HZ BOOKS
华章科技

学电脑从入门到精通

THE SECRETS OF BEING AN EXPERT IN COMPUTER FROM A BEGINNER

无线网络攻防实战

黑客攻防从入门到精通

（智能终端版）

武新华 李书梅 编著

- 简单易学：从易到难、循序渐进、图文并茂、通俗易懂
- 实用性强：无线网络、智能手机以及终端真实攻防技术+案例实战
- 技巧与窍门：丰富的攻防技巧与窍门，帮读者答疑解惑，掌握无线攻防技术

入门到精通丛书
累计销售
30万册

机械工业出版社
China Machine Press

黑客攻防
从入门到精通
（智能终端版）

武新华 李书梅 编著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

黑客攻防从入门到精通（智能终端版）/ 武新华，李书梅，编著 . —北京：机械工业出版社，2015.8

ISBN 978-7-111-51162-5

I. 黑… II. ①武… ②李… 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（2015）第 191997 号

本书紧紧围绕移动黑客攻防展开，在剖析移动设备可能遇到的风险及解决办法的同时，力求对其进行简单明了的讲解，使读者系统地了解移动设备的防御体系，并能够更好地防范黑客的攻击。全书共分为 13 章，包括初识黑客、iOS 操作系统、Android 操作系统、病毒与木马攻防、蓝牙安全攻防、WiFi 安全攻防、拒绝服务攻击曝光、手机游戏安全攻防、QQ 号及电子邮件安全攻防、手机加密技术、移动追踪定位与远程控制技术、移动支付安全防范、手机优化及安全性能的提升。

本书内容丰富、图文并茂、深入浅出，适合对移动设备安全有疑惑或者被移动设备恶意软件、病毒、木马困扰的用户学习使用。

黑客攻防从入门到精通（智能终端版）

出版发行：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：张梦玲　　责任校对：董纪丽

印　　刷：藁城市京瑞印刷有限公司　　版　　次：2015 年 9 月第 1 版第 1 次印刷

开　　本：185mm×260mm　1/16　　印　　张：19.5

书　　号：ISBN 978-7-111-51162-5　　定　　价：49.00 元

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）88379426　88361066　　投稿热线：（010）88379604

购书热线：（010）68326294　88379649　68995259　　读者信箱：hzit@hzbook.com

前言

随着技术的日新月异，移动设备逐渐担当起了越来越重要的角色，智能手机的功能越来越强大，并且能够提供类似于台式计算机和笔记本计算机的功能，新的移动技术和具有 WiFi 功能的产品的广泛使用为新的攻击类型敞开了大门——网络犯罪正通过移动设备向人们靠近。这也使得安全人员面临更严峻的挑战：需要保护移动设备不受移动病毒、蠕虫和间谍软件等传统的恶意软件以及针对移动设备的垃圾邮件的影响。

随着移动设备的广泛应用，移动付款也成为用户青睐的资金交换方式。几乎在任何地方都能通过移动付款并以电子支付的方式进行购物和支付。对于用户来说，这确实很方便。然而，黑客对一些疏于防范的移动设备展开攻击，识别、窃取信用卡账号、勒索银行等行为也越来越多。

在 WiFi 安全方面也存在很大问题。如今，WiFi 的应用也不再局限于计算机，移动设备对其的应用已经占据了相当大的比例。2015 年的“3·15”晚会上，央视曝光了免费 WiFi 的安全问题。在现场，几位工程师利用伪造 WiFi 技术窃取了台下观众的上网内容，并在大屏幕上向大家进行了展示，相信不少读者看了都会心惊胆颤的。

