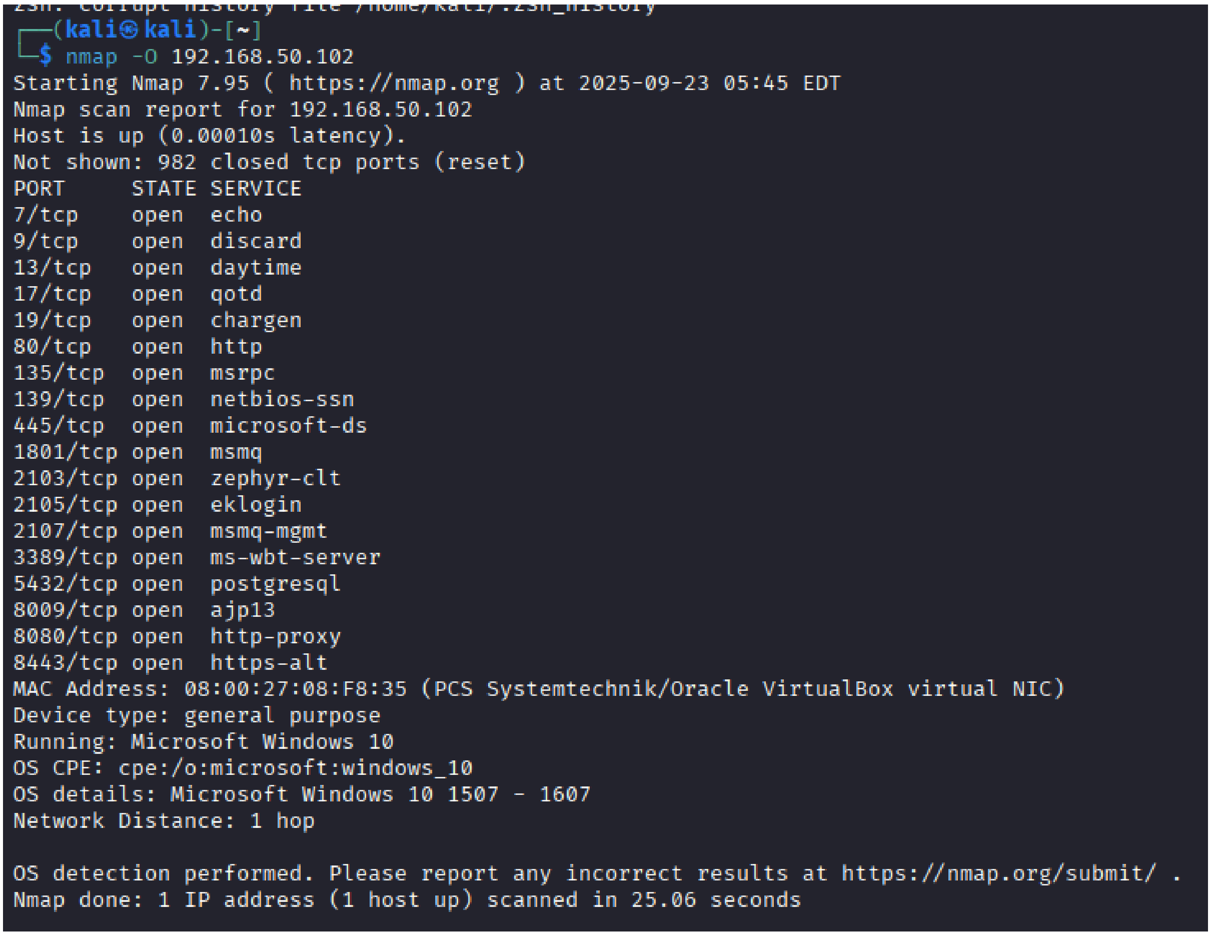
Traccia:

Si richiede allo studente di effettuare le scansioni dell'esercizio precedente con Nmap sul target **Windows** con Windows Firewall abilitato e disabilitato.

Elencare tutti i passaggi compiuti ed i tipi di scansione, con i relativi risultati, durante la fase di scrittura report.

