****

网络安全理论与技术实验

实 验 报 告

|  |  |
| --- | --- |
| **学 院** | 网络空间安全学院 |
| **专 业** | 网络工程 |
| **班 级** | 18272412 |
| **学 号** | 18041618 |
| **学生姓名** | 廖越强 |
| **教师姓名** | 高梦州 |
| **完成日期** | 11.20 |
| **成 绩** |  |
| **实验一 网络信息收集与扫描实验** | | |
| 1. **实验目的** 2. 验证流量管制器的配置过程。 3. 验证通过流量管制阻止病毒快速传播的过程。 4. 验证通过流量管制阻止拒绝服务攻击的过程。 5. 验证流量管制的工作原理。 | | |
| 1. **实验原理**   实施流量管制的前提有两个:一是分类信息流,从图6.18中的路由器Rl接口2和路由器R2接口1输出的信息流中分离出网络192.1.1.0/24和网络192.1.3.0/24中的终端发送给邮件服务器和Web服务器的流量;二是限定这些流量的平均传输速率。  通过规则从IP分组流中鉴别出一组IP分组,规则由一组属性值组成,如果某个IP分组携带的信息和构成规则的一组属性值匹配,意味着该IP分组和该规则匹配。构成规则的属性值通常由下述字段组成:  (1)源IP地址,用于匹配IP分组IP首部中的源IP地址字段值。  (2)目的IP地址,用于匹配IP分组IP首部中的目的IP地址字段值。  (3)源和目的端口号,用于匹配作为IP分组净荷的传输层报文首部中源和目的端口号字段值。  (4)协议类型,用于匹配IP分组首部中的协议字段值。  例如分离出网络192.1.1.0/24中的终端发送给邮件服务器的流量的规则如下:(1)协议类型=TCP。  (2)源IP地址=192.1.1.0/24。  (3)源端口号:任意。  (4)目的IP地址=193.1.2.3/32。  (5)目的端口号=25。  限制流量平均传输速率采用如图6.19所示的令牌桶算法。如果授予每一个令牌P字节的传输能力,且令牌生成器生成令牌的速率是R个令牌/s,则平均传输速率=P×8×R。    如果授予每一个令牌的传输能力是不变的,可以通过改变令牌生成器生成令牌的速率改变平均速率。假定授予每一个令牌P字节的传输能力,如果设定的平均传输速率是Viups ,则生成令牌的速率=V/(P×8)。 | | |
| 1. **实验环境/实验拓扑图** | | |
| 1. **主要操作步骤及实验结果记录** 2. 完成拓扑图连接      1. 完成接口的IP、掩码配置。为router0和router1配置RIP，其中router0配置如下，router类似     配置完后二者的路由表分别如下       1. 完成各个终端的信息配置 2. 完成路由器router1，router2流量管制器的配置，将192.1.1.0/24网段中的终端向email服务器发送的平均流量限制为16000bps。向web服务器发送的流量限制为2000000bps       进入仿真模拟，pc0访问web服务器的TCP报文如下（操作是打开pc0的web brower然后一阵狂点go按钮）    因流量管制而被丢弃的包     1. 将前往web server 的浏览器的流量速率限制为2000000bps，     分组前的ip首部    输出后的ip分组首部，0x25即为之前配置时设置的十进制数值37 | | |
| 1. **实验分析总结及心得**   通过这次实验，我对流量管制这方面的安全知识有了新的认识，学会了防御这些流量攻击的基本操作，对它们的攻击流程有了一个的深刻的认识。也对这数据包传输这个概念有了更深入的理解，明白了做好流量管制，提高网站安全防护的重要性提高了自己的安全意识。 | | |