信息安全
技术大讲堂

从实践中学习
TCP/IP协议

大学霸IT达人◎编著

从理论、应用和实践三个维度讲解TCP/IP协议的相关知识
结合Wireshark和netwox工具对TCP/IP协议进行详细讲解
通过96个实例手把手带领读者从实践中学习TCP/IP协议

机械工业出版社
China Machine Press

信息安全
技术大讲堂

从实践中学习
TCP/IP协议

大学霸IT达人◎编著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

从实践中学习TCP/IP协议/大学霸IT达人编著. —北京：机械工业出版社，2019.7

（信息安全技术大讲堂）

ISBN 978-7-111-63037-1

Ⅰ. 从… Ⅱ. 大… Ⅲ. 计算机网络－通信协议 Ⅳ. TN915.04

中国版本图书馆CIP数据核字（2019）第126612号

从实践中学习 TCP/IP 协议

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：欧振旭 李华君 责任校对：姚志娟

印 刷：中国电影出版社印刷厂 版 次：2019 年 7 月第 1 版第 1 次印刷

开 本：186mm×240mm 1/16 印 张：17.75

书 号：ISBN 978-7-111-63037-1 定 价：79.00 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 读者信箱：hzit@hzbook.com

前言

TCP/IP 协议（TCP/IP Protocol Suite）是互联网通信的基础框架。它采用分层结构，规定了数据如何封装、寻址、传输、路由和接收。为了实现这些功能，TCP/IP 协议包含了几十种网络协议，构成了一个协议族。所以，想要系统地了解网络的运行原理，必须要系统地学习 TCP/IP 协议的相关知识。

由于 TCP/IP 协议对整个互联网运作进行了标准化，所以它包含大量的理论知识。同时，由于大部分协议都被隐藏在系统和软件内部，用户无法直接接触，更不可能复现，因此传统 TCP/IP 协议的学习过程漫长而又枯燥乏味。

本书便是针对这种现状而写，主要是结合理论，并通过实际动手实践，带领读者掌握 TCP/IP 的相关知识。本书结合了 Wireshark 和 netwox 工具对 TCP/IP 协议进行讲解。其中，netwox 工具提供了大量模块，允许用户手动创建各种协议的数据包，而 Wireshark 工具则可以捕获数据包，直观地展现用户创建的数据包。

本书有何特色

1. 结合netwox进行讲解

在 TCP/IP 协议族中，很多协议都是隐藏在系统底层，如 ARP 和 ICMP 协议。用户无法接触到这类协议，只能面对抽象的理论。而 netwox 是一个非常强大的网络工具集，它包含 200 多个模块，可以生成各种网络报文。本书结合该工具，生成讲解所需要的各种报文，这样读者就可以避免单纯地进行理论学习。

2. 基于协议模型逐层讲解

在 TCP/IP 协议族中，各个协议各司其职，分属不同的协议层，从底层开始，逐层依赖，协调工作。为了便于读者掌握该理念，本书严格按照层次结构，逐层讲解每一层的作用和相关协议。

3. 充分讲解网络组成的相关协议

TCP/IP 协议族不仅规范了数据的传输方式，还规定了网络组成方式和运作机制。例如，ARP 协议规范了 IP 和 MAC 地址的转化方式；DHCP 协议规范了主机如何获取 IP 地

址。只有掌握这类协议，才能完整地理解互联网数据传输机制。本书详细地讲解了这类协议，如 ARP、DHCP、DNS 和 ICMP 协议。

4. 详细讲解网络维护类协议

为了方便管理网络，TCP/IP 协议族中包含了大量的维护类协议，如 SNMP、Telnet 和 WHOIS。这些协议广泛应用于实际的网络维护和网络安全领域。本书将详细地讲解这类协议，帮助读者理解协议实际应用的重要性。

5. 内容延伸到安全领域

TCP/IP 协议是网络运行的基础，也是网络安全人员的必备知识。本书从协议报文的基础理论出发，将内容延伸到网络安全领域，充分讲解各个协议在安全领域的应用方式。通过学习，读者可以更深刻地理解网络协议的重要性。

