**《信息安全基础》实验报告**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **姓名** | | **陈鹏宇** | | **年级** | | **2020** |
| **学号** | | **20204227** | | **专业、班级** | | **2020级计算机科学与技术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** | **2023/11/10** | | **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  在仿真平台中完成拒绝服务的攻击和防御实验。  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。  攻击成本=攻击台数\*攻击速率/1000 | | | | | | |
| 三、实验设计  本实验主要包含八个内容：  1.虚假IP地址攻击  2.真实IP地址攻击  3.初级防御实验  4.中级防御实验  5.综合防御实验  6.连接成功率建模  7.服务速率建模  8.攻防博弈 | | | | | | |
| 四、实验过程或算法  1虚假IP地址攻击  我们按照系统默认的参数攻击，失败    设置参数如下后，攻击成功      2真实IP地址攻击  使用默认参数设置攻击，攻击失败    将台数设置为100，速率设置为100，攻击成功。      3初级防御实验  如果按照默认方式，防御失败    设置一个Cookie，不做其他改变，就能够防御成功。    4中级防御实验  默认参数无法防御成功    设置为如下参数，并添加drr模块，防御成功。      5综合防御实验  使用默认参数，防御失败    设置为如下参数，并添加drr和cookie模块，防御成功。    6连接成功率实验  根据概率公式可知：    7服务速率建模实验  第一步：    第二步：    第三步：  8攻防博弈实验  我们设置加带宽的概率为0.6，最终攻击成功。 | | | | | | |
| 1. 实验过程中遇到的问题及解决情况   在进行综合防御实验时，很难将成本控制在20以下，同时确保服务质量。此外，我们还发现连接请求带宽和服务请求带宽并非总是越高越好，因为在某些情况下，增加其中一个带宽可能会导致性能下降。 | | | | | | |
| 六、实验结果及分析和（或）源程序调试过程  1虚假IP地址攻击  用户访问网站时，浏览器与Web服务器之间的通信采用HTTP协议。整个过程分为两个阶段。首先，浏览器与Web服务器建立TCP连接。然后，浏览器发送HTTP请求，服务器返回HTTP响应。在第一个阶段，虚假IP地址攻击会发生。攻击者使用虚假IP地址向Web服务器发送大量TCP连接请求，以消耗服务器的计算资源并降低服务质量。  利用虚假IP地址攻击Web服务器，同时保持攻击成本低于50。我们的目标是将网络服务质量降低到40或更低。已知条件包括防火墙处理连接请求的带宽为每秒500,000个数据包，正常用户到达率为每秒100个，以及用户连接请求速率为每秒100个数据包。在默认情况下，我们会失败，主要原因是IP攻击的数据包只有10000个、因此无法有效的降低连接的成功率。  当我们增加IP攻击的数据包，设置为总和有20\*2500=50000以后，防火墙的连接成功率就会大大降低，甚至直接降低到0。  2真实IP地址攻击  将攻击台数设置成100、速率设置成100就能够完成攻击。如果按照默认方式，会出现成本过高的问题。  3初级防御实验  不使用任何东西当然是没办法防御的，因此我们添加了Cookie。通过使用cookie可以成功防御攻击，主要原因是cookie可以减少服务器的内存消耗。由此导致连接成功率大大提高，即使攻击IP的数量和攻击速率非常高，也可以保持相对良好的服务质量。  4中级防御实验  需要使用drr来实现每个IP请求的均匀处理，然后将连接带宽请求和服务带宽请求分别设置为100和1000000。通过这些措施，实验的成功率可以大幅度提高，因为drr可以确保请求得到平均处理，带宽请求可以提供更优质的连接和服务。这些优化措施可以增加实验的可靠性和稳定性  5综合防御实验  对于这次实验，我们需要综合初级防御和终极防御采用的方式，同时使用cookie和drr策略，然后合理的设置连接带宽和服务带宽，最终能够有效的提高成功率。  6连接成功率  根据概率公式：  7服务速率建模   * 这一秒的总数据量为，人数乘以每个人每一秒的消耗=每个用户的停留时间\*a\*每个人每秒的消耗=a\*w，因此人数为 a\*w/v。 * 期望的肉鸡获得的宽带的数量为q\*z，因此平均s/(x+q\*z)。 * 将第一步的结果带入第二部的x即可。   8攻防博弈实验  我们设置加带宽的概率为0.4到0.6之间，均可以成功，因此我们可以自由进行选择，选择0.4时成功概率较低且收益较低，设置0.6成功的概率较大。 | | | | | | |