

Wireshark

网络分析从入门到实践

李华峰 陈虹 著

- 内容由浅入深，案例环环相扣，实用技巧“做中学”
- 配合虚拟环境，体验身临其境般的攻防演练
- 基于Lua扩展，探索Wireshark丰富多样的功能
- 完整的配套源码，精准复现书中的经典案例



中国工信出版集团

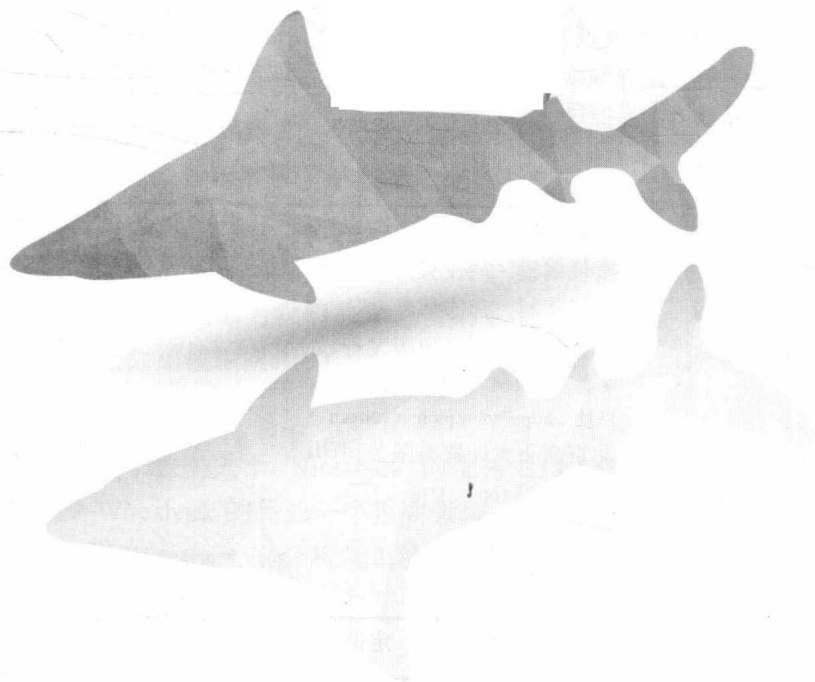


人民邮电出版社
POSTS & TELECOM PRESS

Wireshark

网络分析从入门到实践

李华峰 陈虹 著



人民邮电出版社
北京

图书在版编目 (C I P) 数据

Wireshark网络分析从入门到实践 / 李华峰, 陈虹著

— 北京: 人民邮电出版社, 2019.4

ISBN 978-7-115-50522-4

I. ①W… II. ①李… ②陈… III. ①计算机网络—网
络分析 IV. ①TP393.02

中国版本图书馆CIP数据核字(2018)第300061号

内 容 提 要

Wireshark 是一款开源网络协议分析器,能够在多种平台(例如 Windows、Linux 和 Mac)上抓取和分析网络包。本书将通过图文并茂的形式来帮助读者了解并掌握 Wireshark 的使用技巧。

本书由网络安全领域资深的高校教师编写完成,集合了丰富的案例,并配合了简洁易懂的讲解方式。全书共分 17 章,从 Wireshark 的下载和安装开始讲解,陆续介绍了数据包的过滤机制、捕获文件的打开与保存、虚拟网络环境的构建、常见网络设备、Wireshark 的部署方式、网络延迟的原因、网络故障的原因,并介绍了多种常见的攻击方式及应对策略,除此之外,本书还讲解了如何扩展 Wireshark 的功能以及 Wireshark 中的辅助工具。

本书实用性较强,适合网络安全渗透测试人员、运维工程师、网络管理员、计算机相关专业的学生以及各类安全从业者参考阅读。

-
- ◆ 著 李华峰 陈虹
 - 责任编辑 胡俊英
 - 责任印制 焦志炜

 - ◆ 人民邮电出版社出版发行 北京市丰台区成寿寺路 11 号
 - 邮编 100164 电子邮件 315@ptpress.com.cn
 - 网址 <http://www.ptpress.com.cn>
 - 北京鑫正大印刷有限公司印刷

 - ◆ 开本: 800×1000 1/16
 - 印张: 17
 - 字数: 337 千字 2019 年 4 月第 1 版
 - 印数: 1-2 400 册 2019 年 4 月北京第 1 次印刷
-

