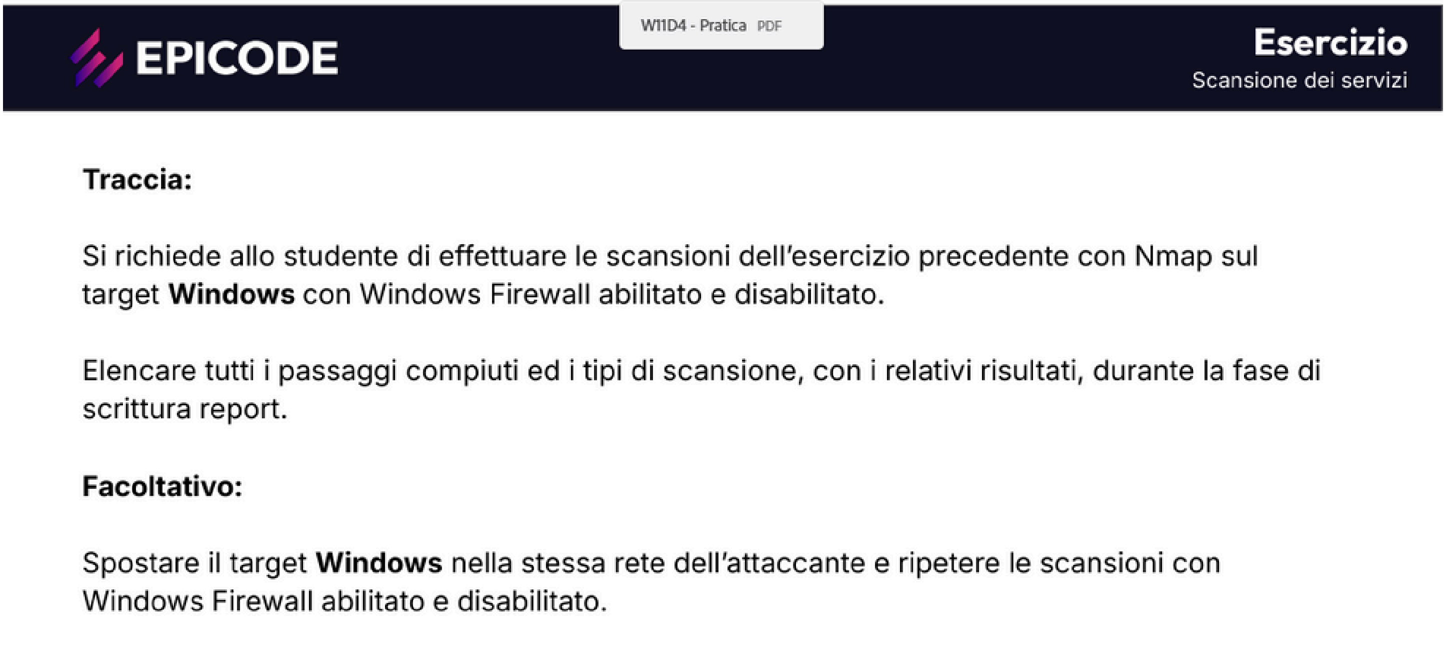
Traccia



W11D4 - Pratica PDF

EPICODE

Esercizio
Scansione dei servizi

Traccia:

