**《信息安全基础》实验报告**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **姓名** | | **孙莹莹** | | **年级** | | **2020级** |
| **学号** | | **20204104** | | **专业、班级** | | **计算机科学与技术卓越一班** |
| **实验名称** | **实验三 拒绝服务攻击与防御仿真实验** | | | | | |
| **实验时间** | **2023.5.7** | | **实验地点** | | **DS3401** | |
| **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。 | | | | | | |
| 1. 实验过程或算法   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。   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： IMG_256 虚假IP地址攻击实验  1. **问题概述：**   虚假IP地址攻击任务发生在上述第一个阶段，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。 任务说明：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。  1. **问题分析：**   在虚假IP地址攻击中，虚假IP攻击台数、虚假IP攻击速率与攻击成本之间的关系是非常密切的。一般来说，攻击者使用更多的虚假IP地址和更高的攻击速率可以使攻击效果更强，并且更难被检测和防御。但同时，这也会增加攻击成本。  具体来说，如果攻击者使用更多的虚假IP地址进行攻击，需要购买更多的IP地址或租用更多的僵尸主机，这会增加攻击成本。类似地，如果攻击者使用更高的攻击速率，需要更多的计算能力和带宽资源，这也会增加攻击成本。当然，攻击者可能会尝试降低攻击速率或减少攻击台数以降低成本，但这也会影响攻击效果。   1. **实验过程：**   首先调整虚假IP攻击台数为40，虚假IP攻击速率为1000：  结果成本为40，服务质量为99。此时攻击效果不佳。    然后调整虚假IP攻击台数为50，虚假IP攻击速率为1000：    由图可见，在增加虚假IP攻击台数之后，变化最大的是连接成功率和服务成功率（大幅下降）。可以认为当攻击台数较少时，连接成功率和服务成功率可能会比较高，因为攻击者可以精细地控制攻击策略并规避检测。但是，当攻击台数增多时，连接成功率和服务成功率可能会下降，因为攻击者可能会采用大量的虚假IP地址来进行攻击，导致目标系统无法承受过多的请求并拒绝服务。 真实IP地址攻击实验  1. **问题概述：**   真实IP地址攻击任务发生在上述第二个阶段，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。  任务说明：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  1. **问题分析：**   在真实IP地址攻击中，真实IP攻击台数、真实IP攻击速率与攻击成本之间存在一定的关系。通常情况下，攻击者可以通过使用大量的僵尸主机来进行分布式拒绝服务（DDoS）攻击，从而达到大规模的攻击效果。攻击者可以租用或控制大量的僵尸主机，这意味着攻击者可以同时攻击多个目标，并能够在短时间内向目标发送大量的流量。  攻击者使用越多的真实IP地址，攻击速率就可能越高，因为攻击者可以利用更多的带宽和计算资源来发起攻击。此外，攻击成本也可能会随着攻击所需的真实IP地址数量增加而上升。  然而，攻击者可能会选择使用较少的真实IP地址来执行攻击，以避免被检测和防御。在这种情况下，攻击者可以使用“IP地址欺骗”的技术，将攻击流量伪装成来自合法的IP地址，这样可以使攻击看起来像是由少数几个主机发起的，但实际上攻击者可能正在使用更多的主机来进行攻击。   