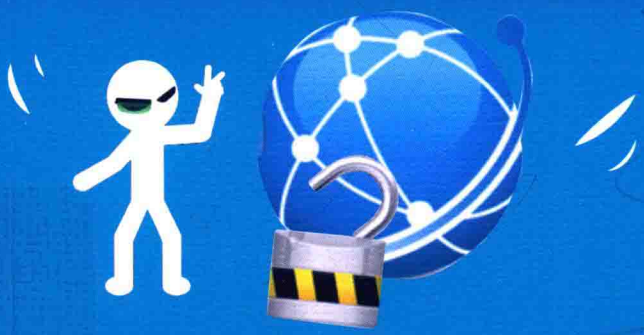
从新手到高手

黑客入门与网络安全实用手册
安全技术全新升级

黑客攻防与网络安全

从新手到高手（实战篇）



网络安全技术联盟 主 编
魏 红 副主编

一线网络安全技术联盟倾心打造
海量王牌资源超值赠送

- 超值赠送1 同步微视频
- 超值赠送2 精美教学PPT课件
- 超值赠送3 黑客工具（107个）速查手册
- 超值赠送4 常用黑客命令（160个）速查手册
- 超值赠送5 180页常见故障维修手册
- 超值赠送6 191页Windows 10系统使用和防护技巧
- 超值赠送7 8大经典密码破解工具详解
- 超值赠送8 加密与解密技术快速入门小白电子手册
- 超值赠送9 网站入侵与黑客脚本编程电子书
- 超值赠送10 黑客命令全方位详解电子书

清华大学出版社

从新手到高手

黑客攻防与网络安全

从新手到高手（实战篇）

网络安全技术联盟　主　编
魏　红　副主编

清华大学出版社
北京

内容简介

本书在剖析用户进行黑客防御中迫切需要或想要用到的技术时，力求对其进行“傻瓜”式的讲解，使读者对网络防御技术有一个系统的了解，能够更好地防范黑客的攻击。全书共分为 15 章，包括网络安全快速入门、搭建网络安全测试环境、黑客入侵方式与 DOS 命令、木马病毒的查杀与预防、系统漏洞与用户账户的安全防护、远程控制入侵系统的安全防护、网络账号及密码的安全防护、浏览器的安全防护、有线局域网的安全防护、无线局域网的安全防护、网站系统的安全防护、电子邮箱与邮件的安全防护、操作系统的安全防护、计算机安全的终极防护、黑客后门入侵痕迹的清理等内容。

另外，本书还赠送海量王牌资源，由于赠送的资源比较多，在本书前言部分对赠送资源的具体内容做了详细说明，帮助读者掌握黑客防守方方面面的知识。

本书内容丰富，图文并茂，深入浅出，不仅适用于网络安全从业人员及网络管理员，而且适用于广大网络爱好者，还可作为大中专院校相关专业的参考书。

图书在版编目(CIP)数据

黑客攻防与网络安全从新手到高手：实战篇 / 网络安全技术联盟主编. —北京：清华大学出版社，2019
（从新手到高手）
ISBN 978-7-302-53011-4

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

中国版本图书馆CIP数据核字（2019）第094003号

责任编辑：张　敏
封面设计：杨玉兰
责任校对：胡伟民
责任印制：丛怀宇

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969, c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015, zhiliang@tup.tsinghua.edu.cn
印 装 者：北京嘉实印刷有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张：**18.25　　**字　　数：**460千字
版　　次：2019年10月第1版　　**印　　次：**2019年10月第1次印刷
定　　价：69.80元

产品编号：082954-01

作者简介

网络安全技术联盟

“网络安全技术联盟”由众多网络安全高手组成，对系统和网络安全中的漏洞非常熟悉，致力于网络安全技术研究和普及，秉承技术自由、技术创新、技术共享、技术进步的原则，为网络安全爱好者提供一个共同进步的平台。

魏红

网络安全工程师，长期从事网络安全、数据通信安全研究工作。

Preface
前 言

随着手机、平板计算机的普及，无线网络的防范变得尤为重要，为此，本书除了讲解有线网络的攻防策略外，还把目前市场上流行的无线攻防等热点融入其中。

本书特色

知识丰富全面：知识点由浅入深，涵盖了所有黑客攻防技术，使读者由浅入深地掌握黑客攻防方面的技能。

图文并茂：注重操作，在介绍案例的过程中，每一个操作均有对应的插图。这种图文结合的方式使读者在学习过程中能够直观、清晰地看到操作的过程以及效果，便于更快地理解和掌握。