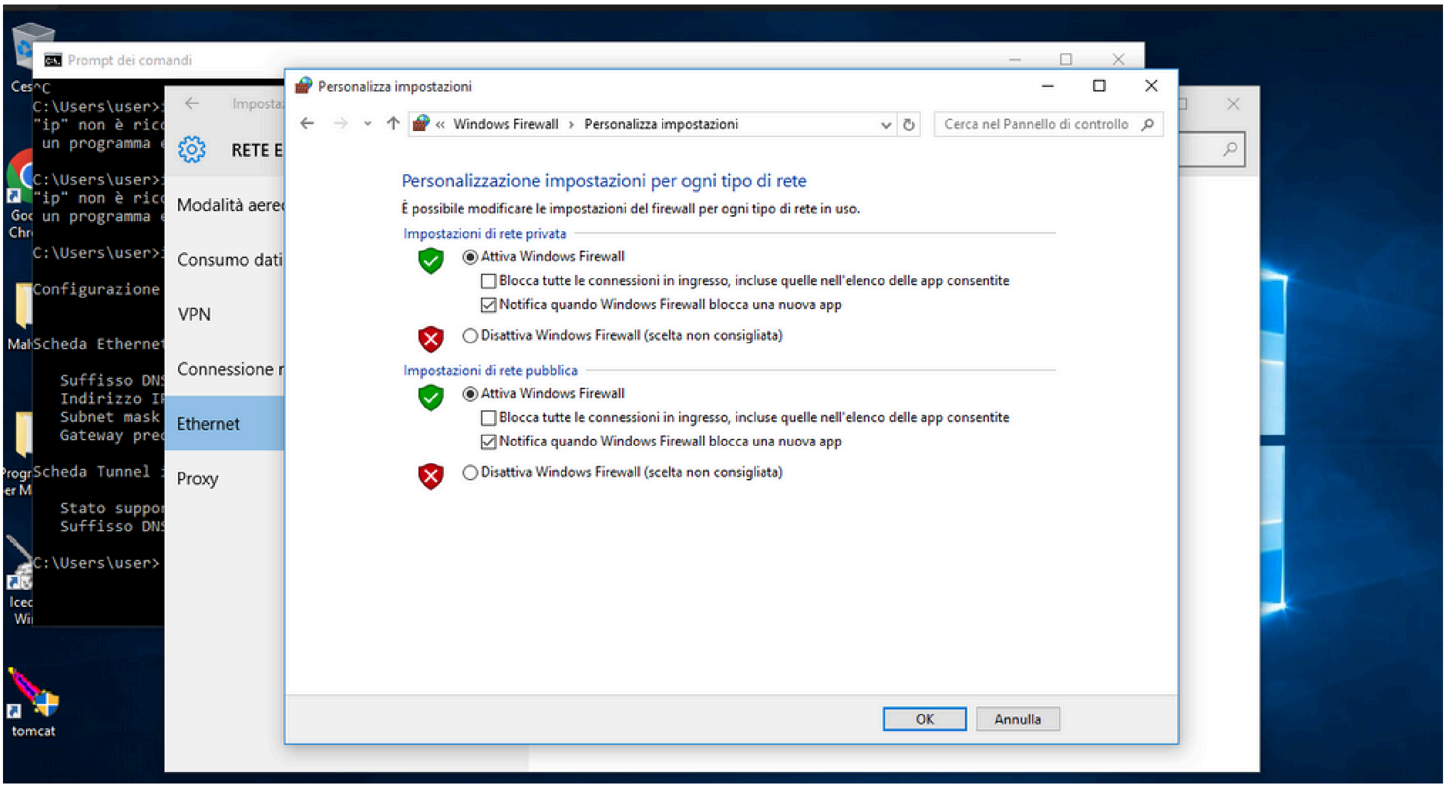
Si richiede allo studente di effettuare le scansioni dell'esercizio precedente con Nmap sul target **Windows** con Windows Firewall abilitato e disabilitato.

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

Facoltativo:

Spostare il target **Windows** nella stessa rete dell'attaccante e ripetere le scansioni con Windows Firewall abilitato e disabilitato.

verifichiamo lo stato del firewall



Personalizza impostazioni

Windows Firewall › Personalizza impostazioni

Personalizzazione impostazioni per ogni tipo di rete

È possibile modificare le impostazioni del firewall per ogni tipo di rete in uso.

Impostazioni di rete privata

● Attiva Windows Firewall

□ Blocca tutte le connessioni in ingresso, incluse quelle nell'elenco delle app consentite

☑ Notifica quando Windows Firewall blocca una nuova app

○ Disattiva Windows Firewall (scelta non consigliata)

Impostazioni di rete pubblica

● Attiva Windows Firewall

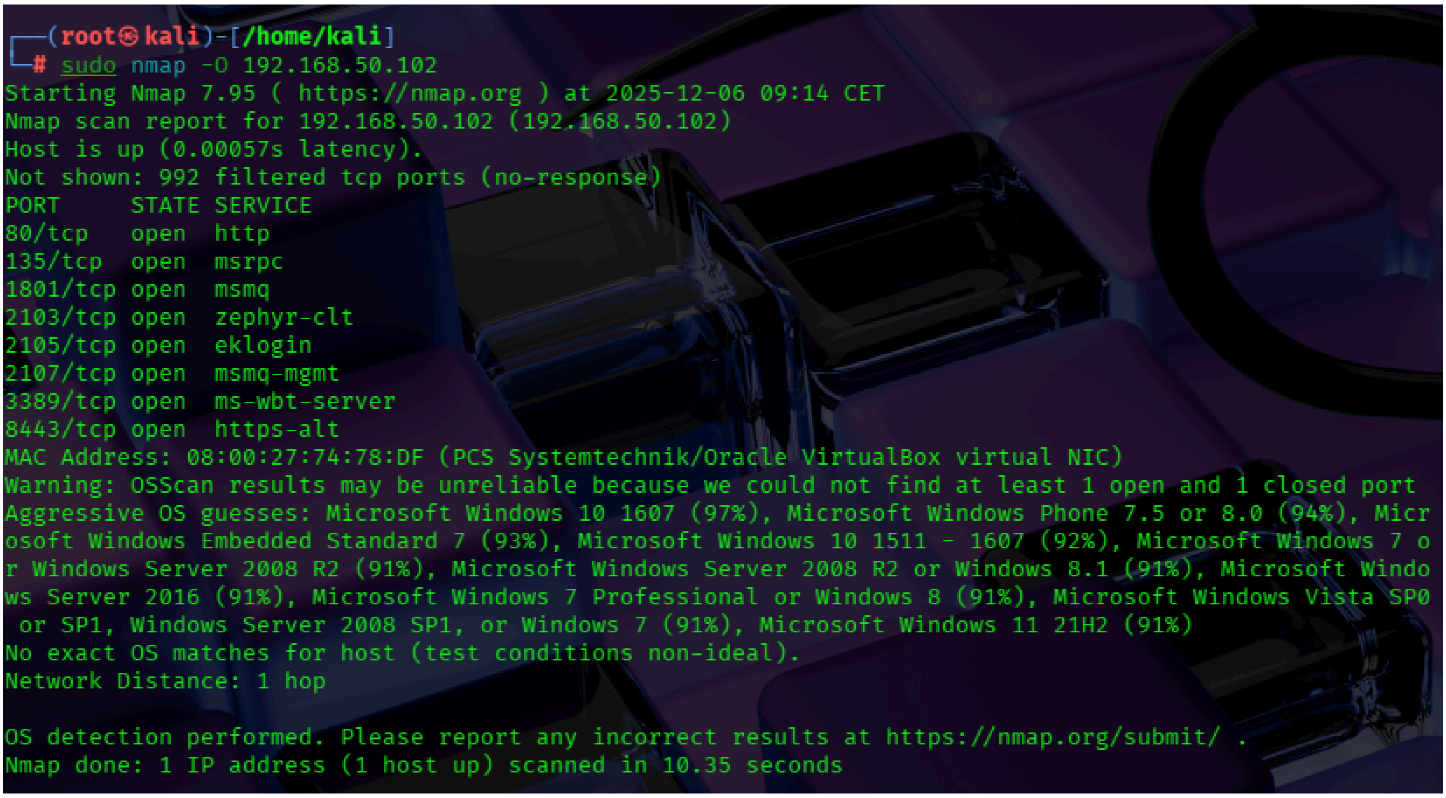
□ Blocca tutte le connessioni in ingresso, incluse quelle nell'elenco delle app consentite

