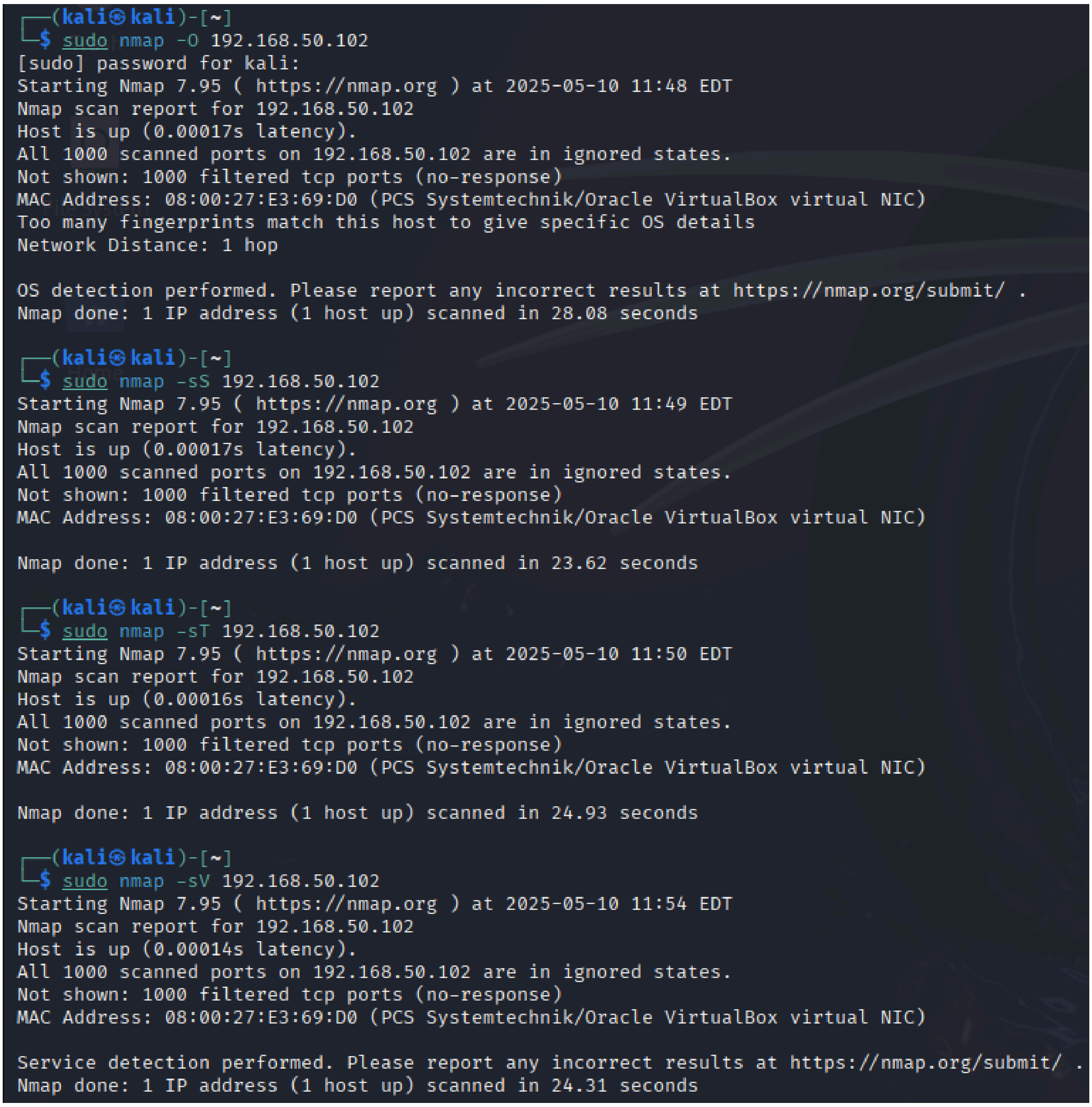
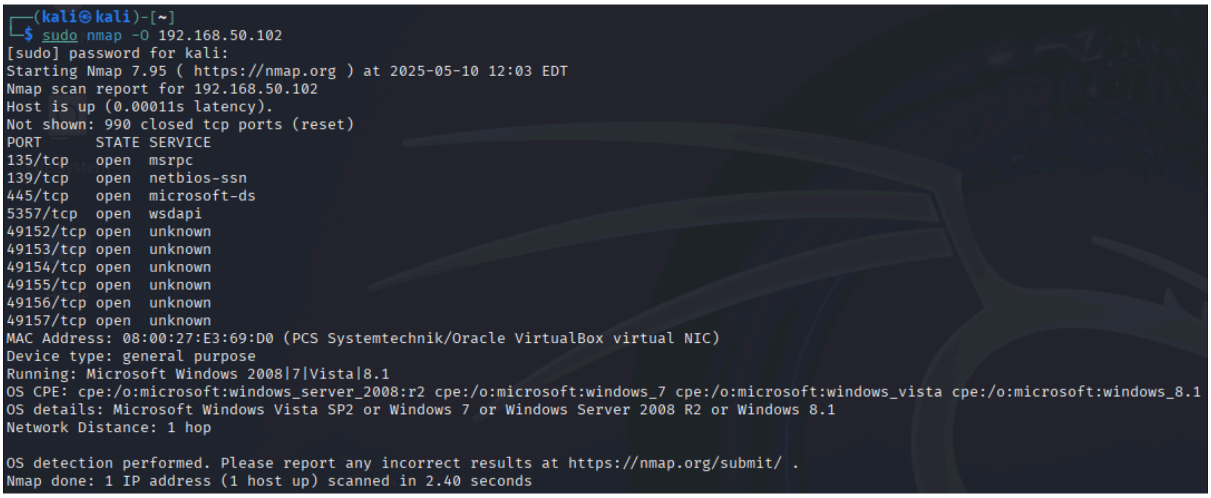


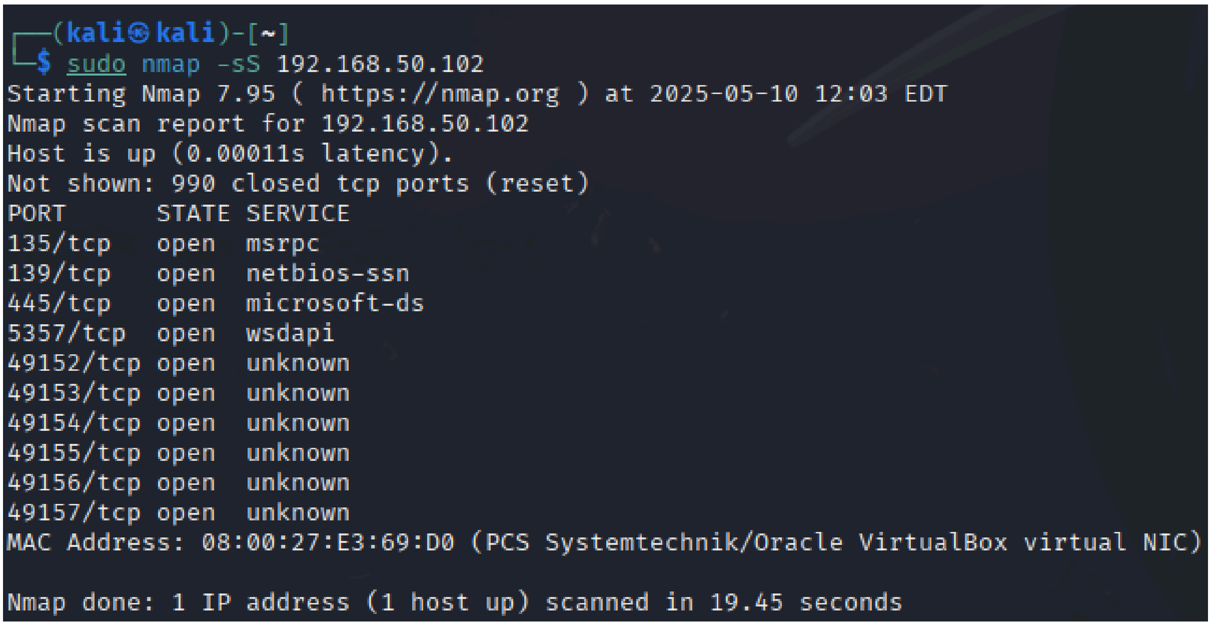
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.102
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 11:48 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00017s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:E3:69:D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
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 28.08 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 11:49 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00017s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:E3:69:D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 23.62 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 11:50 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00016s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:E3:69:D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 24.93 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 11:54 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00014s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:E3:69:D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.31 seconds
```

comandi usati: -O , -sS , -sT , -sV da kali a windows 7 con firewall attivo sulla stessa rete
Tutte confermano che **il firewall blocca ogni tentativo di scansione**, rendendo invisibile l’host a livello di servizio.

