实验二：网络监听工具的安装使用

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **课 程** | 计算机网络基础 | **实验项目** | 实验二 网络监听工具的安装与使用 | **成 绩** |  |
| **学 号** | **202231060920** | **姓 名** | **李浩楠** | **实验日期** | 2024/1/2 |
| **专业班级** | 软件工程2022级3班 | | | **指导教师** | 何中越 |

## 实验场景

本次实验需在小组合作的基础之上完成。每个小组由两位成员组成，相互之间通信，通过网络监听工具截取通信数据包，分析数据包完成实验内容。

小组情况表:

|  |  |  |
| --- | --- | --- |
| 小组成员姓名 | 成员机器IP地址 | 是否本机 |
| 李浩楠 | 192.168.9.179 | 是 |
| 董成阳 | 192.168.9.25 | 否 |

## 一、基本要求

通过本次实验，学生可以掌握如下基本操作：

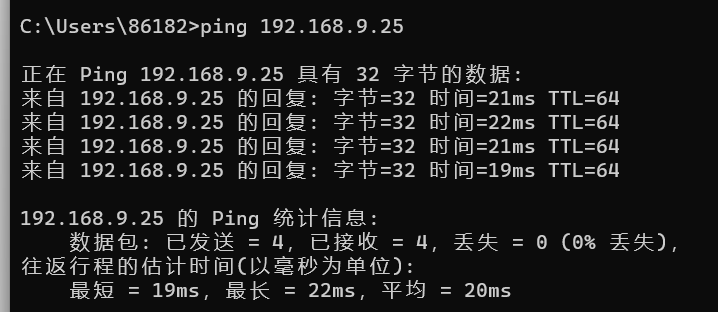
（1）、使用网络监听工具；

（2）、熟悉网络监听工具的原理及被监听的危害；

## 二、实验内容

1. 通过ipconfig命令获取本机IP地址,并填写上面的小组情况表。
2. 下载网络监听工具wireshark和winpcap并安装；

（1）、首先安装winpcap；（2）、安装wireshark。

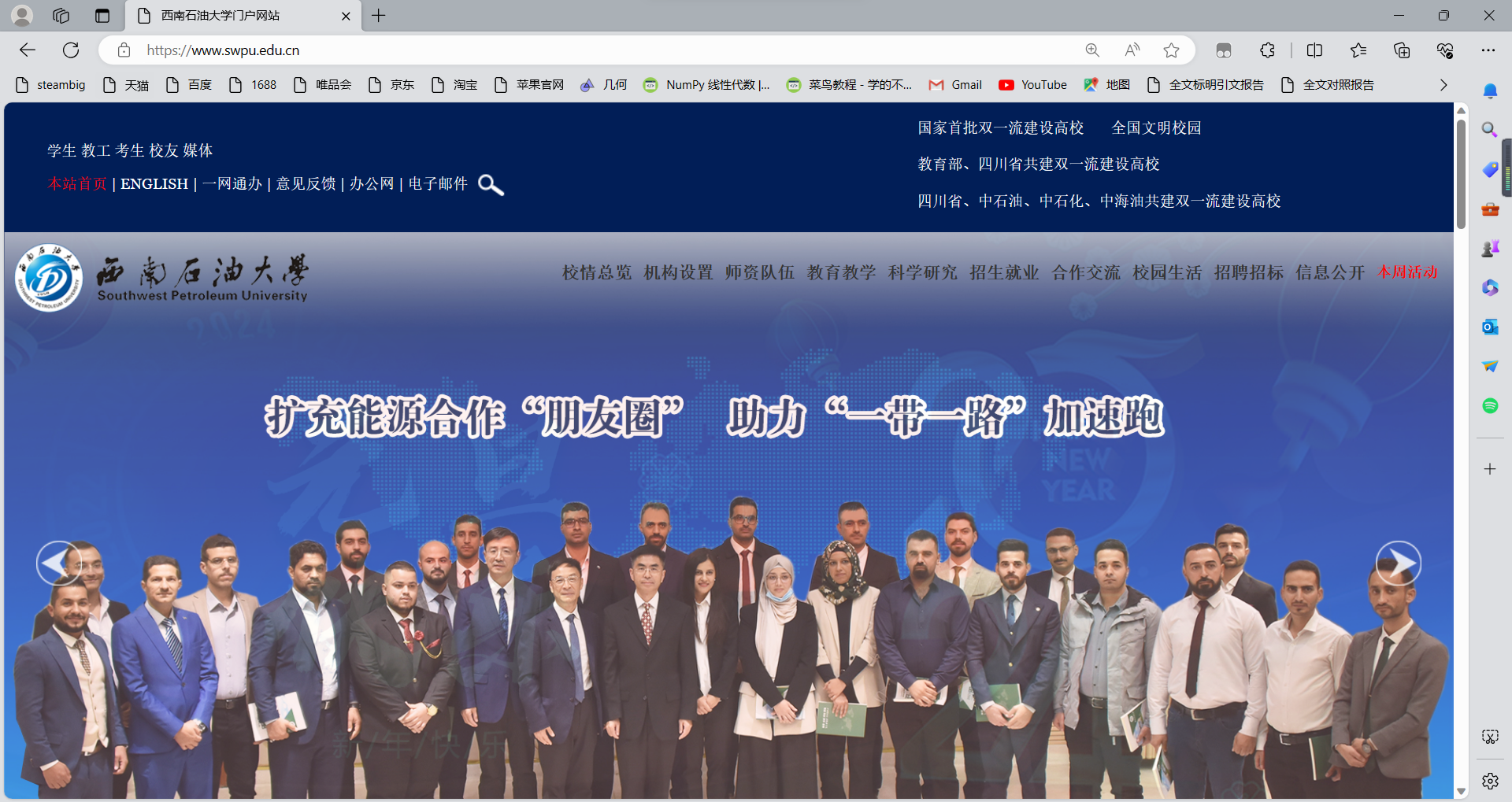
1. 从本机ping小组另一位成员的计算机，使用wireshark截取**ping过程中的通信数据**。
2. 分析截取的由于第3步操作而从本机发送到目的机的数据帧中的IP数据报并填写下表。

