**《网络空间安全概论》实验报告**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **姓名** | |  | | **年级** | | **2021级** |
| **学号** | |  | | **专业、班级** | | **计算机科学与技术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** | **2024.4.27** | | **实验地点** | | **DS3304** | |
| **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。  本实验课程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。  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。  两个任务指标：  ·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：服务质量=连接成功率\*服务成功率\*服务速率。  五个服务质量指标：  ·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.虚拟IP地址攻击**  虚假IP地址攻击任务发生在浏览器与Web服务器之间建立TCP连接阶段，攻击者采用虚假IP地址向Web服务器发出大量TCP连接请求，从而消耗服务器的计算资源，降低其服务质量。  在该实验中，扮演黑客，利用虚假IP地址攻击Web服务器。要求在攻击成本不高于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。  **1.1失败参数/工具选择**  在该平台上，参数设置为：虚假IP攻击台数为10，攻击速率为1000，虽然攻击成本没超过50，但是网络服务质量却超过了40，结果失败，如下图所示。      **1.2成功参数/工具选择**  可适当增加虚拟IP攻击台数，使攻击成本不超过50，但服务质量降低到40以下。参数设置为：虚假IP攻击台数为50，攻击速率为1000，结果成功，如下图所示。      攻击方在单位时间内发送大量数据包，超过防火墙的处理能力，则能达到攻击目的。  **2.真实IP地址攻击**  真实IP地址攻击任务发生在浏览器向服务器发出HTTP请求，服务器向浏览器返回HTTP响应阶段，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。  在该实验中，扮演黑客，利用真实IP地址攻击Web服务器。要求在攻击成本不高于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。  **2.1失败参数/工具选择**  在该平台上，参数设置为：真实IP攻击台数为500，攻击速率为1000，虽然网络服务质量没超过90，但是攻击成本却超过了50，结果失败，如下图所示。      **2.2成功参数/工具选择**  可适当减少真实IP攻击台数，使攻击成本降低。使攻击成本不超过50，但服务质量降低到90以下。参数设置为：真实IP攻击台数为10，攻击速率为1000，结果成功，如下图所示。      **3.初级防御实验**  初级防御实验发生在浏览器与Web服务器之间建立TCP连接阶段，攻击者采用虚假IP地址向Web服务器发出大量连接请求，从而消耗服务器的计算资源，降低其服务质量。  在该实验中，扮演网络管理员，对虚假IP地址攻击进行防御。要求在防御成本不高于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。  **3.1失败参数/工具选择**  在该平台上，参数设置为：连接请求带宽为500000，服务请求带宽为500000，防御失败，如下图所示。      **3.2成功参数/工具选择**  内存占用率为100%，说明发动了SYN攻击，可使用Cookie工具，在使用Cookie工具后，防御成功，如下图所示。    Cookie使用防hash技术防御SYN泛洪攻击，减少服务器内存消耗。  **4.中级防御实验**  中级防御实验发生在浏览器向服务器发出HTTP请求，服务器向浏览器返回HTTP响应阶段，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。  在实验中，扮演网络管理员，对真实IP地址攻击进行防御。要求在防御成本不高于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。  **4.1失败参数/工具选择**  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，但是只采用DRR工具，虽然有一定防御效果，但是服务质量没能达到90，防御失败，如下图所示。    **4.2成功参数/工具选择**  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。连接请求带宽尽量调低（但不能过低，否则不能建立连接），以降低防御成本。参数设置为：连接请求带宽为50000，服务请求带宽为1000000，防御成功，如下图所示。      DRR是一种数据包调度算法，使每个IP的请求被均匀处理。  **5.综合防御实验**  在综合防御实验中攻击者向Web服务器发出大量请求，从而消耗服务器的计算资源，降低其服务质量。  在实验中，扮演网络管理员，对拒绝服务攻击进行防御。要求在防御成本不高于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。  **5.1失败参数/工具选择**  攻击者采用了虚假 IP 和真实 IP 地址混合攻击。因此Cookie和DRR都需要使用，但是只采用Cookie和DRR工具，虽然有一定防御效果，但是服务质量没能达到80，防御失败，如下图所示。    **5.2成功参数/工具选择**  除了Cookie和DRR工具，配额工具可以有效缓解攻击者的慢速攻击，但是需要将惩罚因子调高，使防御成本不超过20。最后，适当提高一点服务请求带宽，使网络质量达到要求。参数设置为：连接请求带宽为500000，服务请求带宽为500000，惩罚因子为0.4，防御成功，如下图所示。        配额：若某个IP的请求数量超过限额，则减小其调度机会。  **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。  用户一次连接失败的概率是(1-p)，三次连接都失败的概率是 (1-p)\* (1-p)\* (1-p) ，那么用户连接成功的概率为 1-(1-p)\* (1-p)\* (1-p)。    **7.服务速率建模**  第一步：估计被服务的用户人数  在稳定状态下，每个用户的服务时间为 w/v，到达率为 a，故正在接受服务的用户人数为 a\*w/v 。    第二步：估计服务速率  由于配额机制的使用，使得 z 个攻击者相当于只有 z\*q 个能正常攻击，故总共有 x+z\*q 个用户共用带宽，故服务速率可表示为 s/(x+z\*q)。    第三步：求解模型  前面两个表达式可构成一个方程组，即 x=a\*w/v，v=s/(x+z\*q)。求解这个方程可得到 v= s/( a\*w/v +z\*q)。    **8.攻防博弈**  利用混合策略纳什均衡，设置加带宽的概率为0.6，在10次攻防实验中的收益大于10，获得胜利。 | | | | | | |
| 五、实验过程中遇到的问题及解决情况  **1.问题：**攻防实验中随机赋值，成功率低  **解决方案：**根据调整攻击台数和攻击速率等参数找出出成本和服务质量计算公式，然后结合成本和服务质量的要求确定调整参数方向，并综合查看连接成功率、连接数、服务成功率、服务速率、内存占用率等参数以及Cookie、DRR、黑名单、配额等防御工具，确定最终的参数大小。 | | | | | | |
| 六、实验结果及分析和（或）源程序调试过程  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。  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。  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。 | | | | | | |