Raul Pastor

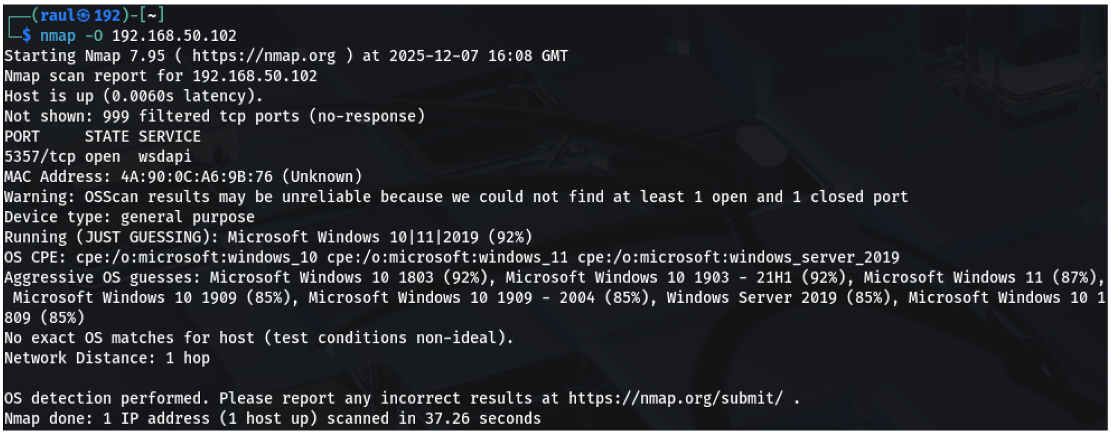
Nmap

L’esercizio di oggi riguarda la creazione di un report con i dettagli di 4 tipi di scansioni sul target Windows(sulla stessa rete) attivando e disattivando il windows firewall.

La prima scansione è la scansione del sistema operativo, la seconda il syn scan, la terza il tcp scan e l’ultima la version scan.

WINDOWS FIREWALL ATTIVO:

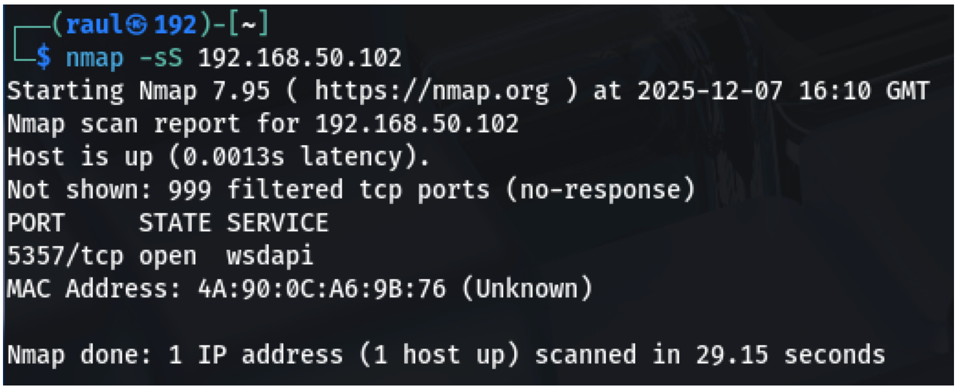
1)



```
┌──(raul㉿192)-[~]
└─$ nmap -O 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 16:08 GMT
Nmap scan report for 192.168.50.102
Host is up (0.0060s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
5357/tcp open  wsdapi
MAC Address: 4A:90:0C:A6:9B:76 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 10|11|2019 (92%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_11 cpe:/o:microsoft:windows_server_2019
Aggressive OS guesses: Microsoft Windows 10 1803 (92%), Microsoft Windows 10 1903 - 21H1 (92%), Microsoft Windows 11 (87%),
 Microsoft Windows 10 1909 (85%), Microsoft Windows 10 1909 - 2004 (85%), Windows Server 2019 (85%), Microsoft Windows 10 1
809 (85%)
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 37.26 seconds
```

