DDOS攻击

## 简介

DoS攻击、DDoS攻击和DRDoS攻击相信大家已经早有耳闻了吧!DoS是Denial of Service的简写，就是拒绝服务，而DDoS就是Distributed Denial of Service的简写，就是分布式拒绝服务，而DRDoS就是Distributed Reflection Denial of Service的简写，这是分布反射式拒绝服务的意思。

不过这3种攻击方法最厉害的还是DDoS，那个DRDoS攻击虽然是新近出的一种攻击方法，但它只是DDoS攻击的变形，它的唯一不同就是不用占领大量的“肉鸡”。这三种方法都是利用TCP三次握手的漏洞进行攻击的。

SYN攻击是当前网络上最为常见DDos攻击，也是最为经典的拒绝服务攻击，它利用了TCP协议实现上的一个缺陷，通过向网络服务所在端口发送大量的伪造源地址的攻击报文，就可能造成目标服务器中的半开连接队列被占满，从而阻止其它合法用户进行访问。这种攻击早在1996年就被发现，但至今仍然显示出强大的生命力。很多操作系统，甚至防火墙、路由器都无法有效地防御这种攻击，而且由于它可以方便地伪造源地址，追查起来非常困难。它的数据包特征通常是，源发送了大量的SYN包，并且缺少三次握手的最后一步握手ACK回复。

DDoS攻击它的原理说白了就是群殴，用好多的机器对目标机器一起发动DoS攻击，但这不是很多黑客一起参与的，这种攻击只是由一名黑客来操作的。这名黑客不是拥有很多机器，他是通过他的机器在网络上占领很多的"肉鸡"，并且控制这些"肉鸡"来发动DDoS攻击，要不然怎么叫做分布式呢。还是刚才的那个例子，你的机器每秒能发送10个攻击数据包，而被攻击的机器每秒能够接受100的数据包，这样你的攻击肯定不会起作用，而你再用10台或更多的机器来对被攻击目标的机器进行攻击的话，那结果就可想而知了。

DRDoS分布反射式拒绝服务攻击这是DDoS攻击的变形，它与DDoS的不同之处就是DrDoS不需要在攻击之前占领大量的"肉鸡"。它的攻击原理和Smurf攻击原理相近，不过DRDoS是可以在广域网上进行的，而Smurf攻击是在局域网进行的。它的作用原理是基于广播地址与回应请求的。一台计算机向另一台计算机发送一些特殊的数据包如ping请求时，会接到它的回应;如果向本网络的广播地址发送请求包，实际上会到达网络上所有的计算机，这时就会得到所有计算机的回应。这些回应是需要被接收的计算机处理的，每处理一个就要占用一份系统资源，如果同时接到网络上所有计算机的回应，接收方的系统是有可能吃不消的，就象遭到了DDoS攻击一样。不过是没有人笨到自己攻击自己，不过这种方法被黑客加以改进就具有很大的威力了。黑客向广播地址发送请求包，所有的计算机得到请求后，却不会把回应发到黑客那里，而是发到被攻击主机。这是因为黑客冒充了被攻击主机。黑客发送请求包所用的软件是可以伪造源地址的，接到伪造数据包的主机会根据源地址把回应发出去，这当然就是被攻击主机的地址。黑客同时还会把发送请求包的时间间隔减小，这样在短时间能发出大量的请求包，使被攻击主机接到从被欺骗计算机那里传来的洪水般的回应，就像遭到了DDoS攻击导致系统崩溃。骇客借助了网络中所有计算机来攻击受害者，而不需要事先去占领这些被欺骗的主机，这就是Smurf攻击。而DRDoS攻击正是这个原理，黑客同样利用特殊的发包工具，首先把伪造了源地址的SYN连接请求包发送到那些被欺骗的计算机上，根据TCP三次握手的规则，这些计算机会向源IP发出SYN+ACK或RST包来响应这个请求。同Smurf攻击一样，黑客所发送的请求包的源IP地址是被攻击主机的地址，这样受欺骗的主机就都会把回应发到被攻击主机处，造成被攻击主机忙于处理这些回应而瘫痪。

DDoS究竟如何攻击?目前最流行也是最好用的攻击方法就是使用SYN-Flood进行攻击，SYN-Flood也就是SYN洪水攻击。SYN-Flood不会完成TCP三次握手的第三步，也就是不发送确认连接的信息给服务器。这样，服务器无法完成第三次握手，但服务器不会立即放弃，服务器会不停的重试并等待一定的时间后放弃这个未完成的连接，这段时间叫做SYN timeout，这段时间大约30秒-2分钟左右。若是一个用户在连接时出现问题导致服务器的一个线程等待1分钟并不是什么大不了的问题，但是若有人用特殊的软件大量模拟这种情况，那后果就可想而知了。一个服务器若是处理这些大量的半连接信息而消耗大量的系统资源和网络带宽，这样服务器就不会再有空余去处理普通用户的正常请求(因为客户的正常请求比率很小)。这样这个服务器就无法工作了，这种攻击就叫做:SYN-Flood攻击。

## 防御

到目前为止，进行DDoS攻击的防御还是比较困难的。首先，这种攻击的特点是它利用了TCP/IP协议的漏洞，除非你不用TCP/IP，才有可能完全抵御住DDoS攻击。不过这不等于我们就没有办法阻挡DDoS攻击，我们可以尽力来减少DDoS的攻击。下面就是一些防御方法：

1. 确保服务器的系统文件是最新的版本，并及时更新系统补丁；
2. 关闭不必要的服务；
3. 限制同时打开的SYN半连接数目；
4. 缩短SYN半连接的time out 时间；
5. 正确设置防火墙；

