DDOS

1.普通拒绝服务攻击

普通拒绝服务攻击是指一些传统的攻击方式，如：SYN FLOOD攻击、ACK FLOOD攻击、CC攻击、UDP  FLOOD攻击 等等，

(1)SYN FLOOD攻击

Syn flood攻击是利用TCP协议的一些特性发动的，通过发送大量 伪造的带有syn标志位的TCP报文 使 目标服务器连接耗尽，达到拒绝服务的目的。

syn flood攻击就是在三次握手机制的基础上实现的。攻击者通过伪造IP 报文，在IP报文的原地址字段随机填入伪造的IP地址，目的地址填入 要攻击的服务器IP地址，其他TTL、ID 以及TCP中的Source Port等随机填入合理数据，TCP的目的端口填入目的服务器开放的 端口 如：80、8080等，syn标志位置 1。然后通过不停的循环讲伪造好的数据包发送 到目的服务器。

(2)ACK FLOOD攻击

ack flood攻击同样是利用TCP三次握手的缺陷实现的攻击， ack flood攻击利用的是三次握手的第二段，也就是TCP标志位syn和ack都置1，攻击主机伪造海量的虚假ack包发送给目标主机，目标主机每收到一个带有 ack标志位的数据包时，都会去自己的TCP连接表中查看有没有与ack的发送者建立连接 ，如果有则发送三次握手的第三段ack+seq完成三次握手，成功建立TCP连接。如果没有则发送ack+rst 断开连接。但是在这个过程中会消耗一定的CUP计算资源，如果瞬间 收到海量的syn+ack数据包将会 消耗大量的cpu资源使得正常的连接无法建立或者增加延迟，甚至造成服务器瘫痪、死机。

(3)CC攻击

CC攻击全称Challenge Collapsar，中文意思是挑战黑洞，因为以前的抗DDOS攻击的 安全设备叫黑洞，顾名思义挑战黑洞就是说黑洞 拿这种攻击没办法，新一代的抗DDOS设备已经改名为ADS(  Anti-DDoS System),基本上已经可以完美的抵御CC攻击了 。

CC攻击的原理是通过代理服务器或者大量“肉鸡”模拟多个用户访问目标网站的动态页面，制造大量的后台数据库查询动作，消耗目标CPU资源，造成拒绝服务。

我们都知道网站的页面有静态和动态之分，动态网页是需要与后台数据库进行交互的，比如一些论坛， 用户登录的时候需要去数据库查询你的等级、权限 等等，当你留言的时候又需要查询权限、同步数据等等，这就消耗很多 cpu资源，造成静态网页能打开，但是需要和数据库交互的动态网页打开慢或者无法打开的现象。

这种攻击方式相对于前两种实现要相对复杂一些，但是防御起来要简单的多，提供服务的企业只要尽量少用动态网页并且让一些操作提供验证码就能很好的抵御一般的 CC攻击。

(4)UDP FLOOD攻击

UDP FLOOD攻击顾名思义是利用UDP协议进行攻击的，UDP FLOOD攻击可以是小数据包冲击设备也可以是大数据包 阻塞链路占尽带宽。不过两种方式的实现很相似，差别就在UDP的数据部分带有多少数据。相比TCP协议的攻击UDP的攻击更直接更好理解，有一定规模之后更难防御，因为UDP攻击的特点就是打出很高的流量，一个中小型的网站出口带宽可能不足1 G，如果遇到10G左右的UDP FLOOD攻击，单凭企业自身是无论如何也防御不住的，必须需要运营商帮你在上游清洗 流量才行，如果遇到100G的流量可能地方的运营商都 没有能力清洗了，需要把流量分散到全国清洗。UDP FLOOD攻击就像是一块大石头，看着普普通通的好像跟现代机枪 炸弹不是一个等级的武器，但是如果石头足够大 ，就不一样了。想想恐龙是怎么灭绝的， 陨石不也是块普通的石头吗！在DDOS 防御领域有一句话：能防住的都是简单的攻击，但简单的攻击不一定防得住。UDP FLOOD正是这种简单有效的攻击方式。