☑ Notifica quando Windows Firewall blocca una nuova app

○ Disattiva Windows Firewall (scelta non consigliata)

Il firewall risulta attivo, iniziamo ad utilizzare i nostri comandi, nel report verranno susseguiti screen dei risultati prima con firewall on e successivamente con firewall off

scansione target FW ON OSfingerprint



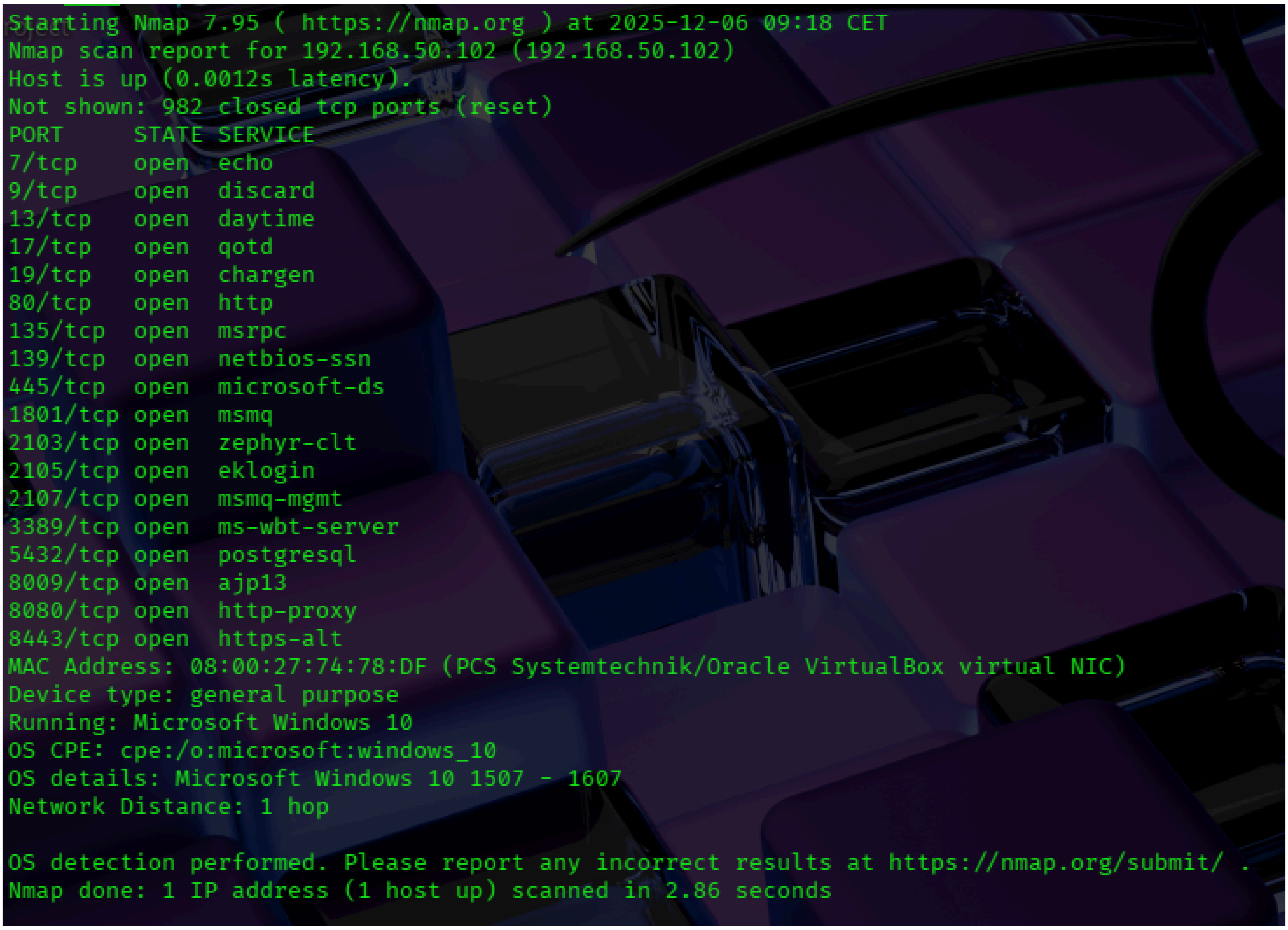
```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -O 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 09:14 CET
Nmap scan report for 192.168.50.102 (192.168.50.102)
Host is up (0.00057s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3389/tcp open  ms-wbt-server
8443/tcp open  https-alt
MAC Address: 08:00:27:74:78:DF (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%), Micr
osoft Windows Embedded Standard 7 (93%), Microsoft Windows 10 1511 - 1607 (92%), Microsoft Windows 7 o
r Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 or Windows 8.1 (91%), Microsoft Windo
ws Server 2016 (91%), Microsoft Windows 7 Professional or Windows 8 (91%), Microsoft Windows Vista SP0
 or SP1, Windows Server 2008 SP1, or Windows 7 (91%), Microsoft Windows 11 21H2 (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 10.35 seconds
```

