享学课堂 Xiangxue 致力于培养卓越的程序员

网络安全

WireShark抓包工具实操

享学课堂 James老师

WireShark介绍

你的电脑

Wireshark（前身 Ethereal）是一个网络包分析工具。该工具主要是用来捕获网络数据包，并自动解析数据包，为用户显示数据包的详细信息，供用户对数据包进行分析。

下载及安装

Kali Linux 系统自带 Wireshark 工具，而 Windows 系统中默认没有安装该工具。因此，本节讲解如何在 Windows 系统中安装 Wireshark 工具。

WireShark应用

网络管理员 使用Wireshark 来检测网络问题，

网络安全工程师 ***使用Wireshark 来检查资讯安全相关问题，***

开发人员 使用Wireshark来为新的通讯协议除错，

普通使用者 使用Wireshark 来学习网络协议的相关知识

当然，有的人也会“居心叵测”的用它来寻找一些敏感信息……-

常见协议包抓取

1，ARP协议

2，ICMP协议

3，TCP协议

4，UDP协议

5，DNS协议

6，HTTP协议

享学课堂 Xiangxue 致力于培养卓越的程序员

网络安全

WireShark抓包入门操作

享学课堂 James老师

混杂模式与普通模式

***混杂模式*：混杂模式就是接收所有经过网卡的数据包，包括不是发给本机的包，即不验证MAC地址。**

***普通模式*：普通模式下网卡只接收发给本机的包（包括广播包）传递给上层程序，其它的包一律丢弃。**

一般来说，混杂模式不会影响网卡的正常工作，多在网络监听工具上使用。

享学课堂 Xiangxue 致力于培养卓越的程序员

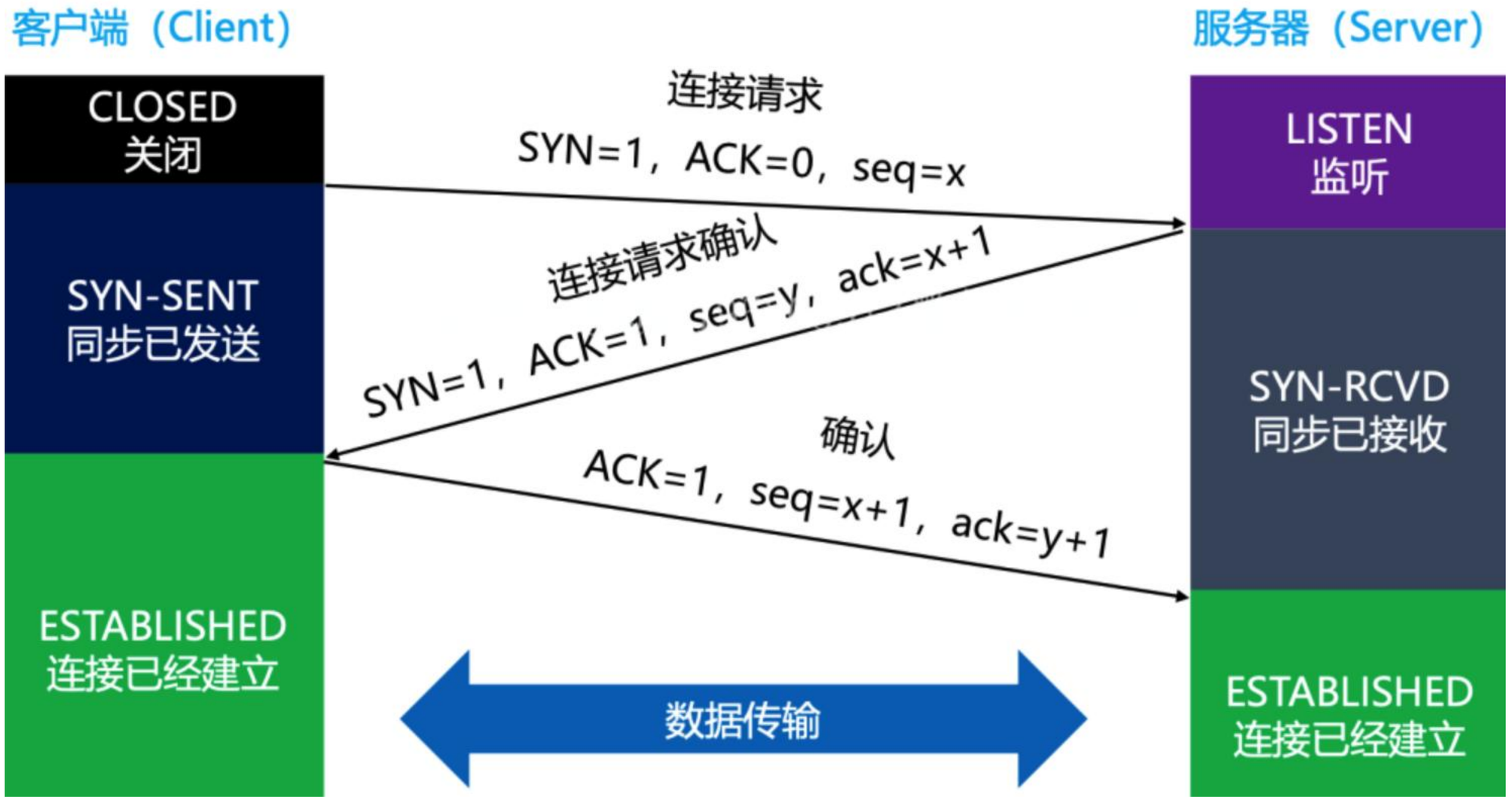
网络安全

WireShark过滤器使用

享学课堂 James老师

黑客 攻击流程

TCP连接三次握手



享学课堂 致力于培养卓越的程序员

网络安全

WireShark之ARP协议分析

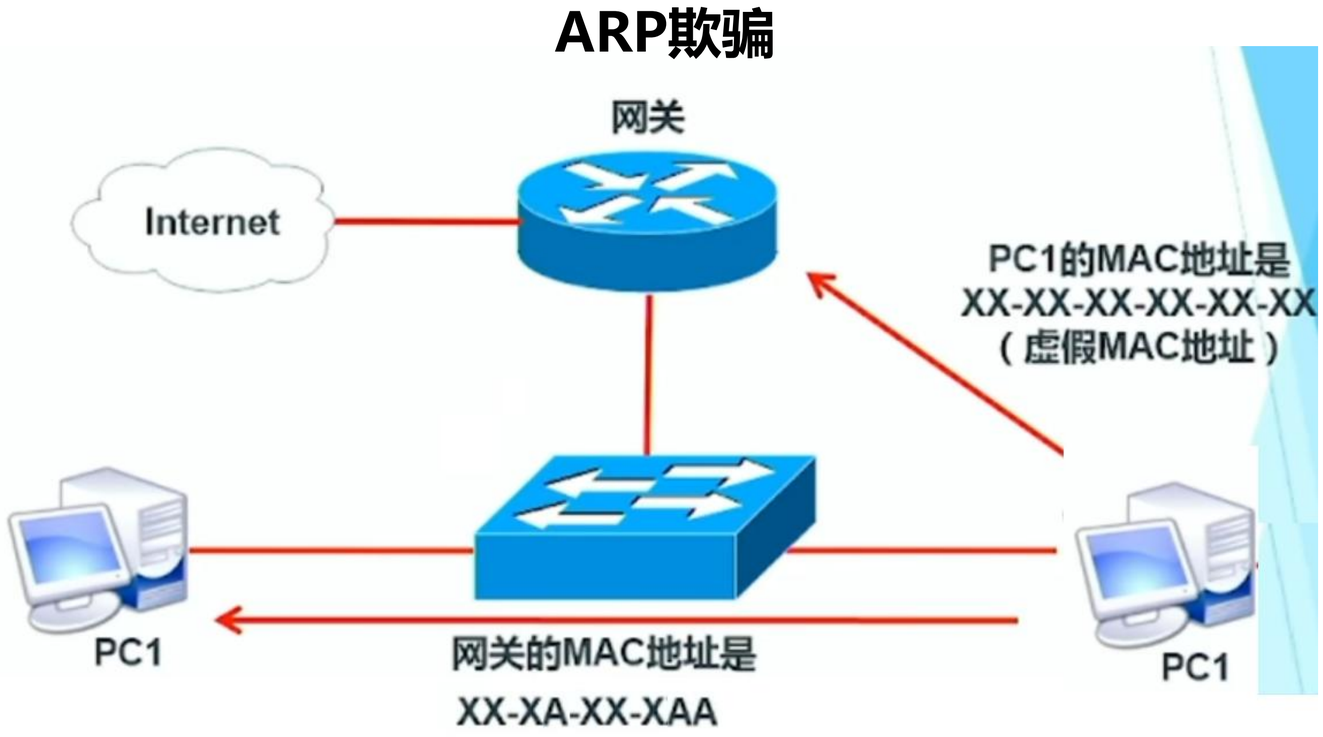
享学课堂 James老师

ARP协议

地址解析协议

ARP（Address Resolution Protocol）

根据IP地址获取物理地址的一个TCP/IP协议。



享学课堂 Xiangxue 致力于培养卓越的程序员

网络安全

WireShark之ICMP协议

享学课堂 James老师

ICMP协议

ICMP（Internet Control Message Protocol）Internet控制报文协议。它是TCP/IP协议簇的一个子协议，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