2.反射型DDOS

 反射放大攻击的原理

很多协议的请求包要远小于回复包，以一个字节的数据换十个字节的数据回来，这就是一种放大，但是你这单纯的放大攻击的是自己啊，所以说想要攻击别人就要在发送请求包时把源地址写成要攻击的人的地址，这样回复的大字节报文就去你要攻击的人那里了，目前来说流量型反射DDOS攻击都是以UDP为载体的



这里放大主要利用的是NTP的monlist（listpeers也行）、DNS的AXFR（ANY也行）、SNMP的getbulkrequest

(1)Monlist(NTP中NTPD中的monlist(ntp\_request.c)功能存在安全漏洞，允许远程攻击者利用漏洞伪造REQ\_MON\_GETLIST或REQ\_MON\_GETLIST\_1请求来放大流量，对目标系统进行拒绝服务攻击。)是返回最近600个与当前NTP服务器通信过的IP地址

(2)AXFR是区域传送（有地方叫域传送），比如freebuf.com下的所有域名返回给请求者

(3)SNMPV2版本中新加的getbulkrequest用于一次请求大量的信息，减少管理站与被管理设备的交互次数

3.新型DDOS攻击 – Websocket和临时透镜

websocket实现DDOS攻击

websocket是HTML5一种新的协议。它实现了浏览器与服务器全双工通信(full-duple)。目前主流的浏览器都能很好地支持websocket，而且用它实现DOS攻击也并不是很难，只要是在js代码中写入相应的代码，当人们打开这个网页是浏览器会自动执行js代码去请求连接要攻击的IP地址，

<!DOCTYPE HTML>

<html>

<head>

<meta charset="utf-8">

<title>websocket test</title>

<script type="text/javascript">

while (2>1){

var ws = new WebSocket("ws://192.168.1.1:80");

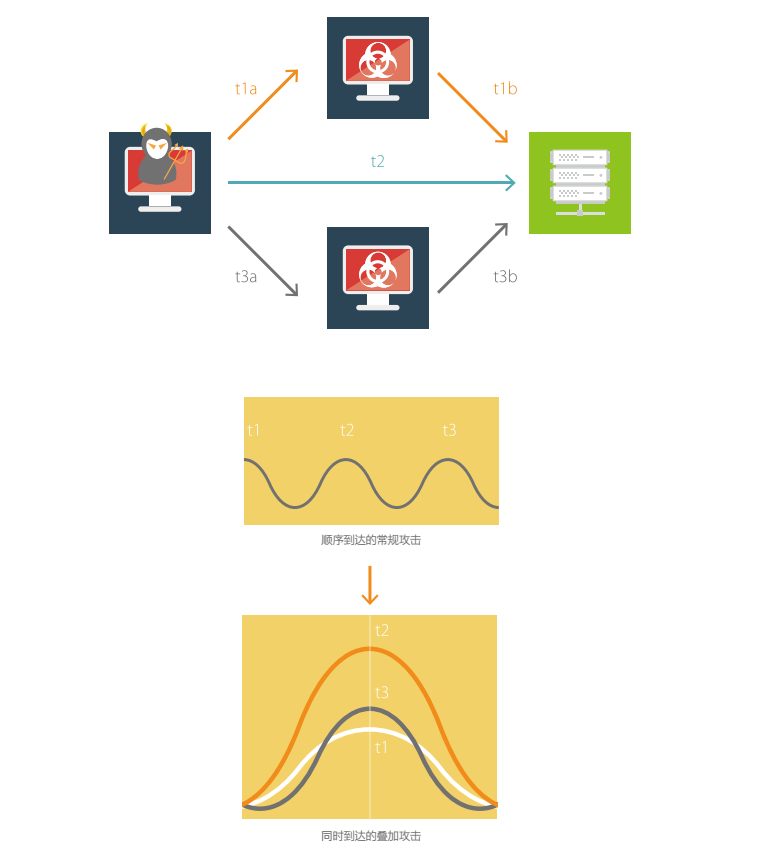
}

 </script>

</html>

意思就是让浏览器不停循环请求192.168.1.1:80

临时透镜攻击



这种攻击是一种典型的延时攻击形式，“ 以时间换数量”，如果攻击者可以控制多个时间段的多个数据包，让他们同时到达目标，这样 就能使流量 瞬间到达一个峰值，对目标造成很大危害。