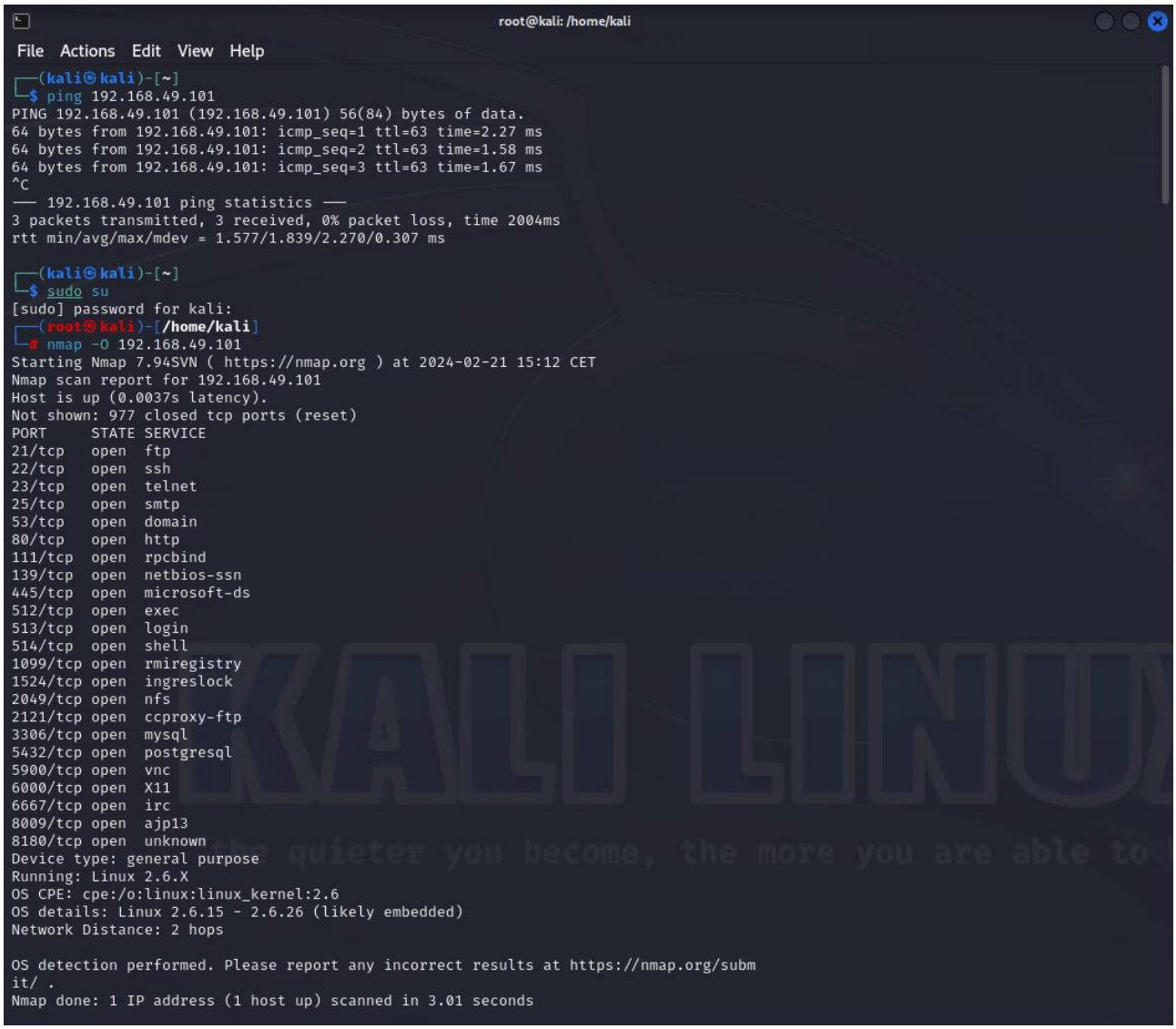
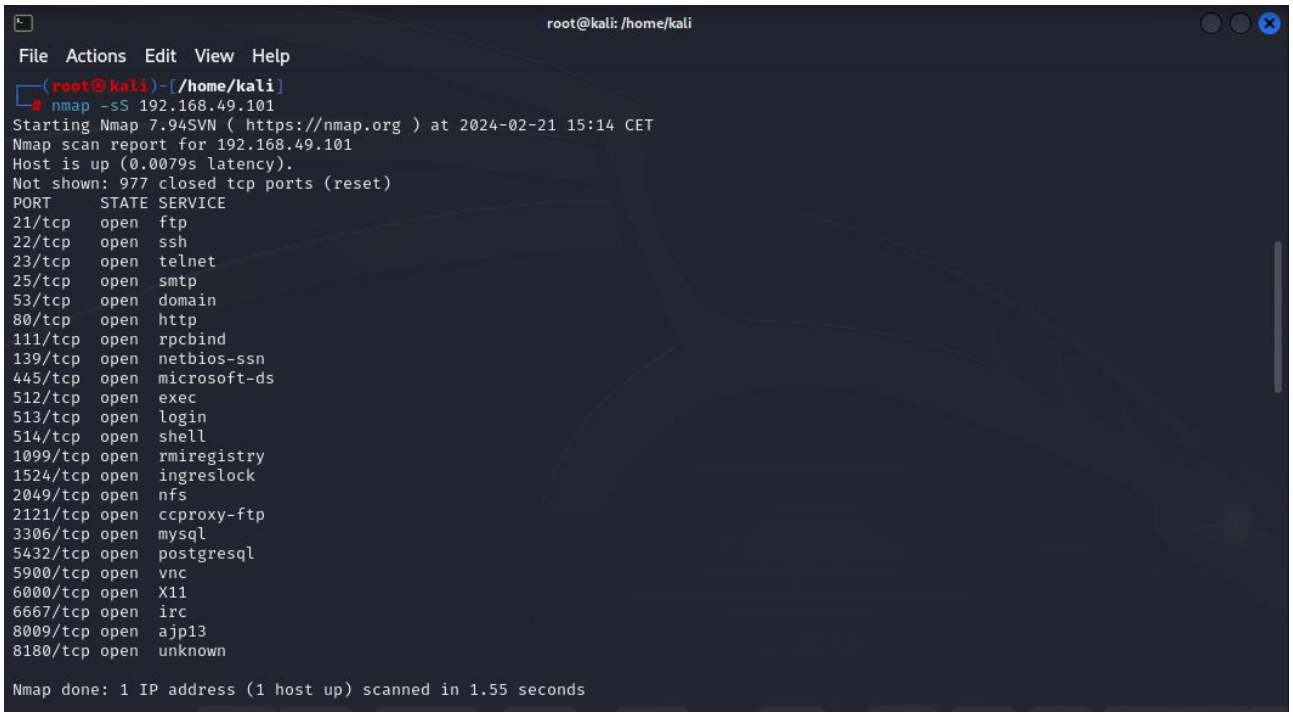
Per quanto riguarda la traccia di oggi il primo passo è stato impostare la rete di windows in modo che pingasse con Kali attraverso Pfsense.

