# 你了解 DDoS 攻击么

最近写的文章都是关于网络安全的内容，同样今天也是网络安全的内容，今天的主题是——DDoS 攻击

# 什么是 DDoS 攻击？

在介绍 DDoS 之前，需要先简单介绍一下什么是 DoS。

**DoS（拒绝服务，Denial of Service）就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应。**这是早期非常基本的网络攻击方式。

举一个简单的例子:

小王开了一家商店，店面不大，加上小王一共有三个服务员。由于他们这里物美价廉，工作人员的态度又比较友善，所以慢慢的生意越来越好。

但是，这家店所在的小镇上有一个恶霸，恶霸看到小王的店很赚钱，想要通过一些下作的手段谋取私利。于是他装扮成普通的顾客，在小王的店里有一搭无一搭的总和店员攀谈，问问这个多少钱，问问那个怎么卖，还时不时的给店员提供一些虚假信息，比如哪里缺货了之类的信息。使店员们都被他搞的团团转。

由于恶霸是装作普通顾客的，小王和店员们又不能彻底不理他，所以就要分出一些精力来服务他，但是由于店内的服务员有限。这样一来，很多其他的顾客就可能受到了冷落。

对于网站来说，其实也是一样的，网站就像是小王的商店一样。对于一个网站来说，他是要搭建在服务器上面的，而由于硬件资源有限，所以服务能力也是有限的（**三个服务员，相当于三个服务器资源**）。如果有人频繁访问或者长时间占用资源，就会导致其他用户的体验有所下降（**服务器资源被占用，导致无法为其他请求服务**）。

这种，利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应的行为，就是 DoS 攻击。

在信息安全的三要素——**保密性**、**完整性**和**可用性**

**机密性**：要求保护数据内容不被泄漏，加密是实现机密性要求的常用手段。

**完整性**：要求保护的数据内容是完整的、没有被篡改的。常见的保证一致性的技术手段是数字签名。

**可用性**：要求保护的资源是“随需而得”。

DoS 针对的目标正是**可用性**。该攻击方式利用目标系统网络服务功能缺陷或者直接消耗其系统资源，使得该目标系统无法提供正常的服务。

那什么是 DDoS 攻击呢？

**分布式拒绝服务(DDoS：Distributed Denial of Service)攻击，是指攻击者利用大量“肉鸡”对攻击目标发动大量的正常或非正常请求、耗尽目标主机资源或网络资源，从而使被攻击的主机不能为正常用户提供服务。**

如果只是一个恶霸的话，只要能够识别出来，然后阻止他进入店铺就行了。

随着恶霸被发现之后，他也想了一个办法，这次他不再自己一个人跑去店里捣乱了，而是纠集了一群无赖，而这些无赖每天都换，店铺里面的服务员根本识别不出来到底谁是恶霸派来的。

无赖们扮作普通客户一直拥挤在商场，赖着不走，真正的购物者却无法进入；或者总是和营业员有一搭没一搭的东扯西扯，让工作人员不能正常服务客户；也可以为商铺的经营者提供虚假信息，商铺的上上下下忙成一团之后却发现都是一场空，最终跑了真正的大客户，损失惨重。**一个无赖去胡闹，就是 DoS 攻击，而一群无赖去胡闹（分布式），就是 DDoS 攻击。**



# DDoS 攻击类型

DDOS 攻击主要分为三类：**流量型攻击；连接型攻击；特殊协议缺陷。**

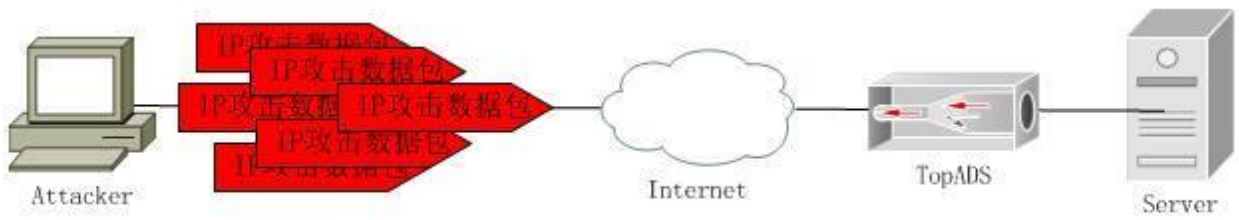
它们都是透过大量合法或伪造的请求占用大量网络以及器材资源，以达到瘫痪网络以及系统的目的。