SVOLGIMENTO:

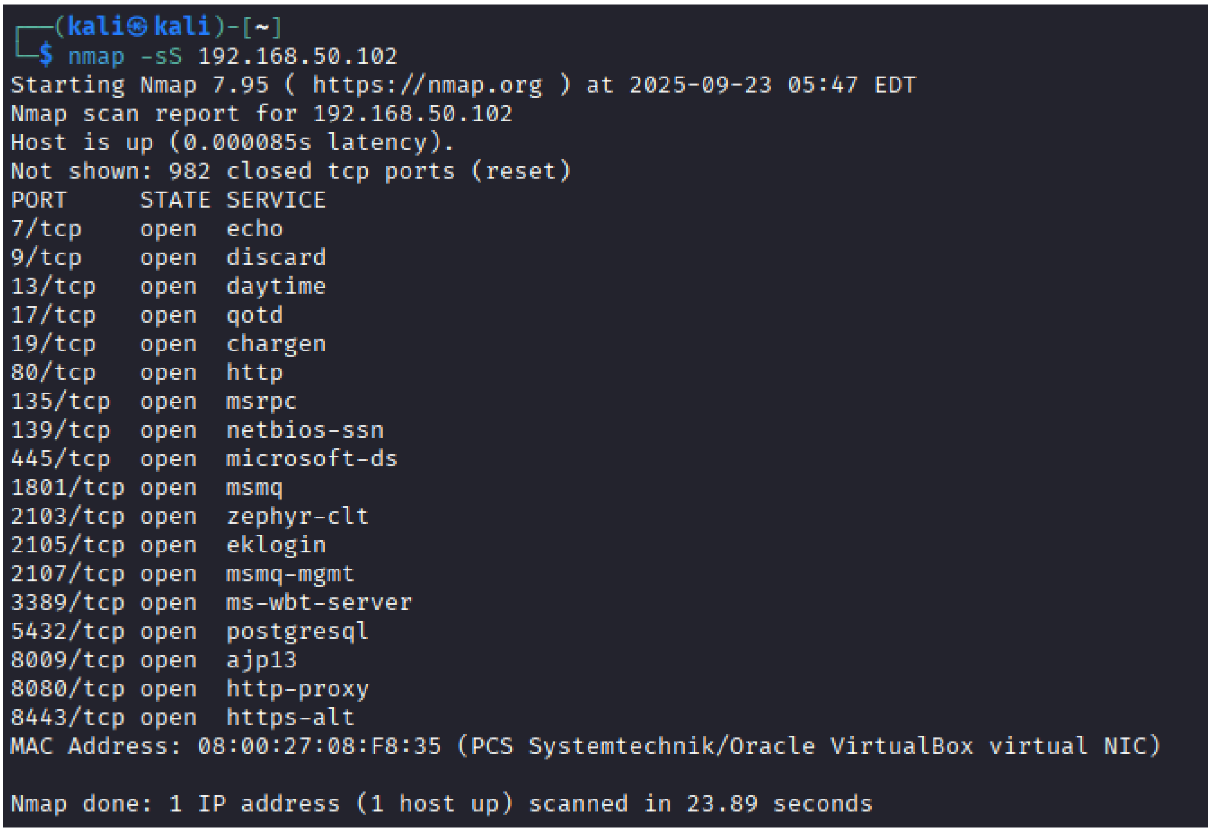
comandi nmap con windows firewall abilitato
OS fingerprint:



```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 05:45 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00010s latency).
Not shown: 982 closed tcp ports (reset)
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3389/tcp open  ms-wbt-server
5432/tcp open  postgresql
8009/tcp open  ajp13
8080/tcp open  http-proxy
8443/tcp open  https-alt
MAC Address: 08:00:27:08:F8:35 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
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 25.06 seconds
```