6. 提供完善的技术支持和售后服务

本书提供了专门的 QQ 交流群（343867787），方便大家交流和讨论学习中遇到的各种问题。同时，本书也提供了专门的售后服务邮箱 hzbook2017@163.com。读者在阅读本书的过程中若有疑问，可以通过该邮箱获得帮助。

本书内容

第 1、2 章详细讲解了网络协议的基础知识，内容包括网络组成、网络协议的结构、网络访问层的构成。另外，还讲解了学习必备的两个工具 Wireshark 和 netwox。

第 3 章讲解了网际层和 IP 协议，内容包括 IP 地址的规范、IP 协议工作方式和报文结构。另外，本章还讲解了如何构建 IP 数据包，基于该协议实施洪水攻击。

第 4、5 章讲解了 ARP 和 ICMP 协议。这两个协议负责局域网内和网际之间的数据传输和寻址的关键环节。其中，ICMP 协议也是网络维护和网络安全的重要协议。

第 6、7 章讲解了传输层和 TCP、UDP 协议。传输层负责用户数据的传输。TCP 和 UDP 是最常见和最重要的数据传输协议，这两个协议代表了数据传输的两种经典方式——连接和无连接。

第 8、9 章讲解了 DHCP 和 DNS 协议。其中，DHCP 协议负责网络设备 IP 地址的获取和维护；DNS 协议则负责域名和 IP 地址的转化规则。而 IP 地址和域名是互联网访问的核心环节，是必须要掌握的内容。

第 10～12 章分别讲解了 Telnet、SNMP 和 WHOIS 协议。这 3 个协议都是典型的网络维护类协议。例如，Telnet 协议用于网络远程登录；SNMP 协议用于网络设备和信息管理；WHOIS 是网络信息查询协议。

第 13、14 章分别讲解了 FTP 和 TFTP 协议。虽然这两个协议都是文件共享类型协议，

但其实现机制不同。它们是常见的两种应用协议类型，TFTP 协议只规范了数据传输方式，而 FTP 协议提供了完备的用户接口——FTP 命令，满足实际应用。

本书配套资源获取方式

本书涉及的相关工具读者可以自行下载。下载途径如下：

- 根据图书中对应章节给出的网址自行下载；
- 加入技术讨论 QQ 群（343867787）获取；
- 登录华章公司网站 www.hzbook.com，在该网站上搜索到本书，然后单击“资料下载”按钮，即可在页面上找到“配书资源”下载链接。

本书内容更新文档获取方式

为了让本书内容紧跟技术的发展和软件更新，我们会对书中的相关内容进行不定期更新，并发布对应的电子文档。需要的读者可以加入 QQ 交流群（343867787）获取，也可以通过华章公司网站上的本书配套资源链接下载。

本书读者对象

- 网络应用程序开发人员；
- 渗透测试技术人员；
- 网络安全和维护人员；
- 信息安全技术爱好者；
- 计算机安全技术自学者；
- 高校相关专业的学生；
- 专业培训机构的学员。

本书阅读建议

- Kali Linux 内置了 Wireshark 和 netwox 工具，使用该系统的读者可以跳过 1.3 节和 1.4 节中的安装部分。
- 在学习阶段中，建议多进行实际操作。使用 netwox 工具构建各种数据包，并使用 Wireshark 工具进行分析。只要大量练习，就能理解和掌握 TCP/IP 协议族的各种协议。
- 在实际应用中，常见的网络协议有几百种。本书只讲解最基础的协议，读者需要归纳总结不同协议的工作模式，然后拓展到其他常见协议中。

本书作者

本书由大学霸 IT 达人技术团队编写。感谢在本书编写和出版过程中给予我们大量帮助的各位编辑！

由于作者水平所限，加之写作时间有限，书中可能还存在一些疏漏和不足之处，敬请各位读者批评指正。

编著者

目录

第1章 网络概述

计算机网络是通过数据通信技术将孤立的计算机连接起来，使其能够共享文件和传输数据。通过实现网络连接，计算机的作用被几十倍、几百倍地放大。由于网络的不断发展，各种应用也随之深入人们生活的方方面面。网络协议作为网络世界的基石，也被不断制定和完善。本章将简要讲解网络和网络协议的基本概念。

