DDOS攻击模拟复现

mochazz / 2017-09-07 10:31:00 / 浏览数 5255 新手 入门资料 顶(0) 踩(1)

0X00前言

我在上一篇文章中，总结了大多数DDOS攻击的原理和防御。这篇文章，我将分享大部分DDOS攻击的实现以及每个实验环境的搭建步骤。严格来说我做的实验应该叫做DO

0X01SYN FLOOD攻击

环境准备

我们选取metasploitable2作为被攻击服务器，在SYN FLOOD攻击发起之前，可以正常访问服务器上的web服务

模拟攻击

SYN
FLOOD攻击的原理就是阻断TCP三次握手的第三次ACK包，即不对服务器发送的SYN+ACK数据包做出应答。由于服务器没有收到客户端发来的确认响应，就会一直保持连接
Flood攻击。所以我们就可以按照这个思路进行数据包构造，这里我使用python的scapy模块来模拟发包

在发送数据包的同时，我们打开wireshark抓包，可以看到目标服务器成功给我们返回SYN+ACK数据包，但是第三个数据包确实RST数据包而不是ACK数据包，这是怎么回事

接下来我们就可以把刚刚构造数据包的思路加上多线程模块写成一个SYN FLOOD攻击脚本，代码如下

脚本使用方法在第15行，执行我们的syn_flood.py脚本后，发现目标服务器的web应用已经无法访问

打开wireshark抓包，可以看到抓取到大量的SYN请求数据包，而且已经没有RST数据包了

我们再登录服务器(metasploitable2)上，查看服务器所建立的连接。使用命令netstat -pantu | grep
SYN查看已建立的SYN连接数，可发现此时已建立了大量连接

0X02DNS放大攻击复现

数据包构造思路

首先，我们需要观察一下DNS递归查询数据包的报文格式。使用dig命令发送DNS查询报文，并同时开启wireshark抓包分析

通过wireshark可以看到返回的数据包大约是请求数据包的7倍。不同域名，dig命令查询所返回的数据包大小不一样

模拟攻击

接下来，我们使用scapy伪造源地址为被攻击目标IP 向DNS服务器发起递归查询，如果向大量的DNS服务器发起递归查询，则DDOS攻击效果更明显。
d.rd=1　　rd：Recursion desired，当rd=1时表示进行递归查询

使用wireshark抓包查看效果，并验证构造的数据包是否正确

确认数据包构造无误后，就可以开始编写脚本进行DNS放大攻击，代码如下

攻击示例

在受害主机上用wireshark抓取数据包查看效果，可以看到DNS服务器返回了大量的查询响应包

0X03TFTP放大攻击复现

环境准备

选择ubuntu安装TFTP服务，并上传一个文件到TFTP服务器的根目录

客户端与服务器建立连接过程

模拟攻击

在攻击机(kali)上使用scapy构造TFTP数据包，并同时打开wireshark抓包分析构造的数据包是否正确

同时TFTP服务器上也使用wireshark抓包，可以看到TFTP服务器将数据包的第一个分块返回了6次，原因在于受害主机并未对TFTP发出的数据包做出ACK响应，TFTP由于未

受害主机(ubuntu)上使用wireshark抓包，发现接受到UDP协议传来的6个数据包

这里计算一下一个数据包的放大倍数：558*6/62=54，如果在加上多线程模块，配合多个主机发包，放大倍数可想而知。

0X04NTP放大攻击复现

环境准备

我们准备一个BodhiLinux模拟公网上开启了NTP服务的服务器
打开BodhiLinux，安装NTP服务

这里有个小问题，默认apt-get install
ntp会安装ntp-4.2.8p6，然而这个版本无法用于本次实验，因为ntp4.2.7及以上的版本中已经禁止了monlist功能，所以需要安装ntp-4.2.6p5，解决方法换Ubuntu14.04.4默
install ntp即可。
Ubuntu14.04.4默认更新(http://www.cnblogs.com/zlslch/p/6860229.html)
查看UDP123端口是否开放：