案例丰富：把知识点融汇于系统的案例实训当中，并且结合经典案例进行讲解和拓展，进而达到“知其然，并知其所以然”的效果。

提示技巧、贴心周到：本书对读者在学习过程中可能会遇到的疑难问题以“提示”的形式进行了说明，以免读者在学习的过程中走弯路。

超值赠送

本书将赠送同步微视频、精美教学PPT课件、黑客工具（107个）速查手册、常用黑客命令（160个）速查手册、180页常见故障维修手册、191页Windows 10系统使用和防护技巧、8大经典密码破解工具详解、加密与解密技术快速入门小白电子手册、网站入侵与黑客脚本编程电子书、黑客命令全方位详解电子书。读者可扫描右方二维码或通过电子邮件zhangmin2@tup.tsinghua.edu.cn获取本书资源。

精美教学幻灯片

赠送资源8本电子书

读者对象

本书不仅适用于网络安全从业人员及网络管理员，而且适用于广大网络爱好者，还可作为大中专院校相关专业的参考书。

写作团队

本书由长期研究网络安全知识的网络安全技术联盟主编，魏红任副主编，另外还有王秀英、王英英、刘玉萍、刘尧、王朵朵、王攀登、王婷婷、张芳、李小威、王猛、王维维、李佳康、王秀荣、王天护、皮素芹等人参与编写工作。在编写过程中，尽所能地将最好的讲解呈现给读者，但也难免有疏漏和不妥之处，敬请不吝指正。若您在学习中遇到困难或疑问，或有何建议，可通过电子邮箱zhangmin2@tup.tsinghua.edu.cn及时获得在线指导和本书的资源。

编 者

Contents

目 录

第1章　网络安全快速入门

随着信息时代的发展和网络的普及，越来越多的人走进了网络生活，然而人们在享受网络带来便利的同时，也时刻面临着黑客们残酷攻击的危险。本章介绍网络安全的相关技术信息，主要内容包括网络中的相关概念、网络通信的相关协议、IP地址、MAC地址、端口、系统进程等。

1.1　网络中的相关概念

在网络安全中，经常会接触到很多和网络有关的概念，如浏览器、URL、FTP、IP地址及域名等，理解这些概念，对保护网络安全有一定的帮助。

1.1.1　互联网与因特网

互联网是指将两台计算机或者是两台以上的计算机终端、客户端、服务端通过计算机信息技术的手段互相联系起来的结果。互联网在现实生活中应用很广泛，在互联网上人们可以聊天、玩游戏、查阅资料等。互联网是全球性的，这就意味着这个网络不管是谁发明了它，是属于全人类的。

因特网是一个把分布于世界各地的计算机用传输介质互相连接起来的网络，它是基于TCP/IP实现的。TCP/IP由很多协议组成，不同类型的协议又被放在不同的层，其中，位于应用层的协议就有很多，如FTP、SMTP、HTTP。

1.1.2　万维网与浏览器

万维网（World Wide Web，WWW）简称为3W，它是无数个网络站点和网页的集合，也是因特网提供的最主要的服务。万维网是由多媒体链接而形成的集合，通常我们上网看到的内容就是万维网的内容。如下图所示为使用万维网打开的百度首页。

提示：互联网、因特网、万维网三者的关系是由互联网包含因特网，因特网包含万维网。凡是由能彼此通信的设备组成的网络就叫互联网。所以，即使仅有两台计算机，不论用何种技术使其彼此通信，也叫互联网。

浏览器是将互联网上的文本文档（或其他类型的文件）翻译成网页，并让用户与这些文件交互的一种软件工具，主要用于查看网页的内容。目前最常用的浏览器有微软公司的Internet Explorer（通常称为IE浏览器），如下图所示是使用IE浏览器打开的页面。

1.1.3 URL地址与域名

URL（Uniform Resource Locator）即统一资源定位器，也就是网络地址，是在因特网上用来描述信息资源，并将因特网提供的服务统一编址的系统。简单来说，通常在IE浏览器或Netscape浏览器中输入的网址就是URL的一种，如百度网址http://www.baidu.com。

