**《信息安全基础》实验报告**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **姓名** | | 黄昊 | | **年级** | | 2020级 |
| **学号** | | 20204205 | | **专业、班级** | | 20计算机科学与技术（卓越）01 |
| **实验名称** | **实验三 拒绝服务攻击与防御仿真实验** | | | | | |
| **实验时间** | **2023/05/07** | | **实验地点** | | **DS3402** | |
| **实验成绩** |  | | **实验性质** | | **□验证性 □设计性 □综合性** | |
| 教师评价：  □算法/实验过程正确； □源程序/实验内容提交 □程序结构/实验步骤合理；  □实验结果正确； □语法、语义正确； □报告规范；  评语：  评价教师签名（电子签名）： | | | | | | |
| 一、实验目的  1. 理解拒绝服务攻击的基本概念和常见拒绝服务攻击与防御技术。  2. 能基于具体场景中的现象和数据建立拒绝服务攻击的数学模型，得出合理的结论  3. 能识别问题中的关键因素，通过探索、优化和折中等方法，给出兼顾多个目标的防御方案。  4. 理解拒绝服务场景中攻击和防御的对抗特性，能利用基本的博弈论方法选择较优的攻防策略。 | | | | | | |
| 二、实验内容  实验包括四类任务：  攻击仿真实验：学生扮演黑客角色对服务器发动攻击。任务目标是在一定的攻击成本内，使网络服务质量下降到某个数值之下。  防御仿真实验：学生扮演网络管理员的角色对拒绝服务攻击进行防御。任务目标是在一定的防御成本内，使网络服务质量保持在某个数值之上。  数学建模实验：根据对拒绝服务攻击过程的理解，写出连接成功率和服务速率的数学表达式。  攻防博弈实验：根据网站或黑客的策略矩阵，利用基本的博弈论方法，设置防御参数，参与攻防仿真实验。 | | | | | | |
| 三、实验原理  IP地址攻击  当用户访问网站时，网页浏览器与Web服务器之间采用HTTP协议进行通信，主要分成两个阶段：   * 第一个阶段，浏览器与Web服务器之间建立TCP连接。 * 第二个阶段，浏览器向服务器发出HTTP请求，服务器向浏览器返回HTTP响应。   虚假IP地址攻击发生在上述第一个阶段，攻击者采用虚假IP地址向Web服务器发出大量TCP连接请求，从而消耗服务器的计算资源，降低其服务质量。  真实IP地址攻击发生在上述第二个阶段，攻击者采用真实IP地址向Web服务器发出大量服务请求，从而消耗服务器的计算资源，降低其服务质量。  应对攻击有四种防御手段:  Cookie：使用防hash技术防御SYN泛洪攻击，减少服务器内存消耗  DRR：一种数据包调度算法，使每个IP的请求被均匀处理  黑名单：若某个IP请求速率过快，则不响应其请求。  配额：若某个IP的请求数量超过限额，则减小其调度机会。 | | | | | | |
| 四、截图及结果分析  ①虚假IP地址攻击  本任务的闯关要求是，在攻击成本不高于50的前提下，使网络服务质量降低到40或以下。  在该平台上，参数设置为：虚假IP攻击台数为10，攻击速率为1000，结果失败，如下图    通过一步步调试，发现虚假IP攻击台数为10时，攻击速率为4999时，结果失败；但攻击速率调为5000时，情况发生了突变，如下两图：    、  同样地，当攻击速率为1000时，攻击台数为49和50的时候，情况也会发生突变：前者服务质量为99，攻击失败；后者为0，攻击成功：      不难发现，这似乎与攻击台数和攻击速率的乘积有关。仔细观察上面的五幅图，除了第一幅图，后面四幅图的内存占用率几乎到100%，若攻击流量占据了服务器100%的计算资源，则会导致服务器不能提供服务。    观察已知条件，不难发现，攻击方如果在单位时间内发送大量数据包，超过防火墙的处理能力，则能达到攻击目的。  ②真实IP地址攻击  在攻击成本不高于50的前提下，使网络服务质量降低到90或以下。  令攻击台数为50，速率为1000时可以成功    当攻击台数为500时，速率为1000时，因为成本过高失败：    当攻击台数和速率低的时候，攻击成本较低。  ③初级防御实验  当防火墙连接带宽和服务带宽均为5e5时，防御失败：    使用cookie时即成功：    使用DRR时失败，黑名单失败，且成本很高。（图略）  已知：  Cookie：使用防hash技术防御SYN泛洪攻击，减少服务器内存消耗  DRR：一种数据包调度算法，使每个IP的请求被均匀处理  黑名单：若某个IP请求速率过快，则不响应其请求。  配额：若某个IP的请求数量超过限额，则减小其调度机会。  已知攻击方采用虚假IP地址向Web服务器发出大量连接请求，而Cookie可以防御SYN泛洪攻击，故设置Cookie可以成功拦截攻击。  ④中级防御攻击  只设置DRR和Cookie时，防御失败：    设置防火墙的连接请求带宽为1e5和服务请求带宽为950000时，连接成功。（只设置了DRR）    分析原因：攻击者采用真实IP地址向Web服务器发出大量服务请求，因此服务请求带宽需要拉大来应对攻击。而由于DRR算法使得每个IP的请求被均匀处理，如果攻击方采用真实IP进行攻击，那么该IP地址攻击频率过高时，其因为DRR算法，导致其请求被处理的速率与正常用户的一致，从而能得到防御。  ⑤综合防御实验  在防御成本不高于20的前提下，使网络服务质量达到80或以上。  采用Cookie和DRR时，防火墙连接请求带宽和服务请求带宽分别为500000和500000时，防御失败：    采用Cookie和DRR时，防火墙连接请求带宽和服务请求带宽分别为430000和610000时，防御成功：    攻击方会发送大量TCP连接请求和HTTP请求，因此Cookie和DRR算法都需要使用。同时，由于连接请求和服务请求都因为攻击而变得非常多，因此两者的带宽也不能小。  ⑥连接成功率建模    如图，只要三次连接被接受一次就算成功，答案为1 - (1 - p) \* (1 - p) \* (1 - p)  ⑦服务速率建模    如图，第一题，当前接受服务的用户个数分别为a\*w/v，  第二题：总带宽为s，服务的用户为(x+z\*q)，故答案为s / (x + z \* q)，  第三题：带入解方程即可，答案为(s - a \* w) / (z \* q)  ⑧攻防博弈    目标是求取双方的纳什均衡点：假设网站加带宽的概率为q，黑客攻击的概率为p，那么：  对于黑客来说，网站选择加带宽的期望为10p-5(1-p),不加带宽的期望为-10p，取等时p=0.2;  对于网站来说，黑客选择攻击的期望收益为-10q+10(1-q)=-20q+10,不攻击的期望收益为5q，相等为0.4  因此，纳什均衡点在(0.2,0.4)，即网站以0.4的概率选择加带宽。 | | | | | | |