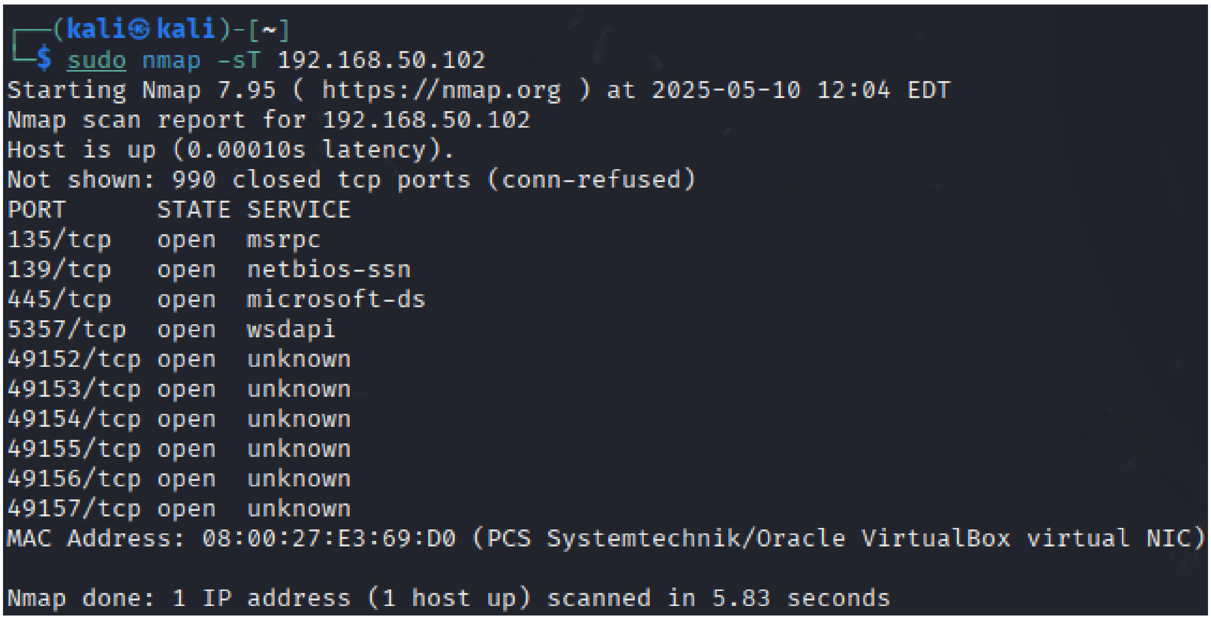
Adesso proviamo con il firewall disabilitato



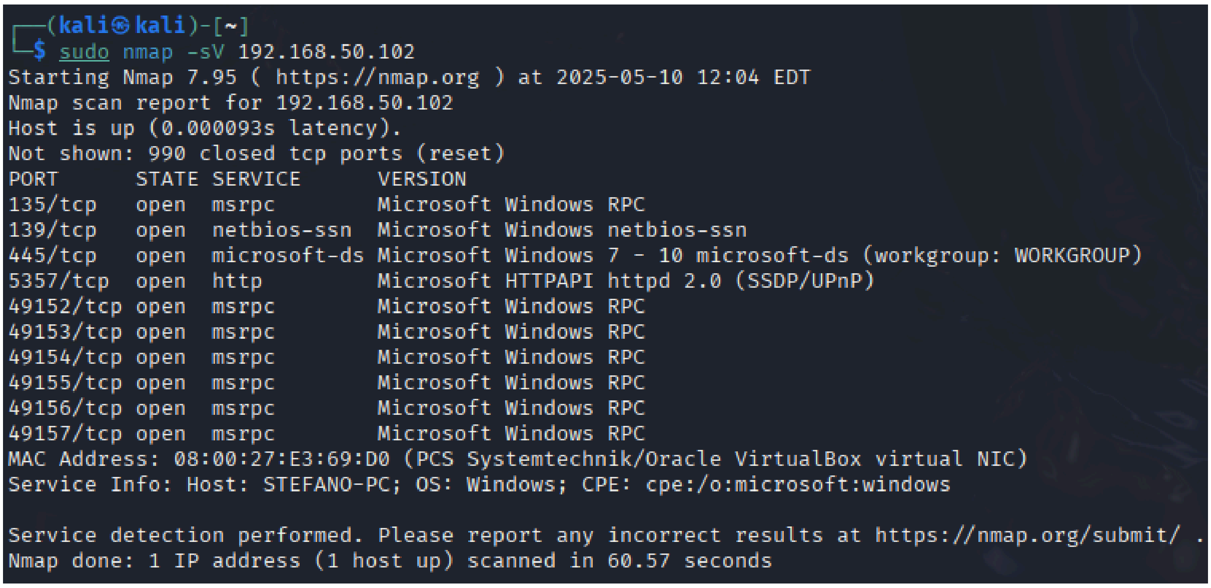
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.102
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 12:03 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00011s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:E3:69:D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 2008|7|Vista|8.1
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows Vista SP2 or Windows 7 or Windows Server 2008 R2 or Windows 8.1