1. **实验过程：**   首先设置真实IP攻击台数为50，真实IP攻击速率为1000：  结果成本为50，服务质量为49    然后不断降低真实IP攻击台数，保持真实IP攻击速率为1000不变：最后降到台数为1，成本为1，服务质量为50。可以发现此时虽然攻击台数少了很多，但是服务质量却只上升了1。  对比仪表盘发现主要是连接数略有下降，而连接成功率略有上升，连接数略有下降可能是因为IP数量较少会使得攻击者的连接速度更慢，从而导致连接数下降。同时，连接成功率略微上升可能是因为攻击者为了提高攻击成功率，会删除已经失效的IP地址，这也会导致IP数量减少，但连接成功率可能会略微上升。    真实IP攻击台数为0的时候，才会攻击失败（显然如果不攻击自然是失败的）： 初级防御实验  1. **问题概述：**   初级防御实验发生在上述第一个阶段，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。  任务说明：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  1. **问题分析：**   DRR和Cookie都可以用于防御虚假IP地址攻击。下面分别介绍它们的作用和效果。   1. DRR   DRR是一种基于比例的负载均衡算法，它可以根据客户端的IP地址分配流量，从而避免来自同一IP的虚假请求过多占用服务器资源。DRR算法会根据各个客户端IP地址的访问次数来调整权重，使得来自同一IP的请求分配的服务资源不会过多。  DRR对于防御虚假IP地址攻击有一定的效果，因为攻击者使用的虚假IP地址访问次数很少，因此会分配到较少的资源，从而减轻服务器负担，确保正常用户的服务质量。但是，如果攻击者使用多台虚假IP来发起攻击，则DRR会失效，因为每个IP地址的请求量都很少，无法有效进行流量分配。  2. Cookie  Cookie是一种存储在客户端浏览器上的小文本文件，服务器可以在客户端的浏览器中存储和检索Cookie来识别用户。服务器可以设置Cookie来记录用户的访问信息，如登录信息、购物车商品信息等。因此，服务器可以使用Cookie来验证请求是否来自合法用户，而非虚假IP地址的攻击者。  Cookie对于防御虚假IP地址攻击是一种比较有效的手段，因为攻击者仅仅伪造IP地址，而其它信息（如HTTP头中的Cookie）还是可信的。服务器可以挖掘用户请求的其它信息，使用Cookie记录下与用户相关的信息。在后续请求时，服务器根据Cookie信息进行验证，从而排除来自虚假IP地址的非法请求。   1. **实验过程：**   基于上述分析，首先尝试添加一个DRR和一个Cookie,成本为15，服务质量为95，成功    然后尝试只适用一个cookie,设置了连接请求带宽为100000，服务请求带宽为500000，此时服务质量只有33，失败。  对比上面有DRR的例子，可以发现服务速率提升了，但是连接数和连接成功率下降了，导致服务质量下降。这是因为去掉DRR后，会导致请求的流量集中在特定的IP地址上。而流量大量集中在特定IP上，如果该IP担负不起这么大的请求量，就会出现连接数减少，服务器负载较重，无法正常处理请求的情况。其次如果服务器无法及时处理集中的流量，部分请求就有可能会超时或失败，从而导致连接成功率下降。虽然服务速率可能会提升，但是这种速率提升是建立在牺牲接受连接数和连接成功率的基础上的。这说明去掉DRR对于虚假IP地址攻击的防御能力和用户体验都有一定的影响。    然后针对上述分析，改善服务器负载过重的问题。尝试更改连接请求带宽为500000，服务请求带宽为500000，此时服务质量上升到95，成本为10，成功。  对比上一个例子可以发现，提高连接请求带宽，可以大大提升连接成功率，这是因为连接请求带宽的大小直接影响着网络连接的质量和速度。当有大量请求同时发生时，如果带宽不足，就会出现请求被阻塞或超时等故障，从而导致连接成功率下降。在这种情况下，提高连接请求带宽可以帮助缓解网络传输时的瓶颈，从而加快连接的建立。具体来说，通过增加带宽，可以让更多的请求同时被接收和处理，减少请求被阻塞的情况，使请求能够更快地被传输到目标服务器，提高连接建立的成功率。因此服务质量得到了提升。   