1.1 网络组成

网络是计算机或类似计算机的网络设备的集合，它们之间通过各种传输介质进行连接。无论设备之间如何连接，网络都是将来自于其中一台网络设备上的数据，通过传输介质传输到另外一台网络设备上。本节将基于这个过程讲解网络的组成。

1.1.1 网卡

网卡也被称为网络适配器（Network Adapter），是连接计算机和传输介质的接口。网卡主要用来将计算机数据转换为能够通过传输介质传输的信号。

1. 网卡种类

网络设备要访问互联网，就需要通过网卡进行连接。由于上网的方式不同，所使用的网卡种类也会不同。网卡的种类有以下几种：

（1）有线网卡

有线网卡就是通过“线”连接网络的网卡。这里所说的“线”指的是网线。有线网卡常见形式如图 1.1 所示。

（2）无线网卡

与有线网卡相反，无线网卡是不需要通过网线进行连接的，而是通过无线信号进行连接。无线网卡通常特指 Wi-Fi 网络的无线网卡。无线网卡常见形式如图 1.2 所示。

（3）蓝牙适配器

蓝牙适配器也是一种无线网卡。蓝牙适配器与无线网卡的区别是数据通信方式不同。蓝牙适配器常见样式如图 1.3 所示。

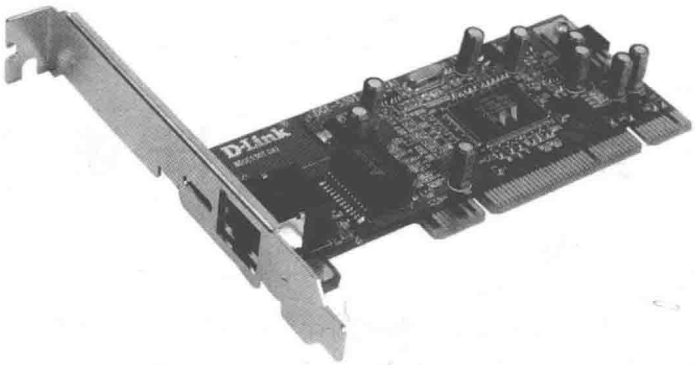

图 1.1　有线网卡

图 1.2　无线网卡

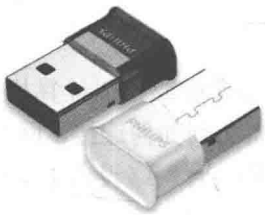

图 1.3　蓝牙适配器

2. 按安装方式分类

网卡通常是网络设备的从属设备。根据其安装方式，网卡可以分为内置网卡和外置网卡。

（1）内置网卡

由于网卡已经成为连接网络的必要设备，所以很多网络设备都内置了网卡。因此，内置网卡也被称为集成网卡。例如，现在的主板都集成了有线网卡，如图 1.4 所示。箭头所指的接口就是内置网卡提供的有线网卡接口。

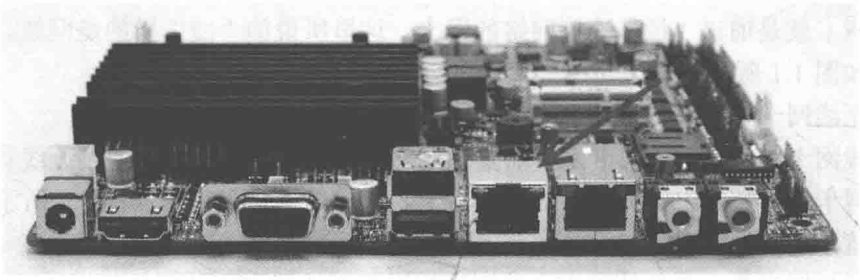

图 1.4　内置网卡