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 2.40 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 12:03 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00011s latency).
Not shown: 990 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
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:E3:69:D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 19.45 seconds
```



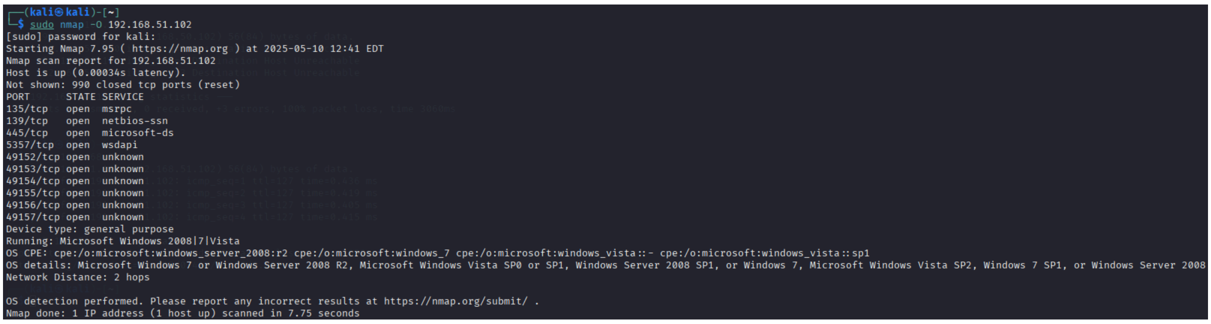
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 12:04 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00010s latency).