因而，面对智能手机和 PDA 受到的安全威胁日益加剧的现状，进行有效的安全应对，让手持移动设备的用户能够将潜在的风险遏制在萌芽状态，就显得非常重要。

本书围绕“攻”“防”两个不同的角度，在讲解存在于移动设备中的安全问题时，介绍相应的防范方法，图文并茂地再现黑客攻防全过程。

在此，感谢广大读者对本书的阅读与支持，由于作者水平有限，书中难免存在疏漏之处，欢迎批评指正。

目录

第3章 Android操作系统 / 43

第4章 病毒与木马攻防 / 69

第5章 蓝牙安全攻防 / 94

第6章 WiFi安全攻防 / 102

第7章 拒绝服务攻击曝光 / 144

第 1 章 初识黑客

黑客这个名词我们并不陌生，随着智能手机行业的蓬勃发展，黑客也把目光从计算机转移到了移动设备上。如今使用移动设备购物、支付的方式越来越普遍。如果移动设备感染了病毒、木马，或者被恶意软件入侵，可能会导致个人隐私被曝光，账户以及财产被窃取。

1.1 认识黑客

1.1.1 什么是黑客

1994 年以来，互联网在全球的迅猛发展为我们提供了方便、自由和无限的财富，政治、军事、经济、科技、教育和文化等各个方面都越来越网络化，互联网逐渐成为人们生活、娱乐的一部分。可以说，信息时代已经到来，信息已成为物质和能量以外维持人类社会的第 3 资源，它是未来生活中的重要介质。随着计算机的普及和互联网技术的迅速发展，黑客也随之出现了。

黑客是指一类拥有熟练计算机技术的人，但大部分媒体将计算机侵入者称为黑客。而实际上，黑客可分为如下几种：

白帽黑客是指有能力破坏计算机安全但没有恶意目的的黑客。白帽黑客一般遵守道德规范并常常试图同企业合作去改善所发现的计算机安全弱点。

灰帽黑客是指处于伦理和法律边缘的黑客。

黑帽黑客别称骇客，经常用于区分黑帽黑客和一般（正面的）有理性的黑客。这个词流行于 1983 年，采用了“Safe Cracker”的相似发音，并被理论化为一个犯罪和黑客的混成语。

1.1.2 手机黑客

智能手机的发展和虚拟支付的进步，给黑客组织进行非法攻击创造了机会。随着移动端市场的扩大，社交软件集结了大量用户，在手机端支付还尚未完全成熟的市场环境下，黑客组

织瞄准时机，将大量新增移动恶意程序和手机银行木马植入社交软件中，直接威胁用户的手机钱包。

移动端这一块蛋糕大而美，人人都想瓜分，这更刺激了非法分子的欲望。专家认为，在未来很长的一段时间内，各种层出不穷的新型病毒和木马将纷纷进入手机用户市场。为此，给手机设一道保护锁已成必然。保护锁可全面抵御病毒、木马和恶意软件的威胁，因此，能有效拦截骚扰电话和短信的卡巴斯基安全软件是手机用户的不二之选。此外，提高自身网络安全防范意识，在正规网站下载软件，切勿单击不明网站链接，是每个网民应具备的技巧。

1.1.3 黑客的特点

黑客的特点一般是：有英文基础、知道常用的黑客术语和网络安全术语、能熟练使用常用的 DOS 命令和黑客工具，还会使用主流的编程语言以及脚本。

在常见的黑客论坛中，经常会看到肉鸡、后门和免杀等词语，这些词语可以统称为黑客术语。除了具有相关的黑客技术之外，黑客一般还拥有 TCP/IP、ARP 等网络协议知识。

而常用 DOS 命令是指在 DOS 环境下使用的一些命令，主要包括 ping、netstat 以及 net 命令等，利用这些命令可以实现不同的功能。例如，使用 ping 命令可以获取目标计算机的 IP 地址以及主机名。黑客工具则是指黑客用来远程入侵或者查看目标计算机是否存在漏洞的工具。例如，使用 X-Scan 可以查看目标计算机是否存在漏洞，利用 EXE 捆绑器可以制作带木马的其他应用程序。

