链滴

云主机安全——防御 CC/DDos 攻击

作者：yuanhenglizhen

原文链接：https://ld246.com/article/1550823924646

来源网站：链滴

沐风

最近年，服务器上云的业务越来越多，主机安全越来越重要。之前去过一家公司，9台阿里云服务器一大半中啦挖矿木马，以及自己之前用华为云的时候也出现过，不过庆幸的是上线没多久，删除重置。这次主要说下关于CC攻击和DDos攻击防范，就最近黑客派被cc攻击引起的想法。写下这篇文章，以后防范做准备，以及给大家分享下学习和想法。

何为CC/DDos攻击

首先说下Dos攻击「也称为洪水攻击」，其目的在于使目标主机资源耗尽，使服务暂时中断或停止，致其正常用户无法访问。

当 黑客 使用网络上两个或以上被攻陷的计算机作为“ 僵尸 ”向特定的目标发动“拒绝服务”式攻击，称为**分布式拒绝服务攻击**（distributed denial-of-service attack， 缩写 ： **DDoS attack**、**DDoS**。

现象：

1. 网络异常缓慢（打开文件或访问网站）
2. 特定网站无法访问
3. 无法访问任何网站
4. 垃圾邮件的数量急剧增加
5. 无线或有线网络连接异常断开
6. 长时间尝试访问网站或任何互联网服务时被拒绝
7. 主机容易断线、卡顿

以上内容来之wiki--CC/DDos攻击

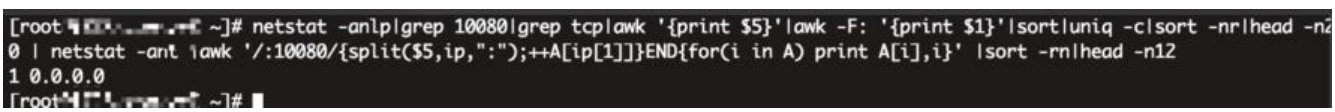
CC攻击全称Challenge Collapsar，中文意思是挑战黑洞，因为以前的抵抗DDoS攻击的安全设备叫洞，顾名思义挑战黑洞就是说黑洞拿这种攻击没办法，新一代的抗DDoS设备已经改名为ADS(Anti-DoS System)，基本上已经可以完美的抵御CC攻击了。CC攻击的原理是通过代理服务器或者大量肉鸡拟多个用户访问目标网站的动态页面，制造大量的后台数据库查询动作，消耗目标CPU资源，造成拒服务。CC不像DDoS可以用硬件防火墙来过滤攻击，CC攻击本身的请求就是正常的请求。

如何防范

查看端口连接，结果为连接数|ip地址，然后可以根据ip查地址所在地，不排除代理访问

```
netstat -anlp|grep 10080|grep tcp|awk '{print $5}'|awk -F: '{print $1}'|sort|uniq -c|sort -nr|head n20 | netstat -ant |awk  '/:10080/{split($5,ip,":");++A[ip[1]]}END{for(i in A) print A[i],i}' |sort -rn head -n200
```

结果如下



封禁可以IP

以下是打的比方

iptables -I INPUT -s 1.1.0.0/16 -j DROP

保存

service iptables save

开源防护

1. net-Shield ▯▯star▯▯star▯▯star▯▯star
▯star

适用于VPS，专用服务器和物联网设备的简单易用的DDoS解决方案 - Beta

2. Anti-DDoS

一个基于iptables的规则防护基本，简单易用

3. cc_iptables

收集处理DDOS，CC攻击各类脚本，包括NGINX日志中的CC攻击IP处理。 http://aqzt.com

4. log2ban

检测和禁止参与DDOS或暴力攻击的IP到Web服务器

5. nginx-ultimate-bad-bot-blocker ▯▯star▯▯star▯▯star
▯star▯▯star

Nginx阻止坏机器人，垃圾邮件推荐人阻止程序，漏洞扫描程序，用户代理，恶意软件，广告软件，索软件，恶意网站，带有反DDOS，Wordpress主题检测器阻止和Fail2Ban监狱重复犯罪者

6. AntiDDOS-system

网页验证码的方式防御