**《信息安全概论》实验报告**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **姓名** | | 谭星 | | **年级** | | 2019级 |
| **学号** | | 20191584 | | **专业、班级** | | 计算机科学与技术卓越01班 |
| **实验名称** | 实验三 拒绝服务攻击与防御仿真实验 | | | | | |
| **实验时间** | 2022.5.5 | | **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、实验项目内容   1. 平台登陆与注册：http://www.ilab-x.com 2. 完成登陆后打开实验链接：http://www.ilab-x.com/details/2020?id=6354&isView=true 3. 在仿真平台中完成拒绝服务的攻击和防御实验。 | | | | | | |
| 三、实验设计  拒绝服务攻击是指利用网络协议的缺陷或直接耗尽被攻击对象的资源，从而使被攻击对象无法正常提供服务的攻击，拒绝服务攻击也是当前最常见的网络攻击之一。 | | | | | | |
| 四、实验过程或算法   1. 实验一：虚拟IP地址攻击   虚拟IP地址攻击的原理是攻击者采用虚拟IP地址向Web服务器发出大量的TCP连接请求，从而消耗服务器计算资源，降低服务质量。由下图可知，当虚拟IP攻击台数为10、攻击速率为1000时，内存占用率在60%左右。    根据攻击原理，适当调大虚拟IP攻击台数，直到虚拟IP攻击台数为50、攻击速率为1000时，因大量连接请求的出现导致服务器内存占用率达到100%，服务质量降为0。     1. 实验二：真实IP地址攻击   真实IP地址攻击的原理是攻击者采用真实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。由下图可知，当真实IP攻击台数为500、攻击速率为1000时，可使网络服务质量降低到38，但是成本过高。    因此，可尝试减少真实IP攻击台数。当真实IP攻击台数为50、攻击速率为1000时，可在降低网络服务质量的同时将成本降低至50。     1. 实验三：初级防御试验   在未部署任何防御工具时，观察到内存占用率达到100%，可判断服务器遭受了SYN攻击。    因此，可通过cookie来进行防御。当服务器在收到syn包时并不马上分配储存连接的数据区，而是根据这个syn包先计算出一个cookie，在确认对方的合法性之后再分配专门的数据区，这样便可有效防御SYN攻击。     1. 实验四：中级防御试验   在未部署任何防御工具时，观察到连接成功率高，服务成功率低，这说明浏览器与服务器可成功建立TCP连接，黑客主要采用真实IP地址攻击。    因此可使用DRR工具限制黑客攻击速率，同时尽量调高服务请求带宽，以满足更多的服务请求。此外，连接请求带宽应适当调低（但不能过低，否则不能建立连接），以降低防御成本。最终，当连接请求带宽为5000、服务请求带宽为1000000时，可将服务质量提高至99。     1. 实验五：综合防御试验   在未部署任何防御工具时，观察到内存占用率为100%，同时黑客连接请求和服务请求的数量相近，可判断攻击者发动了虚假 IP 和真实 IP 地址混合攻击。    由前两个实验可知同时需要Cookie和DRR工具。 此外，配额工具也可以有效缓解攻击者的慢速攻击。在添加这三种工具、且配额的惩罚因子为0.1时，服务质量可提高至88，但成本过高。    因此将惩罚因子调高，降低成本，并适当提高一点服务请求带宽，使网络质量达到要求。最终当连接请求带宽为500000、服务请求带宽为510000、配额惩罚因子为0.5时，可将服务质量提高至88且成本降低为20。     1. 实验六：   一次请求连接的失败率是1-p，若三次都失败的概率是 (1-p)\* (1-p)\* (1-p) ，则连接成功的概率为 1-(1-p)\* (1-p)\* (1-p)。     1. 实验七：   第一步：在稳定状态下，每个用户的服务时间为 w/v，每秒到达的新用户数量为 a，故正在接受服务的用户人数为 a\*w/v。  第二步：配额机制使 z 个攻击者相当于 z\*q 个一般用户，故 x+z\*q 个用户一起共享服务带宽，服务速率可表示为 s/(x+z\*q) 。  第三步：将前两步所得的表达式联立求解方程组，得到v=s/(a\*w/v+z\*q)。     1. 实验八：   利用混合策略纳什均衡，可以求得最佳概率值为 2/3。 | | | | | | |
| 五、实验过程中遇到的问题及解决情况  起初对实验中防火墙各工具的作用不太清楚，查阅资料后可知各工具相应的应用场景。 | | | | | | |
| 六、实验结果及分析和（或）源程序调试过程  实验完成后，返回原页面提交结果，截图如下： | | | | | | |