享学课堂 Xiangxue 致力于培养卓越的程序员

网络安全

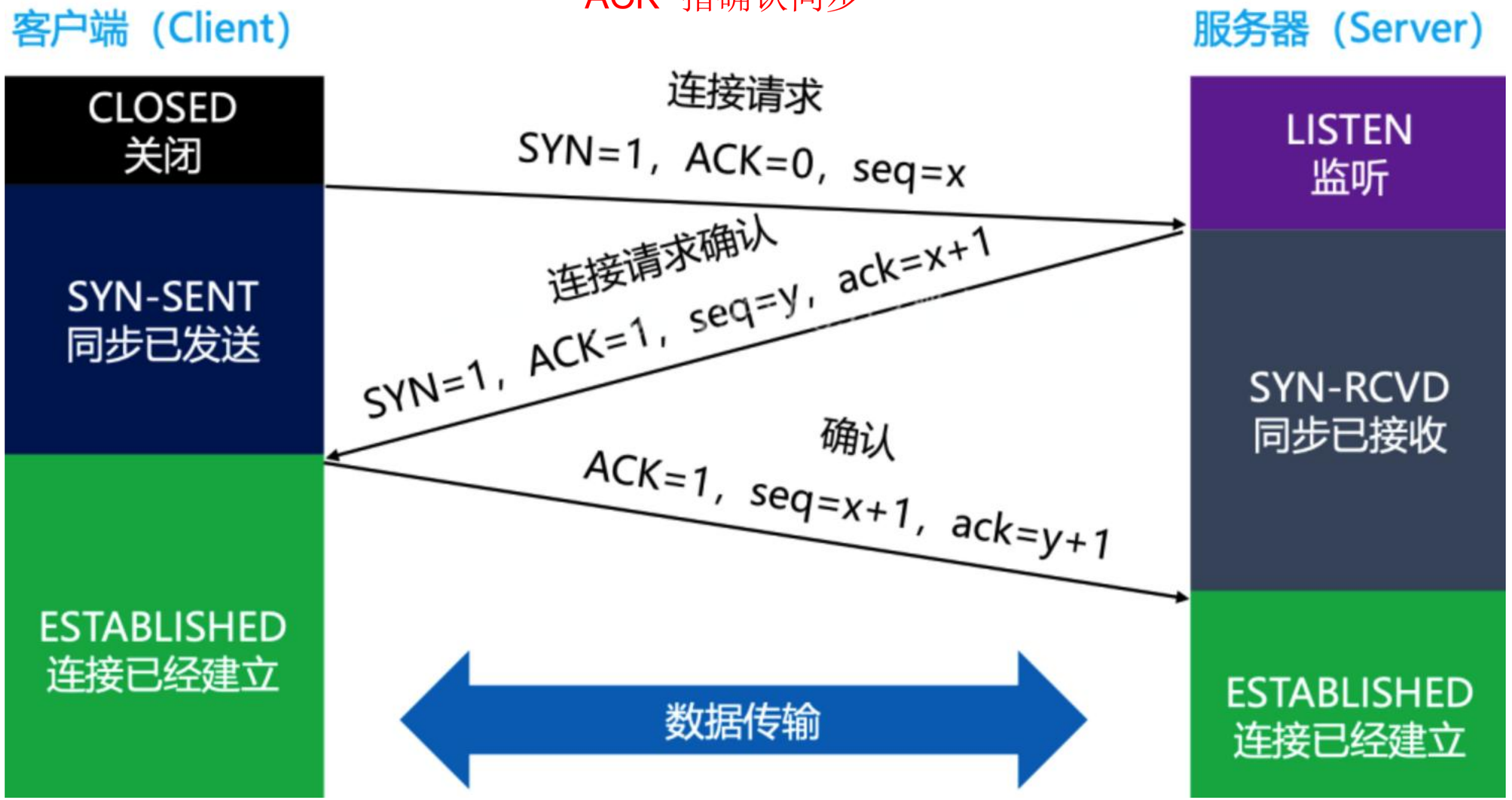
TCP连接的3次握手协议

享学课堂 James老师

TCP连接三次握手

SYN (synchronize) 指请求同步

ACK 指确认同步



享学课堂 致力于培养卓越的程序员

