

**实 验 报 告**

**（ 2020/ 2021 学年 第 一 学期）**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 课程名称 | 网络信息安全 | | | | | |
| 实验名称 | 使用wireshark捕获数据包 | | | | | |
| 实验时间 | 2020 | 年 | 11 | 月 | 18 | 日 |
| 指导单位 | 计算机学院信息安全系 | | | | | |
| 指导教师 | 吴礼发 | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 学生姓名 | 殷祥 | 班级学号 | B18030825 |
| 学院(系) | 计软网安学院 | 专 业 | 信息安全 |

**实 验 报 告**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **实验名称** | | 使用wireshark捕获数据包 | | | | | **指导教师** | | 吴礼发 |
| **实验类型** | | 上机 | | **实验学时** | | 2 | **实验时间** | | 2020.11.18 |
| 1. **实验目的和要求**   1.在Windows 环境下安装和使用wireshark；  2.设置好过滤器后运行wireshark，要求只捕获TCP协议数据包；  3.打开wireshark，同时打开浏览器登录：南京邮电大学邮箱、163或qq邮箱、淘宝（或支付宝），观察wireshark已捕获的数据包，看从中能否发现监听到的用户名和密码。 | | | | | | | | | |
| 二、**实验环境(实验设备)**  1.安装Windows操作系统并连接网络的一台PC机。  2.wireshark以及winpcap | | | | | | | | | |
| **三、实验内容**  1. 利用Wireshark抓取TCP包，找出TCP三次握手数据包，并分析IP包头和TCP包头的结构。  如图所示：  Text  Description automatically generated  2. 登陆南京邮电大学邮箱，发现是通过http明文传输的用户名和密码：  Graphical user interface, text  Description automatically generated  3. 登陆163邮箱，发现会通过TLS协议对流量进行加密，无法看到登陆过程中传输的用户名和密码：  A screenshot of a computer screen  Description automatically generated  4. 登陆淘宝，同样发现也会通过TLS协议对通信流量进行加密：  Graphical user interface, text, application  Description automatically generated | | | | | | | | | |
| **四、实验小结（包括问题和解决方法、心得体会、意见与建议等）**  问题：Wireshark抓包时，不知道对应域名的实际ip，无法过滤出相关的流量包  解决：通过ping域名，可以知道对应的ip地址，进而使用表达式对流量包进行过滤。  心得体会：学校邮箱登陆过程，使用了明文传输用户名和密码，很不安全，应该使用TLS协议对通信流量进行加密。 | | | | | | | | | |
| **五、指导教师评语** | | | | | | | | | |
| **成 绩** |  | | **批阅人** | |  | | **日 期** |  | |