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

浓缩精华本 Mini

新手8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

浓缩精华本 Mini

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、系统安全防御技术等内容。

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中专院校师生的技术参考书籍。

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：hzjsj@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的知识，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

第1章

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。控制消息包括网络通不通、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。