哈尔滨学学院

《计算机网络与信息安全》

分析报告

题 目： （此处输入本组的题目 ）

班 级：

组 长：（此处学号姓名及分工的部分）

组 员：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 分析报告主题：  应用Wireshark对访问WEB网站的过程进行数据的捕获，并应用计算机网络原理相关知识对捕获的内容进行分析。  你们访问的网站为： | | | | | |
| 主要内容：  本次实验活动主要完成的工作是：  　　1.应用Wireshark对访问WEB网站的过程进行数据的捕获；  2.对DNS进行域名与IP解析的过程进行分析；  3．分析web访问的GET及响应过程；  4．对传输层的三次握手过程进行分析  5．对IP数据报进行分析  6．实验总结 | | | | | |
| 理论依据：实验的设计原理 | | | | | |
| 学号 | 姓名 | 职责 | 分工 | 完成度 | 评分 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| 总分： | | | | | |

（报告正文部分格式要求，标题为四号黑体，居中。正文为宋体小四，首行缩进两个字符。行距1.5）

一、实验主题

应用Wireshark对 web网站访问过程进行数据的捕获，并应用计算机网络原理进行数据分析。

二、实验工具

Wireshark

三、实验步骤

本次实验为《计算机网络与信息安全》课程的协议分析实验，实验步骤如下：

1、启动Wireshark，进行\*\*\*设置

2、开启一个\*\*访问

3、根据上文的实验设计原理，做了什么操作，分析捕获了什么数据 。如应用了什么条件的设置，或应用了什么过滤等操作，获得了什么数据以及为什么这样的设计。

四、实验结果

捕获的数据内容为：*（截图）*

截图主要界面，以及主要数据部分。

**五、数据分析**

1、DNS分析：完成人：

找到DNS将web网站解析为IP地址的相应帧，并分析其完成的请求与响应的过程，以及返回的IPV4和IPV6的情况。

从应答报文中得到了：*（截图）*

查询报文分析

以太网帧头部中，查询报文大小是

源MAC地址是 目标MAC地址是：

DNS是基于　　　　　协议。源端口号是 目标端口号是

源IP地址是 目标IP地址是

DNS报文分为

通过对DNS报文分析得到了如下结论：*（首部说明）*

2、HTTP访问分析，完成人：

找到客户端GET主页面以及服务器收到请求并发送响应包，以及服务器发送主页面给客户端的通信过程，并进行分析。

报文内容如下：*（贴图）*

报文内容的解读如下：*（首部说明）*

3、传输层分析，完成人：

传输层协议分析在捕获的数据包中要求找到TCP的三次握手报文等关键环节，并结合网络原理进行分析。同时观察可变窗口的变化，结果理论进行分析说明。

1. 过滤出所有传输层TCP报文内容，从中找出本次HTTP访问的TCP建立连接的三次握手TCP报文（指明行号并贴图），
2. 说明如何判断是本次访问的三次握手的报文。

3．在报文交换的过程中，解读三次握手的报文的传递信息的意义及如何完成三次握手。

4．以第一次握手的报文为例，解读报文头部的信息各代表什么含义？（首部说明）

4、网络层分析，完成人：

网络层协议分析

在捕获的数据包中找到报文头部中关键字段，分析IP数据报的状态，如分片状况，观察TTL的变化，

报文内容为：（截图）

关键字段分析：（首部说明）

六、总结

在这个过程中，进行了什么操作，掌握了什么知识，收获了什么能力，对本课程的认识有了什么不同。小组同学共同完成。

执笔人：