定价: 59.00 元

读者服务热线: (010)81055410 印装质量热线: (010)81055316

反盗版热线: (010)81055315

广告经营许可证: 京东工商广登字 20170147 号

作者简介



李华峰

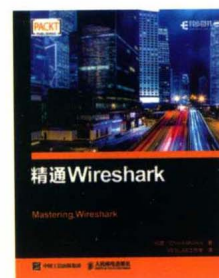
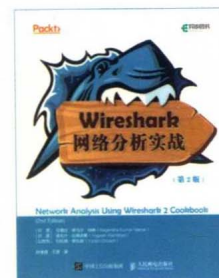
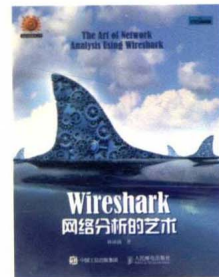
信息安全顾问和自由撰稿人，多年来一直从事网络安全渗透测试方面的研究工作。在网络安全部署、网络攻击与防御以及社会学等方面有十分丰富的实践经验。



陈虹

出身于美术专业的程序开发者。虽然在画室长大，却是实实在在的编程爱好者。目前正在从事软件设计工作。

异步社区Wireshark好书推荐



前言

数百年前显微镜的发明为人类探索微观世界开启了一扇大门，而如今，Wireshark 的出现则为我们观察网络世界打开了另一扇大门。作为世界上最为流行的数据包分析软件，Wireshark 拥有着其他同类工具所不能比拟的强大优势。无论你是一个刚刚开始接触计算机网络知识的大学生，还是一个已经拥有多年从业经验的工程师，Wireshark 都可以给你带来极大的帮助。很多国内外的知名企业也将 Wireshark 的使用技能明确写入了招聘的要求之中。

在开始写作本书之前，我曾经翻译和编写了一些网络安全方面的书籍。这些书籍介绍了很多常见的网络攻击手段，读者在掌握了这些技能之后，大都对其实现细节产生了兴趣。例如到底为什么 Nmap 可以扫描出目标主机的状态，以及为什么中间人攻击就可以监听网络中的通信，泛洪攻击又是如何实现的呢？这些攻击的手段各种各样，实现这些攻击的工具也大都采用了不同的语言，这些都为我们的学习带来了很大的困难。不过，任何的网络攻击行为最终都是通过发送数据包来实现的，如果我们从数据包这个层次来分析问题，一切就会清晰起来。

虽然此前国内外已经有了很多关于 Wireshark 的优秀书籍，但是它们大都着眼于网络故障的排除，并没有涉及 Wireshark 的另外一个重要领域——网络安全。而本书以此作为研究的重点，讲述了如何使用 Wireshark 来分析常见的网络攻击手段，并根据它们的特点给出了解决方案。

目标读者

本书的目标读者如下：

- 网络安全渗透测试人员；
- 运维工程师；
- 网络管理员和企业网管；
- 计算机相关专业的学生；
- 网络安全设备设计与安全软件开发人员；
- 安全课程培训人员。

如何阅读本书

全书分为6个部分共16章，其中前3章为第1部分，主要讲解了 Wireshark 的基本使用方法；第4章~第6章为第2部分，主要讲解了 eNSP 的使用以及网络的一些知识。第7章和第8章为第3部分，讲解了常见网络故障的排除。而第9章~第15章为本书最为重要的部分，主要讲解了如何使用 Wireshark 来分析各种常见的网络攻击，这些内容按照链路层、网络层、传输层和应用层这个顺序来介绍。最后两章讲解了一些 Wireshark 的扩展功能和辅助工具。

第1章“走进 Wireshark”，这一章对 Wireshark 的功能和工作原理进行了简单的介绍，然后讲解了 Wireshark 的下载和安装过程。本章最后演示了一个 Wireshark 的使用实例，这个实例虽然很简单，但是却包含了完整的使用过程。

第2章“过滤无用的数据包”，详细地讲解了 Wireshark 中对数据包的过滤机制，这里面包括捕获过滤器和显示过滤器的使用方法。

第3章“捕获文件的打开与保存”，讲解了 Wireshark 中的各种保存功能，包括对数据包捕获文件保存位置和格式的设置，对过滤器的保存，对配置文件的保存。

第4章“虚拟网络环境的构建”，讲解了 eNSP 和 VMWare 两种工具的使用。在它们的帮助下，我们可以模拟出各种和真实环境一模一样的网络结构，并以此来进行练习。

