|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 姓名：崔文帅 | | 学号：2025060163 | 专业年级：20网工 | 班级： 网3 |
| 分组： | | 实验室：软件学院402 | 指导教师：郭念 | 实验日期：2023-4-21 |
| **实验的准备阶段**  **(指导教师填写)** | **课程名称** | **网络协议分析与攻防技术** | | |
| **实验名称** | 实验七 拒绝服务攻击 | | |
| **实验目的** | 1. 理解ICMP攻击原理，熟悉ICMP攻击方法，熟悉抵御ICMP攻击的方法。 2. 理解SYN攻击原理，熟悉SYN攻击方法，熟悉抵御SYN攻击的方法。 | | |
| **实验内容** | 1. Pingflood是DOS攻击的一种方法，该攻击以多个随机的源主机地址向目的主机发送SYN包，而在收到目的主机的SYN ACK后并不回应，这样，目的主机就为这些源主机建立了大量的连接队列，而且由于没有收到ACK一直维护着这些队列，造成了资源的大量消耗而不能向正常请求提供服务。 2. 运行syn攻击程序，以靶机为目标主机对其发送syn数据包，查看目标主机状态。 | | |
| **实验类型**  （打☑） | ☑验证性 □演示性 □设计性 □综合性 | | |
| **实验的重点、难点** | 1. AWVS的用法。 2. AppScan的用法。 | | |
| **实验环境** | 目标机：192.168.1.3 | | |
| **实验的实施阶段** | **实验步骤及实验结果** | 1. **fakeping攻击** 2. 在命令行下进入 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目录下，运行命令fakeping。Fakeping命令格式：Fakeping 伪装的源地址 目的地址 数据包大小。**实验过程截图如下：**      1. 输入命令fakeping 192.168.1.1 192.168.1.3 100，在操作机主机向192.168.1.3 发送伪装icmp请求信息，请求信息的伪装源地址为 192.168.1.1。**实验过程截图如下：**      1. 在目标机上启动wireshark抓包工具，设置数据包过滤器为“icmp”，抓取被攻击主机icmp的数据包。实验过程截图如下：     可以看到，192.168.1.3主机收到大量的icmp请求数据包。该数据包即为192.168.1.2伪造的源地址为192.168.1.1的发给192.168.1.3的icmp请求数据包。   1. **利用xdos工具进行攻击** 2. 在命令行下打开“ 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\xdos”目录，输入xdos.exe命令，显示出xdos命令使用格式。**实验过程截图如下：**      1. 切换到(192.168.1.3)的目标机器上，打开桌面的wireshark。在filter中输入：ip.dst＝＝192.168.1.3，点击apply。**实验过程截图如下：**      1. 切换回操作机（192.168.1.2），在命令行下输入命令xdos 192.168.1.3 135 -t 3 -s 55.55.55.55，其中135为连接端口，-t 3 表示开启的进程，-s 后跟的ip地址为syn数据包伪装的源地址的起始地址，正在对本地发送syn数据包。**实验过程截图如下：**      1. **利用wireshark软件抓取SYN数据包** 2. 在开始攻击后，想要切换到192.168.1.3，发现切换不过去，是因为一直在进行攻击，使目标机器不能正常服务。停止攻击之后就可以切换到目标机器。查看wireshark抓包详情后，可以看到大量的syn向192.168.1.3主机发送，并且将源地址改为55.55.55.55后面的ip地址。**实验过程截图如下：** | | |
| **实验结果的处理阶段** | **实验结果的分析与总结** | * 1. 根据Pingflood攻击的原理，如何防范这种攻击？   选择合适的防火墙：具有状态检测、细致的数据包完整性检查和很好的过滤规则控制功能；  配置防火墙以预防攻击：用户应该配置一个合理的安全策略   1. 如何防范xdos攻击方式？   定期扫描：通过定期扫描我们可以找到隐藏的安全漏洞，并能够对漏洞进行修补  配置防火墙：防火墙做得到抵御DOS攻击的第一道防线。能够让企业服务器免受许多威胁的侵扰。  优化服务器端口：将不必要的服务和端口关闭，只开放正在使用的端口  部署高防服务器：高防服务器具有超强的抵御能力，能在保证服务器访问速度、稳定的状态下实行防御工作，给用户高速的访问体验。 | | |