主流编程语言可分为 5 类，分别如下。

（1）网页脚本语言（Web Page Script Languages）

网页脚本语言就是网页代码。例如 HTML、JavaScript、CSS、ASP、PHP 和 XML 等。

（2）解释型语言（Interpreted Languages）

解释型语言包括 Perl、Python、REBOL 和 Ruby 等，也常被称为脚本语言，通常被用于和底层的操作系统沟通。这类语言的缺点是效率差、源代码外露，因此不适合用来开发软件产品，一般用于网页服务器中。

（3）混合型语言（Hybrid Languages）

混合型语言的代表是 Java 和 C#，介于解释型语言和编译型语言之间。

（4）编译型语言（Compiling Languages）

C/C++、JAVA 都是编译型语言。

（5）汇编语言（Assembly Languages）

汇编语言是最接近于硬件的语言，不过现在用的人很少。

【提示】

程序语言的学习顺序建议如下。

如果完全没有程序经验，可按照这个顺序：Javascript →解释型语言→混合型语言→编译型语言→汇编学习。

1.2 黑客基础知识

1.2.1 黑客常用术语介绍

1. 肉鸡

肉鸡比喻那些可以随意被黑客控制的计算机，黑客可以像操作自己的计算机那样来操作它们，而不被对方发觉。

2. 木马

木马是指表面上伪装成了正常的程序，但是当这些程序运行时，就会获取系统的整个控制权限。很多黑客都热衷于使用木马程序来控制别人的计算机，比如灰鸽子、黑洞、PcShare 等。

3. 网页木马

网页木马是指表面上伪装成普通的网页文件或是将木马代码直接插入到正常的网页文件中，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木马的服务端下载到访问者的计算机上来自动执行。

4. 挂马

挂马是指在别人的网站文件里面放入网页木马或者是将代码潜入到对方正常的网页文件里，以使浏览者中马。

5. 后门

后门是一种形象的比喻，黑客在利用某些方法成功地控制了目标主机后，可以在对方的系统中植入特定的程序，或者是修改某些设置。这些改动从表面上是很难被察觉的，但是黑客却可以使用相应的程序或者方法轻易地与这台计算机建立连接，重新控制这台计算机，就好像是黑客偷偷配了一把主人房间的钥匙，从而可以随时进出房间而不被主人发现一样。通常，大多数的特洛伊木马程序都可以被入侵者用语言制作后门。

6. IPC$

IPC$ 是共享“命名管道”的资源，它是为了让进程之间通信而开放的命名管道，可以通过验证用户名和密码获得相应的权限，在远程管理计算机和查看计算机的共享资源时使用。

7. 弱口令

弱口令是指那些强度不够，容易被猜解的口令，类似 123、abc 这样的口令（密码）。

8. Shell

Shell 是指一种命令运行环境，比如我们按下键盘上的“开始键 +R”组合键时出现“运行”对话框，在里面输入“ cmd”会出现一个用于执行命令的窗口，这个就是 Windows 的 Shell 执行环境。

9. WebShell

WebShell 就是以 ASP、PHP、JSP 或者 CGI 等网页文件形式存在的一种命令执行环境，也

可以将其称为一种网页后门。

10. 溢出

确切地讲，应该是“缓冲区溢出”，简单解释就是程序对接收的输入数据没有执行有效的检测而导致错误，后果可能是程序崩溃或者是执行攻击者的命令。其大致可以分为两类：①堆溢出；②栈溢出。

11. 注入

由于程序员的水平参差不齐，相当大的一部分应用程序存在安全隐患，用户可以提交一段数据库查询代码，根据程序返回的结果，获得某些想要的数据，这个就是 SQL 注入。

12. 注入点

注入点是可以实行注入的地方，通常是一个访问数据库的连接。根据注入点数据库运行账号的不同权限，所得到的权限也会不同。

13. 内网

内网通俗地讲就是局域网，比如网吧、校园网、公司内部网等都属于此类。查看 IP 地址，如果是在以下 3 个范围之内的话，就说明我们是处于内网之中的：10.0.0.0 ~ 10.255.255.255，172.16.0.0 ~ 172.31.255.255，192.168.0.0 ~ 192.168.255.255。

