《网络空间安全概论》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

在仿真平台中完成拒绝服务的攻击和防御实验，包括

- 虚拟 IP 地址攻击
- 真实 IP 地址攻击
- 初级防御时延
- 中级防御实验
- 综合防御实验
- 连接成功率建模
- 服务速率建模
- 攻防博弈

三、实验设计

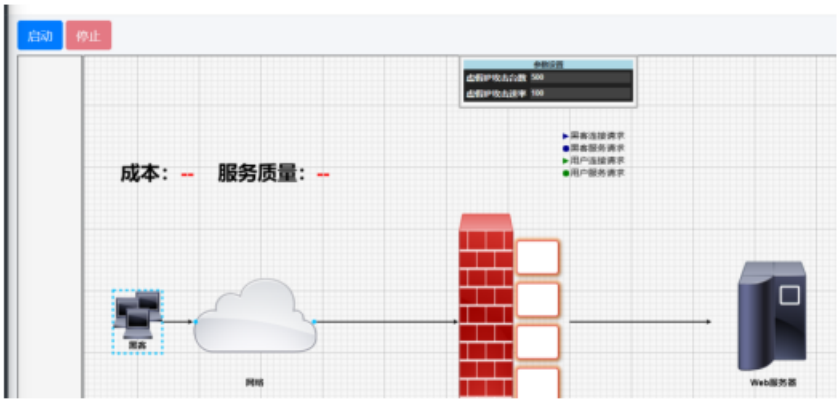
实验原理

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。

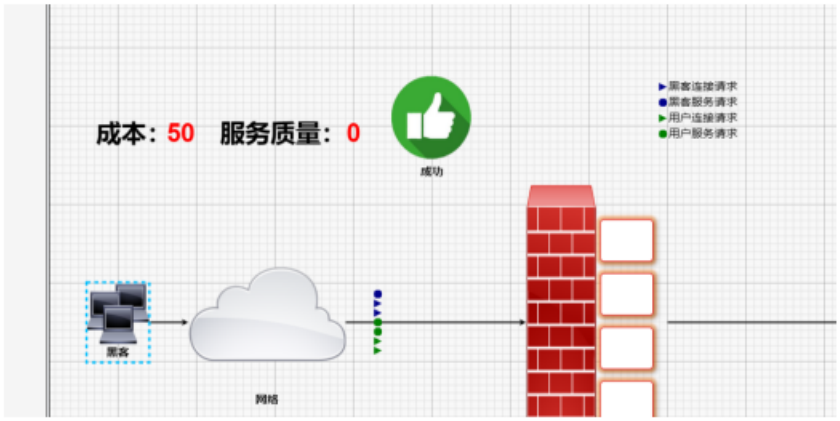
四、实验过程或算法

实验 1：虚拟 IP 地址攻击

实验 1 的要求是在成本不高于 50 的前提下进行虚拟 IP 地址攻击使网络服务质量降低到 40 或以下。将虚拟 IP 攻击台数设置为 500，虚拟 IP 攻击速率设置为 100。

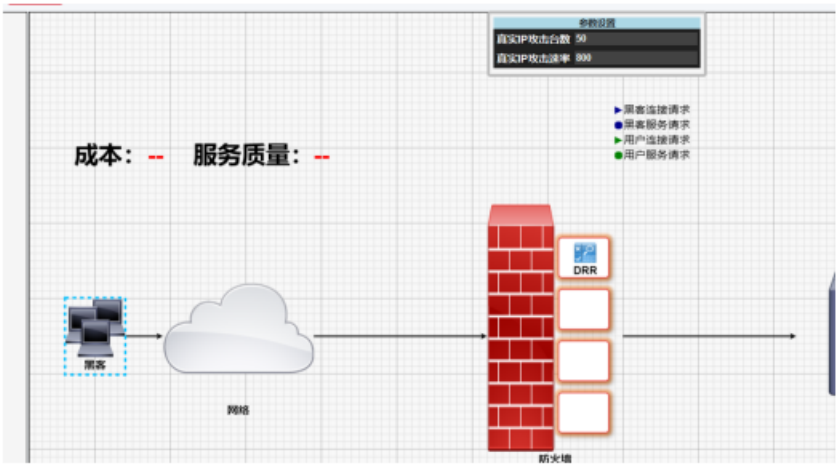


攻击成功，成本为 50，服务质量为 0.