域名（Domain Name）类似于因特网上的门牌号，是用于识别和定位互联网上计算机层次结构的字符标识，与该计算机的因特网协议（IP）地址相对应。但相对于IP地址而言，域名更便于使用者理解和记忆。URL和域名是两个不同的概念，如http://www.sohu.com/是URL，而www.sohu.com是域名，如下图所示为使用URL打开的网页。

1.1.4 IP地址与MAC地址

IP地址用于在TCP/IP中标记每台计算机的地址，通常使用十进制来表示，如192.168.1.100，但在计算机内部，IP地址是一个32位的二进制数值，如11000000 10101000 00000001 00000110（192.168.1.6）。

MAC地址与网络无关，即无论将带有这个地址的硬件（如网卡、集线器、路由器等）接入到网络的何处，都是相同的MAC地址，它由厂商写在网卡的BIOS里。

MAC地址通常表示为12位十六进制数，每2位十六进制数之间用冒号隔开，如08:00:20:0A:8C:6D就是一个MAC地址，其中前6位（08:00:20）代表网络硬件制造商的编号，它由IEEE分配，而后6位（0A:8C:6D）代表该制造商所制造的某个网络产品（如网卡）的系列号。每个网络制造商必须确保它所制造的每个以太网设备前3个字节都相同，后3个字节不同，这样，就可以保证世界上每个以太网设备都具有唯一的MAC地址。

提示： IP地址与MAC地址的区别在于IP地址基于逻辑，比较灵活，不受硬件限制，也容易记忆；MAC地址在一定程度上与硬件一致，基于物理，能够具体标识。这两种地址均有各自的长处，使用时也因条件不同而采取不同的地址。

1.2 认识网络通信协议

“网络通信协议”是计算机网络的一个重要组成部分，是不同网络之间通信、“交流”的公共语言。有了它，使用不同系统的计算机或网络之间才可以彼此识别，识别出不同的网络操作指令，建立信任关系。

1.2.1 TCP/IP

TCP/IP包括两个子协议，即TCP（Transmission Control Protocol，传输控制协议）和IP（Internet Protocol，因特网协议）。在这两个子协议中又包括许多应用型的协议和服务，使得TCP/IP的功能非常强大。

TCP/IP中除了包括TCP、IP两个协议外，还包括许多子协议。它的核心协议包括用户数据报协议（UDP）、地址解析协议（ARP）及因特网控制消息协议（ICMP）等。

1.2.2 IP

IP（Internet Protocol，因特网协议）可实现两个基本功能：寻址和分段。IP可以根据数据报报头中包括的目的地址将数据报传送到目的地址。另外，IP使用4个关键技术提供服务：服务类型、生存时间、选项和报头校验码。

IP的基本任务是通过互联网传送数据报，各个IP数据报之间是相互独立的。IP从源运输实体取得数据，通过它的数据链路层服务传给目的主机的IP层。在传送时，高层协议将数据传给IP，IP再将数据封装为互联网数据报，并交给数据链路层协议通过局域网传送。

1.2.3 ARP

ARP（Address Resolution Protocol，地址解析协议）基本功能就是通过目标设备的IP地址，查询目标设备的MAC地址，以保证通信的顺利进行。在局域网中，网络中实际传输的是“帧”，帧里面有目标主机的MAC地址。

在以太网中，一个主机要和另一个主机进行直接通信，必须要知道目标主机的MAC地址，这个MAC地址就是通过地址解析协议获得的。所谓“地址解析”就是主机在发送数据帧前将目标IP地址转换成目标MAC地址的过程。

1.2.4 ICMP

ICMP（Internet Control Message Protocol，因特网控制消息协议）是TCP/IP中的子协议，主要用于在IP主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、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重要作用。

ICMP对于网络安全非常重要，因为ICMP本身的特点，决定了它非常容易被用来攻击网络上的路由器和主机。例如，可以利用操作系统规定的ICMP数据包最大尺寸不超过64KB这一规定，向主机发起Ping of Death（死亡之Ping）攻击。

