W11D4 – Pratica

Epic Education Srl

Scansione dei servizi con Nmap pt. 2

(target Windows 10 pro)

Simone Giordano

22/09/2025

Contatti:

Tel: 3280063044
Email: mynameisimone@gmail.com
Linkedin: https://www.linkedin.com/in/simone-giordano-91290652/

Sommario

Sintesi esecutiva

Questo documento riporta i risultati di 5 scansioni diverse con NMAP, da Kali (attaccante) a Windows (target) prima con il firewall NON attivo e dopo con il firewall attivo.
Gli stessi test sono stati eseguiti prima con le due macchine situate su due reti diverse e pfSense per metterle in comunicazione e poi con le due macchine all'interno della stessa rete.

In entrambe le configurazioni di rete, il firewall ha impedito il rilevamento di 11 porte e ha triplicato in media i tempi di scansione.

Perimetro

Il target prefissato è la macchina virtuale Windows, situata prima su una rete diversa 192.168.52.0/24 e poi sulla stessa rete della macchina attaccante 192.168.50.0/24.

Panoramica delle vulnerabilità

Elenco porte rilevate con e senza firewall

No firewall	Firewall	Service
7		echo
9		discard
13		daytime
17		qotd
19		chargen
80	80	http
135	135	msrpc
139		metbios-ssn
445		microsoft-ds
1801	1801	msmq
2103	2103	zephyr-clt
2105	2105	eklogin
2107	2107	msmq-mgmt
3389		ms-wbt-server
5432		postgresql
8009		ajp13
8080		http-proxy
8443	8443	https-alt

1 Tecniche di scansione con Nmap su reti diverse

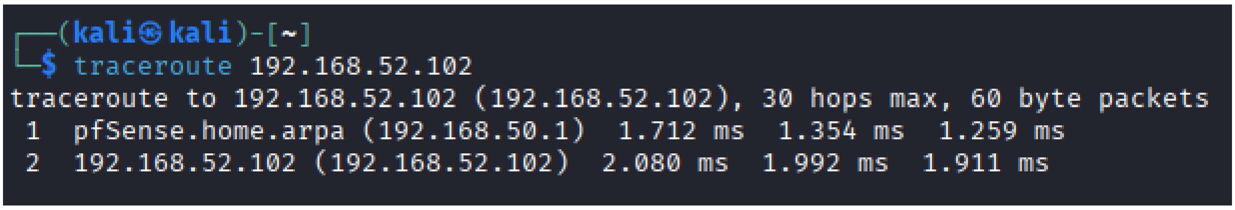
1.1 Configurazione di rete

Kali: 192.168.50.101

Windows: 192.168.52.102

pfSense: configurato con 2 reti interne per le due VM sopra citate e una rete con bridge.

Ognuna delle scansioni verrà eseguita sul target Windows, prima con il firewall disattivato e poi con il firewall attivo.