实验 2：真实 IP 地址攻击

实验 2 的要求是在成本不高于 50 的前提下进行真实 IP 地址攻击使网络服务质量降低到 90 或以下。将虚拟 IP 攻击台数设置为 50，虚拟 IP 攻击速率设置为 800。

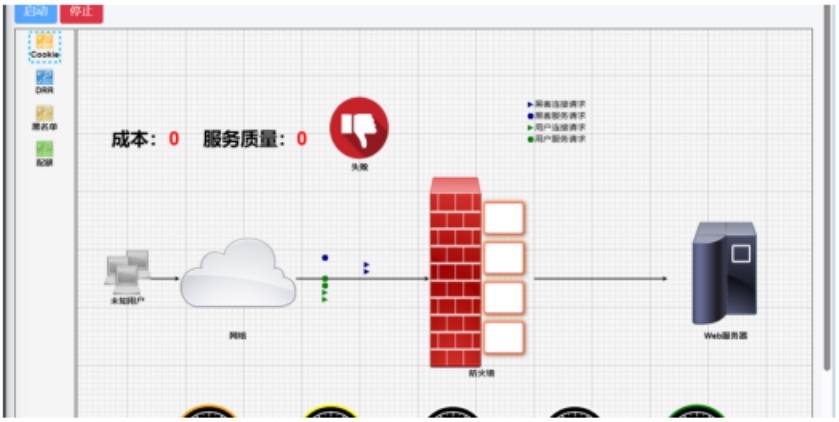


攻击成功，成本为 40，服务质量为 48.

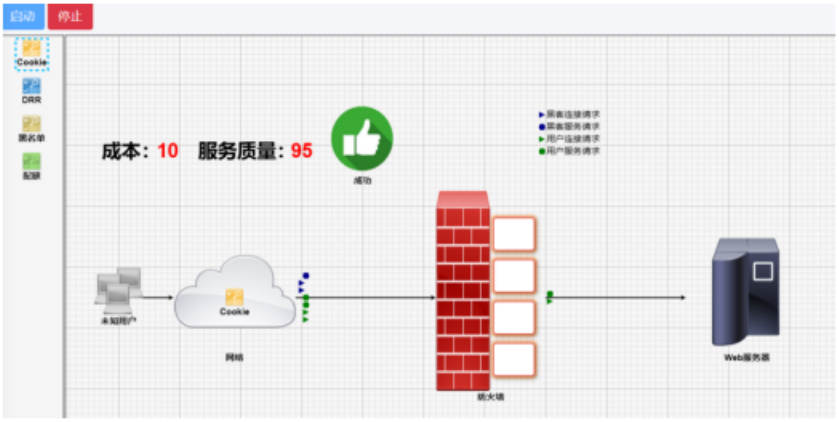
实验 3：初级防御实验

实验 3 的要求是在防御成本不高于 20 的前提下使网络服务质量保持在 90 或以上。

保持默认参数配置时，防御失败。



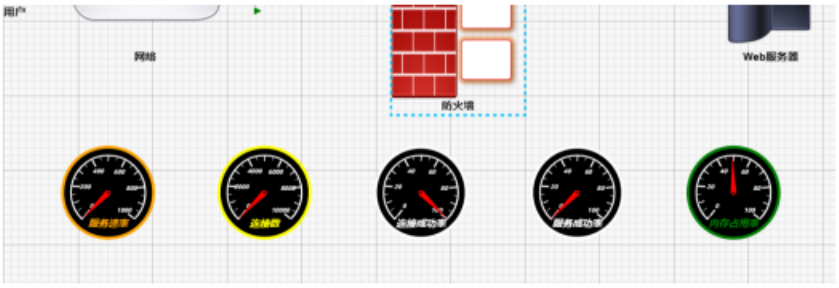
向 web 浏览器中增加 Cookie 设置，保持默认参数不变，**防御成功：成本为 10，服务质量保持为 95.**