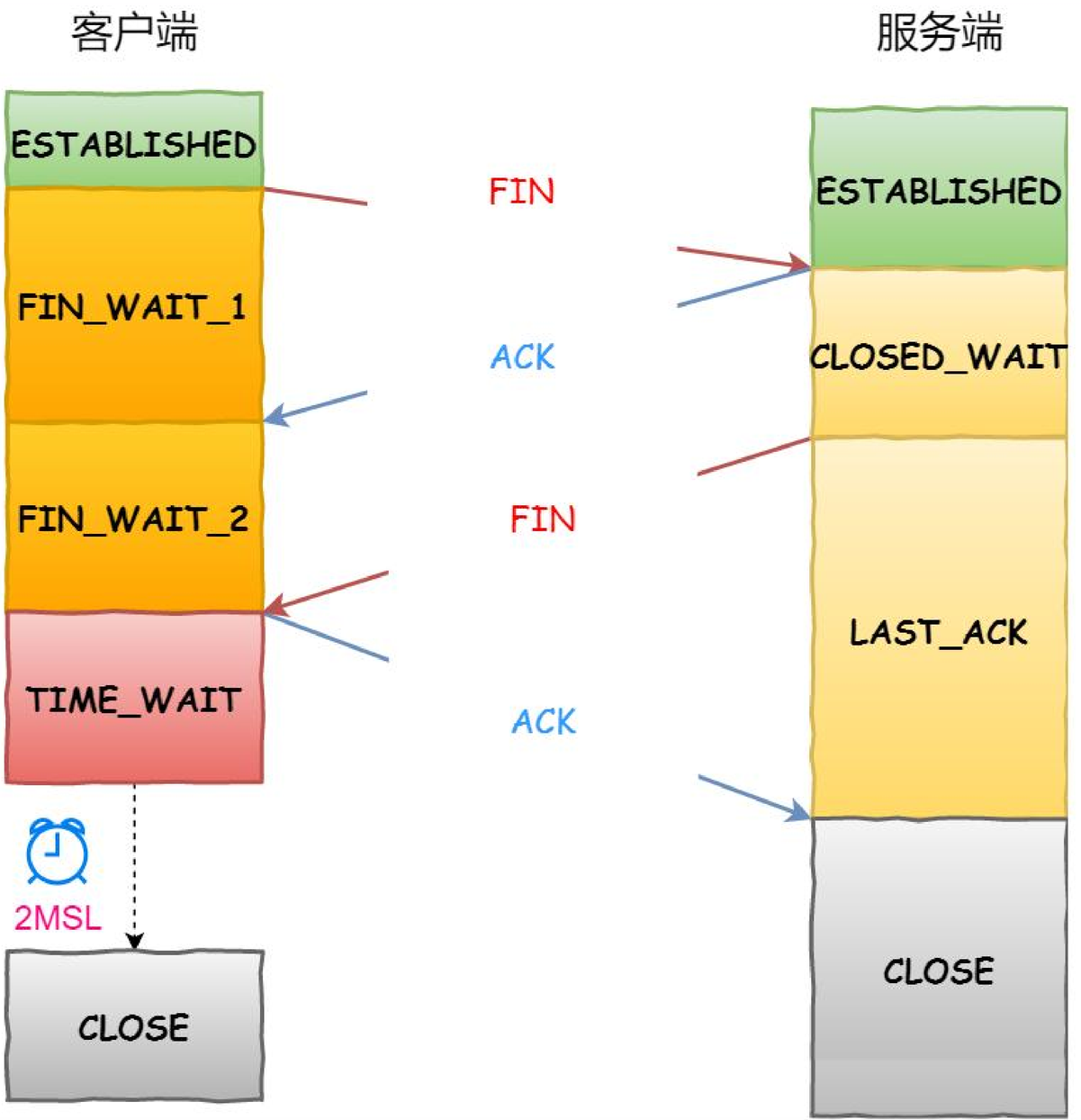
网络安全

TCP连接断开的4次挥手协议

享学课堂 James老师

TCP连接断开四次挥手

SYN 指请求同步
ACK 指确认同步
FIN 指结束



享学课堂 Xiangxue 致力于培养卓越的程序员

网络安全

WireShark抓HTTP协议

享学课堂 James老师