第5章“各种常见的网络设备”，介绍了网络中常见的几种硬件，并给出了一些实例。

了解这些硬件可以更好地帮助我们使用 Wireshark。

第 6 章“Wireshark 的部署方式”，讲解了如何在各种网络情况下进行 Wireshark 的部署。

第 7 章“找到网络发生延迟的位置”，从这一章起我们开始了对网络实际问题的分析。本章就延迟位置的确定进行了讲解，并在这个实例中穿插讲解了 Wireshark 中的时间设置。

第 8 章“分析不能上网的原因”，在这一章中，我们就“不能上网”这个问题进行了分析，在问题分析过程中使用到了很多 Wireshark 的技巧。

第 9 章“来自链路层的攻击——失常的交换机”，从这一章起，我们开始了对网络安全问题的分析。围绕着交换机面临的典型攻击手段——Mac 泛洪攻击，给出了详细的介绍。首先从一个案例开始，对案例中的数据包文件进行了分析和总结，进一步得出了这种攻击的特点，最后给出了这种攻击手段的实现和解决方案。

第 10 章“来自网络层的欺骗——中间人攻击”，对第 ARP 欺骗技术进行了讲解。ARP 欺骗技术是中间人攻击的实现基础，这一章从 ARP 欺骗的原理开始讲解，并在 Wireshark 的帮助下对 ARP 欺骗进行了深入的分析。同时还介绍了 Wireshark 中的强大工具——专家系统的使用方法。最后给出了如何完成 ARP 欺骗，以及如何防御这种攻击的方法。

第 11 章“来自网络层的攻击——泪滴攻击”，讲解了针对 IP 协议的一种典型攻击手段：泪滴攻击。首先讲解了 IP 协议的格式，然后介绍了 IP 协议的一个重要概念：分片。同时也详细讲解了基于这种技术的攻击手段——泪滴攻击。这一章还介绍了 Wireshark 的着色规则，只需查看数据包的颜色，就可以判断出它的类型。在本章的最后，介绍了 IP 协议头中一个很有用的字段 TTL。

第 12 章“来自传输层的洪水攻击（1）——SYN Flooding”，介绍了针对服务器的攻击方式——SYN Flooding 攻击。并在 Kali Linux2 平台中演示了如何进行这种攻击，同时也使用 Wireshark 的流量图对这种攻击进行了分析。

第 13 章“网络在传输什么——数据流功能”，在这一章中，介绍了 TCP 数据的传输，并详细讲解了 Wireshark 中的数据流功能，利用这个功能可以监控整个网络中传输的文件。本章最后给出了一个非常优秀的 Wireshark 学习资源。

第 14 章“来自传输层的洪水攻击（2）——UDP Flooding”，这一章讲解了 UDP Flooding 攻击的原理与实现方法，并使用 Wireshark 中的图表功能对这种攻击的技术进行了分析。最后重点介绍了 Wireshark 中自带的图表功能以及 amCharts 的使用方法。

第 15 章“来自应用层的攻击——缓冲区溢出”，这一章介绍了一种全新的攻击方式——缓冲区溢出，它的攻击建立在应用层的协议上。本章首先介绍了 HTTP 协议，然后模拟了

一次缓冲区溢出的攻击过程。在这个实例中还介绍了数据包的查找功能。在最后介绍了如何使用 Wireshark 来分析 http 协议的升级版 https 协议。

第 16 章“扩展 Wireshark 的功能”，这一章介绍了如何在 Wireshark 中编写插件，这个功能在实际应用中相当有用，相关的实例都采用了 Lua 语言编写。

第 17 章“Wireshark 中的辅助工具”，介绍了 Wireshark 中常见的各种工具，包括 Tshark、Dumpcap、Editcap、Mergecap、Capinfo 和 USBPcapCMD 等工具的功能和使用方法。

大家可以根据自己的需求选择阅读的侧重点，不过我还是推荐按照顺序来阅读，这样可以对 Wireshark 的使用有一个清晰的认识，同时也可以深入了解网络中常见的攻击方法。