实验 4：中级防御实验

实验 4 的要求是在防御成本不高于 20 的前提下使网络服务质量保持在 90 或以上。

可以看到，在默认情况下，连接成功率较高，但是服务成功率为 0.



- 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。

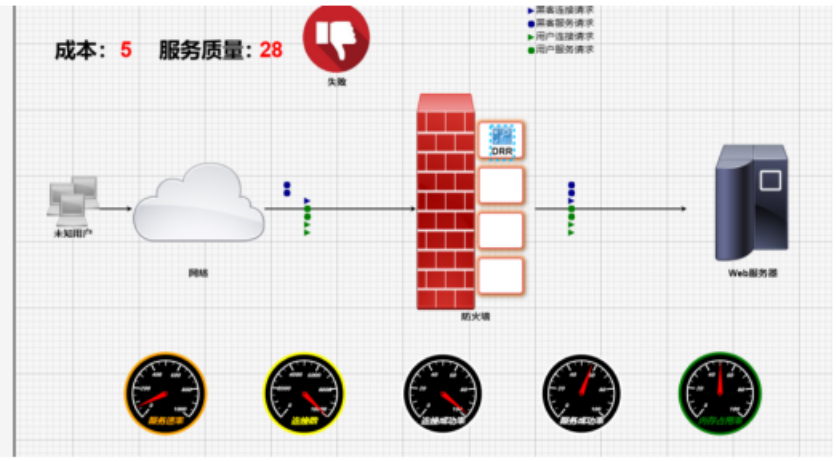
中级防御实验发生在上述第二个阶段，攻击者采用真实IP地址向Web服务器发出大量服务请求，从而消耗服务器的计算资源，降低其服务质量。

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。

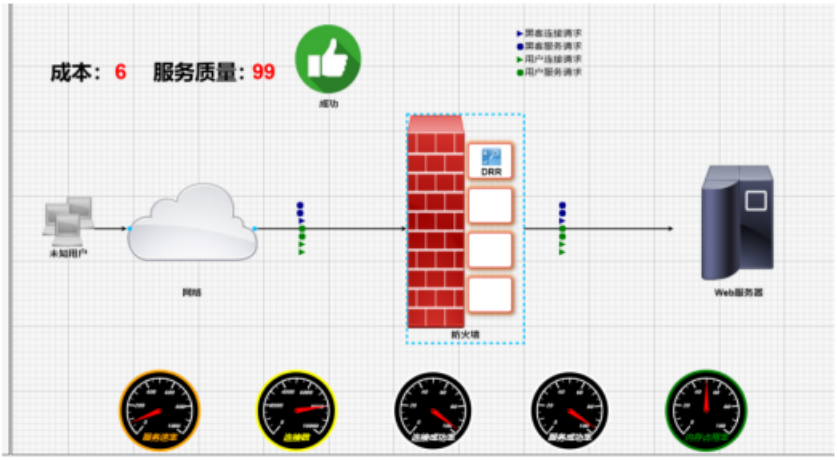
已知条件如下：

引入 DRR 模块并保持默认参数不变：



可以看到用户服务成功率仍较低，因此需要进一步阻隔连接请求带宽，增大服务请求带宽。将连接请求带宽降低到 10，服务请求带宽提升至 1000000.

防御成功：成本为 6，服务质量为 99.

