实验三心得体会

学号	姓名
20319045	刘冠麟

在这次实验中，我负责了实验一的实现与报告编写，通过本次DNS域名系统安全实验，我对网络中的DNS协议及其安全威胁有了更深入的理解。实验的主要目的是掌握DNS缓存污染攻击的原理、DNS拒绝服务攻击的工作机制以及如何防范这些攻击。通过实验，我不仅理解了这些攻击的工作原理，还学会了如何使用相应的工具进行攻击和防范。

在实验一中，我们首先在攻击者主机上查询了imool.net权威域名服务器的地址，确定了攻击脚本需要用到的权威域名服务器源IP。然后在本地域名服务器机器上，修改了本地域名服务器配置，将BIND9随机化端口设置为固定端口，并重新启动BIND9。

接下来，在攻击者主机上，我们使用scapy编写了代码，实现对DNS响应报文的伪造。通过猜测DNS响应报文中的TXID字段来实现碰撞检测，由于python的速度很慢（一般情况下一秒只能发几十个包），我们小组成员尝试了包括使用专门发送大规模数据包的库以及函数、多线程执行、预发送等技巧，提高发包速度，最终成功发起了DNS缓存污染攻击。

实验结果表明，通过DNS缓存污染攻击，攻击者可以向受害者返回伪造的DNS响应，从而控制受害者的网络流量。为进一步验证攻击效果，我们配置了一个钓鱼网站，并在受害者访问钓鱼网站时成功验证了DNS缓存污染攻击的效果。通过实验，我对DNS缓存污染攻击有了更深刻的理解，并认识到其严重的安全威胁。

通过这次实验，我不仅学会了如何使用scapy编写DNS攻击脚本，还熟悉了DNS缓存污染攻击和DNS拒绝服务攻击的工作原理及其防范措施。实验让我对DNS协议及其安全威胁有了更深刻的理解，极大地提高了我的实际操作能力以及网络安全意识。同时，也让我认识到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。