DDOS原理与防御

mochazz / 2017-09-07 10:22:00 / 浏览数 5347 新手 入门资料 顶(0) 踩(0)

0X00前言

暑假无聊，找了一家公司实习，打算学点东西。这家公司早些年是做抗DDOS设备的，培训的时候就很粗略的讲了部分原理，但是我却对DDOS产生了浓厚的兴趣。一但有了

0X01DDOS简介

DDOS(Distributed Denial of
Service)，又称分布式拒绝服务攻击。骇客通过控制多个肉鸡或服务器组成的僵尸网络，对目标发送大量看似合法请求，从而占用大量网络资源，瘫痪网络，阻止用户对网络

0X02DDOS危害

出口带宽堵死
游戏掉线导致客户流失
服务器连接数多，连接资源被耗尽
服务器卡、慢、死机、无法连接

0X03攻击来源

高性能服务器配合发包软件
可联网的设备(如打印机、摄像头、电视等等)
移动设备(数量多，增长速度快，其高性能利于组建僵尸网络)
个人PC(存在漏洞的PC或一些黑客迷自愿成为DDOS一员)
骇客控制的僵尸网络(僵尸网络又分为IRC型、HTTP型、P2P型)

0X04流量特点

IP地址随机或固定某些IP段随机
没有完整完成三次握手
地址多数是伪造的
请求数量大、快

0X05导致DDOS原因

人类因素

金钱利益
政治冲突
宗教冲突
为求出名

非人类因素

带宽上限
协议缺陷
设备性能上限
应用性能上限
系统性能上限

0X06攻击类型及防御

Smurf攻击
攻击者向网关发送ICMP请求包，并将该ICMP请求报文的源地址伪造成受害主机IP地址，目的地址为广播地址。路由器在接受到该数据包，发现目的地址是广播地址，就会将

防护方案：禁止路由器广播ICMP请求包；禁止操作系统对广播发出的ICMP请求包做出响应；配置防火墙静止来自你所处网络外部的ping包

TearDrop攻击

在了解这种攻击之前，需要先知道什么是IP
fragmentation（数据包分片）。数据在网络中传输必定会产生数据包被分片，因为每种网络都有不同的最大单个数据包的大小，也就是常说的MTU（Maximum
Transmission
Unit，最大传输单元）。当要传输的数据超过你要通信的那台主机所处网络的MTU时，数据包就会被分片进行传输，然后在到达目的地再重新组装成原来的数据包，下面是

TearDrop攻击，就是通过设置错误的片偏移，使得数据包到达目的地时，服务器无法重新组合数据包，因为数据包的组合是通过片偏移来组装的，最终导致崩溃。对比一下

这种攻击主要对旧的windows版本和Linux版本有效，防护的话，可以检测发来的数据包片偏移是否合法，如果合法在组装，不合法直接丢弃。例如这个：分片重组检查算法

Land Attack

攻击者发动Land
Attack攻击时，需要先发出一个SYN数据包，并将数据包的源IP与目的IP都设置成要攻击的目标IP，这样目标在接收到SYN数据包后，会根据源IP回应一个SYN+ACK数据包

防御方案参考如下：这种攻击对早期系统有效。通过设置防火墙和路由规则，检测源IP与目的IP相同的数据包，丢弃、过滤这种数据包。

SYN FLOOD攻击

SYN
FLOOD攻击是在TCP三次握手过程中产生的。攻击者通过发送大量伪造的带有SYN标志位的TCP报文，与目标主机建立了很多虚假的半开连接，在服务器返回SYN+ACK数据
FLOOD攻击图示如下

防御：
SYNCheck：使用防护设备，3次握手变成了6次握手，由防护设备检测SYN请求是否合法，通过后再由防护设备将报文转发给服务器，后续报文仍由防护设备代理。
Micro blocks：管理员可以在内存中为每个SYN请求创建一个小索引(小于16字节)，而不必把整个连接对象存入内存。
RST
cookies：在客户端发起第一个SYN请求后，服务器故意回应一个错误的SYN+ACK报文。如果合法用户收到这个报文，就会给服务器响应RST报文。当服务器收到这个报文
STACK
tweaking：管理员可以调整TCP堆栈以减缓SYN泛洪攻击的影响。这包括减小超时时间，等到堆栈存释内放时再分配连接，否则就随机性地删除传入的连接。

ACK FLOOD攻击

ACK FLOOD攻击是利用TCP三次握手过程。这里可以分为两种。

第一种：攻击者伪造大量的SYN+ACK包发送给目标主机，目标主机每收到一个SYN+ACK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ACK包完成TCP连接，如果没有则发送ACK+RST
断开连接。但是在查询过程中会消耗一定的CUP计算资源。如果瞬间收到大量的SYN+ACK数据包，将会消耗服务器的大量cpu资源，导致正常的连接无法建立或增加延迟，