资源与支持

本书由异步社区出品，社区（<https://www.epubit.com/>）为您提供相关资源和后续服务。

配套资源

本书提供配套代码资源，要获得该配套资源，请在异步社区本书页面中点击 **配套资源**，跳转到下载界面，按提示进行操作即可。注意：为保证购书读者的权益，该操作会给出相关提示，要求输入提取码进行验证。

如果您是教师，希望获得教学配套资源，请在社区本书页面中直接联系本书的责任编辑。

提交勘误

作者和编辑尽最大努力来确保书中内容的准确性，但难免会存在疏漏。欢迎您将发现的问题反馈给我们，帮助我们提升图书的质量。

当您发现错误时，请登录异步社区，按书名搜索，进入本书页面，点击“提交勘误”，输入勘误信息，点击“提交”按钮即可。本书的作者和编辑会对您提交的勘误进行审核，确认并接受后，您将获赠异步社区的 100 积分。积分可用于在异步社区兑换优惠券、样书或奖品。

详细信息 写书评 提交勘误

页码: 页内位置 (行数): 勘误印次:

B I U

字数统计

提交

扫码关注本书

扫描下方二维码，您将会在异步社区微信服务号中看到本书信息及相关的服务提示。



与我们联系

我们的联系邮箱是 contact@epubit.com.cn。

如果您对本书有任何疑问或建议，请您发邮件给我们，并请在邮件标题中注明本书书名，以便我们更高效地做出反馈。

如果您有兴趣出版图书、录制教学视频，或者参与图书翻译、技术审校等工作，可以发邮件给我们；有意出版图书的作者也可以到异步社区在线提交投稿（直接访问 www.epubit.com/selfpublish/submission 即可）。

如果您是学校、培训机构或企业，想批量购买本书或异步社区出版的其他图书，也可以发邮件给我们。

如果您在网上发现有针对异步社区出品图书的各种形式的盗版行为，包括对图书全部或部分内容的非授权传播，请您将怀疑有侵权行为的链接发邮件给我们。您的这一举动是对作者权益的保护，也是我们持续为您提供有价值的内容的动力之源。

关于异步社区和异步图书

“异步社区”是人民邮电出版社旗下 IT 专业图书社区，致力于出版精品 IT 技术图书和相关学习产品，为作译者提供优质出版服务。异步社区创办于 2015 年 8 月，提供大量精品 IT 技术图书和电子书，以及高品质技术文章和视频课程。更多详情请访问异步社区官网 <https://www.epubit.com>。

“异步图书”是由异步社区编辑团队策划出版的精品 IT 专业图书的品牌，依托于人民邮电出版社近 30 年的计算机图书出版积累和专业编辑团队，相关图书在封面上印有异步图书的 LOGO。异步图书的出版领域包括软件开发、大数据、AI、测试、前端、网络技术等。



异步社区



微信服务号

目录

第 1 章 走进 Wireshark	1	第 2 章 过滤无用的数据包	20
1.1 Wireshark 是什么	2	2.1 伯克利包过滤	21
1.1.1 Wireshark 的功能	2	2.2 捕获过滤器	23
1.1.2 Wireshark 的历史	3	2.3 显示过滤器	25
1.1.3 Wireshark 的工作原理	3	2.3.1 使用过滤器输入框 创建显示过滤器	25
1.1.4 Wireshark 的优势	4	2.3.2 使用过滤器表达式创建 显示过滤器	26
1.2 如何下载和安装 Wireshark	6	2.3.3 在数据包细节面板中 创建显示过滤器	28
1.2.1 安装前的准备	6	2.4 小结	29
1.2.2 下载 Wireshark	6	第 3 章 捕获文件的打开与保存	30
1.2.3 Wireshark 的安装	7	3.1 捕获接口的输出功能	30
1.3 一次完整的 Wireshark 使用过程	8	3.2 环状缓冲区	33
1.3.1 选择合适的网卡	9	3.3 捕获接口的其他功能	33
1.3.2 开始数据包的捕获	10	3.3.1 显示选项	33
1.3.3 过滤无用的数据	14	3.3.2 解析名称	34
1.3.4 将捕获到的数据包 保存到文件	18	3.3.3 自动停止捕获	35
1.4 小结	19		