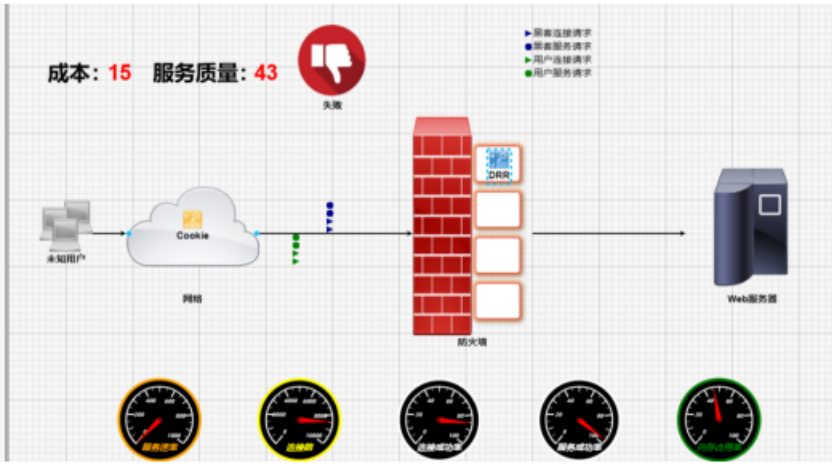


可以看到服务请求率接近 100%，达到了质量要求。

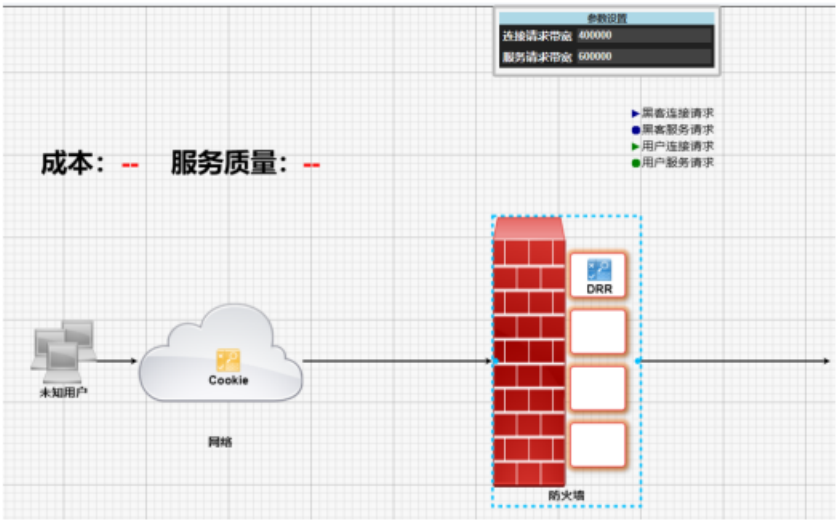
实验 5：综合防御实验

实验 5 的要求是在防御成本不高于 20 的前提下使网络服务质量保持在 80 或以上。

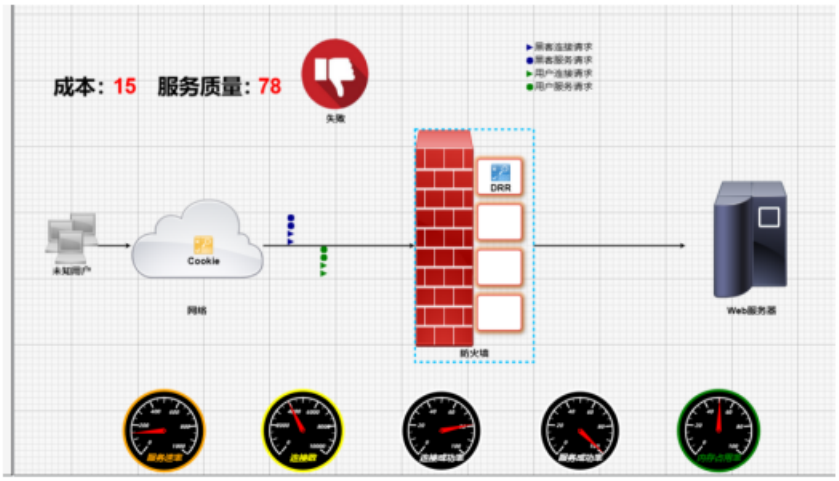
受实验 3，4 的启发，首先加入 cookie 和 DRR 模块，可以看到服务成功率和连接成功率较高，但是服务速率为 0，导致服务质量为 43，未达到要求。