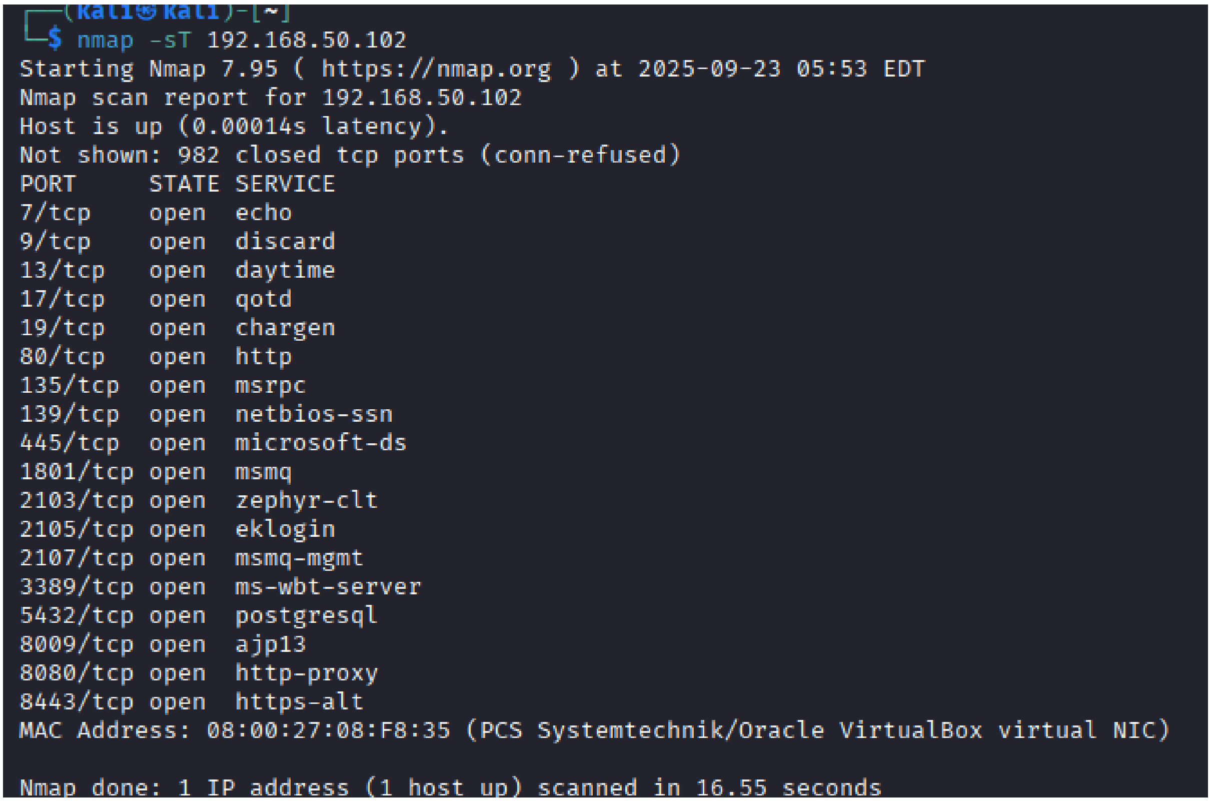
Syn scan:



```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 05:47 EDT
Nmap scan report for 192.168.50.102
Host is up (0.000085s latency).
Not shown: 982 closed tcp ports (reset)
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3389/tcp open  ms-wbt-server
5432/tcp open  postgresql
8009/tcp open  ajp13
8080/tcp open  http-proxy
8443/tcp open  https-alt
MAC Address: 08:00:27:08:F8:35 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 23.89 seconds
```

