▶ 下一章

## 知平 书店 : 查看目录 使用本书 示例捕获文件 科技基金会 ラ支持 章数据包分析技术与网络基础 1.1 数据包分析与数据包嗅探器 1.1.1 评估数据包嗅探器 1.1.2 数据包嗅探器工作过程 1.2 网络通信原理 1.2.1 协议 1.2.2 七层 OSI 参考模型 1.2.3 OSI 参考模型中的数据… 1.2.4 数据封装 1.2.5 网络硬件 1.3 流量分类 1.3.1 广播流量 1.3.2 组播流量

## 1.2.1 协议

▲ 上一章

现代网络是由多种运行在不同平台上的异构系统所组成的。为了帮助 们之间相互通信,我们使用了一套共同的网络语言,并称之为协议。常见 网络协议包括传输控制协议 (TCP)、互联网协议 (IP)、地址解析协议 (ARP) 和动态主机配置协议 (DHCP)。协议栈是由一组协同工作网络协 的逻辑组合而成的。

■ 图书详情

▲ 返回书架

理解网络协议的最佳途径之一是将它们想象成人类口头或书面语言的 用规则。每一种语言都有规则,如动词应该如何结合、人们该如何问候, 甚至该如何礼貌地致谢。网络协议大多也是以同样方式进行工作的,帮助 们定义如何路由数据包、如何发起一个连接,以及如何确认收到的数据。 个网络协议可能非常简单,也可能非常复杂,这取决于它的功能。虽然各 协议往往有着巨大的差异,但它们通常用来解决以下问题。

发起连接: 是由客户端还是服务器发起连接? 在真正通信之前必须要 换哪些信息?

**协商连接参数**:通信需要进行协议加密吗?加密密钥如何在通信双方 行传输?

**数据格式**: 通信数据在数据包中如何排列? 数据在接收设备时以什么 的顺序进行处理?

错误检测与校正: 当数据包花费过长的时间才到达目的地时该如何处 理? 当客户端暂时无法和服务器建立通信时,该如何恢复连接?

连接终止: 一台主机如何告知另一台主机通信已经结束? 为了礼貌地 止通信,应该传送什么样的最终信息?

接网络中嗅探

1.3.3 单播流量

1.4 小结

章监听网络线路

2.1 混杂模式



Wireshark 数据包分析实战(第3版) 作者:[美]克里斯·桑德斯(Chris Sander···