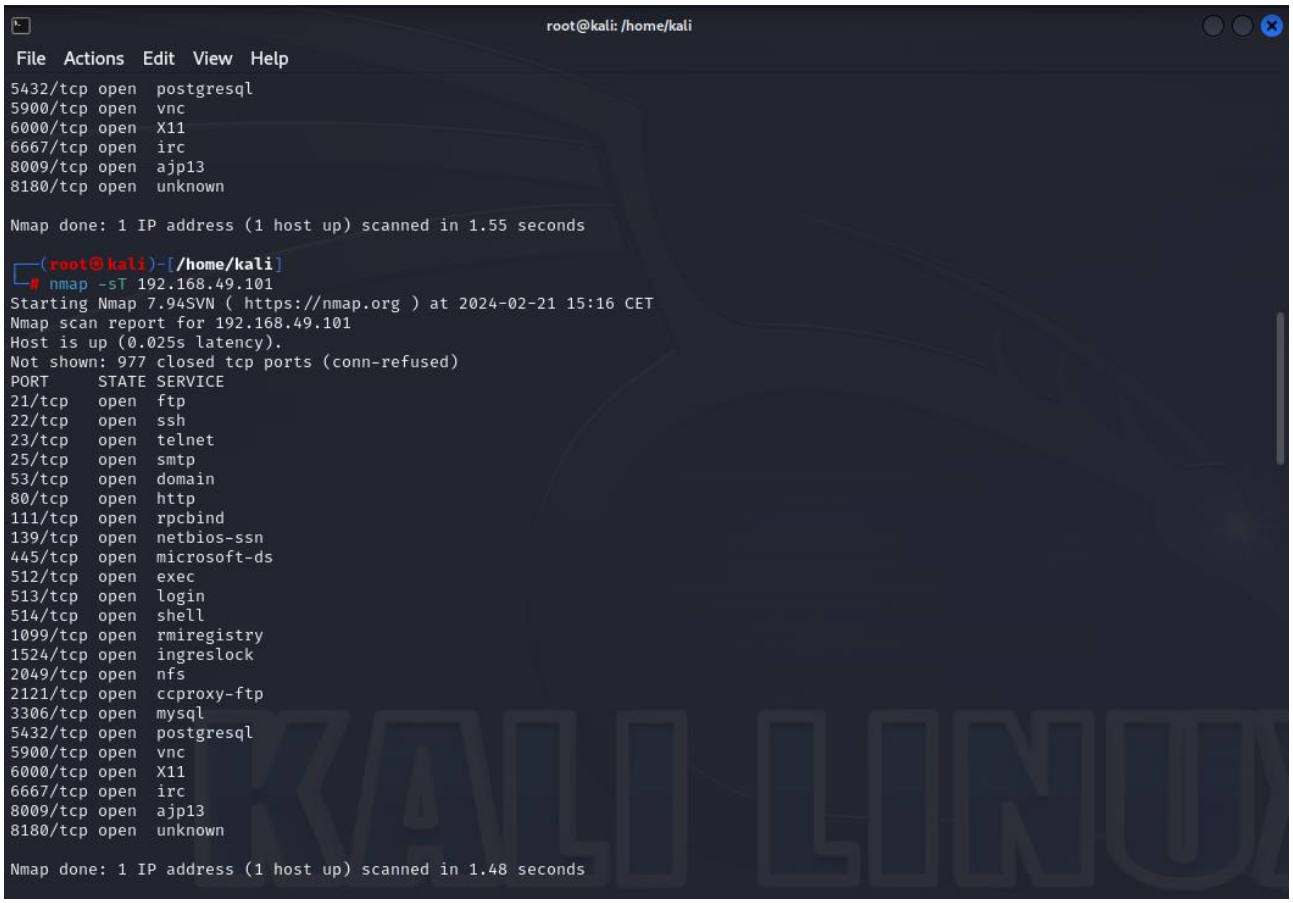
Per quanto riguarda il fingerprint è bastato entrare nella root di Kali, eseguire nmap e lanciare il comando ”-“O prima di inserire l’indirizzo ip di metasploit. Di seguito allego immagine con i dati riportati.