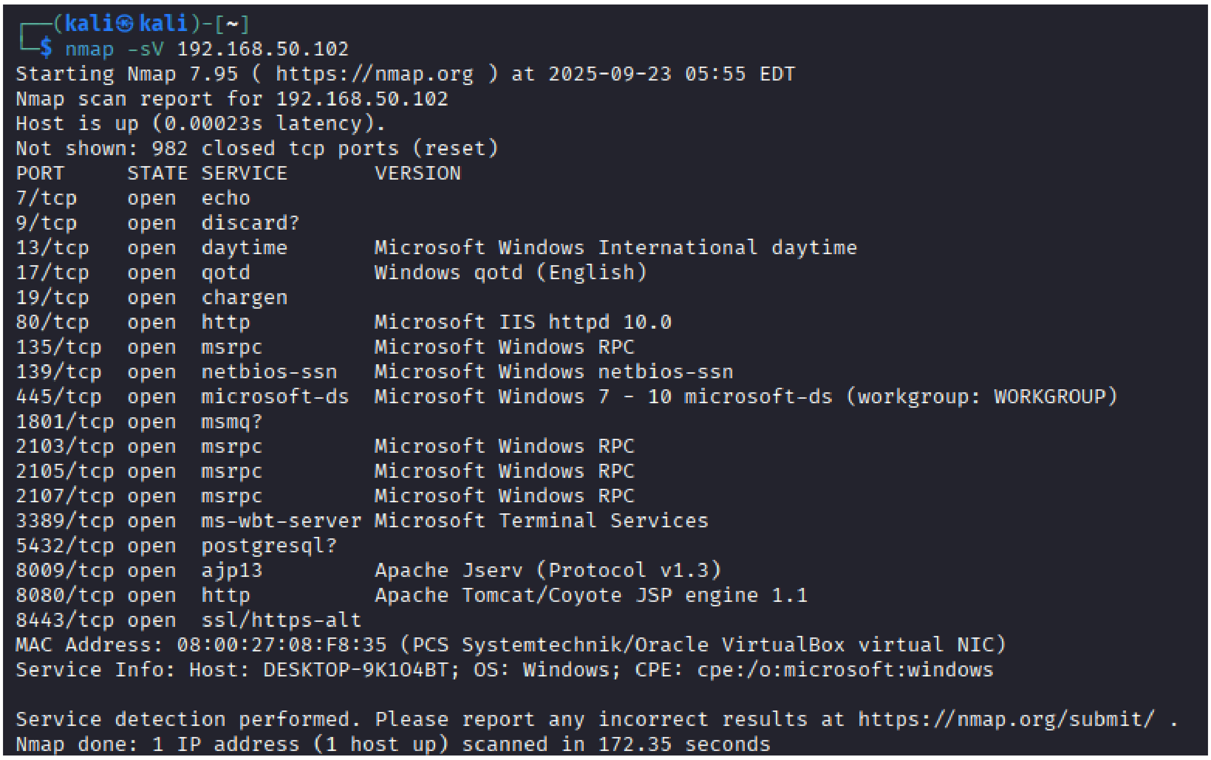
TCP connect:



```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 05:53 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00014s latency).
Not shown: 982 closed tcp ports (conn-refused)
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3389/tcp open  ms-wbt-server
5432/tcp open  postgresql
8009/tcp open  ajp13
8080/tcp open  http-proxy
8443/tcp open  https-alt
MAC Address: 08:00:27:08:F8:35 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.55 seconds
```

Version detection:

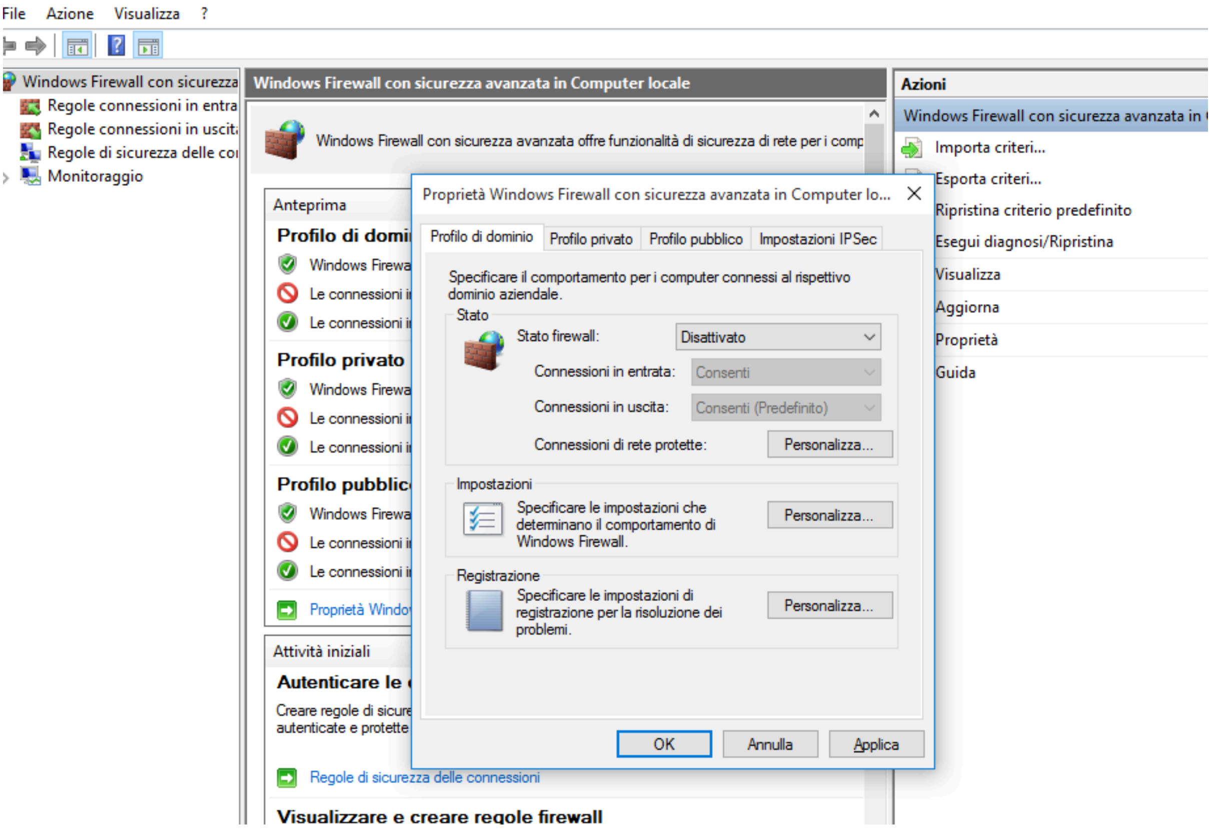


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 05:55 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00023s latency).
Not shown: 982 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
7/tcp    open  echo
9/tcp    open  discard?
13/tcp   open  daytime       Microsoft Windows International daytime
17/tcp   open  qotd          Windows qotd (English)
19/tcp   open  chargen
80/tcp   open  http          Microsoft IIS httpd 10.0
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)
1801/tcp open  msmq?
2103/tcp open  msrpc         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5432/tcp open  postgresql?
8009/tcp open  ajp13         Apache Jserv (Protocol v1.3)
8080/tcp open  http          Apache Tomcat/Coyote JSP engine 1.1
8443/tcp open  ssl/https-alt
MAC Address: 08:00:27:08:F8:35 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-9K104BT; 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 172.35 seconds
```

comandi con nmap con windows firewall disabilitato

Premessa: disabilitazione del firewall procedura effettuata.


File Azione Visualizza ?
Windows Firewall con sicurezza
Regole connessioni in entra
Regole connessioni in uscit
Regole di sicurezza delle co
Monitoraggio
Windows Firewall con sicurezza avanzata in Computer locale