* 禁止对主机的非开放服务的访问；
* 限制特定IP地址的访问；
* 启用防火墙的防DDoS的属性；
* 严格限制对外开放的服务器的向外访问；
* 运行端口映射程序祸端口扫描程序，要认真检查特权端口和非特权端口。

1. 认真检查网络设备和主机/服务器系统的日志。只要日志出现漏洞或是时间变更，那这台机器就可能遭到了攻击。
2. 限制在防火墙外与网络文件共享。这样会给黑客截取系统文件的机会，主机的信息暴露给黑客，无疑是给了对方入侵的机会。
3. 路由器，以Cisco路由器为例

* Cisco Express Forwarding(CEF)
* 使用 unicast reverse-path
* 访问控制列表(ACL)过滤
* 设置SYN数据包流量速率
* 升级版本过低的ISO
* 为路由器建立log server

能够了解DDoS攻击的原理，对我们防御的措施在加以改进，我们就可以挡住一部分的DDoS攻击。

## ACK Flood攻击

ACK Flood攻击是在TCP连接建立之后，所有的数据传输TCP报文都是带有ACK标志位的，主机在接收到一个带有ACK标志位的数据包的时候，需要检查该数据包所表示的连接四元组是否存在，如果存在则检查该数据包所表示的状态是否合法，然后再向应用层传递该数据包。如果在检查中发现该数据包不合法，例如该数据包所指向的目的端口在本机并未开放，则主机操作系统协议栈会回应RST包告诉对方此端口不存在。

## UDP Flood攻击

## UDP Flood是日渐猖厥的流量型DoS攻击，原理也很简单。常见的情况是利用大量UDP小包冲击DNS服务器或Radius认证服务器、流媒体视频服务器。 100k pps的UDP Flood经常将线路上的骨干设备例如防火墙打瘫，造成整个网段的瘫痪。由于UDP协议是一种无连接的服务，在UDP FLOOD攻击中，攻击者可发送大量伪造源IP地址的小UDP包。但是，由于UDP协议是无连接性的，所以只要开了一个UDP的端口提供相关服务的话，那么就可针对相关的服务进行攻击。

## ICMP Flood攻击

## ICMP Flood 的攻击原理和ACK Flood原理类似，属于流量型的攻击方式，也是利用大的流量给服务器带来较大的负载，影响服务器的正常服务。由于目前很多防火墙直接过滤ICMP报文，因此ICMP Flood出现的频度较低。

## Connection Flood攻击

## Connection Flood是典型的并且非常有效的利用小流量冲击大带宽网络服务的攻击方式,，这种攻击方式目前已经越来越猖獗。这种攻击的原理是利用真实的IP地址向服务器发起大量的连接，并且建立连接之后很长时间不释放，占用服务器的资源，造成服务器服务器上残余连接(WAIT状态)过多，效率降低，甚至资源耗尽，无法响应其他客户所发起的连接。

## 其中一种攻击方法是每秒钟向服务器发起大量的连接请求，这类似于固定源IP的SYN Flood攻击，不同的是采用了真实的源IP地址。通常这可以在防火墙上限制每个源IP地址每秒钟的连接数来达到防护目的。但现在已有工具采用慢速连接的方式，也即几秒钟才和服务器建立一个连接，连接建立成功之后并不释放并定时发送垃圾数据包给服务器使连接得以长时间保持。这样一个IP地址就可以和服务器建立成百上千的连接，而服务器可以承受的连接数是有限的，这就达到了拒绝服务的效果。

## HTTP Get攻击

## 用MSSQLServer、MySQLServer、Oracle等数据库的网站系统而设计的，特征是和服务器建立正常的TCP连接，并不断的向脚本程序提交查询、列表等大量耗费数据库资源的调用，典型的以小博大的攻击方法。一般来说，提交一个GET或POST指令对客户端的耗费和带宽的占用是几乎可以忽略的，而服务器为处理此请求却可能要从上万条记录中去查出某个记录，这种处理过程对资源的耗费是很大的，常见的数据库服务器很少能支持数百个查询指令同时执行，而这对于客户端来说却是轻而易举的，因此攻击者只需通过Proxy代理向主机服务器大量递交查询指令，只需数分钟就会把服务器资源消耗掉而导致拒绝服务，常见的现象就是网站慢如蜗牛、ASP程序失效、PHP连接数据库失败、数据库主程序占用CPU偏高。这种攻击的特点是可以完全绕过普通的防火墙防护，轻松找一些Proxy代理就可实施攻击，缺点是对付只有静态页面的网站效果会大打折扣，并且有些Proxy会暴露攻击者的IP地址。

## UDP DNS Query Flood攻击

UDP DNS Query Flood攻击采用的方法是向被攻击的服务器发送大量的域名解析请求，通常请求解析的域名是随机生成或者是网络世界上根本不存在的域名，被攻击的DNS 服务器在接收到域名解析请求的时候首先会在服务器上查找是否有对应的缓存，如果查找不到并且该域名无法直接由服务器解析的时候，DNS 服务器会向其上层DNS服务器递归查询域名信息。域名解析的过程给服务器带来了很大的负载，每秒钟域名解析请求超过一定的数量就会造成DNS服务器解析域名超时。

根据微软的统计数据，一台DNS服务器所能承受的动态域名查询的上限是每秒钟9000个请求。而我们知道，在一台P3的PC机上可以轻易地构造出每秒钟几万个域名解析请求，足以使一台硬件配置极高的DNS服务器瘫痪，由此可见DNS 服务器的脆弱性。同时需要注意的是，蠕虫扩散也会带来大量的域名解析请求。

## 附录

<http://netsecurity.51cto.com/art/201710/553893.htm>

<https://www.zhihu.com/question/19581905>

http://blog.51cto.com/12214964/1865432