第二种：利用TCP三次握手的ACK+SYN应答，攻击者向不同的服务器发送大量的SYN请求，这些SYN请求数据包的源IP均为受害主机IP，这样就会有大量的SYN+ACK应答

通常DDOS攻击会将ACK flood与SYN
flood结合在一起，从而扩大威力。防御方案可参考如下：采用CDN进行流量稀释；避免服务器IP暴露在公网上；通过限速或动态指纹的方式；利用对称性判断来分析出是否

UDP FLOOD攻击

UDP（User Datagram
Protocol，用户数据报协议），是一种无连接和无状态的网络协议，UDP不需要像TCP那样进行三次握手，运行开销低，不需要确认数据包是否成功到达目的地。这就造成U
FLOOD可以使用小数据包(64字节)进行攻击,也可以使用大数据包(大于1500字节,以太网MTU为1500字节)进行攻击。大量小数据包会增大网络设备处理数据包的压力；而对

防御方案：限制每秒钟接受到的流量(可能产生误判)；通过动态指纹学习(需要攻击发生一定时间)，将非法用户加入黑名单。

NTP放大攻击

NTP(Network Time
Protocol，网络时间协议)，是用来使计算机网络时间同步化的一种协议，它可以使计算机与时钟源进行同步化并提供高精度的时间校正，使用UDP123端口进行通信。通常

总结一下这种攻击产生的原因，请求与响应数据包不等价；UDP协议的通信模糊性（无数据传输确认机制）；以及NTP服务器的无认证机制。再来谈谈防御方案：使用防
DDoS 设备进行清洗；加固并升级NTP服务器；在网络出口封禁 UDP 123 端口；通过网络层或者借助运营商实施 ACL 来防御；关闭现在 NTP 服务的 monlist
功能，在ntp.conf配置文件中增加`disable monitor`选项。

DNS放大攻击

DNS(Domain Name
System，域名系统)，由于使用IP地址来记忆各个网站比较困难，所以就产生了使用主机名称来表示对应的服务器，主机名称通过域名解析的过程转换成IP地址。下面来看一

报文首部格式

报文首部各字段含义如下，其中绿色高亮是攻击点之一，之后会分析

下面是问题记录中查询类型可设置的值，我们发现最后一个ANY类型会请求所有记录，这也是一个攻击点

DNS查询可分为递归查询和迭代查询，下面是DNS迭代查询图

再来看DNS递归查询图

从DNS数据包结构以及DNS递归查询过程，我们就可以大致分析出攻击原理。首先，攻击者向僵尸网络发出指令，使僵尸网络中的每一台主机均发出一个伪造源地址的DNS
2671中定义的DNS拓展机制EDNS0。未使用EDNS0时，若响应包大小小于512字节，就使用UDP封装数据；若响应包大小超过512字节，就使用TCP连接或者服务器截断响
RR字段，这两个字段包含了能够处理的最大UDP报文大小信息，所以攻击者将这个信息设置的很大，服务器就会根据这个信息生成响应报文。最后看一下DNS放大攻击演示

防御的话，可以参考以下几点：联系ISP清洗上游流量；DNS服务器只对可信域内提供服务，限制对域外用户提供DNS解析服务；对单个IP的查询速率做限制；拥有足够的带
Request进行过滤。

SNMP放大攻击

SNMP(Simple Network Management
Protocol，简单网络管理协议)，是目前网络中应用最为广泛的网络管理协议，它提供了一个管理框架来监控和维和互联网设备，它使用UDP161端口进行通信。攻击者向互

攻击者先将源地址改成要攻击的目标IP，再使用默认的通信字符串，向大量SNMP设备发出GetBulk请求，设备收到GetBulk请求数据包后，会将一大段的设备检索信息返回

可以采取以下措施进行防御：禁止已开启SNMP的设备响应GetBulk请求，避免自己的设备被黑客利用；更改默认的通信字符串；修改默认端口161；隐藏开启SNMP设备的

TFTP放大攻击

TFTP（Trivial File Transfer Protocol，简单文件传输协议），使用UDP
69端口进行通信，由于TFTP使用的是不可靠的UDP协议，所以他不能确保发送的任何报文都能真正到达目的地，因此他必须使用定时器来检测并重传报文，以下是TFTP传输

超时重传机制

可以看到，TFTP协议将数据分成好多个数据块进行传输，每个数据块最大为512字节，客户端在接受到数据块时，需要给服务器端返回一个ACK确认报文，然后才会继续传输

防御方案可参考如下：不要将TFTP服务器暴露在公网上；对流经TFTP服务的流量进行入侵检测；将重传（数据包）率设置为1；只为信任域内的主机提供服务。

CC攻击

CC攻击（ChallengeCollapsar）又称作HTTP
泛洪攻击，其原理是攻击者控制肉鸡、僵尸网络或使用代理服务器，不停地向目标的web服务发送大量合法请求，使得正常用户的web请求处理缓慢甚至得不到处理，制造大

