1. **实验心得体会如有雷同，雷同各方当次实验心得体会成绩均以0分计。**
2. **在规定时间内未上交实验报告的，不得以其他方式补交，当次心得体会成绩按0分计。**
3. **报告文件以PDF文件格式提交。**

**本报告主要描述学生在实验中承担的工作、遇到的困难以及解决的方法、体会与总结等。**

|  |  |  |
| --- | --- | --- |
| **实验名称** | **计算机网络基础及常用工具** | |
| **组长** | **姓名** | **学号** |
| 李骏豪 | 21307359 |
| **组员** | **叶梓聪** | **21307417** |
| 李骏豪 | 21307359 |
| 梁铭恩 | 21307360 |
| **实验分工** | | |
| **姓名** | **任务** | |
| **叶梓聪** | 主要负责完成了实验1，4，5及实验报告 | |
| 李骏豪 |  | |
| 梁铭恩 |  | |

**（\*请将上表中本人的名字加粗）**

【**交报告**】使用FTP方式提交，推荐使用Filezilla客户端

地址为ftp://ftp.network-security.asia；账号与密码为：student/5ecur1ty

文件以组号（组长学号）+组员学号+实验名称命名

# 本人承担的工作

主要负责完成实验1，4，5及实验报告。

# 遇到的困难及解决方法

（1）在实验四中正常主机执行dhclient -r命令释放从DHCP服务器获取的IP地址，但是释放失败，通过查阅资料，需要执行sudo dhclient -r才能释放成功，同理，在实验五中正常用户主机想要从DHCP服务器获取IP地址，需要执行sudo dhclient命令。

（2）在实验五中，在攻击者主机上配置好内核参数，配置并启动DHCP服务后，正常用户主机申请IP地址并访问外网，但是攻击者主机上缺无法捕获到正常用户主机的数据包，后来询问助教和重新阅读实验指导书，关闭路由器并且攻击者配置内核参数之后，需在正常用户主机上执行IP route flush cache来清空路由缓存，攻击者主机才成功捕获到正常用户主机的数据包。

# 体会与总结

本次实验加深了我对局域网安全的学习与理解，关键实验原理与体会总结如下：

实验一：该实验中，攻击者主机通过发送虚假的ARP Request和ARP Reply包进行缓存投毒攻击，请求和响应数据包使得正常用户将攻击者的MAC地址关联到正确的IP地址上，这种攻击方式巧妙地利用了ARP协议的设计缺陷，体现ARP协议的局限性，同时在这个实验中加深我对ARP协议的工作原理及作用，加深理解局域网中交换机和路由器的工作原理，掌握ARP投毒攻击的基本原理。

实验二：该实验的核心思路是通过编写基于ARP缓存投毒来更改局域网内设备的ARP缓存表，从而实现对网络通信的拦截和篡改，实验中攻击者同时污染用户主机和网关的缓存，使得在用户主机缓存中，网关IP对应的是攻击者的MAC，在网关缓存中，用户主机IP对应的是攻击者的MAC，从而实现攻击者作为中间人窃听正常用户与外网Web服务器交互的网络流量，再一次体现了ARP协议在网络安全中的脆弱性。

实验三：该实验主要是为了学习DHCP协议的工作原理及作用，为后续的实验四和实验五做知识准备，通过配置并启动DHCP服务器，捕获分析DHCP协议报文格式，理解主机通过DHCP服务器自动获取IP地址的过程，也为后续实验中基于DHCP协议的编程打下基础，理解了DHCP分配IP地址的原理后也更加容易理解DHCP环境中存在潜在危险，即如实验四和实验五所涉及的拒绝服务攻击和劫持攻击。

实验四：该实验的本质是为了将DHCP服务器地址池中的地址耗尽，导致正常用户无法在从DHCP服务器中申请到IP地址，使其无法进行网络通信，从而达到DHCP拒绝服务的目的，这体现了DHCP协议的脆弱性。

实验五：该实验的原理相较于前几个实验相对简单，关闭路由器的DHCP服务或者使DHCP服务器拒绝服务，迫使正常用户从攻击者建立的恶意DHCP服务器自动获取IP地址、DNS服务器等配置，从而使得后续正常用户的网络通信都被攻击者劫持，让我更加明白了DHCP在网络自动配置中的核心作用。

通过这次的五个实验，我对网络协议的工作原理和网络安全的复杂性有了更深入的理解，了解攻击手段的同时，也学习了相应的防御措施，体会到攻防平衡的必要性，亲自动手实践比单纯学习理论知识更能加深理解，所有实验都强调了网络安全的重要性，特别是在局域网环境中，协议的安全性尤为关键。