Windows Firewall con sicurezza avanzata offre funzionalità di sicurezza di rete per i comp
Anteprima
Profilo di domi
Profilo privato
Profilo pubblic
Proprietà Windo
Attività iniziali
Autenticare le
Creare regole di sicure autenticate e protette
Regole di sicurezza delle connessioni
Visualizzare e creare regole firewall
Azioni
Windows Firewall con sicurezza avanzata in
Importa criteri...
Esporta criteri...
Ripristina criterio predefinito
Esegui diagnosi/Ripristina
Visualizza
Aggiorna
Proprietà
Guida

Proprietà Windows Firewall con sicurezza avanzata in Computer lo...

Profilo di dominio | Profilo privato | Profilo pubblico | Impostazioni IPSec

Specificare il comportamento per i computer connessi al rispettivo dominio aziendale.

Stato

Stato firewall: Disattivato

Connessioni in entrata: Consenti

Connessioni in uscita: Consenti (Predefinito)

Connessioni di rete protette: Personalizza...

Impostazioni

Specificare le impostazioni che determinano il comportamento di Windows Firewall. Personalizza...

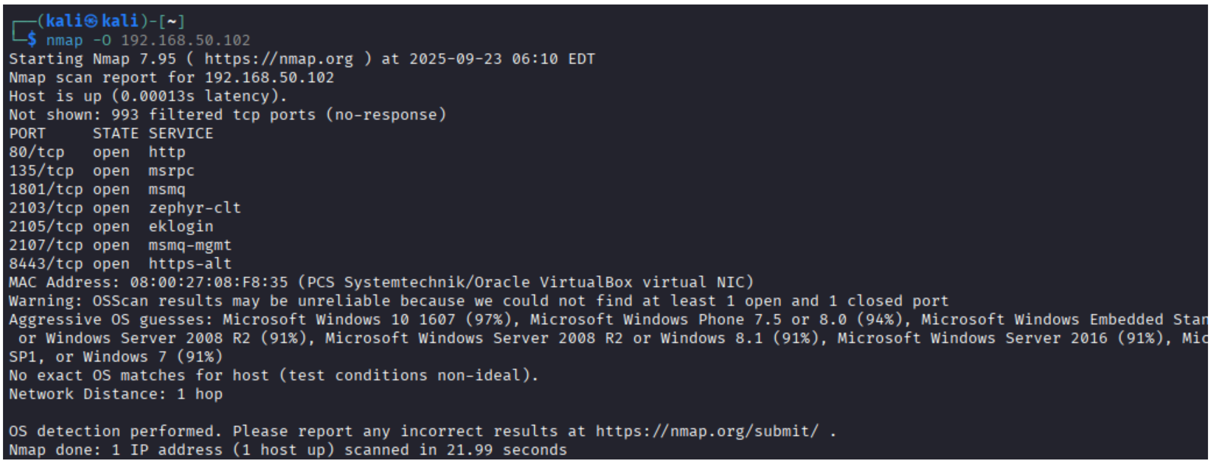
Registrazione

Specificare le impostazioni di registrazione per la risoluzione dei problemi. Personalizza...

OK Annulla Applica

sono andata su windows firewall con sicurezza avanzata poi proprietà di windows firewall e ho disattivato windows firewall.

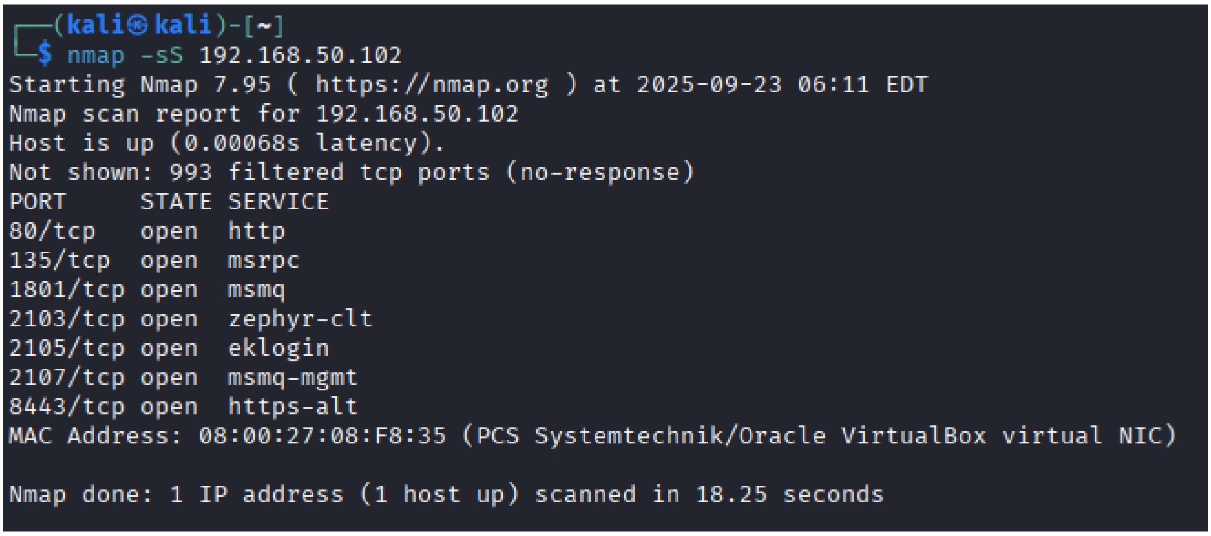
OS fingerprint:



