**《信息安全概论》实验报告**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **姓名** | | *李燕琴* | **年级** | | | *2019级* |
| **学号** | | *20195633* | **专业、班级** | | | *计算机科学与技术（卓越）02班* |
| **实验名称** | **拒绝服务攻击与防御仿真实验** | | | | | |
| **实验时间** | **2022年5月5日** | | | **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。 | | | | | | |
| 三、实验原理  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、截图及结果分析  实验一：在本任务中，你将扮演黑客，利用虚假IP地址攻击Web服务器。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。  失败案例:当虚拟IP攻击台数较多且虚拟IP攻击速率稳定1000不变时，会导致攻击成本剧增，而服务质量为0的情况。这是因为当虚拟ip攻击台数较多时，客户端无法和服务器端正常连接，更别说正常提供服务，故服务质量为0。    成功案例：经过实验发现，攻击台数会比攻击速率更能影响服务器的连接数量，故保证攻击速度不变，增加虚拟IP攻击台数致50（即失败案例的一半），即可成功。    实验二：在本任务中，你将扮演黑客，利用真实IP地址攻击Web服务器。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90或以下。  已知条件如下：   * 防火墙用于处理连接请求的带宽为100,000数据包/秒 * 正常用户的到达率为100个/秒 * 用户连接请求速率为100数据包/秒。   失败案例：默认设置中，服务质量满足要求，但成本过高。按照任务要求，降低成本即可，可以采用降低真实IP攻击台数的方法。      实验三：在本任务中，你将扮演网络管理员，对虚假IP地址攻击进行防御。本任务的闯关要求是，在防御成本不高于20的前提下，使网络服务质量达到90或以上。  已知条件如下：   * 正常用户的到达率为800个/秒 * 用户连接请求速率为100数据包/秒。   失败案例：当不添加任何配置时，保证连接和服务请求带宽为500000的情况下，实验失败。又因给定的正常用户连接请求带宽为800\*100=80000包/秒，说明连接服务请求带宽适宜，且未知用户有恶意攻击情况。 且内存占用率为100%，说明发动了SYN攻击，故可使用Cookie工具。    成功案例：保证原始带宽数据不变，添加cookie工具。    实验四：在本任务中，你将扮演网络管理员，对真实IP地址攻击进行防御。本任务的闯关要求是，在防御成本不高于20的前提下，使网络服务质量达到90或以上。  失败案例：已知条件和实验三一致，保持原始条件，运行发现，连接成功率高，服务成功率低，说明黑客主要采用真实IP地址攻击。应该尽量调高服务请求带宽，并使用DRR工具使每个IP的请求被均匀处理以限制黑客攻击速率。但上面两个步骤导致成本很高，为了降低防御成本，连接请求带宽尽量调低（大于80000即可，理由见实验三）。    图 1 原始条件    图 2 只进行前两步  成功案例：将连接请求设置为100000，服务请求设置为1000000，并添加DRR工具。    实验五：在本任务中，你将扮演网络管理员，对拒绝服务攻击进行防御。本任务的闯关要求是，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。  失败案例：分析同实验三、实验四，在默认设置中，连接成功率和服务成功率都较低，故可以通过cookie和DRR工具来保证这两个参数。此外在有一定连接数的情况下，服务成功率为0，故需要在保证成本的情况下，适当降低连接请求带宽并增加服务请求带宽。    成功案例：    实验六：**连接成功率**  当防火墙的处理带宽不足时，防火墙只能同意部分TCP连接请求。 假设防火墙以概率p同意连接请求，且一般用户在请求连接时最多尝试三次。 请问一般用户可成功连接的概率是多少？ 请用四则运算写出连接成功率的数学表达式。 （格式举例： p+p\*p\*p，注意区分大小写）    实验七：**服务速率**  假设每秒有a个新用户与网站服务器建立 TCP连接。每个用户从建立连接到离开网站请求的总数据量为w。 同时有z台肉机一直在向服务器发送请求。 为了缓解肉机的影响，防火墙规定，当一个客户端请求的数据量超过某个配额后， 相对其它用户，其请求被响应的概率为q。 假设防火墙用于处理服务请求的带宽为s，请问经过一段时间后， 防火墙可稳定提供给用户的服务速率(即防火墙可分配给每个用户的平均带宽)是多少？ 请用四则运算写出服务速率的数学表达式 （表达式用小写的a,q,s,w,z的四则运算表示，如： w\*s/(a\*q+z)）。  实验八： | | | | | | |