以下介绍一些常见 DDoS 攻击：

1、 Ip Flood

攻击原理：此攻击以多个随机的源主机地址向目的主机发送超大量的随机或特定的 IP 包，造成目标主机不能处理其他正常的 IP 报文。

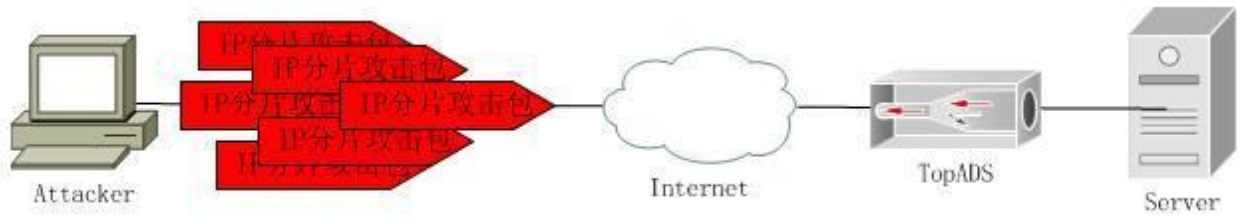
原理图：




2、 Ip Frag Flood

攻击原理：攻击者构造的分片报文，但是不向接收方发送最后一个分片报文，导致接收方要为所有的分片报文分配内存空间，可由于最后一个分片报文永远不会达到，接收方的内存得不到及时的释放，当攻击者这种攻击的分片报文发送的足够多、足够快，很容易占满接收方内存，让接收方无内存资源处理正常的业务，从而达到攻击效果。

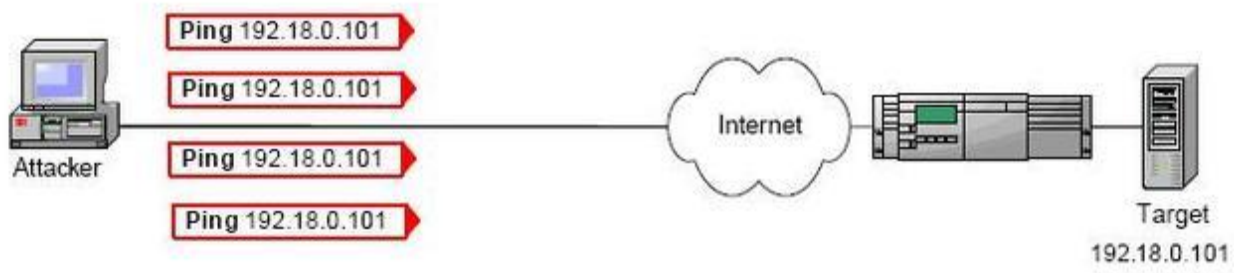
原理图：



3、 Icmp Flood

攻击原理：icmpflood 也就是 ping flood，此攻击在短时间内向目的主机发送大量的 ping 的 echo 报文，主机不断响应，造成网络堵塞、主机资源耗尽。

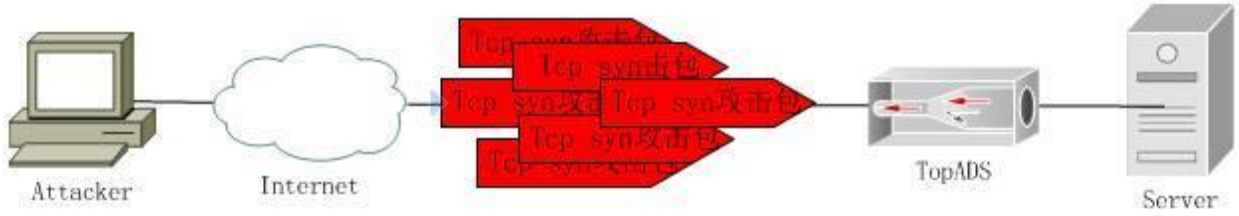
原理图：




4、 Syn Flood

攻击原理：依据 tcp 建立连接的三次握手。此攻击以多个随机的源主机地址向目的主机发送 syn 包，而在收到目的主机的 syn＋ack 包后并不回应，目的主机就为这些源主机建立大量的连接队列，由于没有收到 ack 一直维护这些连接队列，造成资源的大量消耗而不能向正常的请求提供服务。与之类似的攻击方式还有 ackflood、s-ackflood、finflood、rstflood、tcpflood 。

