

**实验报告**

**课程名称： 计算机网络**

**学生姓名： 朱方灏钧 学号： 210111316**

**年级专业： 软件工程 班级： 人大19.11**

**指导教师： 张毅**

**开课学期： 2021 年— 2022 年 第一 学期**

**宜宾学院人工智能与大数据学部实验教学中心**

**宜宾学院人工智能与大数据学部**

**实验报告**

**年级：19.11 专业：软件工程**  **上课日期： 2021**年11月7日

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **实验名称** | **网络抓包工具** | | | | | |
| **学生姓名** | **朱方灏钧** | **学号** | **210111316** | **实验合作者 姓名** | **无** | |
| **指导教师(签名)** |  | **评 阅 日 期** | |  | **实验报告分** |  |
| **实验报告基本内容：**一、实验目的；二、实验内容；三、实验原理；四、实验步骤及结果；五、实验遇到问题及解决方法；六、实验结论 | | | | | | |
| 1. 实验目的：   1、熟悉wireshark工具的主要用途。  2、掌握wireshark工具的基本使用方法。   1. 实验内容：   1、下载wireshark抓包分析工具并安装。注意操作系统版本，特别是32位操作系统和64位操作系统的区别。建议用电脑安装，注意安装时的注意事项。苹果电脑请下载专用版本。  2、查看自己的IP地址和MAC地址。Windows系统用命令提示符查看，在运行中输入CMD，或在开始菜单“Windows附件”/“Windows系统”中打开命令提示符。在命令提示符中输入ipconfig -all，查看本机物理地址和IP地址。MAC系统在系统更偏好设置-网络-选择已连接网络查看本机物理地址和IP地址。  3、启动wireshark软件，选择准备捕获数据包的网卡接口。  4、过几秒钟后停止捕获，观察捕获到的数据包。  5、在过滤条件中，选择查看自己IP地址发出的数据包，使用过滤条件“ip.src==步骤2中查看到的IP地址”，并在数据包详情窗口查看源MAC地址是否是步骤2中查看到的本机的物理地址。   1. 实验原理：   利用wireshark的抓包功能进行实验   1. 实验步骤及结果   2.  IMG_256  3.  IMG_256  4.  IMG_256  5.  IMG_256  6.  IMG_256  **思考题：**   1. 每次自己发出或接收的数据包，自己的IP地址和MAC是否总是对应的？   答：只要是同一网络连接发出或接收的数据包，IP地址和MAC就总是对应的。   1. 尝试写一条规则，查找所有的HTTP协议的数据包。   答：http   1. 尝试写一条规则，查找所有自己的IP地址发出的DNS数据包。   答：ip.src==192.168.0.100 && dns  4、wireshark主要有哪些用途？  答：wireshark网络抓包工具可以看到网络上发出或者接收的所有数据包，通过对数据包进行分析，可以对网络攻击，软件安全性测试，程序调优，分析流程、功能、数据等对网络，网站，程序进行相应的优化，还可以通过分析其他软件的数据进行破解等操作。   1. 实验遇到问题及解决方法   写规则比较难，解决办法：通过规则中的提示进行尝试   1. 实验结论   答：wirespark是一个专业的数据抓包软件，我对此知之甚少，对其中的知识具有强烈的好奇心，希望有一天我能通过这个软件自由的做出很多操作，所以我要更加努力的学习，在其他未知领域有所涉猎。 | | | | | | |
| **指**  **导**  **教**  **师**  **评**  **语** | | | | | | |