risultato: host risponde e ha porte aperte tipiche Windows aperte

Nmap pensa che sia **Windows 10** (probabilità 97%) , ma non è completamente sicuro

scansione target FW OFF OSfingerprint

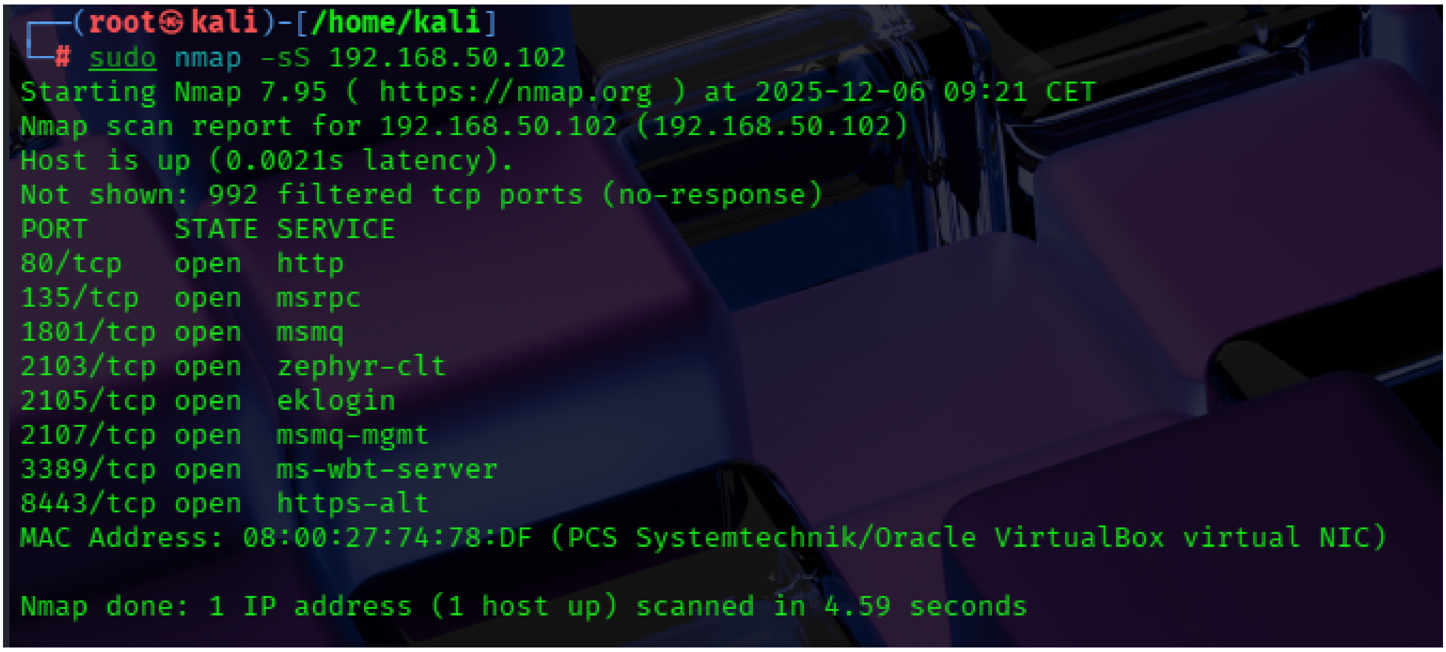


```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 09:18 CET
Nmap scan report for 192.168.50.102 (192.168.50.102)
Host is up (0.0012s latency).
Not shown: 982 closed tcp ports (reset)
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   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: 08:00:27:74:78:DF (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 2.86 seconds
```

risultato: notiamo subito una scnasione più rapida, molte più porte aperte visibili e la sicurezza del sistema operativo (windows 10 range 1507 - 1067) il che ci permetterà di sfruttare vulnerabilità note