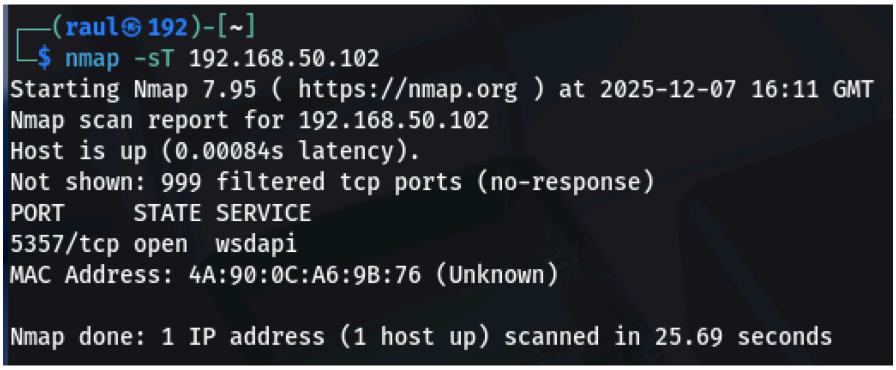
2)



```
┌──(raul㉿192)-[~]
└─$ nmap -sS 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 16:10 GMT
Nmap scan report for 192.168.50.102
Host is up (0.0013s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
5357/tcp open  wsdapi
MAC Address: 4A:90:0C:A6:9B:76 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 29.15 seconds
```

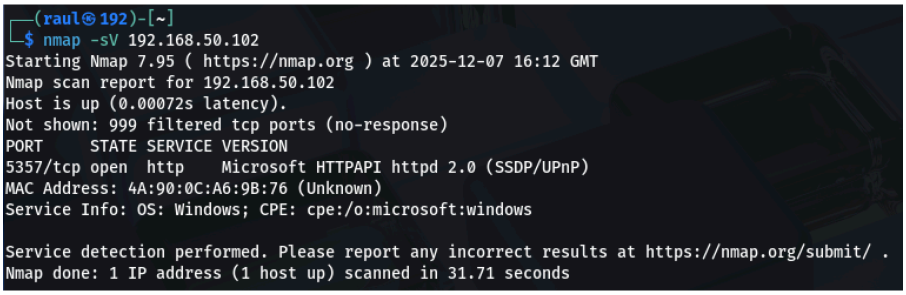
3)



```
┌──(raul㉿192)-[~]
└─$ nmap -sT 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 16:11 GMT
Nmap scan report for 192.168.50.102
Host is up (0.00084s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
5357/tcp open  wsdapi
MAC Address: 4A:90:0C:A6:9B:76 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 25.69 seconds
```

4)

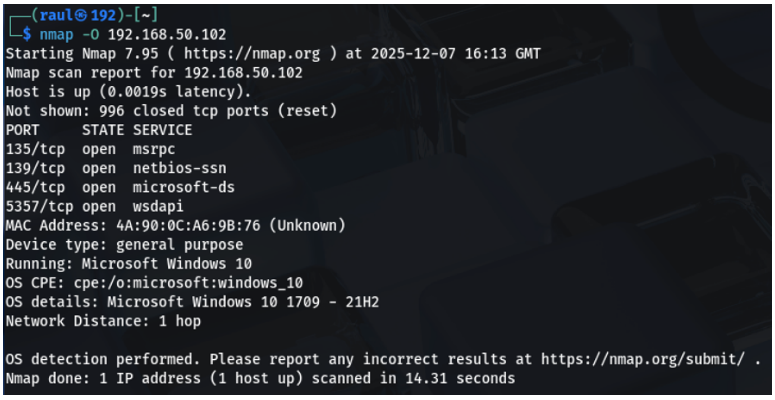


```
┌──(raul㉿192)-[~]
└─$ nmap -sV 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 16:12 GMT
Nmap scan report for 192.168.50.102
Host is up (0.00072s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
5357/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 4A:90:0C:A6:9B:76 (Unknown)
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 31.71 seconds
```

WINDOWS FIREWALL DISATTIVATO:

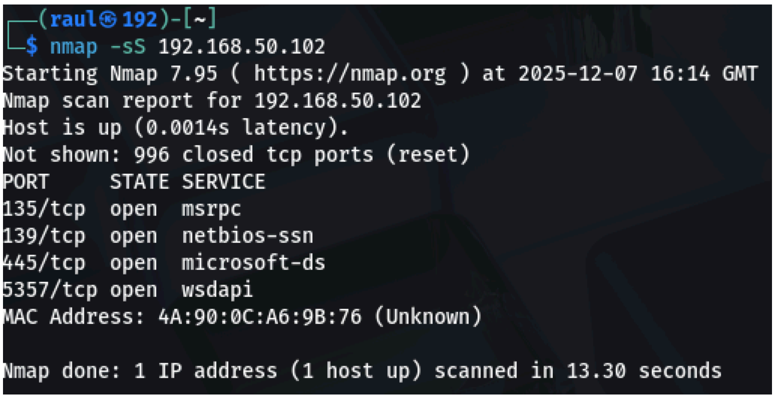
1)



```
┌──(raul㉿192)-[~]
└─$ nmap -O 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 16:13 GMT
Nmap scan report for 192.168.50.102
Host is up (0.0019s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: 4A:90:0C:A6:9B:76 (Unknown)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 21H2
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 14.31 seconds
```

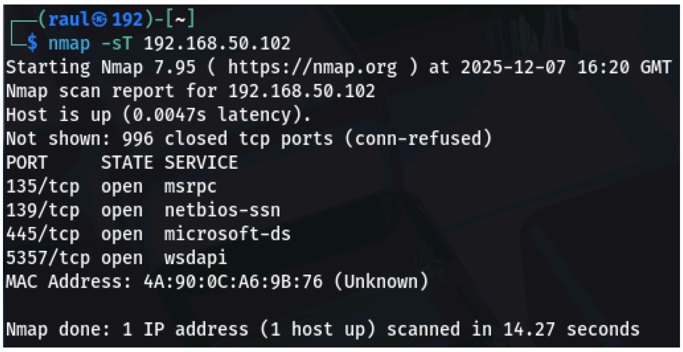
2)



```
┌──(raul㉿192)-[~]
└─$ nmap -sS 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 16:14 GMT
Nmap scan report for 192.168.50.102
Host is up (0.0014s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: 4A:90:0C:A6:9B:76 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
```

3)

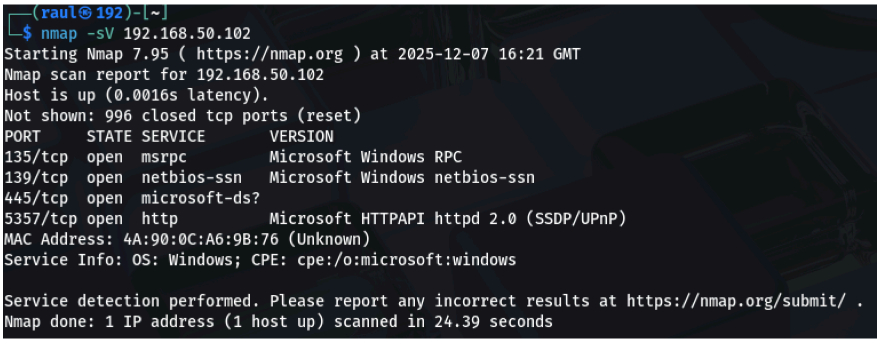


```
┌──(raul㉿192)-[~]
└─$ nmap -sT 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 16:20 GMT
Nmap scan report for 192.168.50.102
Host is up (0.0047s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: 4A:90:0C:A6:9B:76 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 14.27 seconds
```

Raul Pastor

4)



```
┌──(raul㉿192)-[~]
└─$ nmap -sV 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 16:21 GMT
Nmap scan report for 192.168.50.102
Host is up (0.0016s latency).
Not shown: 996 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?
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 4A:90:0C:A6:9B:76 (Unknown)
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 24.39 seconds
```

Come possiamo notare c'è tanta differenza tra lo scan con o senza windows firewall.
l'unica cosa che notiamo con il windows firewall attivo è la porta aperta 5357, ma oltre a questo nmap non è nemmeno sicuro del sistema operativo.
Appena viene rimosso il firewall vengono fuori tutte le criticità di windows 10.

REPORT

Indirizzo ip target: 192.168.50.102

Sistema operativo: Windows 10

Informazioni sulle porte:

PORTA	STATO	SERVIZIO	VERSIONE
135	open	msrpc	Microsoft windows rpc
139	open	netbios-ssn	Microsoft Windows netbios-ssn
445	open	microsoft-ds?	
5357	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)