编辑/etc/ntp.conf文件，开启NTP服务器monlist查询功能：

重启ntp服务，配置文件才会生效：

模拟攻击

此时开启kali模拟黑客扫描公网上可用的NTP服务器，使用nmap可完成该目的

当黑客确定目标后，会扫描目标的UDP123端口服务，确认其UDP123端口是否为NTP服务

查看对方NTP服务器是否开启monlist查询功能

运行上面命令的同时，开启wireshark抓包，可抓取NTP数据包，用于之后的数据包构造

通过scapy按照NTP数据包格式构造发包

再次在kali(攻击机)上用wireshark抓包，验证构造的NTP数据包是否有误

Ubuntu(受害主机)上也用wireshark抓包，验证是否收到NTP服务器返回的数据包

可以看到，受害主机成功接受从NTP服务器返回的查询报文。这里发送一个NTP数据包，收到也只有一个NTP数据包。理论上应该会收到100个数据包，每6个IP封装在1个数
NTP服务器IP
这条命令可以与NTP服务器进行交互，并且NTP服务器的IP列表中会多一个运行这条命令主机的IP。图忘记截了，大家自己试一下，运行这条命令的同时，打开wireshark抓

可以看到我们成功将192.168.100.101添加至NTP服务器的IP列表里

既然这样，我们就可以写一个脚本，将NTP服务器的IP列表增大到600，脚本如下

脚本运行情况

再次查看NTP服务器的IP列表，已成功增大IP列表长度

去掉开头两行非IP行，刚好是600个IP

下面我们再来试一下发送一个NTP查询包，是否能返回100个数据包(总共600个IP，每6个IP封装在一个数据包中)
攻击机(kali)使用scapy构造数据包，并打开wireshark抓包观察数据包正确性

受害主机(ubuntu)wireshark抓包截图，可以看到刚好收到100个数据包

我们可以计算一下放大倍数：482*100/90=535，哇！瞬间变得有趣多了。

0X05SNMP放大攻击复现

环境准备

在windows2003上安装SNMP服务

先插入iso文件，在点击确定

对安装好的SNMP进行配置

模拟攻击

开启scapy开始构造SNMP GetBulk请求

使用wireshark抓包分析

如果需要返回更多的数据，我们可以修改SNMPbulk函数里的max_repetitions属性的值，至于攻击脚本，按照上面其他类型的放大攻击依葫芦画瓢即可。

0X06XSS-DOS

环境准备

准备一个开启了web服务的主机，这里选择Ubuntu做演示

WebSocket协议是基于TCP的一种新的网络协议。它实现了浏览器与服务器全双工(full-duplex)通信(允许服务器主动发送信息给客户端)。

模拟攻击

这里只是演示攻击，为了方便就不利用存储型XSS插入恶意代码，直接在Ubuntu的/var/www/html/目录下添加XSS-DOS.php，代码如下

然后使用我们的主机访问http://190.168.100.102/XSS-DOS.php。192.168.100.102是Ubuntu的IP，192.168.100.105是我本机的IP，由下图可看到，当我本机访问目标服

大家可以观察到，在我们浏览器访问目标服务器一段时间后，我们的浏览器崩溃了，这是因为我们与目标建立的大量的TCP连接，这对我们自己主机也是非常消耗内存的，所

0X07HTTP慢速攻击

环境准备

在攻击端安装slowhttptest工具用于HTTP慢速攻击：

可以使用-h选项来查看使用说明：

这个工具提供了多种方式攻击，细节如下

Slowloris攻击方式

查看服务端建立的连接数：

此时服务器上的web服务已经完全不能访问了。
抓包验证攻击手法：

结尾添加了一个X-***，这样看我们可能看不出什么，我们将这组数据转换成原始数据看看：

我们看到结尾是0d0a，0d表示\r,0a表示\n，也就是说结尾是\r\n。而正常的请求头结尾应该是\r\n\r\n，如果以\r\n结尾，服务器就会认为客户端的数据还没传输完，就需要

Slow post攻击方式

Slow read攻击方式

我们通过设置TCP接收窗口大小为32(-z
32)来限制每次服务器给我们发送的数据大小。通过抓包分析，我们可以观察到目标服务器每次只给我们返回32字节的数据：

Apache range header攻击

虽然实验没有成功将服务器宕机，但是还是有必要了解这种攻击方式，我们还是来抓包看一下：

可以看到客户端发送的HTTP请求头中添加了range字段，大文件分成好多个小段进行传输，这就会消耗服务器大量CPU和内存资源。

0X08总结

终于把大部分的DDOS攻击实现了，在这过程中，自己本身也查阅了大量的书籍、博文。从原理到实践，当中有些东西还需要继续深入下去，还有很多实验还没实现，对于D

上一篇：DDOS原理与防御 下一篇：ThinkerPHP后台存在远程任...

1. 1 条回复

wooyun 2017-09-07 11:20:07

讲的非常不错，辛苦了

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