



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
常州大学图书馆
藏书章



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

版权所有·侵权必究

封底无防伪标均为盗版

本书法律顾问: 北京大成律师事务所 韩光/邹晓东

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

前言

第 1 章 网络概述	1
1.1 网络组成	1
1.1.1 网卡	1
1.1.2 网络电缆	3
1.1.3 网络设备	4
1.2 网络协议	5
1.2.1 什么是网络协议	5
1.2.2 TCP/IP 协议	5
1.2.3 OSI 协议层次	6
1.2.4 TCP/IP 协议层次结构	7
1.3 学习辅助工具——网络工具集 netwox	7
1.3.1 下载及安装	8
1.3.2 层次结构分析	9
1.3.3 使用搜索功能	12
1.3.4 使用模块	12
1.4 学习辅助工具——网络分析工具 Wireshark	14
1.4.1 下载及安装	14
1.4.2 实施抓包	15
1.4.3 使用显示过滤器	17
1.4.4 分析数据包层次结构	19
第 2 章 网络访问层	21
2.1 网络访问层的构成	21
2.1.1 物理层	21
2.1.2 数据链路层	22
2.2 网络体系	22
2.2.1 体系的构成	22
2.2.2 类型	22
2.3 物理地址	23

2.3.1	MAC 地址是预留的	23
2.3.2	MAC 地址格式	23
2.3.3	查询 MAC 厂商	23
2.3.4	查看网络主机 MAC 地址信息	25
2.3.5	根据 MAC 地址获取主机其他信息	26
2.4	以太网	26
2.4.1	以太网连接	27
2.4.2	以太帧结构	28
2.4.3	构建以太帧	29
2.4.4	以太帧洪水攻击	30
2.5	网络配置信息	31
2.5.1	显示网络配置信息	31
2.5.2	显示网络调试信息	33
第 3 章	网际层和 IP 协议	36
3.1	IP 地址	36
3.1.1	为什么使用 IP 地址	36
3.1.2	IP 地址构成	38
3.1.3	子网划分	40
3.1.4	CIDR 格式	40
3.2	IP 协议	41
3.2.1	IP 协议工作方式	42
3.2.2	IP 协议包结构	42
3.3	构造 IP 数据包	44
3.3.1	构建 IP 数据包	44
3.3.2	基于 Ethernet 层构造 IP 数据包	46
3.3.3	利用分片实施洪水攻击	47
第 4 章	ARP 协议	49
4.1	ARP 协议概述	49
4.1.1	为什么需要 ARP 协议	49
4.1.2	基本流程	49
4.1.3	ARP 缓存	50
4.1.4	查看 ARP 缓存	51
4.2	ARP 协议包结构	51
4.2.1	协议包的结构	52
4.2.2	构造 ARP 包	53
4.2.3	免费 ARP 包	55
4.3	基于 ARP 协议扫描	56

4.3.1	扫描单一主机	56
4.3.2	扫描多个主机	58
4.3.3	隐蔽扫描	59
4.3.4	伪造 ARP 响应	63
4.3.5	周期性发送 ARP 响应包	65
第 5 章	ICMP 协议	67
5.1	ICMP 协议概述	67
5.1.1	ICMP 协议作用	67
5.1.2	ICMP 报文结构	67
5.2	IMCP 协议应用——探测主机	69
5.2.1	使用 ping 命令	69
5.2.2	构造 ICMP 数据包	70
5.2.3	伪造 ICMP 数据包	72
5.2.4	构造连续的 ICMP 数据包	73
5.2.5	伪造连续的 ICMP 数据请求包	74
5.2.6	伪造 ICMP 数据包的 IP 层	75
5.2.7	伪造 ICMP 数据包的 Ethernet 层	77
5.3	IMCP 协议应用——路由跟踪	79
5.3.1	使用 traceroute 命令	79
5.3.2	构造 ICMP 请求包进行路由跟踪	81
5.3.3	伪造 ICMP 请求包进行路由跟踪	83
5.4	IMCP 协议其他应用	84
5.4.1	发送 ICMP 时间戳请求	84
5.4.2	伪造请求超时 ICMP 数据包	86
5.4.3	伪造目标不可达	88
5.4.4	伪造参数错误 ICMP 数据包	90
5.4.5	伪造源站抑制 ICMP 数据包	91
5.4.6	伪造重定向 ICMP 数据包	92
第 6 章	传输层和 TCP 协议	96
6.1	基础知识	96
6.1.1	传输层的作用	96
6.1.2	面向连接和无连接	96
6.1.3	端口和套接字	97
6.1.4	多路复用和多路分解	100
6.2	TCP 协议	100
6.2.1	TCP 协议作用	100
6.2.2	TCP 工作模式	100