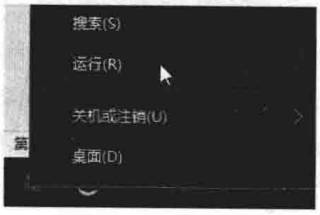
1.3 计算机基本信息的获取

一台计算机的基本信息包括IP地址、物理地址、端口信息、系统进程信息、注册表信息等各种系统信息，用户要想提高计算机的安全系数，必须要学会查看计算机基本信息的方法。

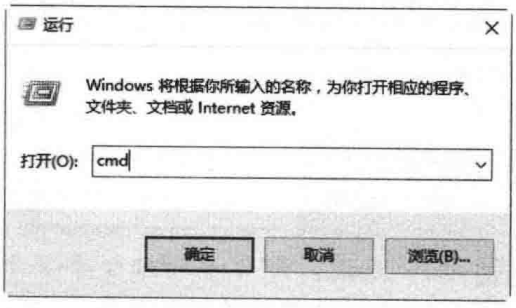
实战1：获取本机的IP地址

在互联网中，一台主机只有一个IP地址，因此，黑客要想攻击某台主机，必须找到这台主机的IP地址，然后才能进行入侵攻击，可以说IP地址是黑客实施入侵攻击的一个关键。使用ipconfig命令可以获取本地计算机的IP地址，具体的操作步骤如下。

Step 01 右击“开始”按钮，在弹出的快捷菜单中执行“运行”命令，如下图所示。



Step 02 打开“运行”对话框，在“打开”文本框中输入cmd命令，如下图所示。



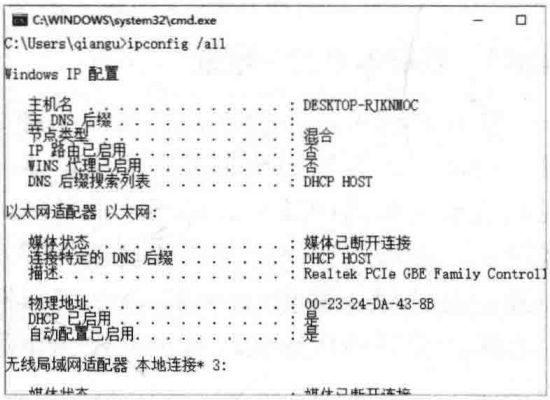
Step 03 单击“确定”按钮，打开“命令提示符”窗口，在“命令提示符”窗口中输入

ipconfig，按Enter键，即可显示出本机的IP配置相关信息。

提示：在“命令提示符”窗口中，192.168.0.130表示本机在局域网中的IP地址。

实战2：获取本机的物理地址

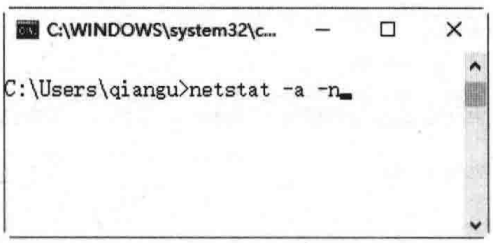
在“命令提示符”窗口中输入ipconfig /all命令，然后按Enter键，可以在显示的结果中看到一个物理地址：00-23-24-DA-43-8B，这就是本机的物理地址，也是本机的网卡地址，它是唯一的。



实战3：查看系统开放的端口

经常查看系统开放端口的状态变化，可以帮助计算机用户及时维护系统安全，防止黑客通过端口入侵计算机。用户可以使用netstat命令查看自己系统端口状态。具体的操作步骤如下。

Step 01 打开“命令提示符”窗口，在其中输入netstat –a –n命令，如下图所示。

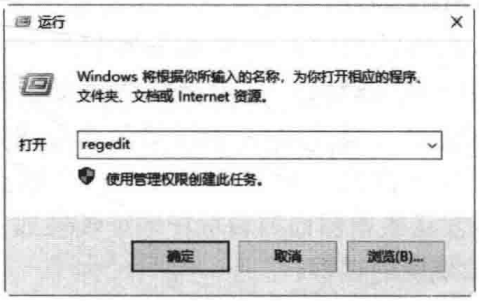


Step 02 按Enter键，即可看到以数字显示的TCP和UCP连接的端口号及其状态，如下图所示。

实战4：查看系统注册表信息

注册表（Registry）是Microsoft Windows中的一个重要数据库，用于存储系统和应用程序的设置信息。通过注册表，用户可以添加、删除、修改系统内的软件配置信息或硬件驱动程序。查看Windows系统中注册表信息的操作步骤如下。

Step 01 在Windows操作系统中选择“开始”→“运行”选项，打开“运行”对话框，在其中输入命令regedit，如下图所示。



Step 02 单击“确定”按钮，即可打开“注册表编辑器”窗口，在其中查看注册表信息，如下图所示。