Not shown: 990 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:E3:69:D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.83 seconds
```



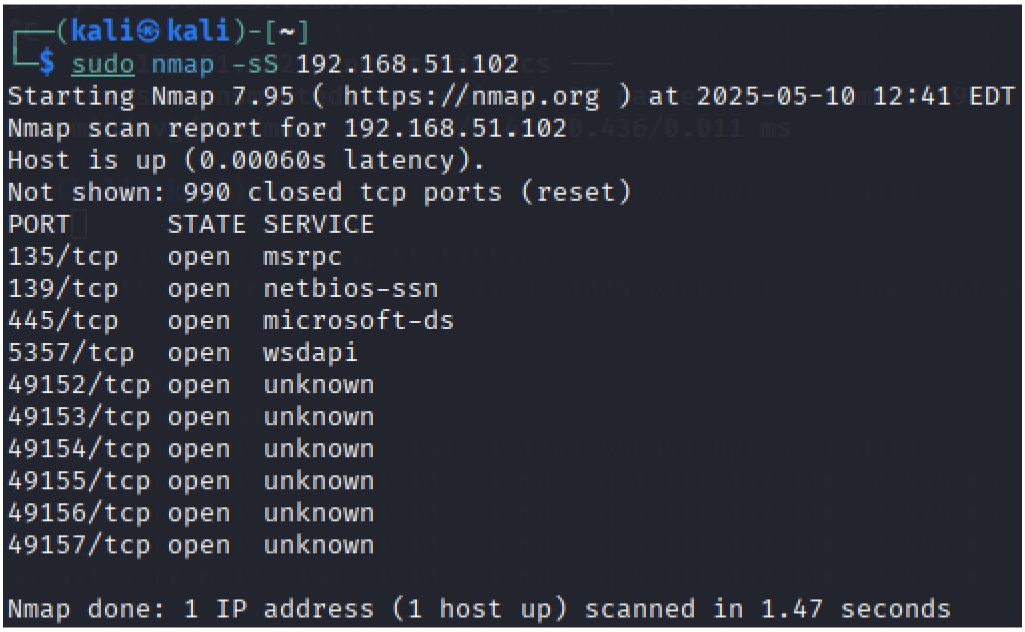
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 12:04 EDT
Nmap scan report for 192.168.50.102
Host is up (0.000093s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
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
MAC Address: 08:00:27:E3:69:D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: STEFANO-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 60.57 seconds
```

comando	firewall attivo	firewall disattivato
-O	Nessun OS identificato	Windows 7 / Vista / Server 2008 R2
-sS	Nessuna porta visibile	10 porte aperte
-sT	Nessuna porta visibile	10 porte aperte
-sV	Nessun servizio rilevato	Tutti i servizi e versioni visibili

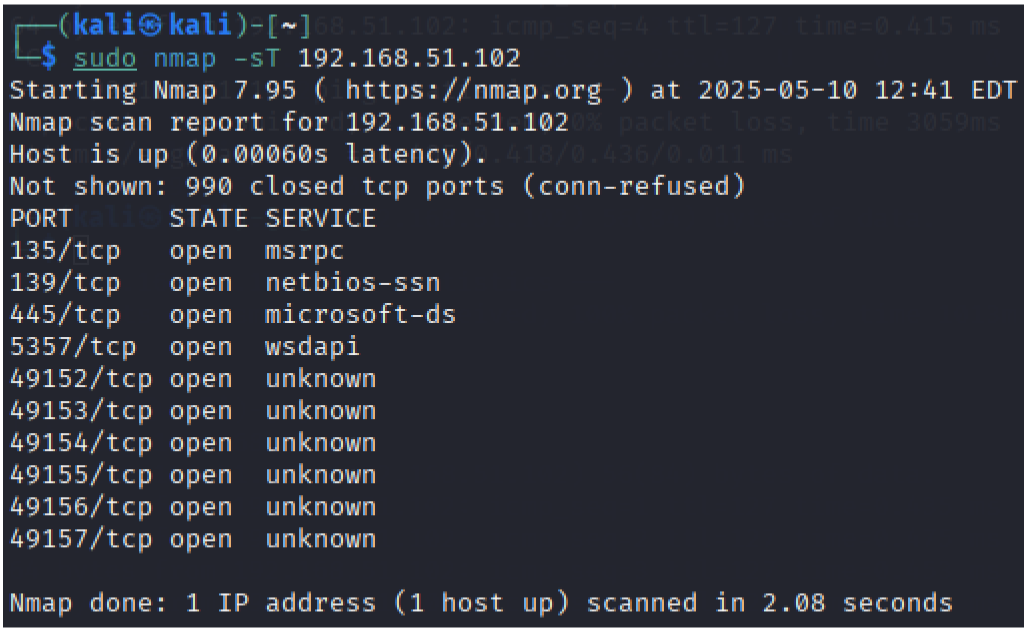
