信息安全技术实验心得体会报告

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	合作完成实验一二及实验报告	
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

1. 本人承担的工作

合作完成实验一二及实验报告

2. 遇到的困难及解决方法

实验一中碰撞成功概率比较低，为了提升发包速度，我们先尝试提前构造好所有要发送的数据包，但是碰撞结果还是不太理想，后来仔细阅读实验指导书，对构建好的数据包进行并行发送，才得以碰撞成功。

信息安全技术实验心得体会报告

3. 体会与总结

域名系统 DNS 作为互联网关键基础设施之一，在计算机网络领域发挥着关键的作用，它负责将域名转换为 IP 地址，从而使得用户能够通过易于记忆的域名来访问互联网上的资源，通过本次实验，我学习了解到了域名系统安全的相关知识，通过两种不同的对域名安全系统的攻击方式，我体会到了域名系统存在安全性问题，本次实验的心得总结如下：

实验 1：DNS 缓存攻击的要点是，攻击者编写 DNS 缓存污染攻击脚本，发起 DNS 缓存污染攻击，目的是在正常用户的域名查询响应到达之前，攻击者将错误的域名解析响应插入到正常用户的 DNS 缓存中，而攻击者攻击成功的要点是在正常用户收到正确的域名解析响应之前，能够破解出正常域名的本地 DNS 服务器发出的查询报文的 TXID 字段，并伪造 DNS 响应报文，这也是本次实验的关键所在，为了提高碰撞成功的概率，需要提升发包的速度，因此我们采用的方法是提前构建好不同 TXID 的包，并通过一个列表保存好，再并行发送，提升发包速度，从而提升碰撞成功率。

实验 2：DNS 拒绝服务攻击的要点，通过伪造 DNS 请求，DNS 服务器反射放大响应，从而实现目标地址（受害者）收到来自大量来自不同 DNS 服务器的响应，造成网络堵塞甚至瘫痪，实验中通过观察受害者收到的数据包大小和流量来分析攻击效果并计算放大倍数。同时，在本次实验中学习了如何防御 DNS 拒绝服务攻击，通过部署和配置限制流量防御机制，可以有效减少和防止此类攻击对网络服务的影响。

域名系统安全是保障互联网正常运行和保护用户数据安全的重要组成部分，DNS 是互联的关键基础设施。本次实验，通过理论学习，实际操作，代码编写，流量分析等，我深入理解了 DNS 安全的重要性，两个攻击实验让我理解到 DNS 存在一定的安全问题，同时在实验中思考如何防范这些安全问题，增强了我实际应对网络攻击的能力和经验，掌握了 DNS 解析过程的工作原理及其关键环节，掌握 DNS 缓存污染攻击和 DNS 拒绝服务攻击的原理、执行条件、攻击过程及危害，并探索应对这两种攻击的防御策略及技术。