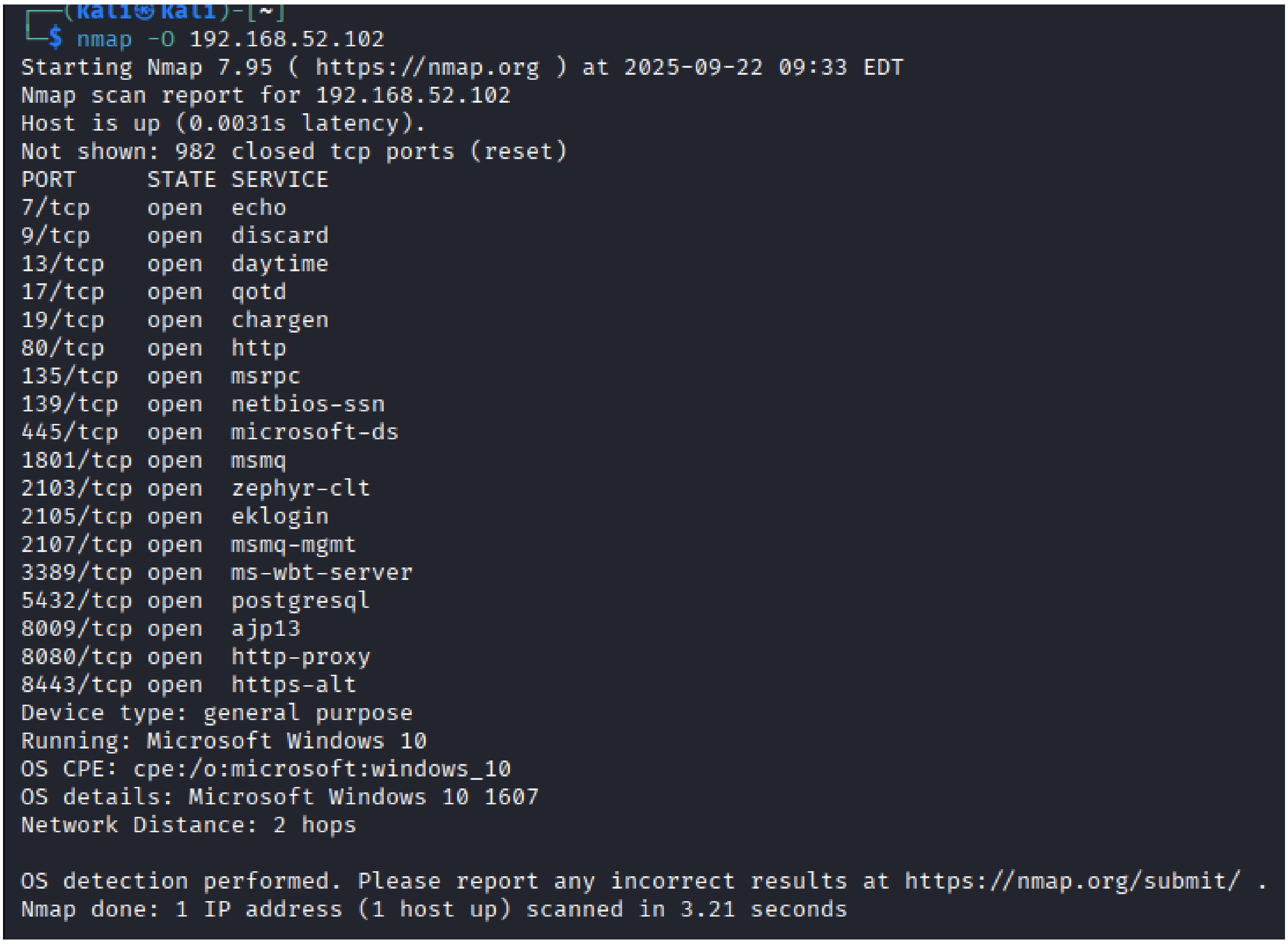


```
┌──(kali㉿kali)-[~]
└─$ traceroute 192.168.52.102
traceroute to 192.168.52.102 (192.168.52.102), 30 hops max, 60 byte packets
 1  pfSense.home.arpa (192.168.50.1)  1.712 ms  1.354 ms  1.259 ms
 2  192.168.52.102 (192.168.52.102)  2.080 ms  1.992 ms  1.911 ms
```