|  |  |
| --- | --- |
| IP协议版本号 | 4 |
| 服务类型 | 0x00 |
| IP报文头长度 | 20 |
| 数据报总长度 | 60 |
| 标识 | 0x9ec8(40648) |
| 数据报是否要求分段 | 要求 |
| 分段偏移量 | 0 |
| 在发送过程中经过几个路由器 | 1 |
| 上层协议名称 | ICMP(1) |
| 报文头校验和 | 0x0000 |
| 源地址 | 192.168.9.179 |
| 目标地址 | 192.168.9.25 |

1. 分析截取的由于第3步操作而从目的机返回到本机的数据帧中的IP数据报并 填写下表。

|  |  |
| --- | --- |
| IP协议版本号 | 4 |
| 服务类型 | 0x00 |
| IP报文头长度 | 20 |
| 数据报总长度 | 60 |
| 标识 | 0x5a0c(23052) |
| 数据报是否要求分段 | 要求 |
| 分段偏移量 | 0 |
| 在返回过程中经过几个路由器 | 1 |
| 上层协议名称 | ICMP(1) |
| 报文头校验和 | 0x8c98 |
| 源地址 | 192.168.9.25 |
| 目标地址 | 192.168.9.179 |

1. 从本机启动浏览器，通过HTTP协议进行某网页的访问。



1. 分析截取的由于第6步操作而从本机发送到目的机的数据帧中的TCP数据报并填写下表。

|  |  |
| --- | --- |
| 数据发送端口号 | 53550 |
| 通信目标端口号 | 443 |
| TCP报文序号 | 1 |
| TCP报文确认号 | 1 |
| 下一个TCP报文序号 | 2 |
| 标志位含义（如“确认序号有效”） | 确认号有效 |
| 窗口大小 | 515 |
| 校验和 | 0xdba5 |
| 源IP地址 | 192.168.9.179 |
| 目标IP地址 | 119.39.154.7 |

1. 分析截取的由于第6步操作而从目的机返回到本机的数据帧中的TCP数据报并 填写下表。

|  |  |
| --- | --- |
| 数据发送端口号 | 443 |
| 通信目标端口号 | 53550 |
| TCP报文序号 | 1 |
| TCP报文确认号 | 2 |
| 下一个TCP报文序号 | 无 |
| 标志位含义（如“确认序号有效”） | 确认号有效 |
| 窗口大小 | 190 |
| 校验和 | 0x3ce2 |
| 源IP地址 | 119.39.154.7 |
| 目标IP地址 | 192.168.9.179 |

## 三、实验报告

1、记录实验内容各步骤的实验结果，对照课本内容对网络层和传输层数据包进行复习整理。

## 四、总结

1.Wireshark是一款功能强大的网络抓包工具，可以用于分析和调试网络通信过程。

2.通过使用Wireshark进行ping抓包和访问网页的TCP抓包，可以深入了解网络通信的细节和原理。

3.在实际应用中，可以使用Wireshark来排查网络故障、分析网络性能等问题。