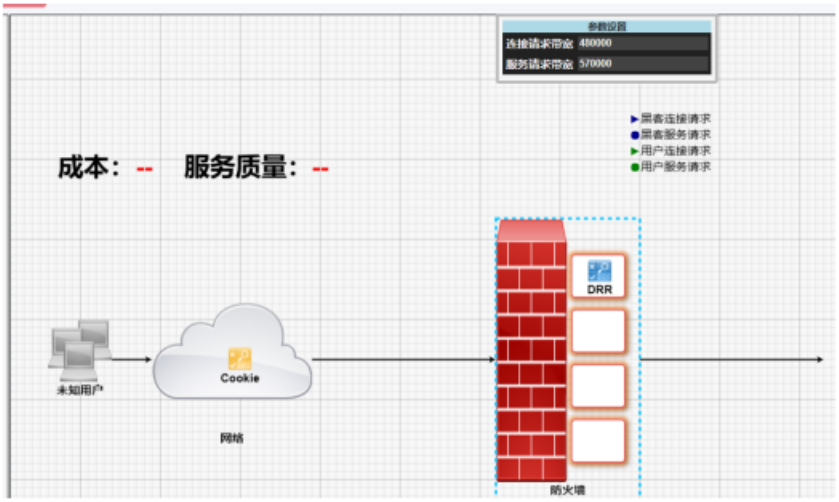
因此调整参数适当增加服务请求带宽，将连接请求带宽从 500000 降低到 400000；服务请求带宽增加到 600000.



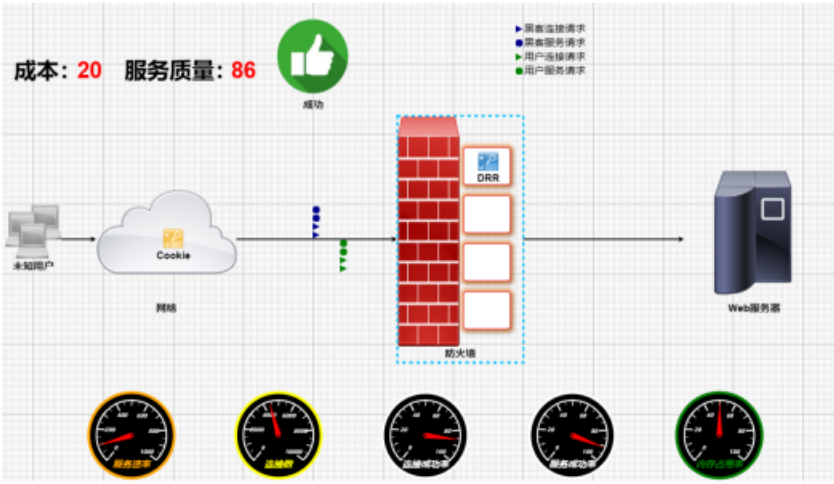
实际效果为成本为 15，服务质量为 78，服务质量仍未达到要求。



可以看到连接成功率下降较多，因此调整增加连接请求带宽到 480000，降低服务请求带宽为 570000.



防御成功：成本为 20，服务质量为 86.



实验 6：连接成功率建模

由于一次连接成功率为 p，则一次不成功的概率为 $1-p$，三次均不成功的概率为 $(1-p)(1-p)(1-p)$，则用户连接成功的概率为 $1-(1-p)(1-p)(1-p)$.

实验 7：服务速率建模

每秒的用户数为 a，每个用户请求的数据量为 w，则总的请求数据量为 aw，而服务速率为 v，则当前接受服务的用户数约为 aw/v.

