|  |  |  |  |
| --- | --- | --- | --- |
| **《计算机网络》实验报告** | | | |
| **实验编号** | 实验一 | **实验名称** | Protocol Layers |
| **姓名** | 叶俊 | **学号** | 202200201151 |
| **班级** | 菁英班 | **成绩** | 、 |
| 1. **实验目的**   借助WireShark软件，了解协议和分层是如何在数据包中表示的。 | | | |
| 1. **实验要求**   wireshark：使用wireshark软件工具用于捕获和检查数据包跟踪。  wget / curl:本实验使用wget (Linux和Windows)和curl (Mac)来获取web资源。wget和curl是获取URL的命令行程序。 | | | |
| 1. **实验内容** 2. Capture a Trace 3. Inspect the Trace 4. Packet Structure 5. Protocol Overhead 6. Demultiplexing Keys | | | |
| 1. **实验过程** 2. 安装WireShark      1. wget安装      1. 第一步Capture a Trace 2. Wireshark配置，这里只选择WLAN以排除其他接口的干扰，并输入tcp port 80进行筛选，最后开始      1. 本地与网站交互 输入命令wget [http://www.baidu.com](https://www.baidu.com/)      1. Wireshark捕获，及时停止捕获，点击NO，页面显示如下：     wget捕获成功：     1. 第二步 Inspect the Trace 检查跟踪   这几个为数据包    Wireshark在界面下方向我们了展示它可以识别的帧中携带的更高层的数据包、段和消息结构，每个帧中包含一个包，当我们选择一个协议为HTTP，消息列为GET的数据包，信息展示如下，由五部分组成：  （1）Frame: 此部分提供有关捕获的数据帧的基本信息，包括帧的编号、时间戳、帧的长度以及捕获该帧的网络接口等。  （2）Ethernet II: 在这一层，你会看到以太网帧头信息，如源MAC地址、目标MAC地址和以太网类型。  （3）Internet Protocol Version 4 (IPv4): 这一行展示了IP头部信息，包括源IP地址、目标IP地址、协议版本、头部长度、服务类型、总长度、标识、标志、片偏移、生存时间(TTL)、协议（通常是TCP或UDP）以及头部校验和。  （4）Transmission Control Protocol (TCP): 在TCP层，你可以看到端口号（源端口和目标端口）、序列号、确认号、数据偏移、保留、控制位、窗口大小、校验和以及紧急指针等。  （5）Hypertext Transfer Protocol (HTTP): 在HTTP协议层，Wireshark会展示HTTP请求的详细信息，    这是具体信号     1. 第三步 Packet Structure数据包结构   选中HTTP GET数据包，分别查看数据包每一段的大小信息：  第一条为“Frame”，它的长度为190 B，这是该数据包的总字长。    第二条为Ethernet层，总字长为14 B    第三条为IP协议层，总字长为20 B    第四条为TCP协议层，总字长为20 B    第五层为HTTP协议层，总字长为136 B    最终得出数据包结构如下：（单位：Byte）   |  |  |  |  | | --- | --- | --- | --- | | Ethernet | IP | TCP | HTTP | | 14bytes | 20bytes | 20bytes | 136bytes |  1. 第四步Protocol Overhead协议开销   找到一个包含SYN和ACK信号的TCP数据包：    总开销即为：66+54+190+56=366 B  由上一步说明可知，HTTP协议数据包中HTTP部分字长为136 B，因此有效信息占比为136/366 = 37.15%   1. 第五步Demultiplexing Keys解复用密钥   Ethernet层和IP层数据中有个字段用于表示自己的下一层： | | | |
| **四．实验心得**  通过本次实验，我深入了解了Wireshark和wget的使用方法，并掌握了数据包的捕获与解析技巧，从而加深了我对网络协议工作原理的认识。在初次尝试使用wget http://www.baidu.com命令时，我未能通过Wireshark捕获到HTTP GET请求。经过仔细排查，我意识到大多数现代网站已经转向使用HTTPS协议，这使得数据在传输过程中被加密，因此无法直接进行解析。这一发现促使我进一步探究了HTTPS的加密机制。  此次实践经历不仅让我认识到理论知识与实际操作相结合的重要性，还显著提升了我的问题分析和解决能力。同时，这次实验也激发了我对网络技术更浓厚的兴趣，为我在网络领域的深入学习奠定了坚实的基础。 | | | |