《信息安全基础》实验报告

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

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。在仿真平台中完成拒绝服务的攻击和防御实验：

1. 攻击仿真实验：学生扮演黑客角色对服务器发动攻击。任务目标是在一定的攻击成本内，使网络服务质量下降到某个数值之下；

2. 防御仿真实验：学生扮演网络管理员的角色对拒绝服务攻击进行防御。任务目标是在一定的防御成本内，使网络服务质量保持在某个数值之上；

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：根据网站或黑客的策略矩阵，利用基本的博弈论方法，设置防御参数，参与攻防仿真实验。

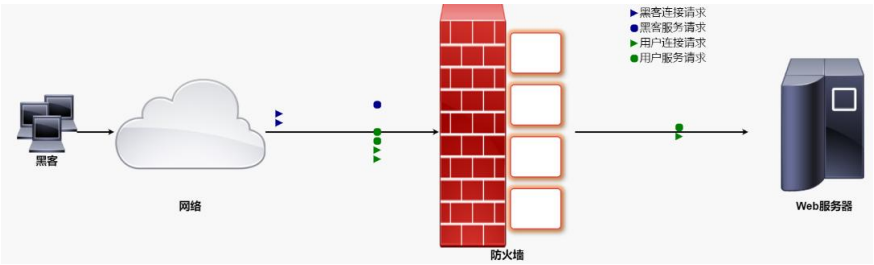
三、实验设计

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。

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。本次实验主要考虑了两种攻击方式和四种防御工具：虚假 IP 地址攻击、真实 IP 地址攻击；Cookie、DRR、黑名单、配额。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。防御工具中，Cookie 使用防 hash 技术防御 SYN 泛洪攻击，减少服务器内存消耗；DRR 使每个 IP 的请求被均匀处理；黑名单对 IP 请求速率过快的主机不响应其请求；配额对某个 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：成本和服务质量。成本即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。服务质量即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：

服务质量=连接成功率×服务成功率×服务速率

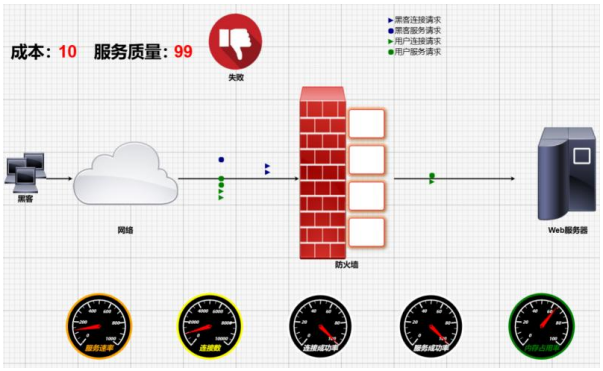
在攻防实验中，会通过仿真的数据仪表盘表示网络通信的状态，仪表盘显示与服务质量相关的 5 个重要指标：

- 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。

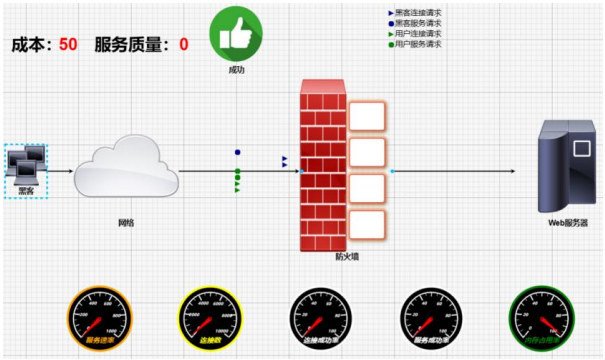
四、实验过程或算法

1. 虚假 IP 地址攻击：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。

虚假 IP 地址攻击就是攻击者采用虚假 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。题干中说防火墙用于处理连接请求的带宽为 500000 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。因此防火墙最多能够同时处理的连接请求数为：500000 / 100 = 5000。先看初始设定值：