```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 06:10 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00013s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
8443/tcp open  https-alt
MAC Address: 08:00:27:08:F8:35 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 10 1607 (97%), Microsoft Windows Phone 7.5 or 8.0 (94%), Microsoft Windows Embedded Star
 or Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 or Windows 8.1 (91%), Microsoft Windows Server 2016 (91%), Mic
SP1, or Windows 7 (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 21.99 seconds
```

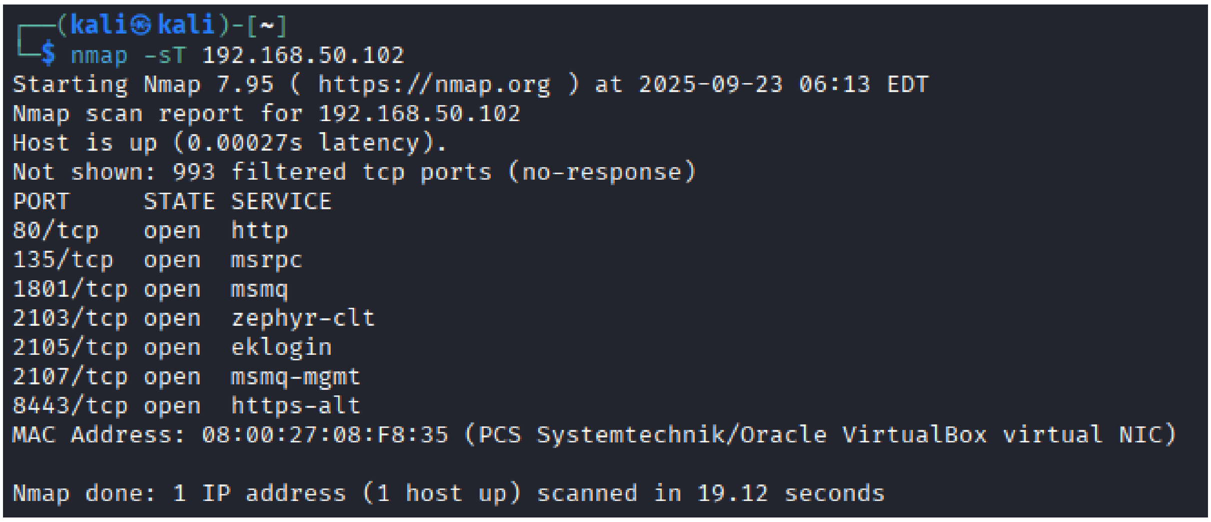
Syn scan:



```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 06:11 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00068s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
8443/tcp open  https-alt
MAC Address: 08:00:27:08:F8:35 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 18.25 seconds
```

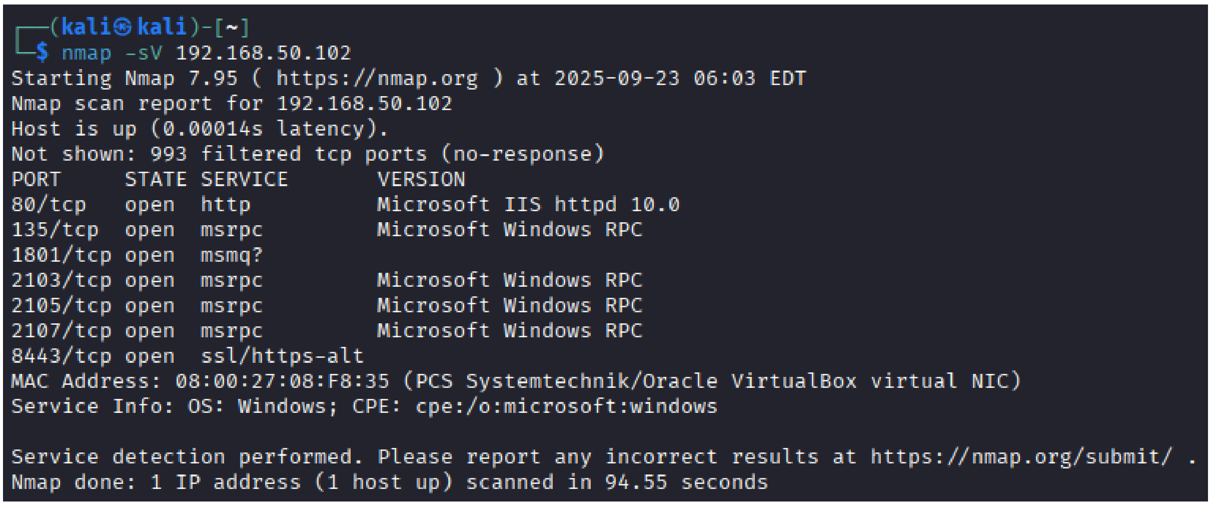
TCP connect:



```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 06:13 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00027s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
8443/tcp open  https-alt
MAC Address: 08:00:27:08:F8:35 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 19.12 seconds
```

Version detection:



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 06:03 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00014s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
135/tcp  open  msrpc         Microsoft Windows RPC
1801/tcp open  msmq?
2103/tcp open  msrpc         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
8443/tcp open  ssl/https-alt
MAC Address: 08:00:27:08:F8:35 (PCS Systemtechnik/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 94.55 seconds
```

Report:

1. Titolo

Scansione Nmap su target Windows — Confronto tra Windows Firewall abilitato e disabilitato

2. SOMMARIO:

Sono state effettuate scansioni Nmap sul target Windows in due condizioni: con Windows Firewall abilitato e con Windows Firewall disabilitato. Le scansioni includono: discovery (ping), TCP SYN scan, UDP scan, detection di versione (-sV) e riconoscimento OS (-O). I risultati mostrano differenze nel comportamento delle porte e nei servizi scoperti tra le due condizioni, con rilevanti implicazioni per la visibilità e la sicurezza del target.

3. Obiettivo

- Valutare come il firewall Windows influisca sui risultati delle scansioni Nmap.
- Documentare le porte aperte/filtrate/chiuse, i servizi rilevati e l’accuratezza del fingerprinting OS/Version detection in entrambe le condizioni.

4. Ambiente di test

- Target: IP 192.168.50.102

- Sistema operativo target: Windows 10
- Rete: laboratorio virtual box
- Strumento: Nmap

---

5. Comandi eseguiti

comando: nmap -O <target>

-O: abilita la OS detection rilevazione del sistema operativo

comando: nmap nmap -sS <target>

Syn scan: scansione più veloce non completa il 3 way handshake la connessione rimane half open

comando: nmap -sT <target>

TCP connect scansione che stabilisce una connessione tcp completa, il 3 way handshake viene completato scansione più facile da rilevare nei log.

comando: nmap -sV <target>

version detection: nmap prova a parlare con le porte aperte per capire quale servizio è in esecuzione e la sua versione.

Verifica stato firewall abilitato/disabilitato

come possiamo vedere dagli screenshot quando il firewall abilitato le porte trovate aperte e servizi trovati sono di più rispetto a quando il firewall è disabilitato.

osservazione: scusa valerio ma i risultati non dovrebbero essere diversi nel senso che quando il firewall è abilitato si dovrebbero trovare meno cose perchè il firewall filtra le porte ecc mentre quando era disabilitato si trovavano meno cose, boh non lo in caso spiegamelo nelle note della correzione.