14. 外网

外网直接连入互联网，可以与互联网上的任意一台计算机互相访问。

15. 免杀

通过加壳、加密、修改特征码和加花指令等技术来修改程序，使其逃过杀毒软件的查杀。

16. 加壳

利用特殊的算法，改变 EXE 可执行程序或者 DLL 动态连接库文件的编码（比如实现压缩、加密），以达到缩小文件体积或者加密程序编码，甚至是躲过杀毒软件查杀的目的。目前较常用的壳有 UPX、ASPack、PePack、PECompact 和 UPack 等。

17. 花指令

花指令是几句汇编指令，可让汇编语句进行一些跳转，使得杀毒软件不能正常地判断病毒文件的构造。通俗地讲，就是杀毒软件是从头到脚按顺序来查找病毒的，如果我们把病毒的头和脚颠倒位置，杀毒软件就找不到病毒了。

1.2.2 IP 地址概念

所谓 IP 地址，就是一种主机编址方式，给每个连接在互联网上的主机分配一个 32bits（比特）地址，也称为网际协议地址。

按照传输控制协议 /Internet 协议（Transport Control Protocol/Internet Protocol，TCP/IP）的规定，IP 地址用二进制来表示，每个 IP 地址长 32bits，比特换算成字节就是 4 个字节。例如，一个采用二进制形式的 IP 地址是“00001010000000000000000000000001”，这么长的地址人们处理起来会很费劲，为了方便使用，IP 地址经常被写成十进制的形式，中间使用符号“.”将

其分为不同的字节，即用 XXX.XXX.XXX.XXX 的形式来表现，每组 XXX 代表小于等于 255 的 10 进制数，如 192.168.38.6。IP 地址的这种表示方法称为“点分十进制表示法”，这显然比二进制的 1 或 0 容易记忆。

一个完整的 IP 地址信息通常应包括 IP 地址、子网掩码、默认网关和 DNS 等 4 部分内容。它们 4 个只有在协同工作时，用户才可以访问互联网并被互联网中的计算机所访问（采用静态 IP 地址接入互联网时，ISP 应当为用户提供全部的 IP 地址信息）。

1. IP 地址

企业网络使用的合法 IP 地址，由提供互联网接入的服务商（ISP）分配，私有 IP 地址则可以由网络管理员自由分配。但网络内部所有计算机的 IP 地址都不能相同，否则会发生 IP 地址冲突，导致网络连接失败。

2. 子网掩码

子网掩码是与 IP 地址结合使用的一种技术，其主要作用有两个，一是用于确定地址中的网络号和主机号，二是用于将一个大 IP 网络划分为若干个子网络。

3. 默认网关

默认网关是指如果一台主机找不到可用的网关，就把数据包发送给默认指定的网关，由这个网关来处理数据包。从一个网络向另一个网络发送信息时，必须经过一道“关口”，这道关口就是网关。

4. DNS

DNS 服务用于将用户的域名请求转换为 IP 地址。如果企业网络没有提供 DNS 服务，则 DNS 服务器的 IP 地址应当是 ISP 的 DNS 服务器。如果企业网络自己提供了 DNS 服务，则 DNS 服务器的 IP 地址就是内部 DNS 服务器的 IP 地址。

1.3 智能手机操作系统

智能手机操作系统是一种运算能力及功能比传统功能手机更强的操作系统。使用最多的操作系统有 iOS、Android、Windows Phone、Symbian 和 BlackBerry OS。它们之间的应用软件互不兼容。

智能手机可以像个人计算机一样安装第三方软件，并且能够显示与个人计算机所显示出的一致的网页，它具有独立的操作系统以及良好的用户界面，拥有很强的应用扩展性，能轻松随意地安装和删除应用程序。

1.3.1 iOS

iOS 智能手机操作系统的原名为 iPhone OS，其核心与 Mac OS X 的核心同样都源自于 Apple Darwin。它主要是供 iPhone 和 iPod Touch 使用的，该操作系统大概占用 1.1GB 的存储空间。