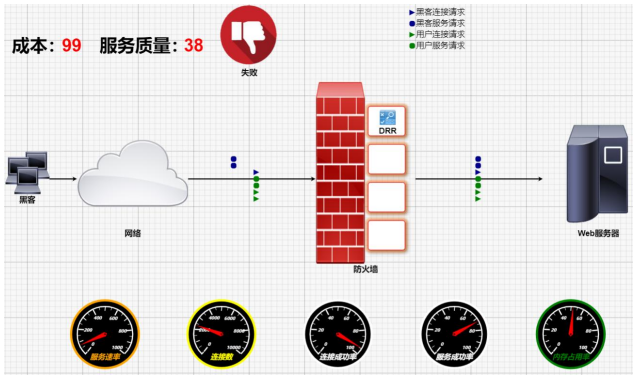
显然其前四个指标都高了，尤其是连接成功率和服务成功率，为了降低连接成功率和服务成功率，需要上调虚假 IP 攻击速率；但这样又会大大提高成本，为了保证成本低于 40，需要降低攻击台数：



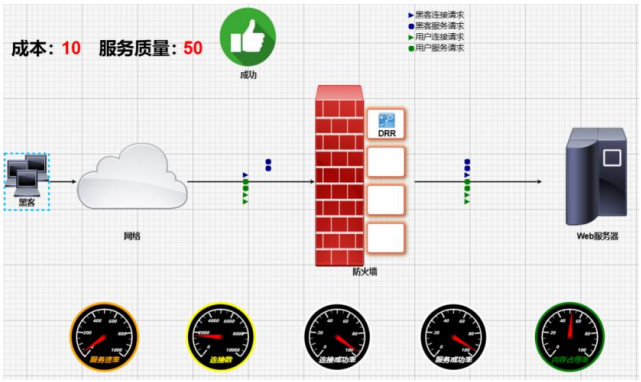
攻击成功！

2. 真实 IP 地址攻击实验：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。

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。先看初始设定值：

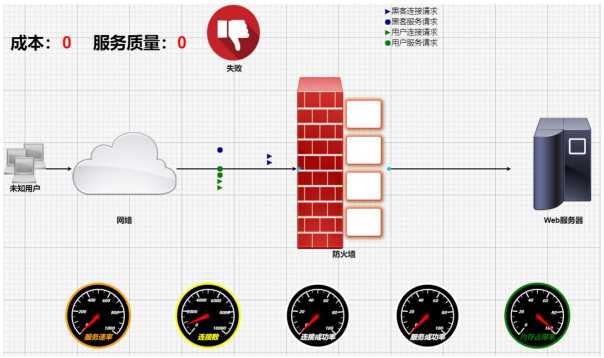


服务质量达标了，但是成本太高了，降低攻击台数后攻击成功：

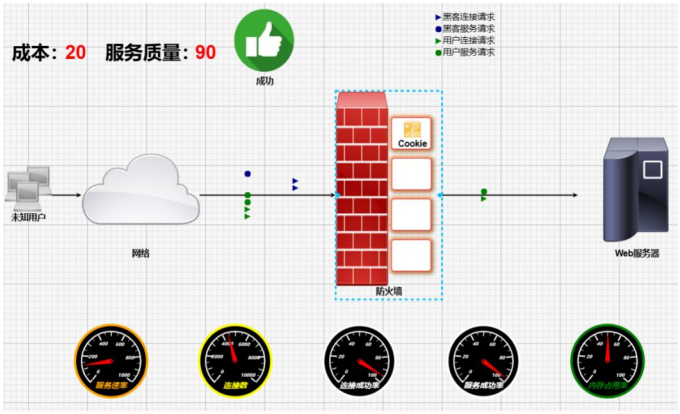


攻击成功！

3. 初级防御实验：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。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。先看初值：

