**计算机网络课程实验报告**

**实验3：典型网络协议的深入认识与分析**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 姓名 |  | | 院系 | |  | | | 学号 | |  | |
| 任课教师 | |  | | | | 指导教师 |  | | | | |
| 实验地点 | |  | | | | 实验时间 |  | | | | |
| 实验课表现 | | 出勤、表现得分(10) | |  | | 实验报告  得分(40) |  | | 实验总分 | |  |
| 操作结果得分(50) | |  | |
| 实验目的： | | | | | | | | | | | |
| 熟悉并掌握Wireshark的基本操作；学会使用Wireshark分析各层协议的数据包格式。认识各个协议层之间的数据封装关系。 | | | | | | | | | | | |
| 实验内容： | | | | | | | | | | | |
| 1. 学习Wireshark的使用 2. 利用Wireshark分析HTTP协议 3. 利用Wireshark分析TCP协议 4. 利用Wireshark分析IP协议 5. 利用Wireshark分析Ethernet数据帧 | | | | | | | | | | | |
| 实验要求：（学生对预习要求的回答）（20分） | | | | | | | | | | | |
| * + 根据自己的理解，描述HTTP协议的工作过程（400字以内）。（10分）  1. 客户端通过查找URL里的域名所指的IP 2. 客户端向服务器的80端口发起TCP连接请求 3. 服务器与客户端建立TCP连接 4. 客户端通过TCP连接发送HTTP报文 5. 服务器解析请求并发送响应 6. 对于HTTP1.0，此时即断开TCP连接；对于HTTP1.1，客户端可能根据收到的HTML页面中的链接继续发出请求      * + 根据自己的理解，描述TCP协议的工作过程（400字以内）（10分）  1. 首先需要三次握手建立TCP连接 2. 使用滑动窗口发送数据，ACK序列号是期待接收的最小序列号 3. 如果三次接到同一ACK认为后续数据包已经丢失，立即开始重传 4. 断开连接时先发FIN，对方回复ACK，关闭连接，再发送FIN，收到后发送ACK并关闭，连接断开。 | | | | | | | | | | | |
| 思考题：（20分） | | | | | | | | | | | |
| 思考题1：（15分） | | | | | | | | | | | |
| 用自己的语言描述主要协议的捕获、分析过程（HTTP、 TCP、 IP、 ARP）？  HTTP：  在filter里填写http，即可捕获HTTP协议的数据。以访问<http://gaia.cs.umass.edu/ethereal-labs/alice.txt>为例，捕获的数据如下：    第一次访问时浏览器发出如下GET请求    服务器给出200响应，并附有alice.txt的内容    第二次再访问时HTTP报头里包含if-modified-since字段    由于文件没有变化，服务器响应304，并且不再发送alice.txt的内容    TCP：  在filter里填写http，即可捕获HTTP协议的数据。以访问<http://gaia.cs.umass.edu/ethereal-labs/TCP-ethereal-file1.html> 并上传alice.txt为例，捕获到大量的数据包，其中连接建立时如下：    可以看到浏览器发出了两个并行的TCP连接，分别在51174和51175端口，而服务器也对两个TCP连接都做出了相应。  发送数据时的部分包截图如下：    可以看到本机发出的TCP包大小为1514字节，而服务器响应的ACK为60字节。ACK包含期望接受的序列号以及窗口大小。  IP：  在filter里指定IP和访问的目的ip地址即可捕获IP协议。    可以从下面的协议内容里看到IP数据包的组成和内容。  ARP：  使用arp –a可以查看缓存    清空缓存后发出连接，即可在wireshark中捕获 | | | | | | | | | | | |
| 思考题2：（5分） | | | | | | | | | | | |
| * 实验结论，以及实验中遇到的其他问题是如何解决的？  1. 刚开始绑定网卡时，由于使用了虚拟机，错误的绑定到了虚拟机的虚拟网卡接口上，导致捕获不到数据包。更改为真实的有限网卡接口之后捕获成功。 2. 由于我电脑开了wifi热点，导致使用我wifi的同学的数据包也都被我捕获到了。后来我下课后单独实验就没有干扰了。 | | | | | | | | | | | |
| 选做内容，加分项目成果展示（过程描述、截图） | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 指导教师评语： | | | | | | | | | | | |
| 日期： | | | | | | | | | | | |