3.4	保存捕获到的数据	35	第 6 章	Wireshark 的部署方式	79
3.5	保存显示过滤器	37	6.1	完成远程数据包捕获	79
3.6	保存配置文件	39	6.2	集线器环境	84
3.7	小结	42	6.3	交换环境	84
第 4 章	虚拟网络环境的构建	43	6.3.1	端口镜像	85
4.1	虚拟网络设备的构建工具		6.3.2	ARP 欺骗	88
	eNSP	43	6.3.3	网络分路器	90
4.1.1	eNSP 的下载与安装	44	6.4	完成本地流量的捕获	91
4.1.2	使用 eNSP 创建一个		6.5	完成虚拟机流量的捕获	92
	实验环境	48	6.6	小结	94
4.2	虚拟 PC 的工具 VMware	51	第 7 章	找到网络发生延迟的位置	95
4.3	在虚拟环境中引入		7.1	建立一个可访问远程 HTTP	
	Kali Linux 2	52		服务器的仿真网络	95
4.4	在虚拟环境中安装其他操作		7.2	观察远程访问 HTTP 的	
	系统	57		过程	100
4.5	eNSP 与 VMware 的连接	58	7.3	时间显示设置	103
4.5.1	VMware 中的网络		7.4	各位置延迟时间的计算	107
	连接	58	7.4.1	网络传输延迟的	
4.5.2	通过 eNSP 中的云与			计算	108
	VMware 相连	60	7.4.2	客户端延迟的计算	109
4.6	小结	65	7.4.3	服务端延迟的计算	109
第 5 章	各种常见的网络设备	66	7.5	小结	110
5.1	网线	66	第 8 章	分析不能上网的原因	111
5.2	集线器	69	8.1	建立一个用于测试的仿真	
5.3	交换机	71		网络	111
5.4	路由器的工作原理	77	8.2	可能导致不能上网的原因	113
5.5	小结	78			

8.3 检查计算机的网络设置	113	第 10 章 来自网络层的欺骗——	
8.3.1 确保网卡正常启动	113	中间人攻击	140
8.3.2 检查 IP 配置的正确性	114	10.1 中间人攻击的相关理论	140
8.3.3 检查与网关的连接是否正常	120	10.1.1 ARP 协议的相关理论	141
8.3.4 获取域名服务器的 IP 地址	121	10.1.2 ARP 欺骗的原理	146
8.4 检查网络路径的连通性	122	10.2 使用专家系统分析中间人攻击	146
8.5 其他情形	124	10.3 如何发起中间人攻击	150
8.6 小结	125	10.3.1 使用 arpspoof 来发起攻击	150
第 9 章 来自链路层的攻击——		10.3.2 使用 Wireshark 来发起攻击	153
失常的交换机	126	10.4 如何防御中间人攻击	154
9.1 针对交换机的常见攻击方式	127	10.4.1 静态绑定 ARP 表项	154
9.1.1 MAC 地址欺骗攻击	127	10.4.2 使用 DHCP Snooping 功能	154
9.1.2 MAC 地址泛洪攻击	128	10.4.3 划分 VLAN	155
9.1.3 STP 操纵攻击	128	10.5 小结	155
9.1.4 广播风暴攻击	129	第 11 章 来自网络层的攻击——	
9.2 使用 Wireshark 分析针对交换机的攻击	129	泪滴攻击	156
9.2.1 统计功能	130	11.1 泪滴攻击的相关理论	156
9.2.2 MAC 地址泛洪攻击	134	11.1.1 IP 协议的格式	157
9.2.3 找到攻击的源头	135	11.1.2 IP 分片	158
9.3 使用 macof 发起 MAC 地址泛洪攻击	137	11.1.3 泪滴攻击	161
9.4 如何防御 MAC 地址泛洪攻击	138	11.2 Wireshark 的着色规则	162
9.5 小结	139	11.3 根据 TTL 值判断攻击的来源	166

