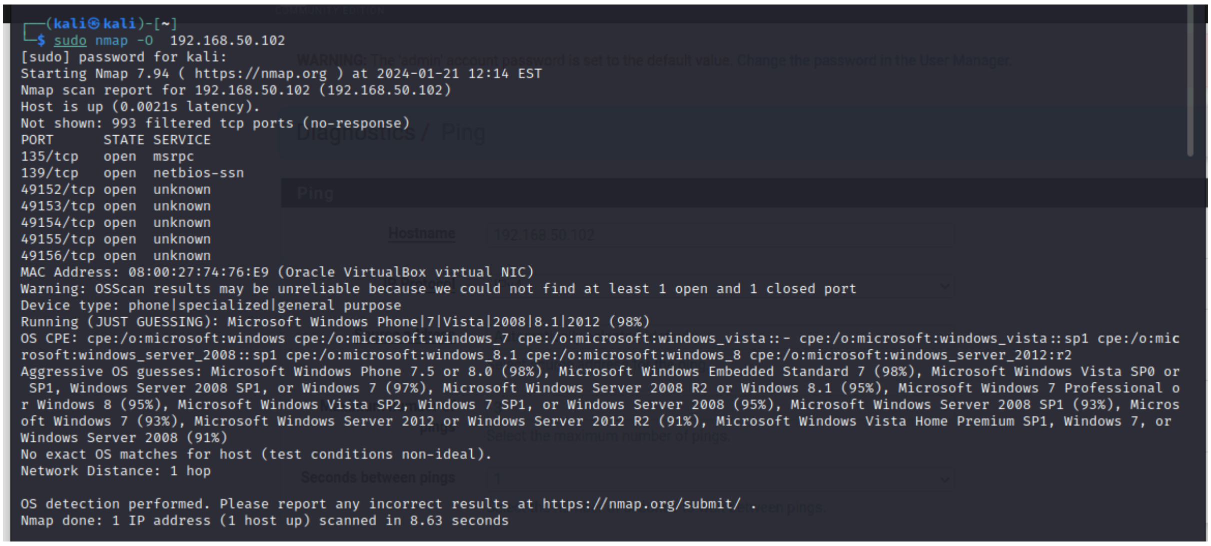
Esercitazione W11D1 Pratica 2

Ilaria Pedrelli

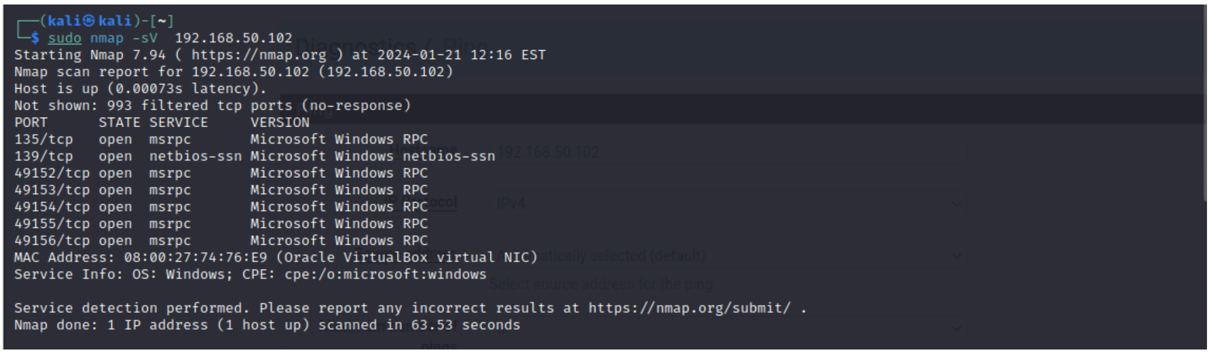
Tecniche di scansione con Nmap

Di seguito le scansioni effettuate su macchina target Win7 su stessa rete e con Firewall attivo.