Per il Syn scan è bastato inserire il comando “-sS” quindi facendo un syn stealth ed ancora l’indirizzo ip di Metasploitable.



Per la parte del TCP Connect si utilizza il comando “-sT” che esegue una scansione TCP connect. In questo caso stabiliamo una connessione completa con il server. Ovviamente questa scansione è più facilmente rilevabile.



Per l’ultima parte su Meta si usa il comando “-sV” dove va a scannerizzare i servizi attivi sulle porte aperte e ne determina la versione. Questo può aiutare ad identificare eventuali vulnerabilità.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 15:16 CET
Nmap scan report for 192.168.49.101
Host is up (0.0075s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix,
 Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org
/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 44.96 seconds
```

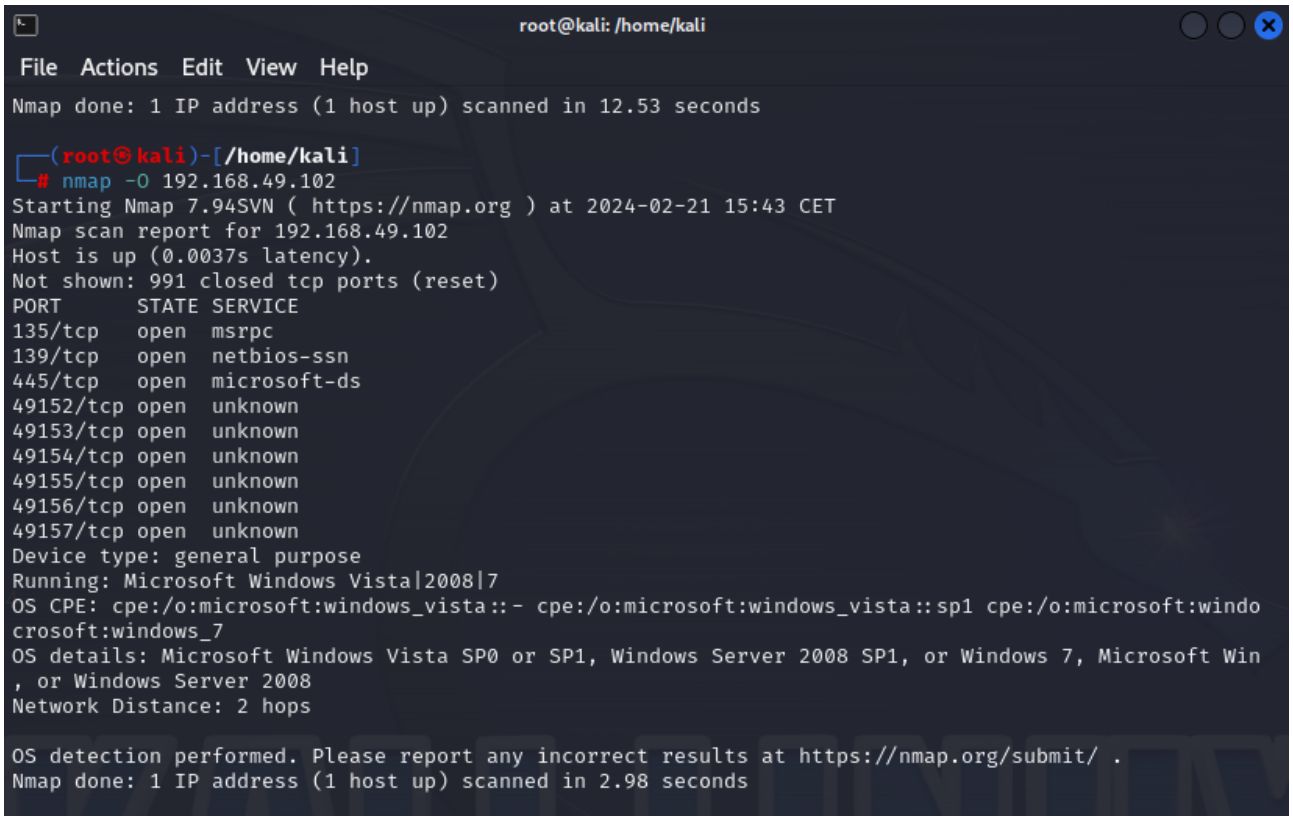
Windows

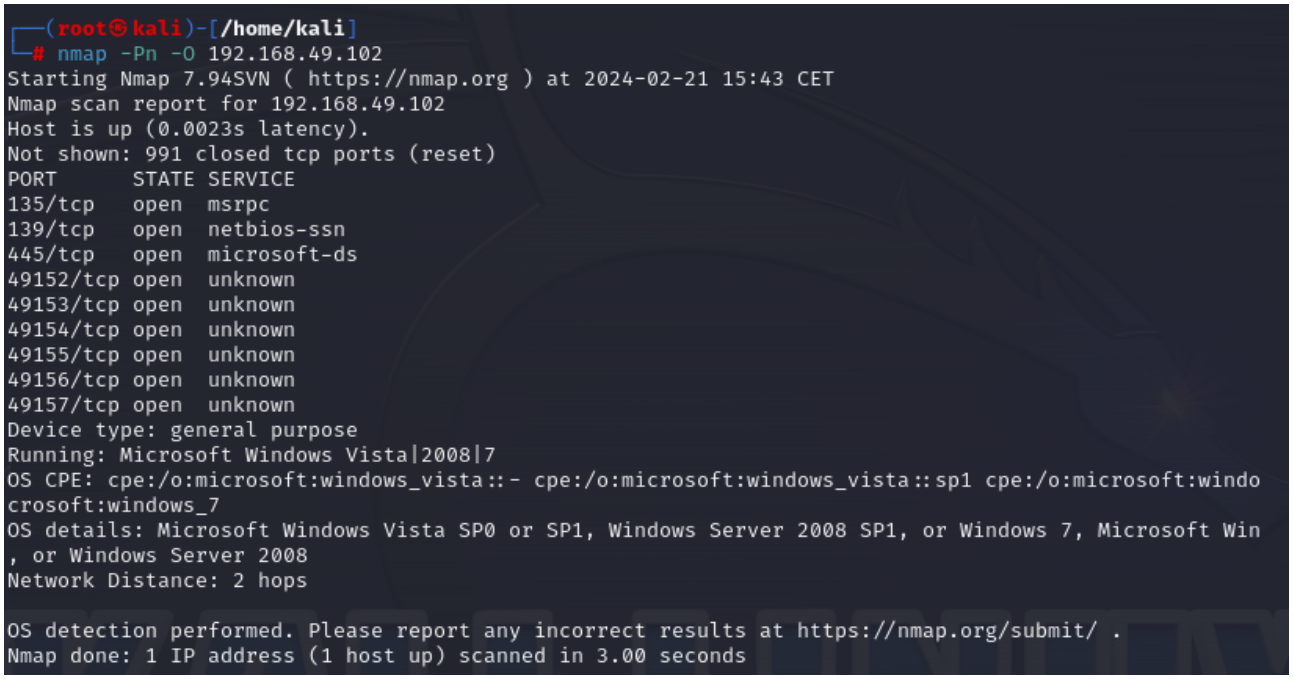
Per quello che riguarda Windows per prima cosa sono andato ad effettuare un fingerprint con il firewall attivo ma ovviamente l'host veniva identificato come disattivo.

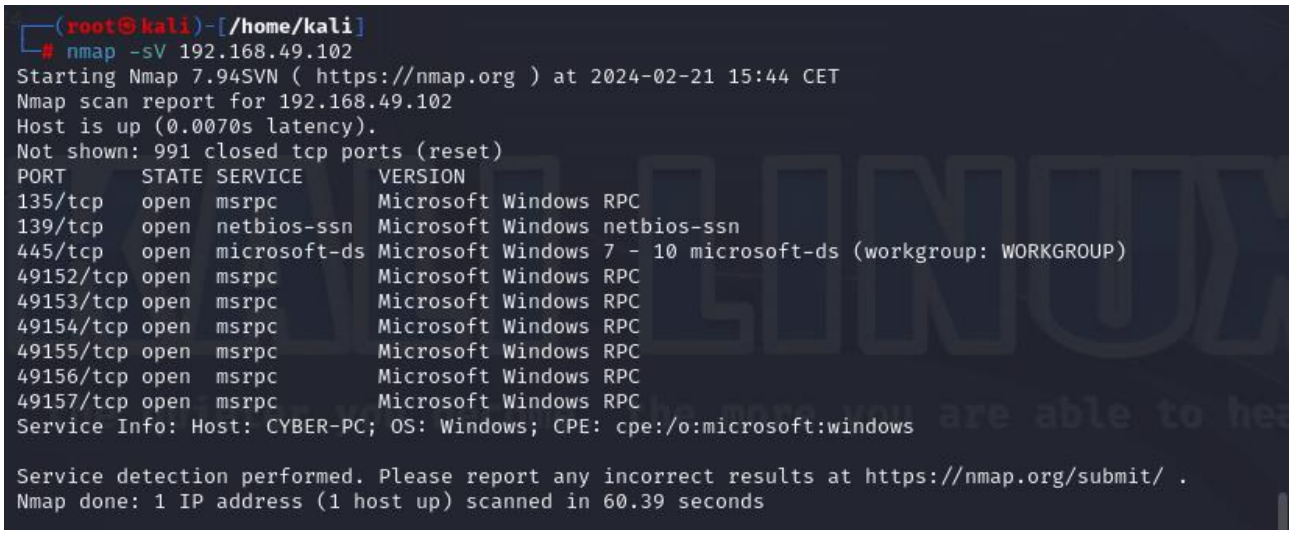
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.49.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 15:18 CET
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.13 seconds
```

