**深 圳 大 学 实 验 报 告**

**课程名称：­ 计算机安全导论**

**实验项目名称­： 拒绝服务攻击实验**

**学院： 计算机与软件学院**

**专业： 软件工程（腾班）**

**指导教师： 陈飞**

**报告人： 黄亮铭 学号： 2022155028 班级： 腾班**

**实验时间： 2024年11月09日-2024年11月24日**

**实验报告提交时间： 2024年11月24日**

**教务部制**

|  |
| --- |
| 实验目的与要求：   1. 理解syn、ICMP攻击原理 2. 熟悉syn、ICMP攻击方法 3. 熟悉抵御syn、ICMP攻击的方法 |
| 实验环境：  SimpleISES客户端  Synflood、Ping工具  Wireshark |
| 实验原理：  参考实验手册 |
| 实验内容：   1. 运行syn、icmp攻击程序 2. 查看主机状态 3. 理解syn、icmp攻击原理 |
| 实验步骤与结果：  （依照实验内容，逐条撰写实验过程与实验所得结果：包括网络架构，核心数据包，调试过程。请附上相关截图，及注意格式排版的美观。实验提交时，以上为评分依据，请不删除本行）  ICMP攻击fakeping   1. 在命令行下进入目录*C:\实验工具集\06\_网络与无线安全\01\_典型协议攻击\第1节ICMP 攻击-fakeping*，然后运行命令*fakeping.exe*，结果如下图所示，说明运行成功。     图1运行命令   1. 输入命令*fakeping 192.168.1.1 192.168.1.3 100*，从操作机向目的主机发送ICMP伪装信息，结果如下图所示，说明ICMP伪装信息已经成功向目的主机发送。     图2发送ICMP伪装信息   1. 在被攻击主机启动wireshark抓包工具，设置过滤器为ICMP，抓取被攻击主机的ICMP数据包，结果如下图所示，发现有大量的ICMP请求数据包。     图3查看ICMP请求数据包   1. 观察图3，我们可以看到大量的源地址为192.168.1.1，目的地址为192.168.1.3的ICMP数据包，说明目的主机一直被攻击。   利用TCP协议实现synflood攻击   1. 在命令行下进入目录*C:\实验工具集\06\_网络与无线安全\01\_典型协议攻击\第3节 SYN攻击*，然后运行命令*xdos.exe*，结果如下图所示，说明运行工具成功。     图4运行结果   1. 切换到目的主机，打开wireshark抓包工具。然后在过滤器中输入*ip.dst==192.168.1.3*，点击apply。结果如下图所示，说明过滤器已经生效。     图5设置结果   1. 切回操作主机，在命令行输入命令*xdos 192.168.1.3 135 -t 3 -s 55.55.55.55*。结果如下图所示，说明已经开始向目的主机发起攻击。     图6发送syn数据包   1. 发现无法切换到目的主机，分析原因：目的主机一直被攻击，无法正常服务。在操作主机停止攻击后重新切换到目的主机，发现wireshark抓包工具抓取到大量的syn数据包。结果如下图所示，说明目的主机一直遭受攻击。     图7查看目的主机抓包结果  思考题   1. 根据Pingflood攻击原理，如何防范这种攻击？  * 通过设置防火墙来阻止ICMP ping请求到达网络内部设备。 * 在路由器上实施过滤规则，以检查进入的数据包。 * 通过设置处理ICMP数据包的速率限制或者限制允许的ping请求大小来防范Pingflood攻击。  1. 如何防范xdos攻击？  * 关闭或限制对不常用端口和应用程序的外部访问。 * 限制主机在特定时间内接受的请求数量。 * 使用入侵检测系统、防火墙和日志监控工等具持续观察网络流量，监控xdos攻击的早期迹象，如网络流量的异常峰值、不寻常的流量模式、来自同一IP等并及时作出响应。 |
| 实验结论：  （撰写实验收获及思考）   1. 通过本次拒绝服务攻击实验，我深入理解了Pingflood和xdos攻击的原理及其对网络服务的影响。 2. 通过本次实验，我加深了对网络攻击和防御机制的理解。 3. 通过Wireshark抓包工具，我们直观地看到了大量恶意数据包的生成和传输，这些数据包导致了目标主机资源的耗尽，从而无法正常提供服务。 4. 通过本次实验，我意识到网络安全的重要性，并学会了如何采取有效的措施来保护网络不受拒绝服务攻击的影响。 |
| 指导教师批阅意见：  成绩评定：  指导教师签字：  年 月 日 |
| 备注： |

注：1、报告内的项目或内容设置，可根据实际情况加以调整和补充。

2、教师批改学生实验报告时间应在学生提交实验报告时间后10日内。