实验二心得体会

学号	姓名
20319045	刘冠麟

在这次实验中我负责了实验二、实验三、和实验四的实现与报告编写，通过本次局域网安全实验，我对网络中的ARP和DHCP协议有了更深入的理解。实验的主要目的是掌握ARP协议的工作原理、ARP投毒攻击的原理，以及DHCP协议的工作机制和相关的安全威胁。通过实验，我不仅理解了这些协议的工作原理，还学会了如何防范相关的攻击。

在实验中，我首先配置了网络环境，学会了通过使用WireShark分析Web访问过程流量，对于未进行ARP投毒的情况下攻击者显然无法捕获被攻击用户的HTTP请求。为了进行ARP投毒，我沿用了实验一中编写的ARP投毒代码，编写了基于ARP缓存投毒的中间人攻击脚本，发起攻击后再使用WireShark验证攻击效果，实验结果表明，通过ARP投毒攻击，攻击者可以截获和篡改网络流量，甚至可以捕获敏感信息如用户名和密码。

在实验三中，我进行了路由器DHCP服务器的配置，并且学会对路由器的DHCP记录和地址池等信息进行分析；并且使用了WireShark分析DHCP流量，成功捕获了DHCP服务器分配IP的四个过程（DHCP Discover、DHCP Offer、DHCP Request、DHCP ACK），对DHCP的过程有了更深刻的了解，为实验四作了铺垫。

在实验四中，我使用了scapy编写了DHCP攻击脚本，通过大量发送DHCP请求，可以耗尽DHCP服务器的地址池，导致正常用户无法获取IP地址，实验证实了DHCP协议的脆弱性。

通过这次实验，我不仅学会了如何使用WireShark对DHCP、HTTP流量捕获和分析，熟悉了ARP投毒攻击以及DHCP拒绝服务攻击的大致流程，令我对ARP和DHCP这两个协议有了更深刻的理解，极大地提高了我的实际操作能力以及网络安全意识，让我认识到了网络协议的潜在风险，巩固了我的信息安全知识，令我受益匪浅。