1.2 OS fingerprint

nmap -O 192.168.52.102

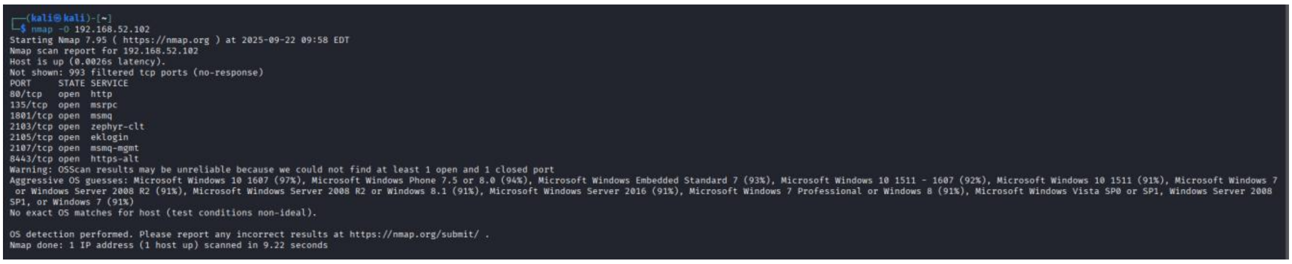
Firewall disattivato



```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.52.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 09:33 EDT
Nmap scan report for 192.168.52.102
Host is up (0.0031s 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
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1607
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 3.21 seconds
```

Firewall attivo



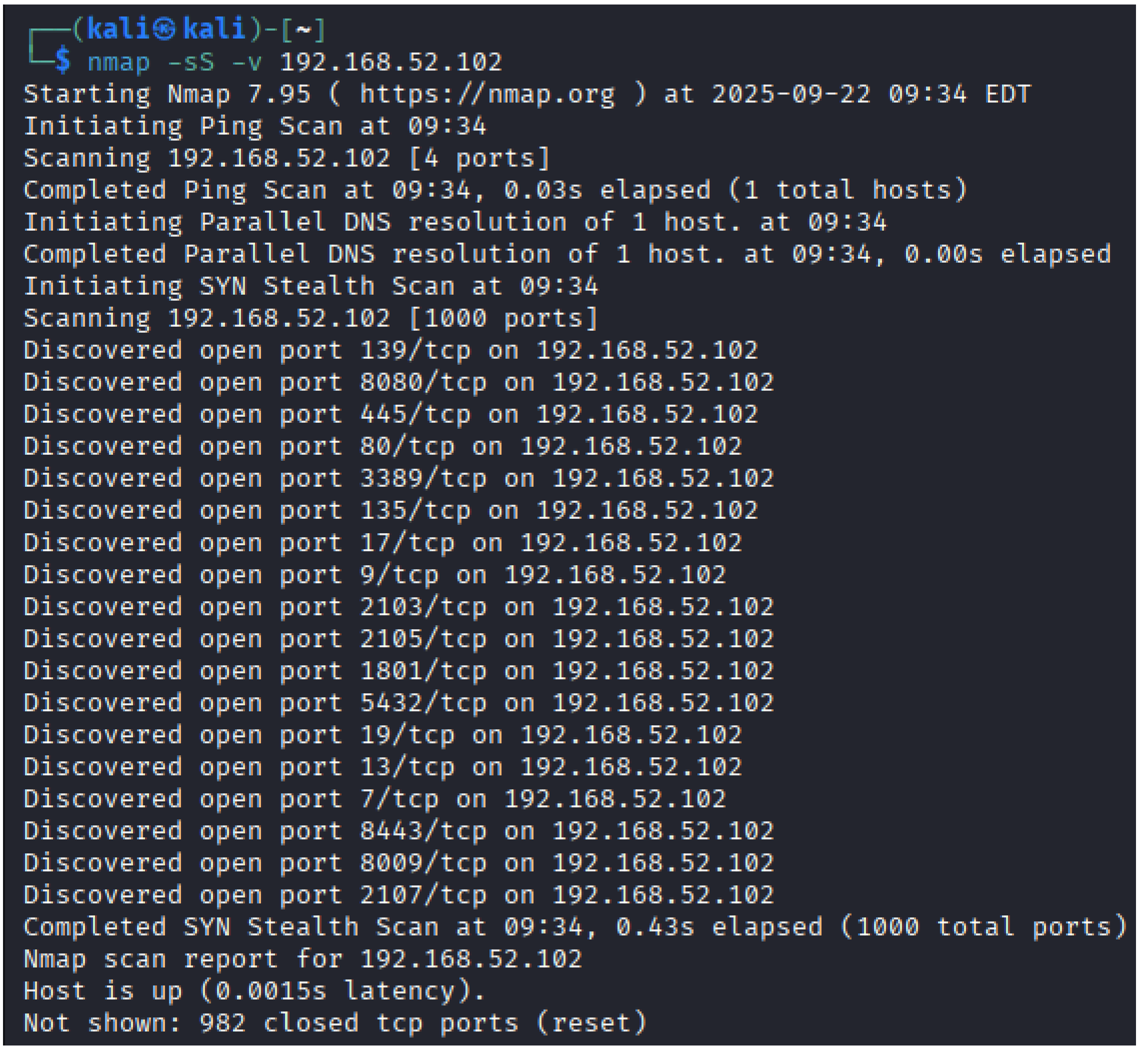
```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.52.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 09:58 EDT
Nmap scan report for 192.168.52.102
Host is up (0.0026s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
8443/tcp open  https-alt
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 Standard 7 (93%), Microsoft Windows 10 1511 - 1607 (92%), Microsoft Windows 10 1511 (91%), Microsoft Windows 7
 or Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 or Windows 8.1 (91%), Microsoft Windows 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%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.22 seconds
```