6.2.3	TCP 数据格式	105
6.3	TCP 建立连接	107
6.3.1	第 1 次握手	107
6.3.2	第 2 次握手	108
6.3.3	第 3 次握手	109
6.3.4	分析握手过程中字段的变化	109
6.3.5	构造 3 次握手包	112
6.4	数据传输	116
6.4.1	数据分片	116
6.4.2	滑动窗口机制	117
6.4.3	数据重发	119
6.4.4	TCP 流控制	121
6.5	TCP 断开连接	124
6.5.1	第 1 次挥手	124
6.5.2	第 2 次挥手	125
6.5.3	第 3 次挥手	125
6.5.4	第 4 次挥手	126
6.5.5	分析挥手过程字段的变化	127
6.6	TCP 协议应用——扫描主机	130
6.6.1	构造 TCP Ping 包实施扫描	130
6.6.2	伪造 TCP Ping 包实施扫描	131
6.7	TCP 协议应用——扫描 TCP 端口	132
6.7.1	构造 TCP 端口扫描包	132
6.7.2	伪造 TCP 扫描包	134
6.7.3	防御扫描	134
6.8	TCP 协议应用——探测防火墙	137
6.9	TCP 协议应用——跟踪路由	142
6.9.1	构造 TCP 包进行路由跟踪	142
6.9.2	伪造 TCP 包进行路由跟踪	143
6.10	TCP 协议应用——检测网络性能	144
6.11	TCP 协议应用——干扰连接	145
6.11.1	重置会话	145
6.11.2	检查盲注攻击漏洞	147
第 7 章	UDP 协议	149
7.1	UDP 协议作用	149
7.2	UDP 数据格式	149
7.2.1	UDP 报文格式	149

7.2.2	分析 UDP 数据包	150
7.3	构造 UDP 包	152
7.3.1	基于 IPv4 伪造 UDP 包	152
7.3.2	基于 Ethernet 和 IPv4 伪造 UDP 数据包	154
7.4	UDP 协议应用——扫描主机和端口	156
7.4.1	扫描主机	156
7.4.2	扫描端口	159
7.5	UDP 协议应用——路由跟踪	161
7.6	UDP 协议应用——网络性能测试	163
第 8 章	DHCP 协议	165
8.1	地址分配	165
8.1.1	静态分配	165
8.1.2	动态分配	165
8.1.3	零配置	166
8.2	DHCP 工作方式	166
8.2.1	发现阶段 (DHCP Discover)	167
8.2.2	提供阶段 (DHCP Offer)	167
8.2.3	选择阶段 (DHCP Request)	167
8.2.4	确认阶段 (DHCP ACK)	168
8.2.5	IP 续期	168
8.3	DHCP 报文格式	169
8.3.1	DHCP Discover 报文	170
8.3.2	DHCP Offer 报文	173
8.3.3	DHCP Request 报文	174
8.3.4	DHCP ACK 报文	176
8.4	DHCP 协议应用——获取 IP 地址	177
8.5	DHCP 协议应用——获取 DHCP 服务器信息	182
第 9 章	DNS 协议	185
9.1	域名	185
9.1.1	域名的作用	185
9.1.2	域名的结构	185
9.1.3	域名的分类	185
9.2	域名解析	186
9.2.1	DNS 资源记录	186
9.2.2	实施 DNS 查询请求	187
9.2.3	域名解析流程	188
9.2.4	获取 Bind DNS 服务器版本	190

9.3	DNS 报文格式	190
9.3.1	基础结构部分	190
9.3.2	问题部分	194
9.3.3	资源记录部分	195
9.4	DNS 协议应用——伪造 DNS 服务器	199
9.5	DNS 协议应用——伪造 DNS 响应	200
第 10 章	Telnet 协议	202
10.1	Telnet 协议概述	202
10.1.1	Telnet 协议的作用	202
10.1.2	工作流程	202
10.1.3	常用命令	203
10.2	使用 Telnet 服务	204
10.2.1	建立 Telnet 客户端/服务	204
10.2.2	远程登录并执行命令	205
10.3	Telnet 协议包分析——透明模式	205
10.3.1	TCP 连接	206
10.3.2	Telnet 协商	206
10.3.3	Telnet 认证	208
10.3.4	命令交互	211
10.3.5	断开连接	212
10.4	Telnet 协议包分析——行模式	213
10.5	暴力破解 Telnet 服务	218
第 11 章	SNMP 协议	219
11.1	SNMP 协议工作方式	219
11.1.1	SNMP 协议概述	219
11.1.2	SNMP 架构组成	220
11.1.3	工作原理	220
11.1.4	通信方式	221
11.1.5	操作类型	222
11.2	信息格式	223
11.2.1	对象标识符 (OID)	223
11.2.2	对象下面的分组	224
11.2.3	数据类型 (值类型)	224
11.3	报文分析和构建	225
11.3.1	报文格式	225
11.3.2	构建 SNMP Get 请求	227
11.3.3	构建 SNMP Walk 请求	229