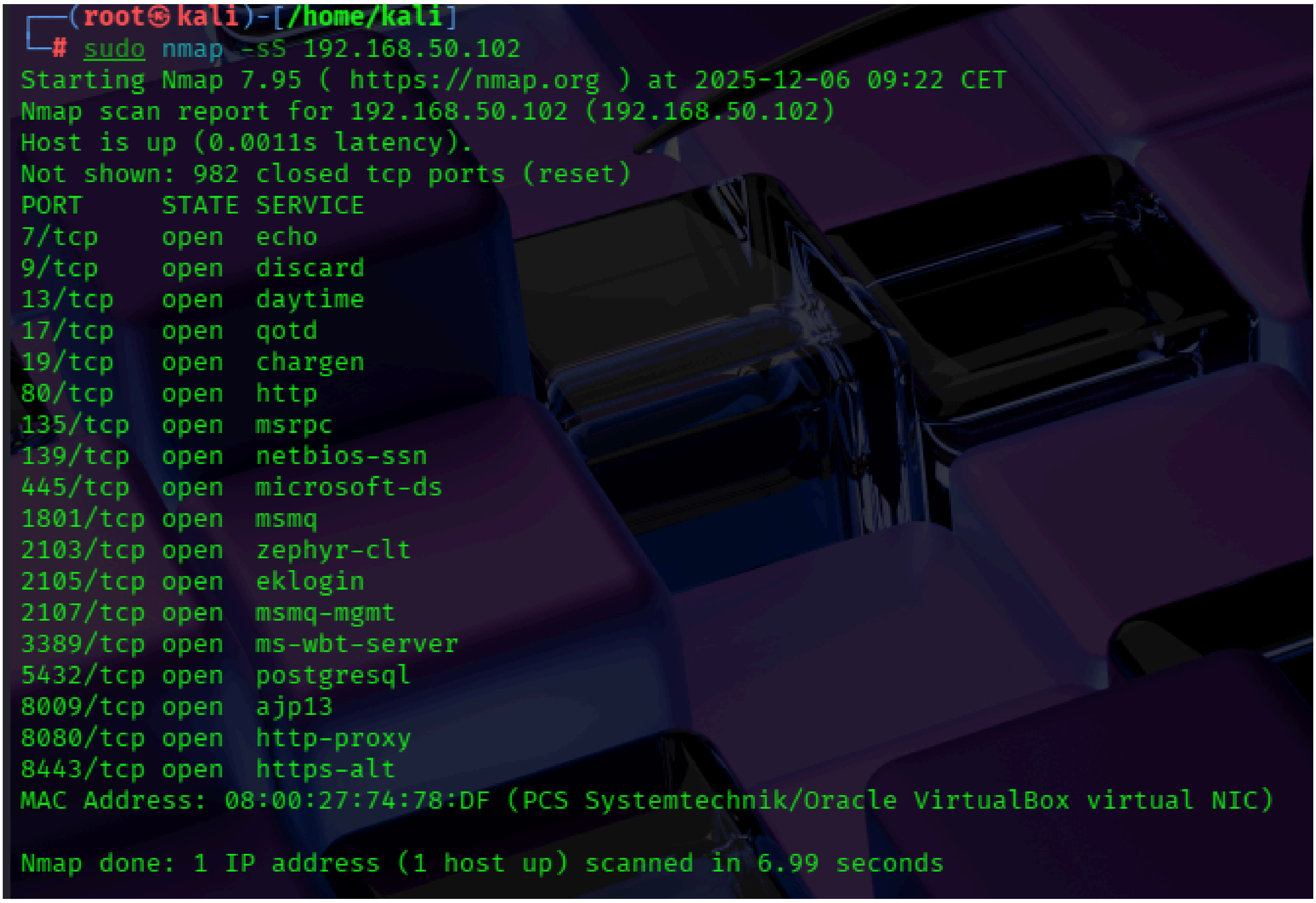
SYN/SCAN target FW ON



```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sS 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 09:21 CET
Nmap scan report for 192.168.50.102 (192.168.50.102)
Host is up (0.0021s latency).
Not shown: 992 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
3389/tcp open  ms-wbt-server
8443/tcp open  https-alt
MAC Address: 08:00:27:74:78:DF (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.59 seconds
```