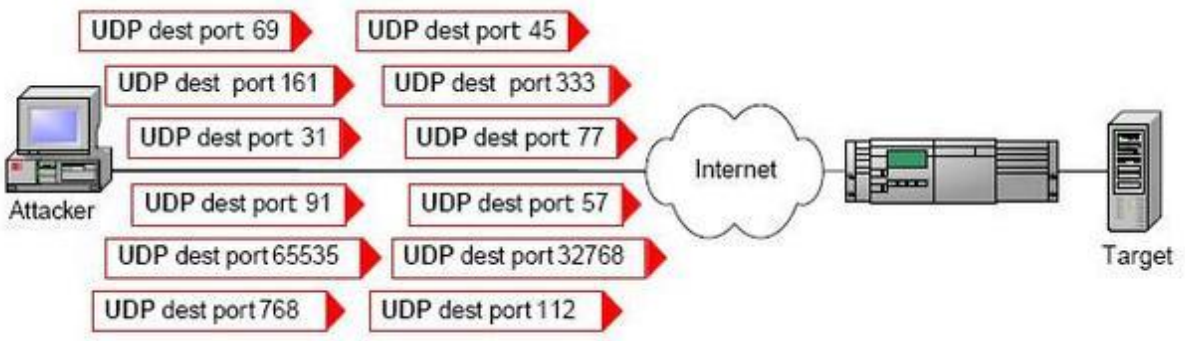
原理图：




5、 Udp Flood

攻击原理：此攻击在短时间那模拟随机的源端口地址向随机的目的端口发送大量的 udp 包，造成目标主机不能处理其他 udp 的请求。

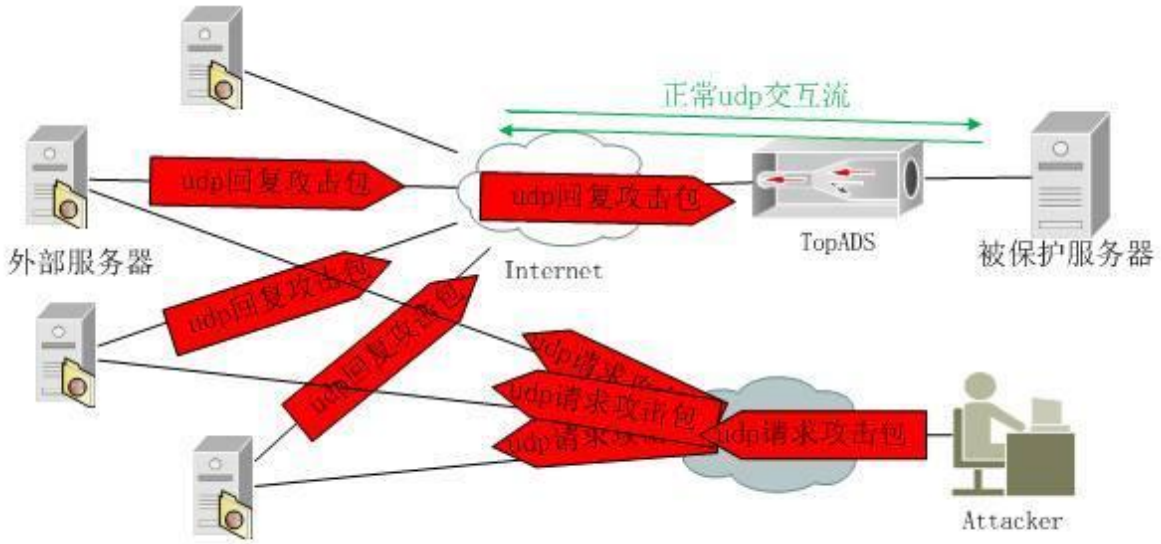
原理图：




6、 Udp 反射 Flood

攻击原理：有时被保护服务器也有同外部服务器进行 udp 交互的需求，攻击者就会利用此交互对被保护服务器进行 udp 反射放大攻击。此攻击在短时间那冒充被攻击地址向外部公用的服务器发送大量的 udp 请求包，外部服务器收到虚假的 udp 请求就会回复大量的回应包给被攻击服务器地址，造成目标主机被保护服务器不能处理其他正常的交互流。

原理图:




# DDoS 的危害

当服务器被 DDos 攻击时，一般会出现以下现象：

- 被攻击主机上有大量等待的 TCP 连接；
- 网络中充斥着大量的无用的数据包；
- 受害主机无法正常和外界通讯；
- 受害主机无法处理所有正常请求；严重时会造成系统死机。
- 对于用户来说，在常见的现象就是网站无法访问。


# DDoS 的防范

为了对抗 DDoS 攻击，你需要对攻击时发生了什么有一个清楚的理解。简单来讲，DDoS 攻击可以通过利用服务器上的漏洞，或者消耗服务器上的资源(例如 内存、硬盘等等)来达到目的。

一般来说，可以用以下办法防范：

1、如果可以识别出攻击源，如机器 IP 等，可以在防火墙服务器上放置一份 ACL（访问控制列表）来阻断这些来自这些 IP 的访问。

2、对于带宽消耗型攻击，最有效的办法那就是增加带宽。

3、提高服务器的服务能力，增加负载均衡，多地部署等。

4、优化资源使用提高 web server 的负载能力。例如，使用 apache 可以安装 apachebooster 插件，该插件与 varnish 和 nginx 集成，可以应对突增的流量和内存占用。

5、使用高可扩展性的 DNS 设备来保护针对 DNS 的 DDOS 攻击。可以考虑购买 Cloudfair 的商业解决方案，它可以提供针对 DNS 或 TCP/IP3 到 7 层的 DDOS 攻击保护。

6、启用路由器或防火墙的反 IP 欺骗功能。

7、付费，使用第三方的服务来保护你的网站。

8、监控网络和 web 的流量。时刻观察流量变化

9、保护好 DNS 避免 DNS 放大攻击。

**对于网络攻击，没有任何办法彻底阻止和避免 ，只能尽最大努力不断提高黑客攻击成本。**