**DDOS (Distributed denial of Service)**

1. 阳谋, 通过大量的访问挤占对方服务器带宽, 从而影响正常业务访问.

2. BotNets: 通过僵尸网络发起攻击, 一般多个设备可能被感染木马或者病毒.

3. ICMP flood (为了不暴露ip地址, 都会伪造), UDP flood, TCP flood(占满TCP链接表): SYN flood (一般都会伪造IP), 因为TCP有3次链接机制, 无法伪造IP (伪造IP地址不会收到回复), 但是可以利用重传机制, 对方会多次尝试发送回复SYN+ACK直到超时, 相当于请求一次, 对方回复10次 (攻击网络带宽)

4. 针对TCP还有RST flood. 4次挥手断开连接, 为了防止异常可以通过RST数据强制切断连接, 类似盲打, 从而使攻击目标断开与服务器的连接 (间接的拔网线)

5. IP, TCP, UDP 都是针对网络资源进行攻击. 还有针对服务器内部资源攻击(消耗目标的计算和I/O): HTTP flood, 针对服务器数据库I/O, 虽然HTTP访问无法伪造IP (HTTP 基于TCP), 但可以借助网络代理主机得到不同的真实IP发起攻击.

Chart

Description automatically generated

6. 反射攻击 (借刀杀人): 发起地址为攻击目标IP, 收件地址为互联网上的第三方机器(反射器), 发起请求后回复数据就会涌入攻击目标IP地址. \*放大器, 比如DNS服务器, 多采用UDP, 60字节的请求会有3000字节的返回, 将放大后的请求流量引到攻击目标IP (DNS劫持)

防御策略：

1. 治理伪造IP: 让路由设备 (nat 协议) 检测出不属于本网段的数据并且过滤掉. 或者使用分布式过滤, 真实的IP链路不可能作假, 比如C->B, 却经过了A的路由, 此时则很有可能涉及IP伪造.

2. 流量平衡: CDN节点 (静态资源作为缓存分发给各个CDN节点) 分担流量, 用户请求时从最近的CDN节点返回.

3. 流量清洗: 建立流量清洗设备, 比如TCP flood, 如果应答SYN+ACK没有回复并且超时, 则断开连接. 如果是正常请求, 则转发到后方服务器.

4. 根据历史经验建立白名单和黑名单. 或者识别程序发送的请求和正常人类用户的请求.