SYN/SCAN target FW OFF

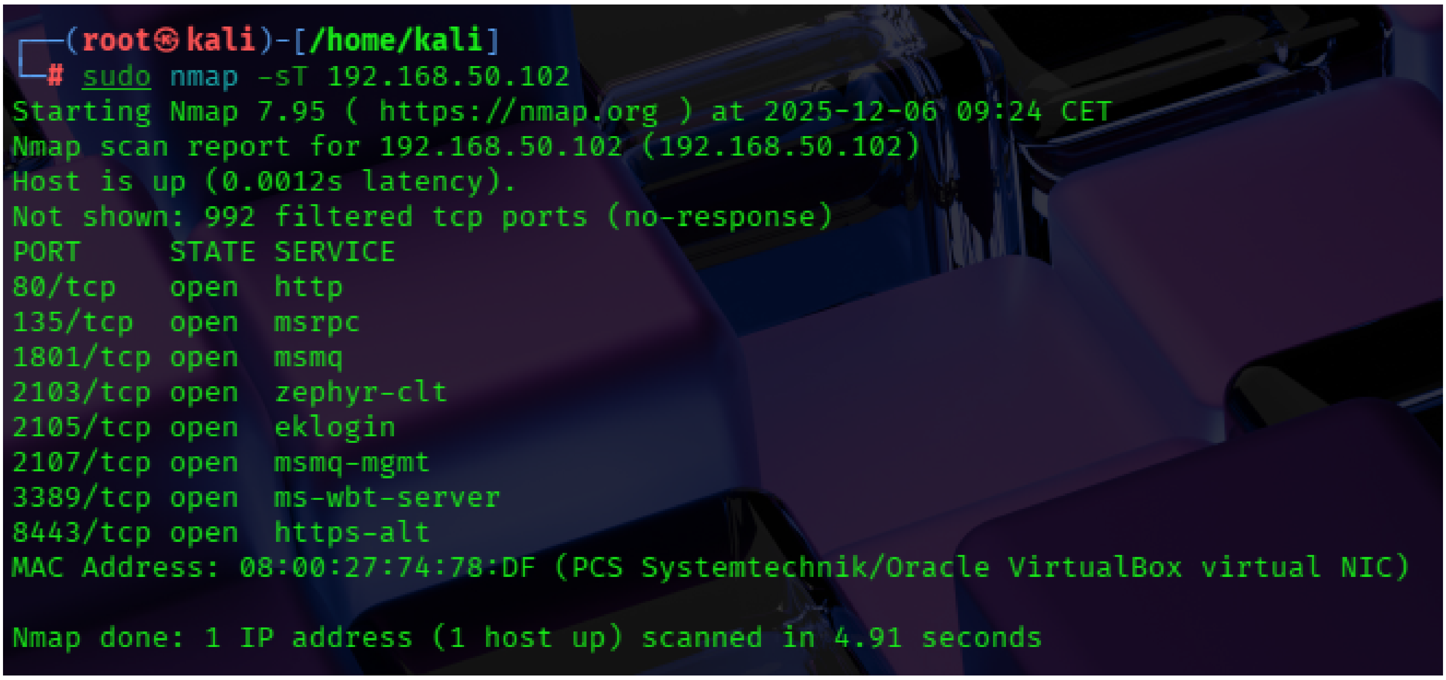


```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sS 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 09:22 CET
Nmap scan report for 192.168.50.102 (192.168.50.102)
Host is up (0.0011s latency).
Not shown: 982 closed tcp ports (reset)
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    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: 08:00:27:74:78:DF (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.99 seconds
```

Risultato: anche in questo caso la differenza principale sta nel numero di porte aperte individuate, procediamo ora con un tentativo più invasivo, il tcp scan