Successivamente ho utilizzato il comando "-sP" insieme al comando di fingerprint "-O" e senza usare il ping effettivamente l'host è risultato online ma non ha fornito comunque molti dettagli utili.

Subito dopo sono andato a disattivare il Firewall di windows ed ho provato gli stessi comandi usati su Meta ottenendo i seguenti risultati.


root@kali: /home/kali
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 12.53 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.49.102
Starting Nmap 7.94SVN (https://nmap.org) at 2024-02-21 15:43 CET
Nmap scan report for 192.168.49.102
Host is up (0.0037s 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:windo
crosoft:windows_7
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Win
, 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 2.98 seconds


┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn -O 192.168.49.102
Starting Nmap 7.94SVN (https://nmap.org) at 2024-02-21 15:43 CET
Nmap scan report for 192.168.49.102
Host is up (0.0023s 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:windo
crosoft:windows_7
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Win
, 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 3.00 seconds


┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.49.102
Starting Nmap 7.94SVN (https://nmap.org) at 2024-02-21 15:44 CET
Nmap scan report for 192.168.49.102
Host is up (0.0070s latency).
Not shown: 991 closed tcp ports (reset)
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open msrpc Microsoft Windows RPC
49153/tcp open msrpc Microsoft Windows RPC
49154/tcp open msrpc Microsoft Windows RPC
49155/tcp open msrpc Microsoft Windows RPC
49156/tcp open msrpc Microsoft Windows RPC
49157/tcp open msrpc Microsoft Windows RPC
Service Info: Host: CYBER-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.39 seconds