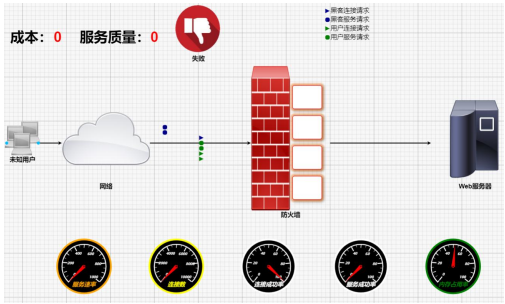


连接成功率和服务成功率太低，需要增加服务请求带宽，然后微调连接请求带宽即可：

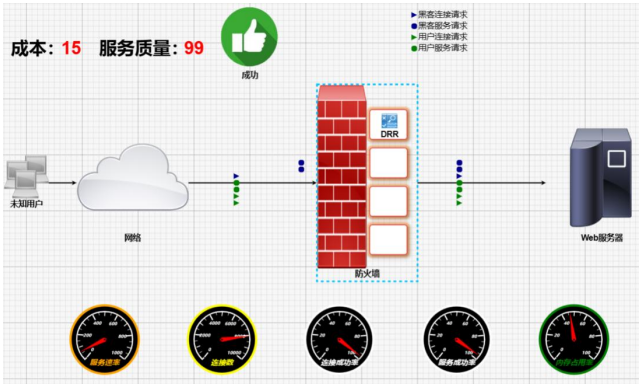


防御成功！

4. 中级防御实验：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。先看初值：

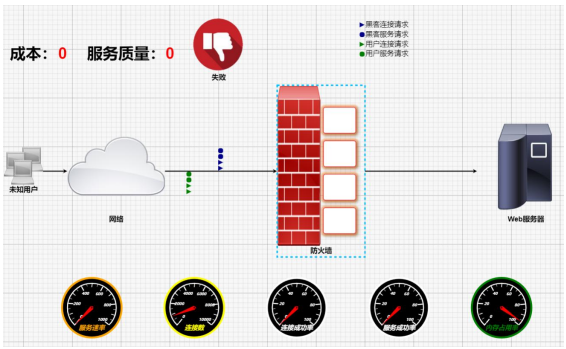


连接数和服务成功率太低，但连接成功率很高，可能是 IP 请求处理不均匀导致，需要再防火墙上加 DRR 使每个 IP 的请求被均匀处理：

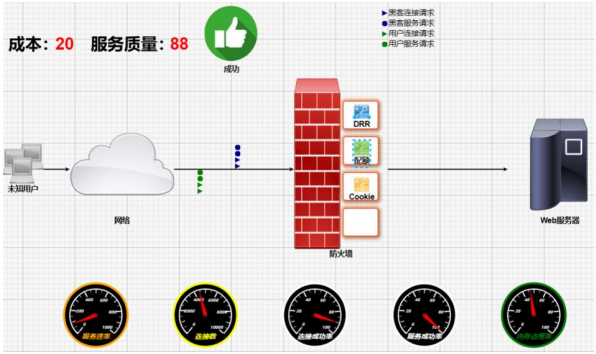


防御成功！

5. 综合防御实验：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。先看初值：



连接成功率太低，需要提高连接带宽，并增加配额对请求数量超过限额的 IP 减小其调度机会；服务成功率太低，可以在防火墙中增加 DRR 使每个 IP 的请求被均匀处理；看到图中内存占用率爆满，可以通过增加 Cookie 减少服务器内存消耗：



防御成功！

6. 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。

成功连接率 = P(第一次连接成功) + P(第二次连接成功) + P(第三次连接成功)；

P(第一次连接成功) = p，因为在第一次连接时，如果防火墙同意连接请求，那么连接就会成功；

P(第二次连接成功) = (1-p) * p，因为在第一次连接时，如果防火墙拒绝连接请求，那么一般用户会进行第二次连接尝试，如果第二次连接请求被防火墙同意，那么连接就会成功；

P(第三次连接成功) = (1-p) * (1-p) * p，因为在前两次连接尝试中，如果防火墙都拒绝了连接请求，那么一般用户会进行第三次连接尝试，如果第三次连接请求被防火墙同意，那么连接就会成功；

因此，一般用户成功连接的概率可以表示为：

成功连接率 = p + (1-p) * p + (1-p) * (1-p) * p

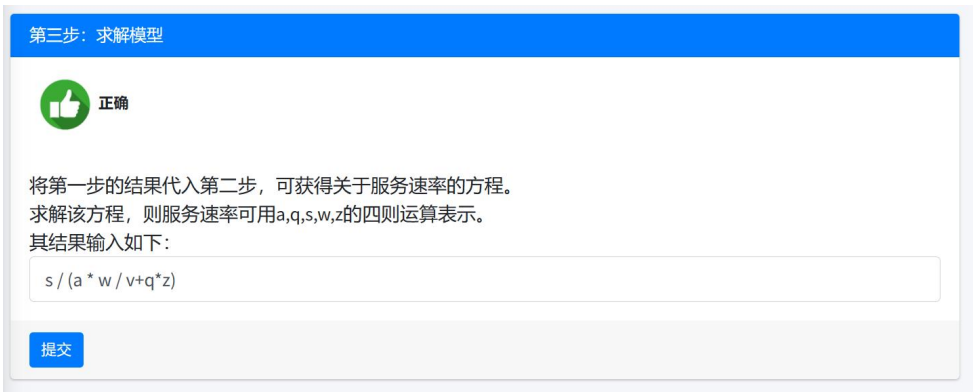
7. 服务速率：假设每秒有 a 个新用户与网站服务器建立 TCP 连接。每个用户从建立连接到离开网站请求的总数据量为 w。 同时有 z 台肉机一直