TCP/SCAN target FW ON

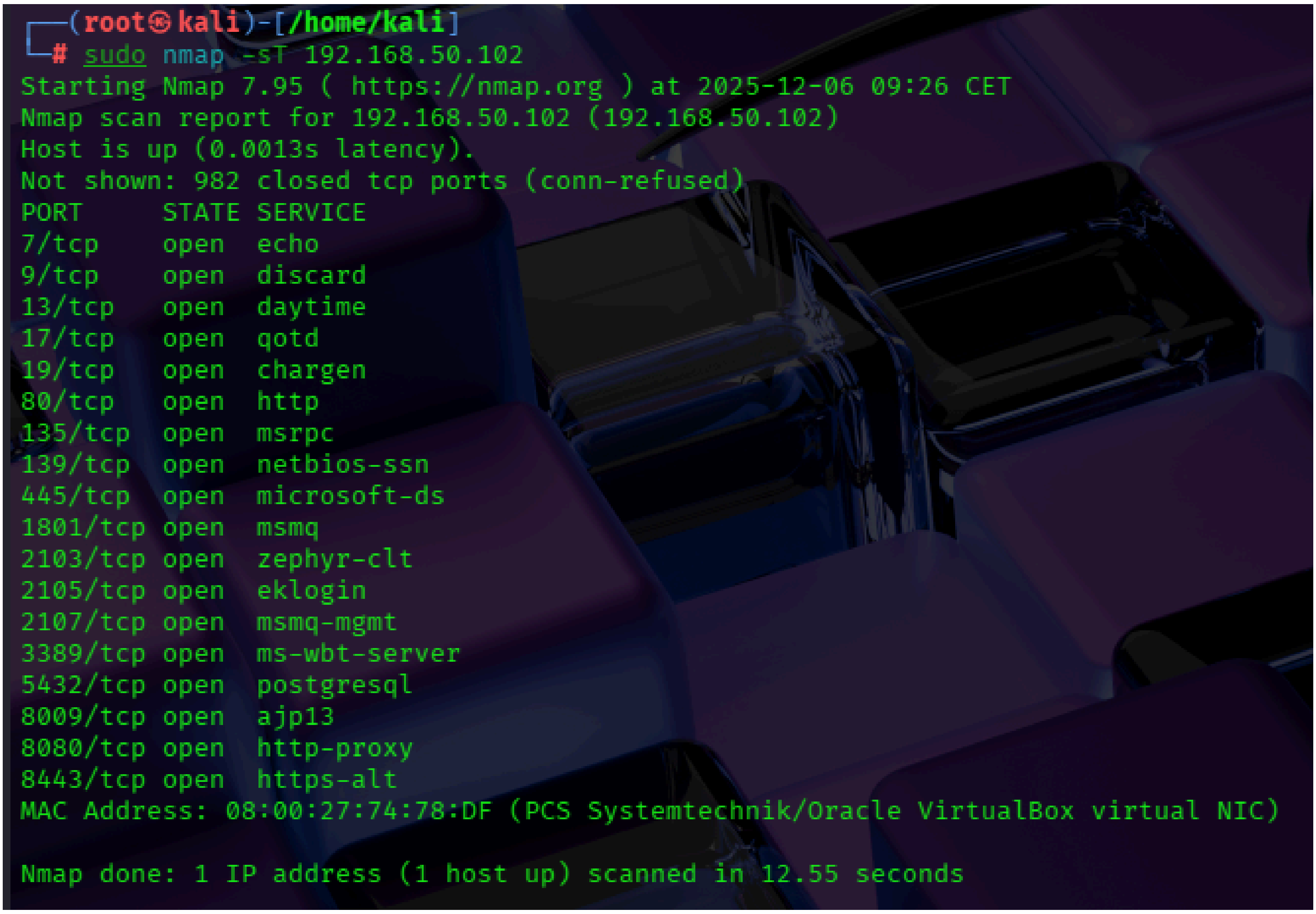


```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sT 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 09:24 CET
Nmap scan report for 192.168.50.102 (192.168.50.102)
Host is up (0.0012s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3389/tcp open  ms-wbt-server
8443/tcp open  https-alt
MAC Address: 08:00:27:74:78:DF (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.91 seconds
```

risultato: con il firewall abilitato il risultato è stato uguale, quindi abbiamo aumentato inutilmente il rischio di essere individuati, ripetiamo a FW off

TCP/SCAN target FW OFF



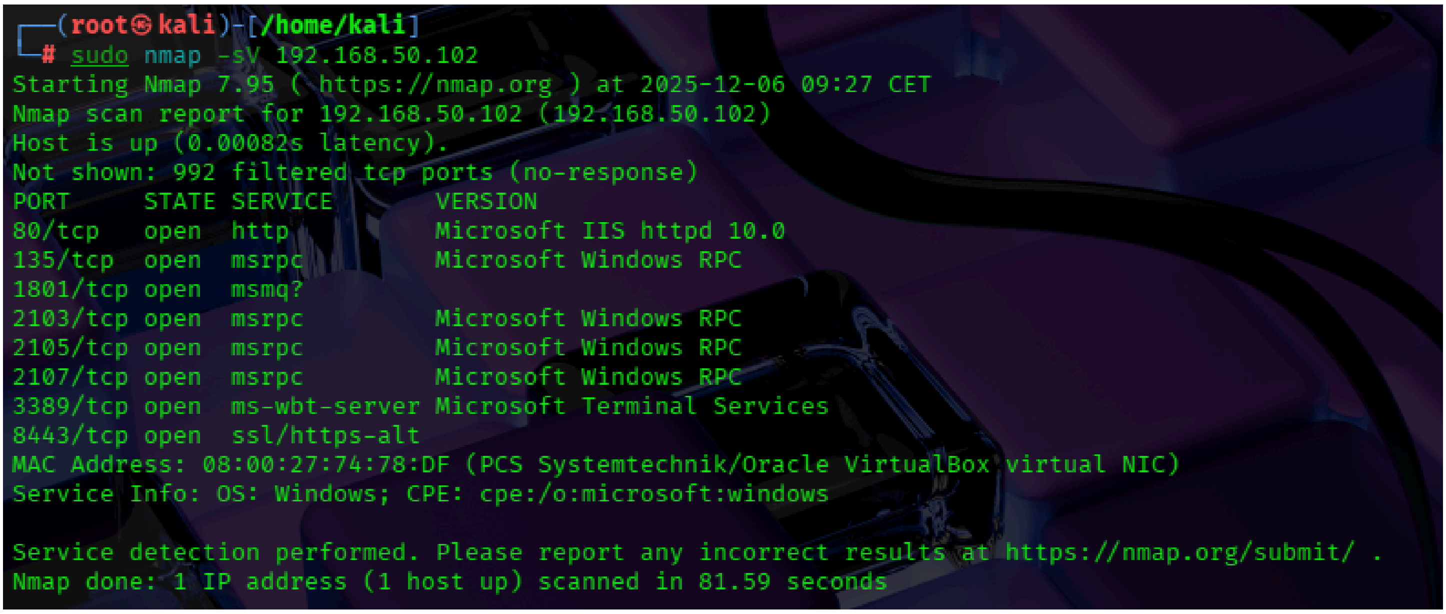
```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sT 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 09:26 CET
Nmap scan report for 192.168.50.102 (192.168.50.102)
Host is up (0.0013s latency).
Not shown: 982 closed tcp ports (conn-refused)
PORT     STATE SERVICE
7/tcp    open  echo
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: 08:00:27:74:78:DF (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 12.55 seconds
```

