**《网络空间安全概论》实验报告**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **姓名** | |  | | **年级** | |  |
| **学号** | |  | | **专业、班级** | |  |
| **实验名称** | **实验三 拒绝服务攻击与防御仿真实验** | | | | | |
| **实验时间** |  | | **实验地点** | |  | |
| **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   * 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。 * 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 * 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。 * 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. 攻击仿真实验：扮演黑客对服务器发动攻击。使用可接受的攻击成本使网络服务质量降低至指定值及以下。 2. 防御仿真实验：扮演网络管理员对拒绝服务攻击进行防御。使用可接受的防御成本使网络服务质量维持在指定值及以上。 3. 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。 4. 攻防博弈实验：根据网站和黑客的策略矩阵，结合博弈论原理，确定增加带宽的概率，以尽可能提高网站的防御收益。 | | | | | | |
| 三、实验设计  拒绝服务攻击是当前最活跃的网络攻击手段之一，它利用庞大的计算资源或网络协议缺陷阻碍被攻击对象向用户提供正常服务的能力。本实验课程的仿真的场景是黑客对Web服务器进行拒绝服务攻击，网络管理员对此攻击进行防御。  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。   本实验主要考虑两种攻击方式和四种防御工具。黑客可能会控制大量的肉鸡（即被黑客控制的计算机）在以上两个阶段对服务器发动攻击。网站则会部署防火墙对拒绝服务攻击进行防御。  **两攻击方式：**   * 虚假IP地址攻击：在网站访问的第一个阶段，攻击者采用虚假IP地址向服务器发出大量请求，大量消耗服务器的计算资源。 * 真实IP地址攻击：在网站访问的第二个阶段，攻击者使用真实IP地址向服务器发出大量请求，从而占用服务器的计算资源，使其服务质量严重降低。   **四种防御工具：**     * 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。   **实验任务指标：**  攻防实验能否成功由两个指标决定：   * 成本：发动攻击或防御的成本，由一个介于0到99之间的整数表示。 * 服务质量：用户感知的平均网络服务质量，由一个介于0到99之间的整数表示。其计算公式如下：     在攻防实验中，会通过仿真的数据仪表盘表示网络通信的状态，仪表盘显示与服务质量相关的5个重要指标：   * 连接成功率：发出TCP连接请求的用户中，最终成功建立连接的比例。 * 连接数：当前的TCP连接个数，包括黑客和用户的连接。 * 服务成功率：在建立TCP连接的用户中，最终获得服务的比例。 * 服务速率：对于获得服务的用户，其服务请求的平均处理速度。 * 内存占用率：服务器内存被占用的比例。 | | | | | | |
| 四、实验过程或算法  **1.虚假IP地址攻击：**  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。已知条件如下：   * 防火墙用于处理连接请求的带宽为500,000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。   默认的参数设置和输出如下图所示：      根据已知条件可知，完全占据防火墙的计算资源需要用户数 = 500,000 / 100 / 100 = 50。多次测试可知，成本 = 虚假IP攻击台数 \* 虚假IP攻击速率 / 1000。假设每个虚假攻击台对应一个用户，且虚假IP攻击速率不变，则需要的虚假攻击台数为50：    **2.真实IP地址攻击：**  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。   根据已知条件可知，占据防火墙(100 - 90) / 100 \* 100% = 10%的计算资源需要用户数 = 100,000 / 100 / 100 \* 10% = 1，成本分析同上。假设每个真实攻击台对应一个用户，且真实IP攻击速率不变，则需要的真实攻击台数为1：      **3.初级防御**  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。   默认设置下，服务器运行情况如下图所示：    观察仪表盘可知，内存的占有率几乎达到了100%。因此应当使用Cookie防hash技术防御SYN泛洪攻击，减少服务器内存消耗。    **4.中级防御**  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。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。   默认设置下，服务器运行情况如下图所示：    观察仪表盘可知，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。应该使用DRR工具限制黑客攻击速率，使每个IP的请求被均匀处理。同时尽量调低连接请求带宽，调高服务请求带宽。      **5.综合防御**  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80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。   默认设置下，服务器运行情况如下图所示：    此时服务器的运行情况同任务3。因此需要添加Cookie工具：    此时服务器的运行情况同任务4。因此需要添加DRR工具：    此时服务器的服务速率几乎为0，说明黑客主要采用慢速攻击，可以采用配额工具有效缓解，但需要将惩罚因子调高以降低防御成本：    **6.连接成功率建模**  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）：  P（连接成功）= 1 - P（三次连接失败） = 1 - P（连接失败）^3 = 1 - (1 - p) ^ 3    **7.服务速率建模**  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)）：        **8.攻防博弈**  假设某网站获悉有黑客可能于今晚对自己发动拒绝服务攻击。网站可以选择增加带宽或不增加带宽，黑客也可能发动攻击或不发动攻击。双方的收益如下，请你确定增加带宽的概率。系统将模拟10次攻击。如果你在10次攻防实验中的收益大于10，则获得胜利，否则将失败。    根据参考资料，用等值法求解混合策略纳什均衡点：   * 网站选择加带宽的收益期望值： E(A) = -10q + 10(1-q) * 网站选择加带宽的收益期望值： E(B) = 5q   由E(A) = E(B)可得 q = 0.4。同理可得：   * 黑客选择攻击的收益期望值： E(C) = 10p - 5(1-p) * 黑客选择不攻击的收益期望值： E(D) = -10p   由E(A) = E(B)可得 p = 0.2。故混合策略纳什均衡点为(0.2, 0.4)，即网站以0.4的概率选择加带宽，黑客以0.2的概率选择攻击。 | | | | | | |
| 五、实验过程中遇到的问题及解决情况  **问题1：**  不理解实验参数设置和工具配置的工作原理。  **原因和解决办法：**  多次实验，对照实验数据和实验指导书验证各个参数的含义；对照实验任务说明和实验指导书确认仪表盘数据和工具配置策略的内在联系。 | | | | | | |
| 六、实验结果及分析和（或）源程序调试过程  在经过合理分析和多次测试后，各个实验均已达成任务目标：  **1.虚假IP地址攻击**    **2.真实IP地址攻击**    **3.初级防御**    **4.中级防御**    **5.综合防御**    **6.连接成功率建模**    **7.服务速率建模**    **8.攻防博弈** | | | | | | |