肉机获得带宽的概率为 q，肉机数为 z，则实际的肉机数为 zq，加上用户数得到总的服务对象个数 $zq+x$，则服务速率则为 $s/(zq+x)$.

将取得的结果带入 v 得到最终服务建模：

实验 8：攻防博弈

从黑客方，用户加带宽和不加带宽的情况下，期望收益均一致的情况下，黑客攻击的概率为 0.2；从用户方，同理，用户加带宽的概率 0.4. 但实际情况下，运行多次，发现黑客攻击的概率基本在 80%，加带宽概率为 0.4-0.6 之间可以成功。

五、实验过程中遇到的问题及解决情况

问题 1 对连接请求带宽和服务请求带宽的实际含义未能充分理解

通过观察下方的服务速率、服务成功率、连接数和连接成功率和内存使用率等数据仪表盘，对连接请求带宽和服务请求带宽进行动态调整。

问题 2 进行防御实验时，无论如何调整两个带宽类型，均无法达到对应要求

刚开始没有注意到可以额外添加元器件，通过查询相关资料，对 Cookie 和 DRR 模块有了初步了解，添加到对应位置之后，并进一步调整参数才得以完成实验。

问题 3 进行博弈实验时，发现理论计算出的攻击概率和实际的攻击概率相差较大，难以计算出加带宽的概率区间

最好的方法将加带宽的概率从 0-1 按步长为 0.1 进行尝试，发现加带宽的概率在 0.4-0.6 之间均可能达到满足实验要求的收益，最高收益可达 80.

六、实验结果及分析和（或）源程序调试过程

完成以上实验之后，提交实验得到结果，均达到了实验要求。

1. IP 地址攻击

对于虚拟 IP 地址攻击，在防火墙处理连接请求的带宽为每秒 500,000 个数据包的情况下，只要 IP 攻击台数×攻击速率达到 50000，均可将服务质量降低为 0，但成本为上限 50，由此可推测适当降低两者之积仍可将服务质量降低到 40 以下，并同时减少成本。

对于真实 IP 地址攻击，在本实验中攻击台数×攻击速率 = 40000，成本达到上限。同样可以减少两者的乘积。经实验，当攻击台数为 100，攻击速率为 100 时，仍可达到要求。

2. 防御实验

用户访问网站时，浏览器与 Web 服务器之间的通信采用 HTTP 协议。整个过程分为两个阶段：首先，浏览器与 Web 服务器建立 TCP 连接。然后，浏览器发送 HTTP 请求，服务器返回 HTTP 响应。

初级防御攻击针对第一阶段，因此需要尽可能减少重复连接次数。在 web 浏览器处引入 Cookie 机制，可以在用户本地进行缓存，减少服务器的内存消耗，防止攻击 IP 不必要的重复连接，大大提高重复连接成功率，保持相对较好的服务质量。

中级防御攻击针对第二阶段，设置的 Cookie 能保证连接成功率，但无法控制服务请求成功率。引入 DRR，因为 DRR 可以实现每个 IP 请求的均匀处理。同时增大服务请求带宽，降低连接请求带宽，可以保持良好的服务质量。不能过多增大连接请求数量，否则会加大成本使用。

综合防御攻击针对两个阶段。因此首先使用 Cookie 作用于第一阶段，使用 DRR 作用域第二阶段，但此时服务质量只有 48。但观察到服务请求率几乎为 0，因此适当增加服务请求带宽，降低连接请求带宽，因为此时成本已达 15，不能同时增大。

3. 博弈实验

攻防博弈实验，由于攻击者的实际攻击概率分布未知，通过理论计算出来仅为 0.2 与实际情况有较大的不符。通过多次实验，发现攻击概率在 0.8 左右，而当加带宽的概率为 0.6 时，实际收益相对较高。

通过本次实验，较好地理解了网络中的攻防流程和具体操作措施，加深了对基本网络服务过程和性能参数有了进一步的理解。