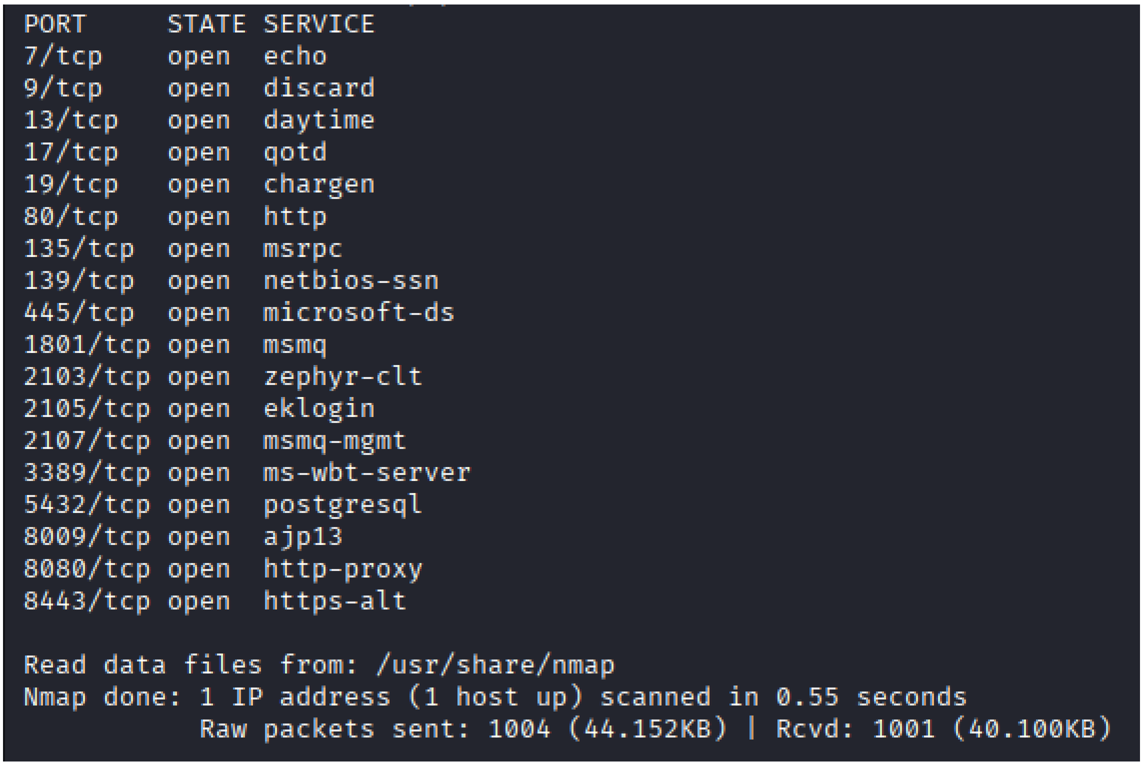
1.3 Syn scan

nmap -sS -v 192.168.52.102

Firewall disattivato



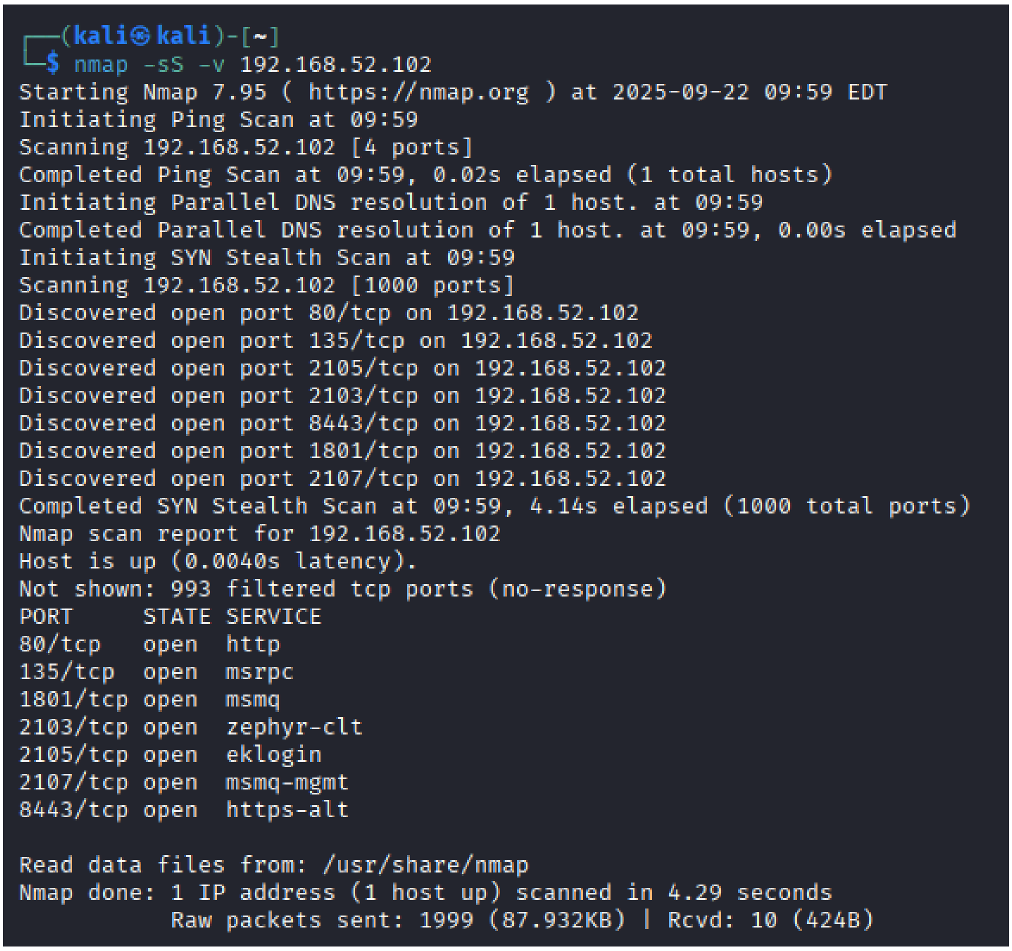
```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -v 192.168.52.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 09:34 EDT
Initiating Ping Scan at 09:34
Scanning 192.168.52.102 [4 ports]
Completed Ping Scan at 09:34, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:34
Completed Parallel DNS resolution of 1 host. at 09:34, 0.00s elapsed
Initiating SYN Stealth Scan at 09:34
Scanning 192.168.52.102 [1000 ports]
Discovered open port 139/tcp on 192.168.52.102
Discovered open port 8080/tcp on 192.168.52.102
Discovered open port 445/tcp on 192.168.52.102
Discovered open port 80/tcp on 192.168.52.102
Discovered open port 3389/tcp on 192.168.52.102
Discovered open port 135/tcp on 192.168.52.102
Discovered open port 17/tcp on 192.168.52.102
Discovered open port 9/tcp on 192.168.52.102
Discovered open port 2103/tcp on 192.168.52.102
Discovered open port 2105/tcp on 192.168.52.102
Discovered open port 1801/tcp on 192.168.52.102
Discovered open port 5432/tcp on 192.168.52.102
Discovered open port 19/tcp on 192.168.52.102
Discovered open port 13/tcp on 192.168.52.102
Discovered open port 7/tcp on 192.168.52.102
Discovered open port 8443/tcp on 192.168.52.102
Discovered open port 8009/tcp on 192.168.52.102
Discovered open port 2107/tcp on 192.168.52.102
Completed SYN Stealth Scan at 09:34, 0.43s elapsed (1000 total ports)
Nmap scan report for 192.168.52.102
Host is up (0.0015s 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

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds
           Raw packets sent: 1004 (44.152KB) | Rcvd: 1001 (40.100KB)
```