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？

（1）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。 假设每秒到达的新用户数为 a，用户请求的数据量为 w，服务速率为 v，则当前接受服务的用户数=a*(w/v)；

（2）在稳定状态下，肉机和用户将共享服务带宽。由于使用了配额机制， 相比一般用户，肉机获得带宽的概率仅为 q。假设服务带宽为 s，当前接受服务的用户数为 x，肉机数为 z，则服务速率=s/(x+q*z)；

（3）将（1）中结果代入（2）中 x，则防火墙可稳定提供给用户的服务速率=s/(a*(w/v)+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

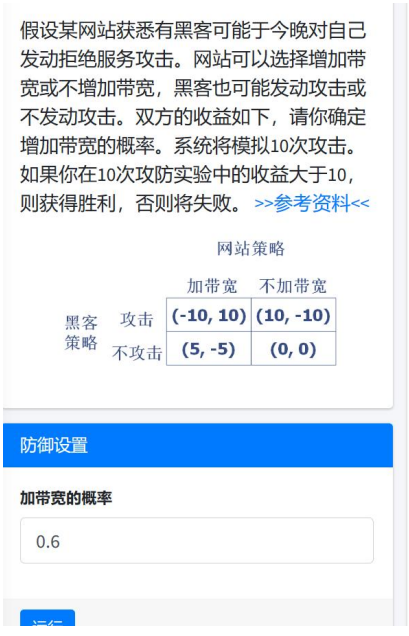
击。网站可以选择增加带宽或不增加带宽，黑客也可能发动攻击或不发动攻击。双方的收益如下，请你确定增加带宽的概率。系统将模拟 10 次攻击。如果你在 10 次攻防实验中的收益大于 10，则获得胜利，否则将失败。

概率为 0.5 时收益为负：

失败

#	网站	黑客	收益
1.	加带宽	不攻击	-5
2.	不加带宽	不攻击	0
3.	不加带宽	攻击	-10
4.	不加带宽	不攻击	0
5.	不加带宽	攻击	-10
6.	不加带宽	攻击	-10
7.	加带宽	攻击	10
8.	不加带宽	攻击	-10
9.	加带宽	攻击	10
10.	加带宽	攻击	10
总收益：			-15

概率为 0.6 时收益大于 10：



成功

#	网站	黑客	收益
1.	加带宽	攻击	10
2.	加带宽	攻击	10
3.	加带宽	攻击	10
4.	加带宽	攻击	10
5.	加带宽	攻击	10
6.	不加带宽	攻击	-10
7.	加带宽	攻击	10
8.	加带宽	攻击	10
9.	不加带宽	攻击	-10
10.	不加带宽	攻击	-10
总收益：			40

五、实验过程中遇到的问题及解决情况

1. 问题：一开始做攻防实验时，参数设定全靠随机赋值，成功率很低：

解决办法：根据服务质量公式并结合成本可以有方向地调节参数数值，还可以通过查看下方服务速率、连接数、连接成功率、服务成功率、内存占用率等数值调整参数并选择合适的防御工具；

六、实验结果及分析和（或）源程序调试过程

本次实验主要考虑了两种攻击方式和四种防御工具：虚假 IP 地址攻击、真实 IP 地址攻击；Cookie、DRR、黑名单、配额。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。防御工具中，Cookie 使用防 hash 技术防御 SYN 泛洪攻击，减少服务器内存消耗；DRR 使每个 IP 的请求被均匀处理；黑名单对 IP 请求速率过快的主机不响应其请求；配额对某个 IP 的请求数量超过限额，则减小其调度机会。

本次实验依次进行了攻击仿真、防御仿真、数学建模、攻防博弈，通过扮演黑客和网络管理员角色对服务器发动攻击或进行防御。任务目标是在一定的攻击成本内，使网络服务质量下降到某个数值之下或保持在某个数值之上。我还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。并根据网站或黑客的策略矩阵，利用基本的博弈论方法，设置防御参数，参与攻防仿真实验。