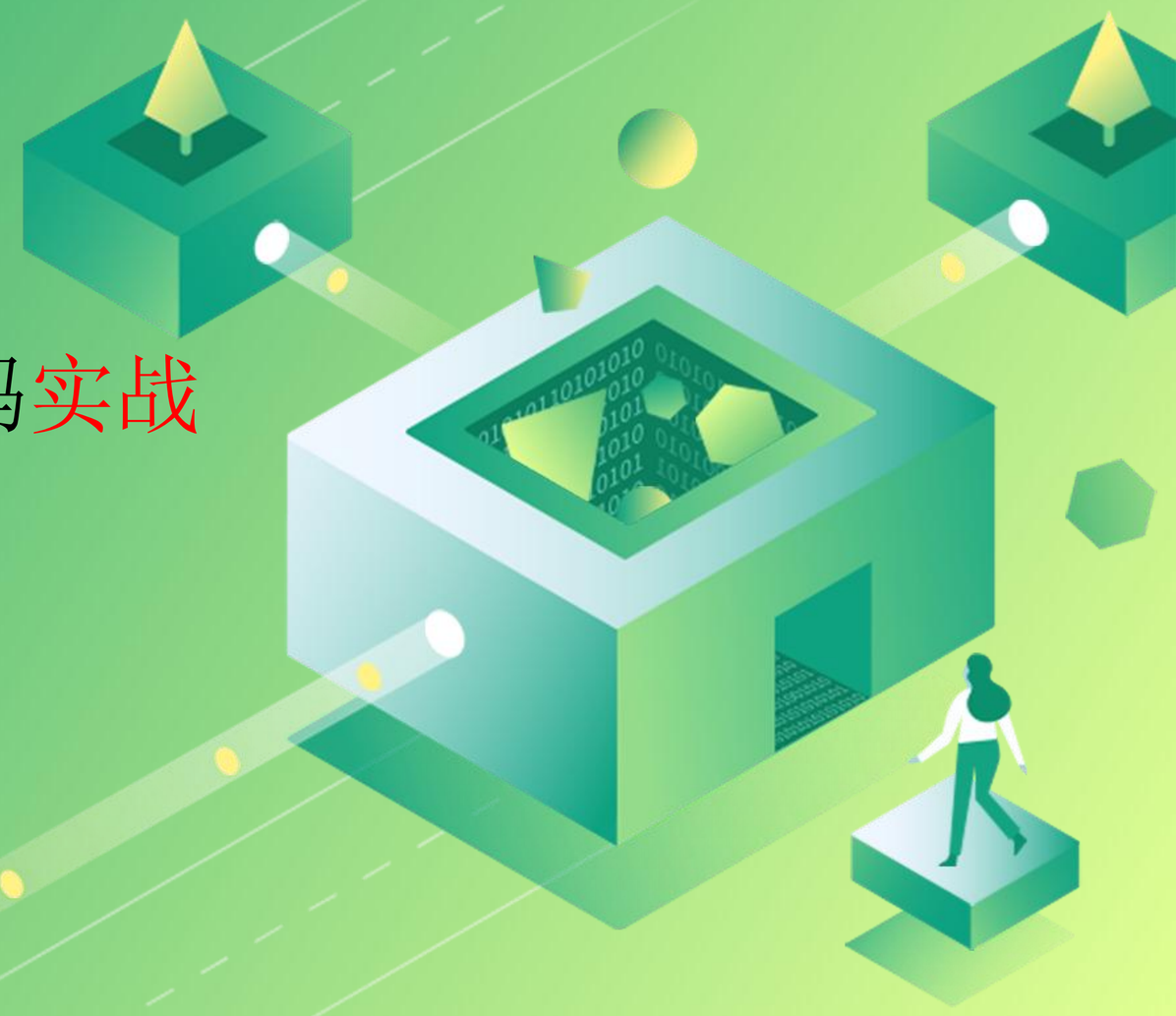
HTTP协议

属于应用层上层协议，其底层是对TCP协议的封装

享学课堂 Xiangxue 致力于培养卓越的程序员

网络安全

黑客利用WireShark获取用户密码实战



享学课堂 James老师

物料准备

1，NGINX
2，VM虚拟机
3，kali操作系统