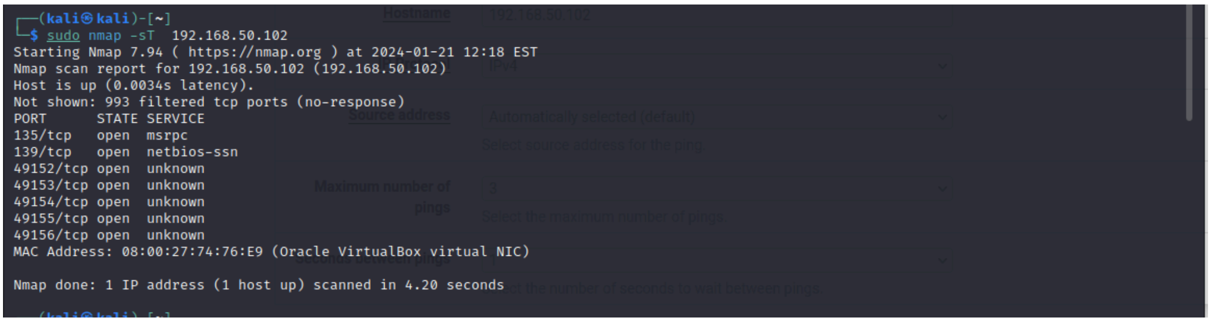
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O  192.168.50.102
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-21 12:14 EST
Nmap scan report for 192.168.50.102 (192.168.50.102)
Host is up (0.0021s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 08:00:27:74:76:E9 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: phone|specialized|general purpose
Running (JUST GUESSING): Microsoft Windows Phone|7|Vista|2008|8.1|2012 (98%)
OS CPE: cpe:/o:microsoft:windows cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:mic
rosoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_server_2012:r2
Aggressive OS guesses: Microsoft Windows Phone 7.5 or 8.0 (98%), Microsoft Windows Embedded Standard 7 (98%), Microsoft Windows Vista SP0 or
 SP1, Windows Server 2008 SP1, or Windows 7 (97%), Microsoft Windows Server 2008 R2 or Windows 8.1 (95%), Microsoft Windows 7 Professional o
r Windows 8 (95%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (95%), Microsoft Windows Server 2008 SP1 (93%), Micros
oft Windows 7 (93%), Microsoft Windows Server 2012 or Windows Server 2012 R2 (91%), Microsoft Windows Vista Home Premium SP1, Windows 7, or
Windows Server 2008 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds
```



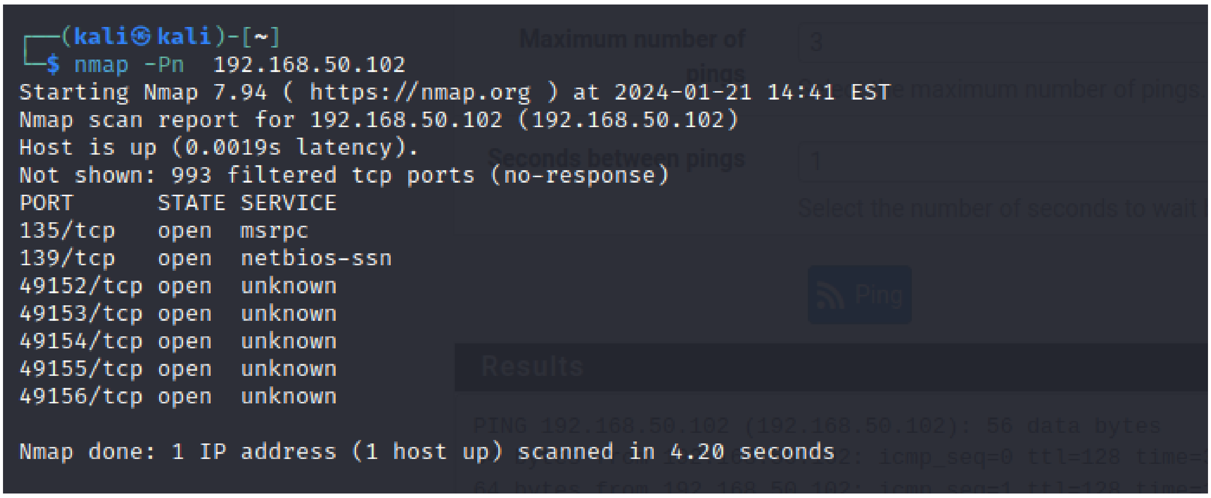
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV  192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-21 12:16 EST
Nmap scan report for 192.168.50.102 (192.168.50.102)
Host is up (0.00073s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE     VERSION
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
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
MAC Address: 08:00:27:74:76:E9 (Oracle VirtualBox virtual NIC)
Service Info: 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 63.53 seconds
```



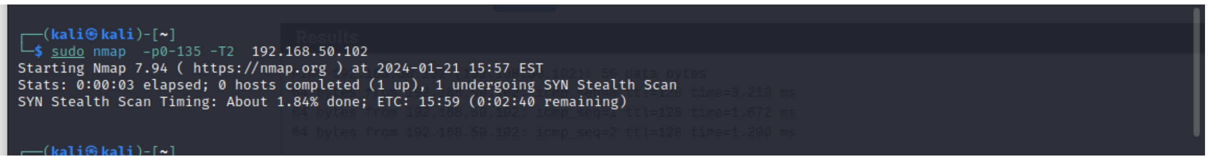
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT  192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-21 12:18 EST
Nmap scan report for 192.168.50.102 (192.168.50.102)
Host is up (0.0034s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 08:00:27:74:76:E9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.20 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn  192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-21 14:41 EST
Nmap scan report for 192.168.50.102 (192.168.50.102)
Host is up (0.0019s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 4.20 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap  -p0-135 -T2  192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-21 15:57 EST
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 1.84% done; ETC: 15:59 (0:02:40 remaining)


┌──(kali㉿kali)-[~]
```