L’altra parte dell’esercizio vuole che facciamo le stesse identiche cose ma con rete diversa: iniziamo con il firewall disattivato (kali 192.168.50.100) (windows 192.168.51.102)



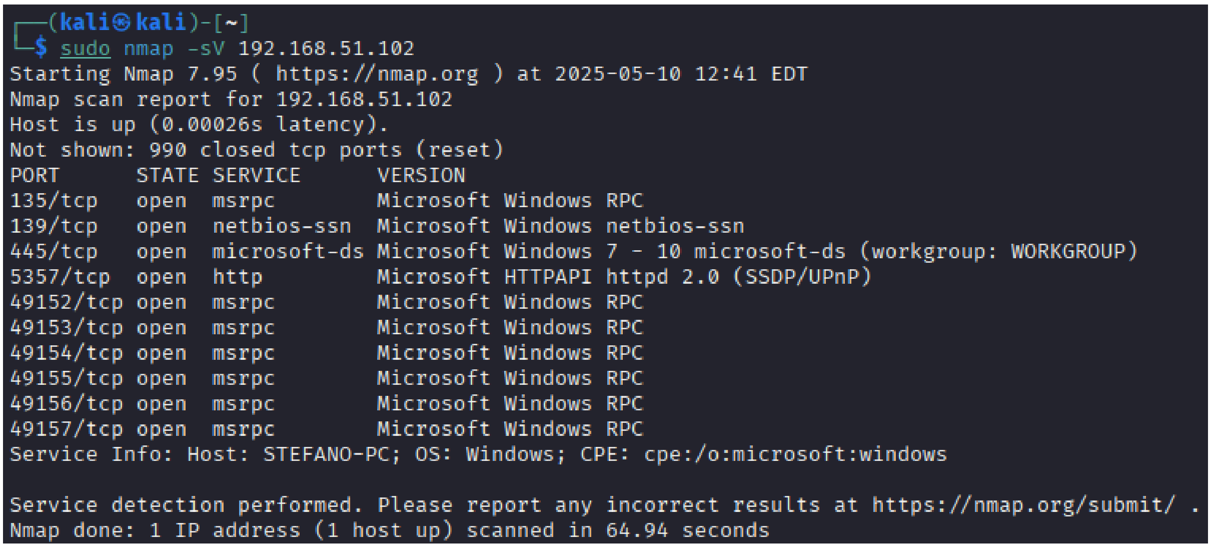
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.51.102
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 12:41 EDT
Nmap scan report for 192.168.51.102
Host is up (0.00034s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
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 2008|7|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows 7 or Windows Server 2008 R2, 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 7.75 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.51.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 12:41 EDT
Nmap scan report for 192.168.51.102
Host is up (0.00060s latency).