11.4	小结	168	14.1.1	UDP 协议	199
第 12 章	来自传输层的洪水攻击 (1) —— SYN Flooding	169	14.1.2	UDP Flooding 攻击	200
12.1	拒绝服务攻击的相关理论	170	14.2	模拟 UDP Flooding 攻击	201
12.1.1	TCP 连接的建立方式	170	14.3	使用 Wireshark 的绘图功能来分析 UDP Flooding 攻击	201
12.1.2	SYN flooding 攻击	173	14.4	如何防御 UDP Flooding 攻击	207
12.2	模拟 SYN flooding 攻击	173	14.5	amCharts 的图表功能	209
12.2.1	构造一个仿真环境	173	14.6	小结	214
12.2.2	使用 Hping3 发起 SYN flooding 攻击	174	第 15 章	来自应用层的攻击——缓冲区溢出	215
12.3	使用 Wireshark 的流向图功能来分析 SYN flooding 攻击	175	15.1	缓冲区溢出攻击的相关理论	215
12.4	如何解决 SYN Flooding 拒绝服务攻击	177	15.1.1	Wireshark 观察下的 HTTP 协议	216
12.5	在 Wireshark 中显示地理位置	178	15.1.2	HTTP 的请求与应答	216
12.6	小结	184	15.1.3	HTTP 的常用方法	217
第 13 章	网络在传输什么——数据流功能	185	15.1.4	HTTP 中常用的过滤器	217
13.1	TCP 的数据传输	185	15.2	模拟缓冲区溢出攻击	218
13.2	Wireshark 中的 TCP 流功能	187	15.3	使用 Wireshark 分析缓冲区溢出攻击	222
13.3	网络取证实践	192	15.4	使用 Wireshark 检测远程控制	227
13.4	小结	198	15.5	Wireshark 对 HTTPS 协议的解析	230
第 14 章	来自传输层的洪水攻击 (2) —— UDP Flooding	199	15.6	小结	232
14.1	UDP Flooding 的相关理论	199	第 16 章	扩展 Wireshark 的功能	233
			16.1	Wireshark 编程开发的基础	233

16.1.1	Wireshark 中对 Lua 的支持	234
16.1.2	Wireshark 中 Lua 的初始化	235
16.2	使用 Lua 开发简单扩展功能	235
16.3	用 Wireshark 开发新的协议解析器	236
16.3.1	新协议的注册	236
16.3.2	解析器的编写	239
16.4	测试新协议	241
16.5	编写恶意攻击数据包检测模块	245
16.6	小结	248

第 17 章 Wireshark 中的辅助工具249

17.1	Wireshark 命令行工具	249
17.2	Tshark.exe 的使用方法	250
17.3	Dumpcap 的用法	252
17.4	Editcap 的使用方法	253
17.5	Mergecap 的使用方法	254
17.6	capinfos 的使用方法	255
17.7	USBPcapCMD 的使用方法	256
17.8	小结	258

第 1 章

走进 Wireshark

在 1000 多年前的唐代，高僧玄奘为了探究佛教各派学说的分歧，独自一人西行了五万里到达印度那烂陀寺，将 600 多部经书带回了中国，期间共经历了 17 年。而在进入工业时代之后，从北京乘坐飞机到达新德里只需要 7 小时。在互联网时代的今天，如果将这些经书以计算机数据的形式存储起来，那么只需要在几秒（甚至更短），就可以将它们通过网络从新德里传输到北京。

网络的出现改变了我们的工作和生活方式。可以这样说，我们无时无刻都离不开网络，它已经像电力一样成为了这个世界不可或缺的资源之一。但是在享受着网络带来便利的同时，却很少有人关心其中的运行机制，当然人们也无法用肉眼观察到网络世界。

因此，当你希望能够深入地了解网络，一个可以观察到它内部活动的“显微镜”将会是必不可少的。目前世界上可以实现这种功能的“网络显微镜”其实有很多，如果你听过著名的哈佛大学公开课《计算机科学 cs50》的话，那么一定会注意到 David J. Malan 在上课时使用的 TcpDump，这就是一个很受欢迎的“网络显微镜”。另外比较著名的例如 Sniffer、Ethereal 和 Wireshark 等，它们都曾经或者正在人们对网络世界的观察中起着重要的作用。不过，本书要介绍的并非 TcpDump，因为它没有尽如人意的图形化操作界面。而 Wireshark 则在拥有了 TcpDump 的各种优势的同时，还弥补了 TcpDump 的这个缺陷，成为了当前最为流行的网络分析工具。在本书中，我们将在 Wireshark 的帮助下体验网络世界的神奇。

在本章中，我们先来简单地了解 Wireshark，这部分内容将会围绕以下几个主题展开：

- Wireshark 是什么；
- Wireshark 是如何工作的；
- 如何下载和安装 Wireshark；