Firewall attivo



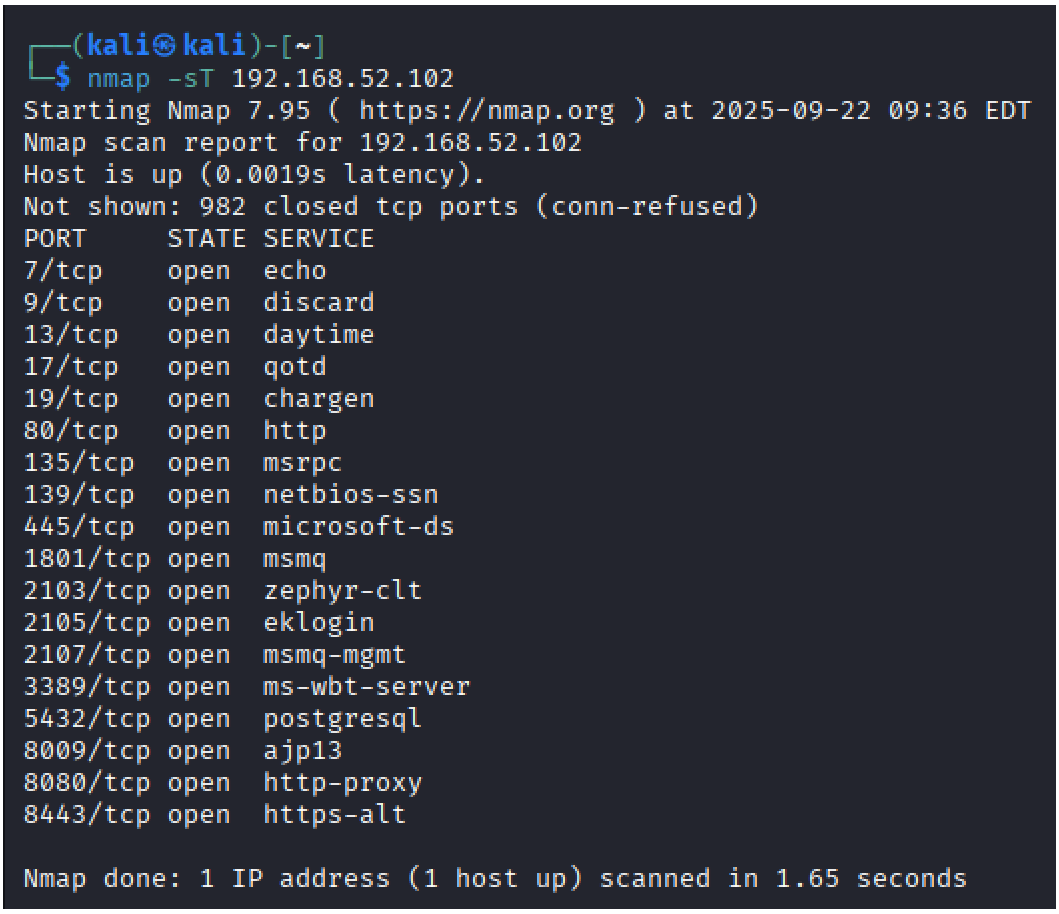
```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -v 192.168.52.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 09:59 EDT
Initiating Ping Scan at 09:59
Scanning 192.168.52.102 [4 ports]
Completed Ping Scan at 09:59, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:59
Completed Parallel DNS resolution of 1 host. at 09:59, 0.00s elapsed
Initiating SYN Stealth Scan at 09:59
Scanning 192.168.52.102 [1000 ports]
Discovered open port 80/tcp on 192.168.52.102
Discovered open port 135/tcp on 192.168.52.102
Discovered open port 2105/tcp on 192.168.52.102
Discovered open port 2103/tcp on 192.168.52.102
Discovered open port 8443/tcp on 192.168.52.102
Discovered open port 1801/tcp on 192.168.52.102
Discovered open port 2107/tcp on 192.168.52.102
Completed SYN Stealth Scan at 09:59, 4.14s elapsed (1000 total ports)
Nmap scan report for 192.168.52.102
Host is up (0.0040s 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

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.29 seconds
           Raw packets sent: 1999 (87.932KB) | Rcvd: 10 (424B)
```