中级防御实验  1. **问题概述：**   中级防御实验发生在上述第二个阶段，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。 任务说明：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。  1. **问题分析：**   DRR和黑名单可用于防御真实IP地址攻击。  1. DRR的作用  DRR能够有效防御真实IP地址攻击，因为攻击者通过同一IP地址发起攻击，导致服务器资源容易集中在某一IP上，如果使用DRR算法进行流量分配，则可以减少来自同一IP地址的请求量。但是如果攻击者使用多个真实IP地址来发起攻击，则DRR算法防御效果会降低。  2. 黑名单的作用  黑名单是一种常见的防御真实IP地址攻击的方法，它基于一定的规则将非法的IP地址列入黑名单，从而防止其发起攻击。当检测到来自黑名单中的IP地址时，系统会直接拦截或限制请求，从而防止攻击者继续发起攻击。不过，黑名单需要及时更新，才能保证防御措施的有效性。   1. **实验过程：**   放置一个DRR和一个黑名单，设置连接请求带宽为100000，服务请求带宽为800000，此时服务质量为99，但成本过高，为99.    然后保持其他设置不变，降低黑名单的服务速率阈值到900，此时成本为20，服务质量为99。  对比失败案例，发现降低黑名单的服务速率阈值之后，连接数和连接成功率略有提升，因为黑名单服务速率最大值下降了，那么可能有一部分黑名单没有被拦截而是成功连接，也可能是因为更少的正常用户被误判和误封，而能够正常连接。同时防御成本降低了也是因为这样可以减少误判和误封，减少了需要手动解封的次数，同时提高了识别的准确性。降低黑名单服务速率阈值，可以更精细地控制流量的阈值，使其更易于识别和过滤非法或恶意流量，减少因未能检测到攻击流量而引起的损害。     综合防御实验  1. **问题概述：**   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。  任务说明：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。  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  1. **问题分析：**   DRR，cookie 和配额都是防御拒绝服务攻击的常用手段，它们的作用分别是：  1.DRR：当服务器负载较高时，DRR 会自动降低请求处理速率，从而避免服务器崩溃。使用 DRR 可以有效防御 DDoS 攻击。  2.Cookie：在防御拒绝服务攻击中，可以使用 Cookie 来识别正常的用户请求和恶意的攻击请求。对于恶意的攻击请求，可以通过设置 Cookie 的方式拒绝其访问。  3.配额：配额是一种限制每个用户访问服务器资源的数量的机制。在防御拒绝服务攻击中，可以使用配额来限制每个用户的访问频率，从而避免恶意攻击者占用过多的服务器资源。   1. **实验过程：**   首先放置一个cookie,一个DRR和一个配额，其他设置不变。此时成本为35，而服务质量为88。成本太高而导致失败。    然后将配额的惩罚因子修改为0.4，此时成本为20，而服务质量为88。成功。  对比两个例子，发现提高配额的惩罚因子，主要是服务成功率下降了，其他没有大的变化。这是因为提高配额的惩罚因子意味着对于每个请求，系统会限制客户端可以发送的数量。如果客户端发送请求的速度过快，超过了这个限制，那么系统会拒绝这些请求。这种限制可以减轻服务器的负载，从而防止拒绝服务攻击。如果提高惩罚因子，那么客户端可能会因为请求被拒绝而无法正常访问系统，从而导致服务成功率下降。  此外，提高配额的惩罚因子还会导致防御成本下降。这是因为当惩罚因子较高时，服务器需要处理的请求数量会减少，从而减少了服务器的负载和网络带宽的使用。因此服务器可以更好地处理来自其他客户端的请求，从而提高了系统的整体性能和可靠性。因此，提高配额的惩罚因子是一种有效的防御拒绝服务攻击的方法，但需要权衡好服务成功率和防御成本。   连接成功率建模 假设一般用户请求连接时最多尝试三次，那么连接成功的条件是这三次中至少有一次被防火墙同意。