11.3.4	构建 SNMP Trap 请求	231
11.3.5	构建 SNMP Inform 请求	233
11.3.6	构建 SNMP Set 请求	234
第 12 章	WHOIS 协议	236
12.1	工作流程	236
12.2	获取 WHOIS 服务器	237
12.2.1	常用 WHOIS 服务器	237
12.2.2	获取 WHOIS 服务	238
12.3	获取 WHOIS 信息	239
第 13 章	FTP 协议	242
13.1	FTP 协议概述	242
13.1.1	FTP 服务构成	242
13.1.2	数据格式	243
13.2	FTP 工作流程	243
13.2.1	建立连接阶段	244
13.2.2	身份认证阶段	244
13.2.3	命令交互阶段	244
13.2.4	断开连接阶段	244
13.2.5	验证工作流程	244
13.3	FTP 命令及应答码	246
13.4	FTP 内部命令	249
13.5	FTP 基本使用	251
13.5.1	构建 FTP 服务器	251
13.5.2	下载文件及校验	251
13.5.3	列出 FTP 服务器上目录列表信息	252
13.5.4	下载文件	252
13.5.5	上传文件	253
13.5.6	FTP 删除文件	253
13.5.7	下载目录	254
13.5.8	上传目录	255
13.5.9	递归删除目录	255
13.6	暴力破解 FTP 服务	256
第 14 章	TFTP 服务	258
14.1	TFTP 协议概述	258
14.1.1	协议模式	258
14.1.2	报文类型	258

14.1.3 构建 TFTP 服务器	259
14.2 下载文件	259
14.2.1 工作流程	259
14.2.2 报文格式	260
14.2.3 构建 RRQ 包	261
14.3 上传文件	265
14.3.1 工作流程	265
14.3.2 构建 WRQ 包	267

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分是数据通信方式不同。蓝牙适配器常见样式如图 1.3 所示。

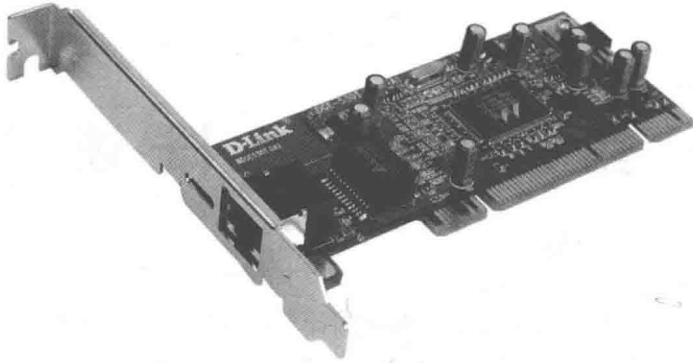


图 1.1 有线网卡



图 1.2 无线网卡

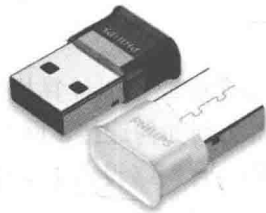


图 1.3 蓝牙适配器

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。

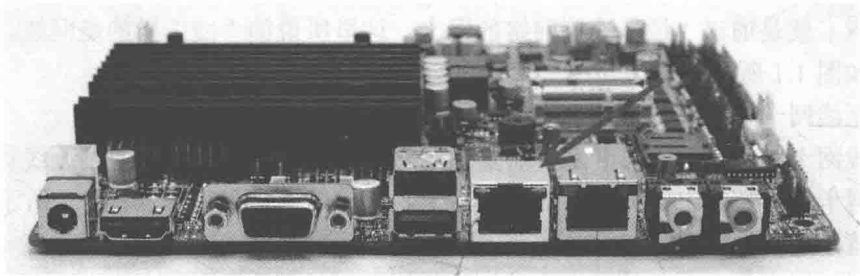


图 1.4 内置网卡