防御方案：必要时将网页做成静态，减少数据库的使用；限制连接数量；修改最大超时时间；让用户手动输入验证码；在response报文中添加特殊字段，验证IP合法性；屏

HTTP慢速攻击

Slow HTTP Dos
AttACKs（慢速HTTP拒绝服务攻击），黑客模拟正常用户向web服务器发送慢速http请求，由于是慢速的，服务器端需要保持连接资源，直到数据传输结束或请求结束才可

Slowloris攻击方式
HTTP协议规定请求头以一个空行结束，所以完整的http请求头结尾是\r\n\r\n。然而使用非正常的\r\n来结尾，就会导致服务端认为我们的请求头还没结束，等待我们继续发
Return Line Feed）表示回车换行

Slow post攻击方式
在http头部信息，可以使用content-length声明HTTP消息实体的传输长度，服务器端会content-length的值作为HTTP
BODY的长度。利用这一特点，攻击者把content-length设置得很大的，然后缓慢发送数据部分，比如一次只发送一个字节，这样服务器端就要一直保持连接，直到客户端传

Slow read攻击方式
攻击者发送一个完整的HTTP数据请求，之后服务器会给出响应，这时攻击者在将自己的TCP窗口大小设置的很小，服务器会根据客户的TCP窗口大小来传送数据。由于客户端

Apache range header攻击
这种攻击方式只针对apache，当客户端传输大文件时会有range字段，表示将大文件分段，分成几个小段进行传输。例如攻击者将一个文件按照一个字节一段，分成好多段
上面这4种攻击方式，也可以参考这篇文章：CC攻击。了解了攻击原理，我们就可以有针对性地进行防御，这里说一下apache的防护策略：设置并使用以下模块
mod_reqtimeout模块，控制请求数据传输的超时时间及最小速率，防护配置如下

mod_qos模块，Apache的一个服务质量控制模块，用户可配置各种不同阈值，防护配置如下

mod_security模块，一个开源的WAF模块，有专门针对慢速攻击防护的规则，防护配置如下

以上是针对Apache的一些防护策略，至于其他中间件的防护，可以参考这篇文章：How to Protect Against Slow HTTP AttACKs

XSS-DOS

利用网站存在的存储型XXS漏洞，在网站中插入恶意的javascript代码。代码的功能是不断向web服务器发起大量请求，从而导致服务器宕机，无法响应正常用户的请求。客

由于这种攻击的是由存储型XSS导致的，我们再防御方面就要考虑如何防御存储型XSS。防御策略如下：对用户的输入以及url参数进行特殊字符过滤；对输出内容进行编码转

时间透镜攻击

通过控制相同源和相同目的IP报文，使得走不同路径的数据包，在同一时刻到达目标服务器，从而达到流量集中攻击的目的。这种攻击其实我也还弄不太懂，详细信息可以阅
Lensing and its Application in Pulsing Denial-of-Service
Attacks，或者看看这个视频，还有这份中文分析：时间透镜及其在脉冲拒绝服务攻击的应用。看一下freebuf上的一个分析图

防御方案：增加抖动，干扰攻击路径，使得数据包无法预期到达；由运营商禁止源路由。

其他防御措施：
采用高性能的网络设备；充足的网络带宽保证；升级主机服务器硬件；避免将服务器的真实IP暴露在公网中；使用CDN对流量进行稀释，当大流量稀释到各个CDN节点时，

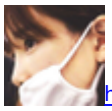
0X07总结

这篇文章是自己对DDOS学习的一个总结，当中参考了不少文章书籍，当然还有很多类型的DDOS文中未提及，需要再深入学习，文中若有原理性错误，还望大家指出修正。
参考：

CC攻击
HTTP FLOOD
UDP FLOOD
SNMP GETBULK
SMURF DDOS ATTACK
DNS Amplification AttACK
NTP Amplification AttACKs Using CVE-2013-5211
SNMP REFLECTION/AMPLIFICATION
How To Mitigate Slow HTTP DoS AttACKs in Apache HTTP Server
How to Protect Against Slow HTTP AttACKs
Temporal Lensing and its Application in Pulsing Denial-of-Service Attacks
《TCP-IP协议族(第4版)》
《破坏之王-DDoS攻击与防范深度剖析》

上一篇：s2-052 有成功复现的吗，论坛... 下一篇：DDOS攻击模拟复现

1. 3 条回复


hades 2017-09-07 10:30:06

内容很完整，够幸苦~~

0 回复Ta


wooyun 2017-09-07 11:27:31

这个内容写的确实好，来个PDF就完美了

0 回复Ta

asdpppp 2017-09-08 02:39:56

感谢分享文章，希望可以写更多关于ddos 的 文章

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板