**深 圳 大 学 实 验 报 告**

**课程名称：­ 计算机网络**

**实验项目名称： 数据包抓取与分析**

**学院： 计算机与软件学院**

**专业： 软件工程**

**指导教师： 姚俊梅**

**报告人：郭昌华 学号：2022190025 班级： 02B**

**实验时间： 2024年3月29日**

**实验报告提交时间： 2024年3月31日**

**教务处制**

|  |  |
| --- | --- |
| **实验目的**  学习安装、使用协议分析软件，掌握基本的数据报抓取、过滤和分析方法，能分析 HTTP、TCP等协议。 | |
| **实验环境**   1. 使用具有Internet 连接的Windows 操作系统； 2. 抓包软件Wireshark。 | |
| **实验内容：**   1. 安装学习Wireshark 软件； 2. 抓包与分析HTTP 协议； 3. 分析TCP 协议； 4. 分析TCP 三次握手； |
| **实验步骤：**    图1: Wireshark的初始界面  1.2 如图2, 进入Wireshark主界面, 开始捕获分组.    图2: Wireshark的主界面  其中分组详情栏的解释如图3.    图3: Wireshark的分组详情栏的解释  1.3 使用过滤器  过滤器包括协议过滤、IP地址过滤、模式过滤、端口过滤.   1. 协议过滤   以过滤HTTP协议为例. 如图4, 在过滤器中输入”http”并回车, 观察到分组列表栏中的条目的Protocol都为HTTP.  注意上述操作只会过滤使用HTTP协议的条目, 而不会过滤HTTPS协议的条目.    图4: HTTP协议过滤   1. IP地址过滤       图7: IP地址过滤   1. 模式过滤   过滤分组列表栏中的http情求方法为GET的分组. 如图8, 观察到条目的Info中以GET开头.    图8: 模式过滤   1. 端口过滤   过滤分组列表兰中tcp端口号为80的分组. 如图9, 观察到条目的Info中的端口号都为80.    图9: 端口过滤  **抓包与分析HTTP协议**   1. 开启Wireshark抓包，在过滤器中输入http，即过滤http协议的分组。 2. 打开浏览器，输入一个网址（例如ieeexplore.ieee.org）。注意：为了避免浏览器缓存起作用，最好使用chrome浏览器的incognito隐身模式。     2.4 逐个查看分组详情栏, 检查哪些条目是浏览网页产生的分组. 如图11, 分析得前两个分组是浏览网页产生的, 可从分组列表栏中得知此次浏览网页的源IP地址和目的地IP地址, 从分组详情栏得知此次浏览网页的用户名和主机名.    图11: 浏览网页产生的分组   1. **分析TCP协议**   3.1 分析2.4中的分组的TCP协议信息. 如图12, 在分组详情栏中得知本次TCP连接的源端口号、目的端口号、序列号、确认号、报头长度、标志位、窗口大小、校验和、数据.    图12: TCP协议的详情  3.2 追踪上述分组的TCP流. 如图13, 右键该条目, 追踪流-TCP流.    图13: 追踪TCP流  3.3 如图14, 找到Info中带有[SYN]、[SYN, ACK]、[ACK]的前三个分组, 发现它们在HTTP GET请求之前, 它们是TCP建立的分组.  原理: ①TCP建立在HTTP GET请求前; ②TCP建立连接时会设置标志位SYN.    图14: TCP建立的分组   1. **分析TCP三次握手**     图15: TCP三次握手示意图  4.1 TCP第一次握手(SYN), 在分组详情栏中得知序号1457584277, 且Flags中的SYN位置1.    图16: TCP第一次握手(SYN)  4.2 TCP第二次握手(SYNACK), 在分组详情栏中得知序号、确认、ACK位置1、SYN位置1. 观察到确认号 = SYN序号 + 1. 即1457584278，同时有SYNACK=3485505084    图17: TCP第二次握手(SYNACK)  4.3 TCP第三次握手(ACK), 在分组详情栏中得知确认号、ACK位置1、SYN位置0. 观察到确认号 = SYNACK序号 + 1. 即3485505085    图18: TCP第三次握手(ACK) |
| **实验结果：**  在实验过程中，通过分析Wireshark提供的 TCP协议的数据包，我能清楚地识别出TCP数据包的源端口、目的端口、序号、确认号、标志位等关键信息。  利用Wireshark揭示TCP连接建立过程中的三次握手。实验中，我跟踪了客户端与服务器之间的数据交换，清晰地捕捉到了SYN、SYN-ACK和ACK三个阶段的数据包。首先，客户端发送带有SYN标志的数据包发起连接请求；随后，服务器回应一个SYN-ACK数据包表示确认并同步序列号；最后，客户端回复一个ACK数据包确认连接建立。这一系列动作生动展示了TCP连接建立的可靠性和有序性。  即之前提到的:  图15: TCP三次握手示意图  通过本次实验，我不仅掌握了Wireshark软件的基本操作和功能，而且加深理解了HTTP协议和TCP协议的实际应用及工作原理，特别是TCP三次握手的重要意义。 |
| **实验小结：**   Wireshark作为一个强大的网络封包分析工具，其详尽细致的数据展示让我对网络协议有了更为深入的认知。我对TCP三次握手有了比较清晰的认识。 |
| **指导教师批阅意见：**  **成绩评定：**  **指导教师签字：**  年 月 日 |
| 备注： |