根据概率论知识，这个事件的概率可以用排列组合来计算：  p(连接成功) = 1 - [p(三次都被防火墙拒绝)]= 1 - (1 - p)3  其中，p(三次都被防火墙拒绝)表示三次连接请求都被防火墙拒绝的概率，即每次连接都以概率1-p被防火墙拒绝，因此三次都被拒绝的概率为(1 - p)3。  所以，一般用户可成功连接的概率是1-(1 - p)3。写成四则运算的表达式就是：1-(1-p)\*(1-p)\*(1-p)。   服务速率建模 （1）估计被服务的用户人数    在稳定状态下，单位时间到达的用户数等于完成服务后离开的用户数。因此，在任何时刻，当前接受服务的用户数与单位时间内完成服务后离开的用户数相等。假设当前接受服务的用户数为n，则有：  n = a \* T  其中，T为一个用户完成服务的平均时间。  每个用户完成服务需要请求的数据量为w，而服务速率为v，则完成服务的平均时间为：  T = w / v  将T代入上式得到当前接受服务的用户数：  n = a \* w / v  （2）估计服务速率    因为肉机获得贷款的概率为q,那么获得服务占用带宽的肉机数量：  t = q \* z  然后加上接受服务的用户数x,即可得到享受服务带宽的用户总数  n = x + q \* z  服务速率等于每个用户获得的平均带宽，因此就等于服务带宽除以用户总数：  h = s/(x+q\*z)  （3）求解模型    将第一步的结果n = a \* w / v带入到第二步的 h = s/(x+q\*z)，其中x等于n,即可得到结果：  V\_service = s/(a\*w/v+q\*z) 攻防博弈   根据混合策略纳什均衡：在多人参与的博弈中，假设每个参与者按一定概率配置选择策略，如果任何一个参与人单独改变其概率配置都不会提高收益的数学期望，则该状态构成混合策略纳什均衡。  用等值法进行求解：以网站方而言，它选择加带宽的概率q应该使得下面的情况成立，无论黑客如何选择p值（即选择策略攻击的概率），其收益的期望值是相同的。  黑客选择策略攻击的收益期望值： E(A) = -10q + 10(1-q)  黑客选择策略不攻击的收益期望值： E(B) = 5q  使E(A)=E(B)，解得q=0.4，即加带宽的概率应当为0.4。 | | | | | | |
| 五、实验结果及分析和（或）源程序调试过程  （1）实验结果及分析：  所有实验的结果和相应的分析已经在上面给出，此处不再赘述。  （2）思考与总结：  1.**在虚假和真实IP地址攻击中**，攻击参数与攻击成本之间的关系是复杂的，这取决于多种因素。攻击参数可以包括攻击流量的大小、攻击持续时间和攻击目标的数量等。攻击成本则可以包括攻击者使用的资源成本（例如带宽和计算能力）以及攻击者需要付出的时间成本。通常情况下，攻击参数越高，攻击成本也就越高。比如，攻击流量大、攻击持续时间长、攻击目标多的攻击会比较耗费攻击者的资源和时间，因此成本更高。  IP地址攻击对网络服务质量的影响也是很显著的。由于攻击流量大且持续时间长，攻击会占用网络带宽和系统资源，导致合法用户无法访问受攻击的服务或访问速度变慢。攻击还可能使得服务器崩溃或被迫重启，进一步影响服务可用性和稳定性。因此，IP地址攻击是一种非常破坏性的网络攻击方式，需要采取有效的防御措施来保护网络安全。  2.**要防御虚假IP地址攻击和真实IP地址攻击**，首先是可以实施防火墙策略，限制流量来源。一些防火墙产品（如cookie）能够识别和阻止虚假IP地址攻击，如果防火墙检测到IP地址不合法，则可以将其封锁或者转发给安全团队进行进一步分析。还可以添加身份验证机制。要求用户或设备在访问资源之前进行身份验证、授权或者验证数字证书等。如果有攻击者使用伪造IP地址进行攻击，则会被拒绝访问。黑名单和白名单也很有用，将已知恶意IP地址列入黑名单，并限制它们与服务器的连接。另一方面，将经过认证的可信IP地址列入白名单，以促进合法的流量运行。除了实验中用到的防御工具，还可以在服务器日志中监视和追踪IP地址。攻击者通常会使用大量不同的IP地址对目标进行攻击。通过在服务器日志中监视IP地址，可以识别出一些可疑的流量来源，并进行进一步的分析，以便更好地防御攻击和保护系统安全。 | | | | | | |