Not shown: 990 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
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.47 seconds
```

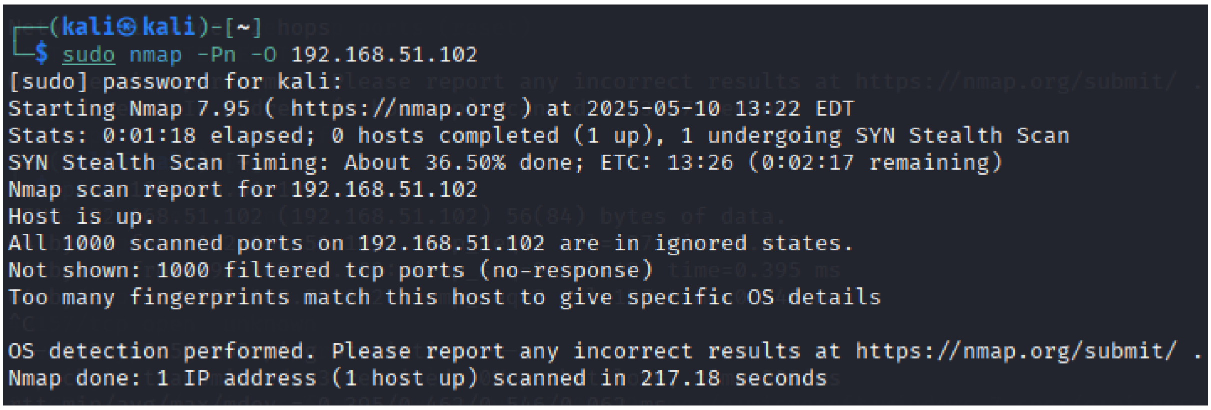


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.51.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 12:41 EDT
Nmap scan report for 192.168.51.102
Host is up (0.00060s latency).
Not shown: 990 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.08 seconds
```

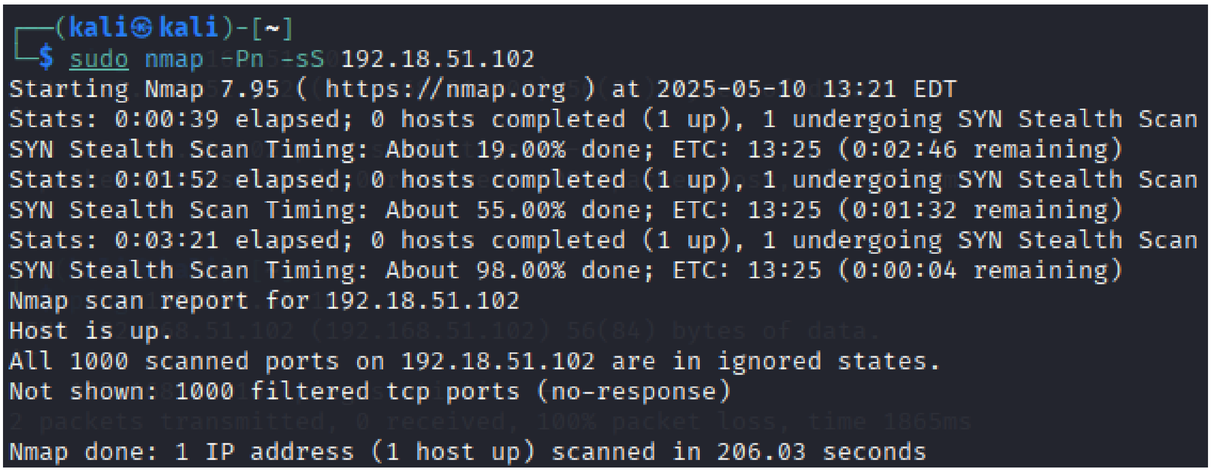


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.51.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 12:41 EDT
Nmap scan report for 192.168.51.102
Host is up (0.00026s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
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: STEFANO-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 64.94 seconds
```

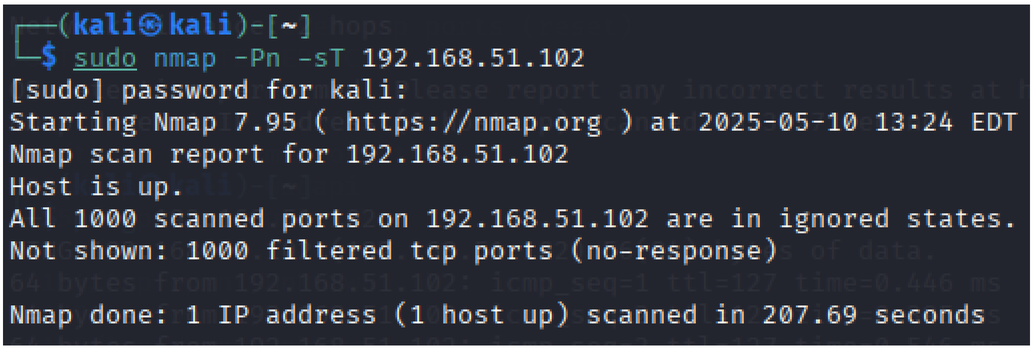
Adesso proviamo con il firewall attivato:



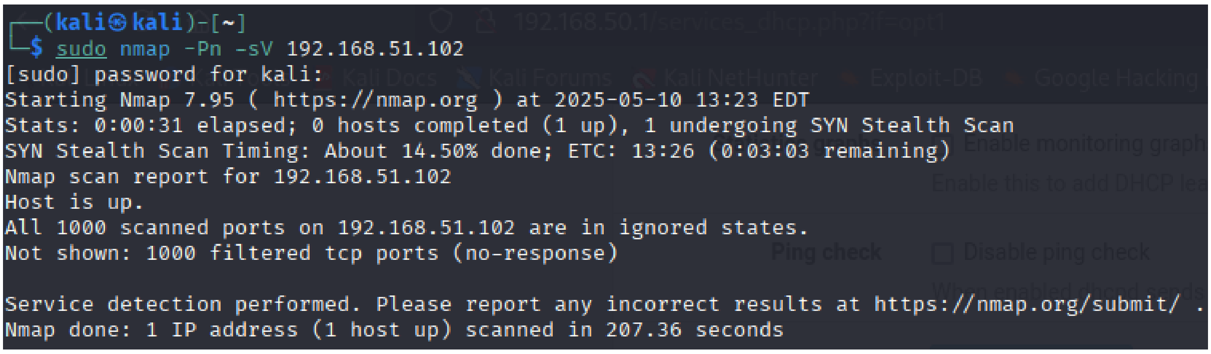
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -Pn -O 192.168.51.102
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 13:22 EDT
Stats: 0:01:18 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 36.50% done; ETC: 13:26 (0:02:17 remaining)
Nmap scan report for 192.168.51.102
Host is up.
All 1000 scanned ports on 192.168.51.102 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 217.18 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -Pn -sS 192.18.51.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 13:21 EDT
Stats: 0:00:39 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 19.00% done; ETC: 13:25 (0:02:46 remaining)
Stats: 0:01:52 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 55.00% done; ETC: 13:25 (0:01:32 remaining)
