**《网络空间安全概论》实验报告**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **姓名** | |  | | **年级** | | 2022 |
| **学号** | |  | | **专业、班级** | | 计算机科学与技术专业卓越1班 |
| **实验名称** | **实验二 拒绝服务攻击与防御仿真实验** | | | | | |
| **实验时间** | 3.29 | | **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。 | | | | | | |
| 1. 实验项目内容 2. 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。 3. 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。 4. 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。 5. 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。 | | | | | | |
| 1. 实验设计   拒绝服务攻击（Denial of Service, DoS）是当前最活跃的网络攻击手段之一，攻击者通过消耗大量计算资源或利用网络协议的缺陷，阻碍被攻击对象向正常用户提供服务的能力。  本实验课程的仿真场景为：黑客对 Web 服务器发起拒绝服务攻击，而网络管理员则进行防御。  在用户访问网站时，网页浏览器与 Web 服务器之间通过 HTTP 协议进行通信，主要分为两个阶段：  1.建立 TCP 连接阶段：浏览器与服务器之间首先建立 TCP 连接；  2.发送 HTTP 请求阶段：浏览器向服务器发送 HTTP 请求，服务器返回 HTTP 响应。  本实验主要模拟两种攻击方式及四种防御工具的效果。攻击者可能控制大量“肉鸡”（被攻陷的计算机），在上述两个阶段对服务器发起攻击，而网站会通过防火墙部署防御措施。  **两种攻击方式**  虚假 IP 地址攻击：在建立 TCP 连接阶段，攻击者使用伪造的 IP 地址向服务器发送大量请求，大量占用服务器计算资源。  真实 IP 地址攻击：在发送 HTTP 请求阶段，攻击者使用真实的 IP 地址发起大量请求，占用服务器资源，导致服务质量严重下降。  **四种防御工具**  Cookie：采用防 hash 技术防御 SYN 泛洪攻击，以减少服务器内存消耗。  DRR（Deficit Round Robin）：一种数据包调度算法，用于均衡各 IP 地址请求的处理机会。  黑名单：当某个 IP 的请求速率过高时，将其列入黑名单，不再响应其请求。  配额：为每个 IP 设置请求限额，当其请求数量超过限额时，减少该 IP 的调度机会。  IMG_256  **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。 | | | | | | |
| 1. 实验过程或算法   **4.1虚拟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。   IMG_256  **4.1.1失败案例**  设定虚拟IP攻击台数为20，虚拟IP攻击速率为1000时，攻击失败，原因是服务质量没有降低到要求，如图所示：  IMG_256  **4.1.2成功案例**  于是我们调高IP攻击台数，调高到50台时，攻击成功。  IMG_256  **4.2真实IP地址攻击：**  **4.2.1失败案例**  设定真实IP攻击台数为50，真实IP攻击速率为1000时，攻击失败，原因是成本没有达到要求，如图所示：  IMG_256  **4.2.2成功案例**  于是我们降低IP攻击台数，当攻击台数为1时，成功攻击。  IMG_256  **4.3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。  **4.3.1 失败案例**  默认设置下，服务器运行失败，如下图所示：  IMG_256  **4.3.2 成功案例**  注意到失败案例当中，内存占有率特别高，说明遭到了泛洪攻击，于是我们使用Cookie防hash技术防御SYN泛洪攻击，减少服务器内存消耗，于是成功抵御攻击。  IMG_256  **4.4 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  **4.4.1 失败案例**  默认设置下，服务器运行失败，如下图所示：  IMG_256  **4.4.2 成功案例**  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到5000，调高服务请求带宽到1000000。  IMG_256  **4.5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。  **4.5.1失败案例**  默认情况下如图所示：  IMG_256  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，并且内存占有率也很高，于是采用DRR+Cookie的方式：  IMG_256  4.5.2 成功案例  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，最后我们惩罚因子调到0.4时成功实现保护：  IMG_256  4.6**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）：  这道题很简单：连接成功概率P=1-不成功的概率。  IMG_256  IMG_256  4.7**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)）：  IMG_256  IMG_256  IMG_256  **4.8 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。  IMG_256  根据参考资料的公式，对于网站来说，需要找到平衡点，假设加宽带的概率为P，则有公式-10P+10（1-P）=5P,解得P=0.4： IMG_256 | | | | | | |
| 1. 实验过程中遇到的问题及解决情况   **问题一：虚拟 IP 的计算结果与预期不符**  现象：计算完成后发现答案与预期不一致，且输入系统后成本远高于预期。  解法：经过分析，发现问题出在项目本身，而非我们的计算公式。可能是由于设计者在配置带宽时多输入了一个“0”，导致数值偏大。  **问题二：综合防御实验总是无法通过**  解法：采用逐步排查的方法。首先根据仪表盘观察系统存在的问题，然后再针对性地选择额外的防御措施进行补充。  **问题三：攻防博弈实验中计算结果为 0.4，但评分未达标**  现象：计算得出的最优解为 0.4，但实验运行的均分未达标，因此怀疑答案错误。  解法：多尝试几次实验，因为系统存在一定随机性。虽然 0.4 是理论上的最优解，但无法保证每次运行都达到最佳效果。 | | | | | | |
| 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**  IMG_256  **2.真实IP地址攻击**  IMG_256  **3.初级防御**  IMG_256  **4.中级防御**  IMG_256  **5.综合防御**  IMG_256  **6.连接成功率建模**  IMG_256  **7.服务速率建模**  IMG_256  IMG_256  IMG_256  **8.攻防博弈**  IMG_256 | | | | | | |