中的漏洞并加以完善，而邪派黑客则是通过各种黑客技能对系统进行攻击、入侵或者做一些其他有害于网络的事情。

无论哪类黑客，他们最初的学习内容都是本书所涉及的内容，而且掌握的基本技能也都是一样的。即便日后他们各自走上了不同的道路，但是所做的事情也差不多，只不过出发点和目的不一样而已。

黑客的行为主要有以下几种。

**其一，学习技术。**互联网上的新技术一旦出现，黑客就必须立刻学习，并用最短的时间掌握这项技术。这里所说的掌握并不是一般的了解，而是阅读有关的“协议”、深入了解此技术的原理。否则一旦停止学习，仅依靠他以前掌握的内容，也许都不能维持他的“黑客”身份超过一年。

**其二，伪装自己。**黑客的一举一动都会被服务器记录下来，所以黑客会伪装自己，使得对方无法辨别其真实身份。这需要有熟练的技巧，包括伪装自己的 IP 地址、使用跳板逃避跟踪、清理记录扰乱对方线索、巧妙躲开防火墙等。

伪装是需要非常过硬的基本功才能实现的，初学者不可能在短时间内学会伪装，本书并不鼓励读者利用自己学习的知识对网络进行攻击，否则一旦自己的行迹败露，最终害的还是自己。

**其三，发现漏洞。**漏洞对黑客来说是最重要的信息，黑客要经常学习别人发现的漏洞，并努力自己寻找未知漏洞，从海量的漏洞中寻找有价值的、可被利用的漏洞进行试验。当然，他们最终的目的是通过漏洞进行破坏或者修补上这个漏洞。

**其四，利用漏洞。**对于正派黑客来说，漏洞需要被修补；对于邪派黑客来说，漏洞主要是用来搞破坏。

作为一名黑客，道德是非常重要的，这往往决定一个黑客的前途和命运。如果一名黑客在开始学习时就是为了扬名或非法获利，那就不能称之为黑客。但是，虚拟的网络世界不能用现实中的规范去管理，而黑客又是在这个虚拟世界中最渴望自由和共享的。虽然网络上的黑客道德或规则出现很多，也有很多黑客章程，但这些所谓的道德往往只是一纸空文，而黑客们真正遵守的是来自内心真诚的道德，是一种信仰而不是人为的、外在的一种守则。也只有这些来自于黑客内心中的道德才可以真正地约束他们。

现在有不少人以盗取他人的游戏账号、银行卡号、窃取公司机密、攻击别人网站、敲诈、

欺骗等非法获利，这些都是违法行为，这些人都不能称为“黑客”，应该称为“骇客”更为合适，他们最终会受到法律的严惩。

## 1.1.4 黑客术语

### 1. 肉鸡

“肉鸡”是一种很形象的比喻，比喻那些可以被黑客控制的电脑，对方可以是 Windows 系统，也可以是 UNIX/Linux 系统，可以是个人电脑，也可以是大型的服务器，黑客可以像操作自己的电脑那样来操作“肉鸡”，而不被对方发觉。

### 2. 木马

木马程序表面上伪装成正常的程序，一旦被用户运行，就会获取系统的控制权限。有很多黑客热衷于使用木马程序来控制他人的电脑，如灰鸽子、黑洞、PcShare 等。

### 3. 网页木马

表面上伪装成普通的网页文件或是将黑客代码直接插入正常的网页文件中，当有人访问时，网页木马就会利用对方系统或者浏览器的漏洞自动将配置好的木马服务端下载到访问者的电脑上并自动执行。

### 4. 挂马

在别人的网站中放入网页木马，或是将黑客代码潜入对方正常的网页中，以使浏览者中木马病毒。

### 5. 后门

后门是一种很形象的比喻，入侵者在利用某些方法成功地控制目的主机后，可以在对方的系统中植入特定的程序，或者修改某些设置。这些改动从表面上很难被察觉，但是入侵者却可以使用相应的程序或者方法轻易地与这台电脑建立连接，重新进行控制。这就好像是入侵者偷偷地配了一把主人房间的钥匙，可以随时进出而不被主人发现一样。通常大多数的木马程序都可以被黑客用于制作后门。

### 6. 端口

端口（Port）相当于一种数据的传输通道。用于接受某些数据，然后传输给相应的服务。电脑将这些数据处理后，再将相应的回复通过开启的端口传给对方。一般每一个开放的端口对应了相应的服务，要关闭这些端口只需要将对应的服务禁用即可。

### 7. rootkit

rootkit 中 root 术语来自于 UNIX 领域，由于 UNIX 主机系统管理员账号为 root 账号，该账号拥有最小的安全限制，完全控制主机并拥有管理员权限称为“root”了这台电脑。rootkit 是攻击者用来隐藏自己的行踪和保留 root（根权限，可以理解成 Windows 下的 system 或者管理员权限）访问权限的工具。攻击者通过远程攻击的方式获得 root 访问权限，或者是先使用密码猜解的方式获得对系统的普通访问权限，进入系统后，通过对方系统内存在的安全漏洞获得系统的 root 权限。然后，攻击者就会在对方的系统中安装 rootkit，以达到自己长久控制对方系统的目的。rootkit 与木马和后门很类似，但远比木马、后门要隐蔽。简单地说，rootkit