Stats: 0:03:21 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 98.00% done; ETC: 13:25 (0:00:04 remaining)
Nmap scan report for 192.18.51.102
Host is up.
All 1000 scanned ports on 192.18.51.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 206.03 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -Pn -sT 192.168.51.102
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 13:24 EDT
Nmap scan report for 192.168.51.102
Host is up.
All 1000 scanned ports on 192.168.51.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 207.69 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -Pn -sV 192.168.51.102
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 13:23 EDT
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 14.50% done; ETC: 13:26 (0:03:03 remaining)
Nmap scan report for 192.168.51.102
Host is up.
All 1000 scanned ports on 192.168.51.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 207.36 seconds
```

noteremo che abbiamo aggiunto il comando -Pn per saltare il “ping” dato che probabilmente il firewall di windows ha delle restrizioni che non permettono il ping su reti diverse, al contrario di quando è sulla stessa rete ma ha il firewall abilitato riusciamo comunque a pingare cambiando delle regole ICMPv4 request echo.

Scenario	**Ping**	**Scansione Nmap**	**Porte rilevate**	**Servizi identificati**	**Note**
Stessa rete Firewall **abilitato**	no/sì dipende dalla regola	si	no (filtrate)	no	Il firewall blocca ICMP e TCP in ingresso, anche in LAN
Stessa rete Firewall **disabilitato**	si	si	si	si	Tutto accessibile, fingerprint OS riuscito
Reti diverse Firewall **abilitato**	no/sì dipende dalla regola	comando aggiuntivo usato “-Pn”	no (filtrate)	no	Firewall blocca tutto il traffico da reti diverse
Reti diverse Firewall **disabilitato**	si	si	si	si	Funziona come in LAN, nessun blocco