risultato: anche in questo caso non ci sono differenze tra SYN e TCP scan

Version Detection target FW ON

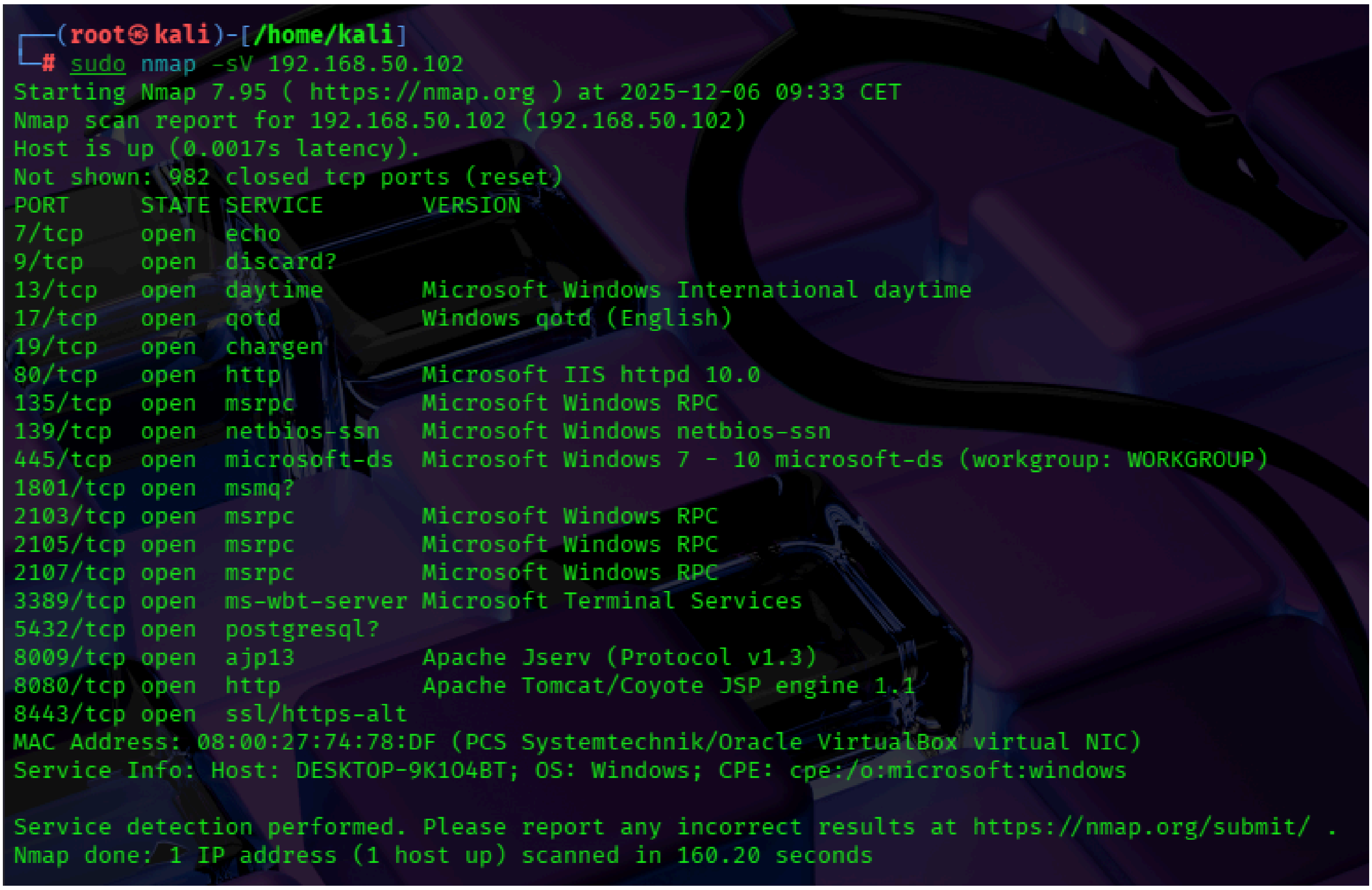
processo quasi infinito, interrotto manualmente



```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sV 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 09:27 CET
Nmap scan report for 192.168.50.102 (192.168.50.102)
Host is up (0.00082s latency).
Not shown: 992 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
3389/tcp open  ms-wbt-server Microsoft Terminal Services
8443/tcp open  ssl/https-alt
MAC Address: 08:00:27:74:78:DF (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 81.59 seconds
```

Version Detection target FW OFF



```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sV 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 09:33 CET
Nmap scan report for 192.168.50.102 (192.168.50.102)
Host is up (0.0017s 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: 08:00:27:74:78:DF (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-9K1O4BT; 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 160.20 seconds
```