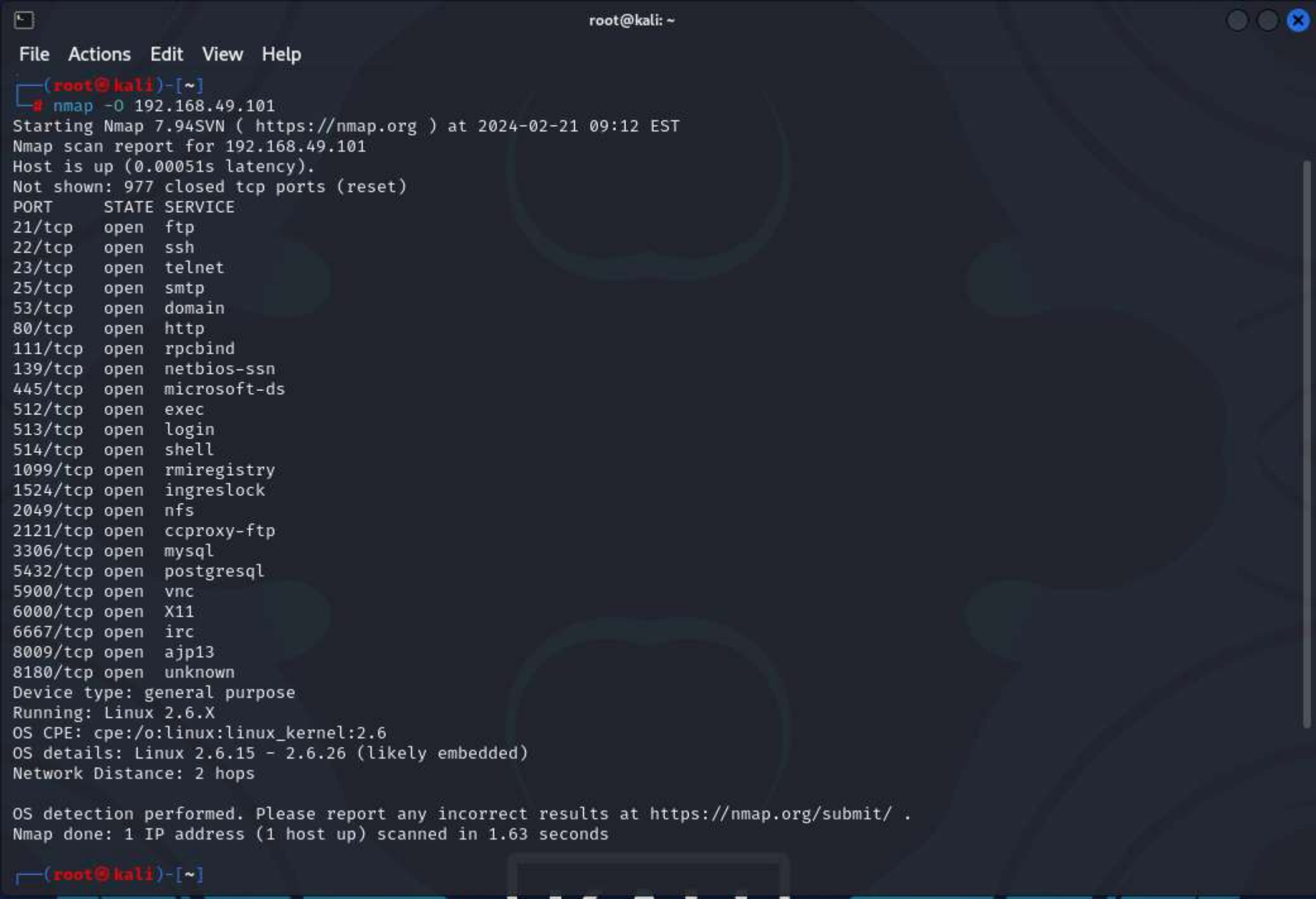
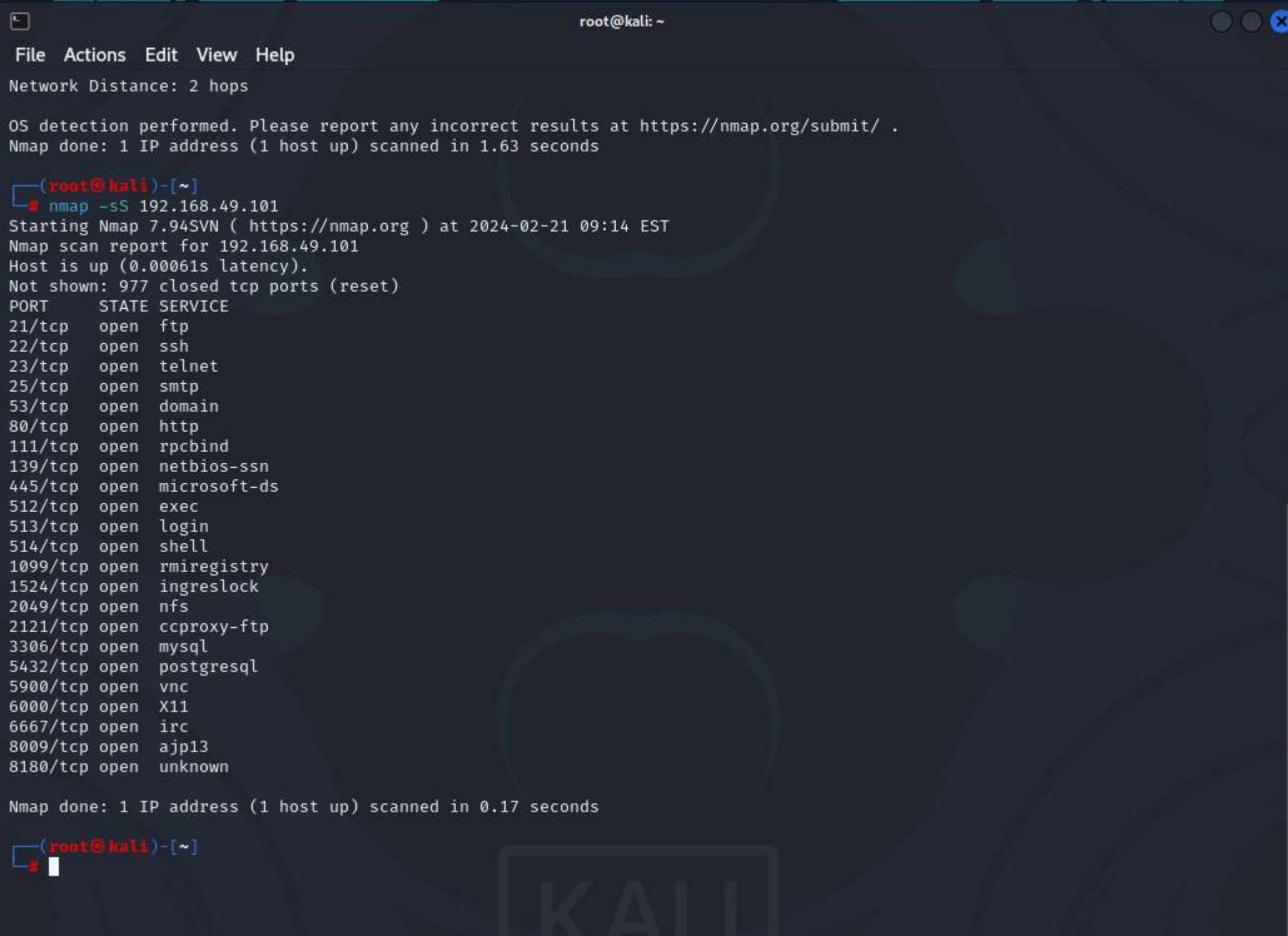
Nell'esercizio di oggi abbiamo eseguito delle scansioni di rete sulle nostre macchine virtuali.Il motivo per cui le eseguiamo sono di individuare le vulnerabilita' e di eseguire in maniera effettiva un penetration testing.
Nel primo caso eseguiamo il comando -O su meta per identificare il sistema operativo dell'indirizzo ip target.
Nel secondo caso eseguiamo il comando -sS per identificare le porte aperte relative al target.
Nel terzo caso il comando -sT esegue una scansione piu' invasiva creando di fatto un collegamento con le porte TCP sul target di riferimento.
Il comando -sV si utilizza per effettuare un check delle versioni dei servizi.
Abbiamo anche eseguito questi comandi sulla mv windows 7 e abbiamo notato che il firewall blocca la richiesta di comunicazione, mentre col firewall giu' esegue la scansione normalmente dandoci tutte le informazioni.


root@kali: ~
File Actions Edit View Help
┌──(root㉿kali)-[~]
└─# nmap -O 192.168.49.101
Starting Nmap 7.94SVN (https://nmap.org) at 2024-02-21 09:12 EST
Nmap scan report for 192.168.49.101
Host is up (0.00051s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.63 seconds
┌──(root㉿kali)-[~]


root@kali: ~
File Actions Edit View Help
Network Distance: 2 hops
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.63 seconds
┌──(root㉿kali)-[~]
└─# nmap -sS 192.168.49.101
Starting Nmap 7.94SVN (https://nmap.org) at 2024-02-21 09:14 EST
Nmap scan report for 192.168.49.101
Host is up (0.00061s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
┌──(root㉿kali)-[~]
└─#

```
┌──(root㉿kali)-[~]
└─# nmap -sT 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:16 EST
Nmap scan report for 192.168.49.101
Host is up (0.00064s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds

┌──(root㉿kali)-[~]
└─#
```

```
┌──(root㉿kali)-[~]
└─# nmap -O 192.168.49.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:17 EST
Nmap scan report for 192.168.49.102
Host is up (0.00048s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o
:microsoft:windows_7
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7
SP1, or Windows Server 2008
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.90 seconds
```

```
┌──(root㉿kali)-[~]
└─# nmap -Pn -O 192.168.49.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:22 EST
Nmap scan report for 192.168.49.102
Host is up.
All 1000 scanned ports on 192.168.49.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 210.82 seconds

┌──(root㉿kali)-[~]
└─#
```