1.4 TCP connect

nmap -sT 192.168.52.102

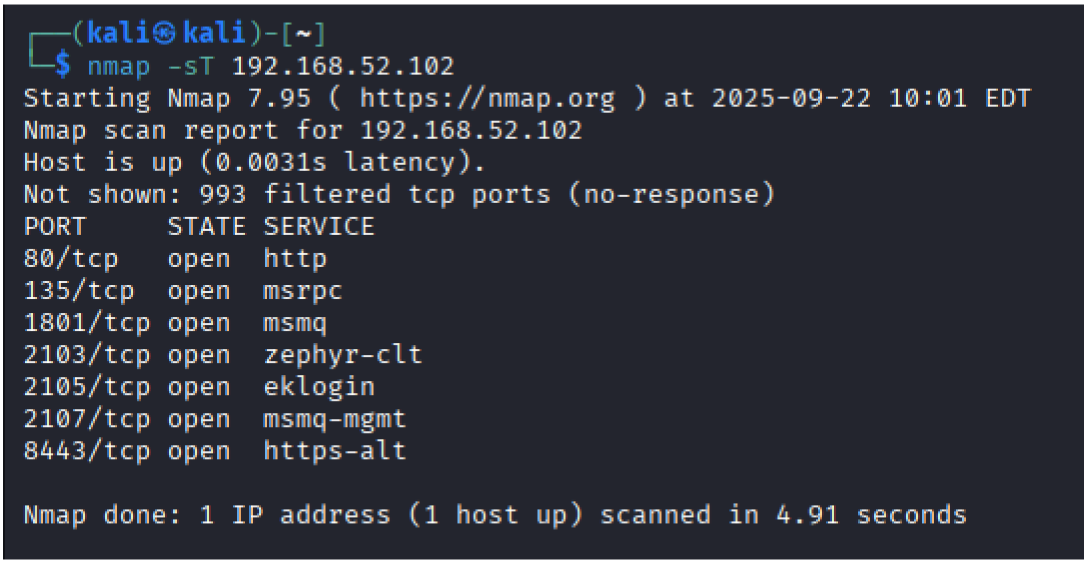
Firewall disattivato



```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.52.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 09:36 EDT
Nmap scan report for 192.168.52.102
Host is up (0.0019s 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

Nmap done: 1 IP address (1 host up) scanned in 1.65 seconds
```

Firewall attivo



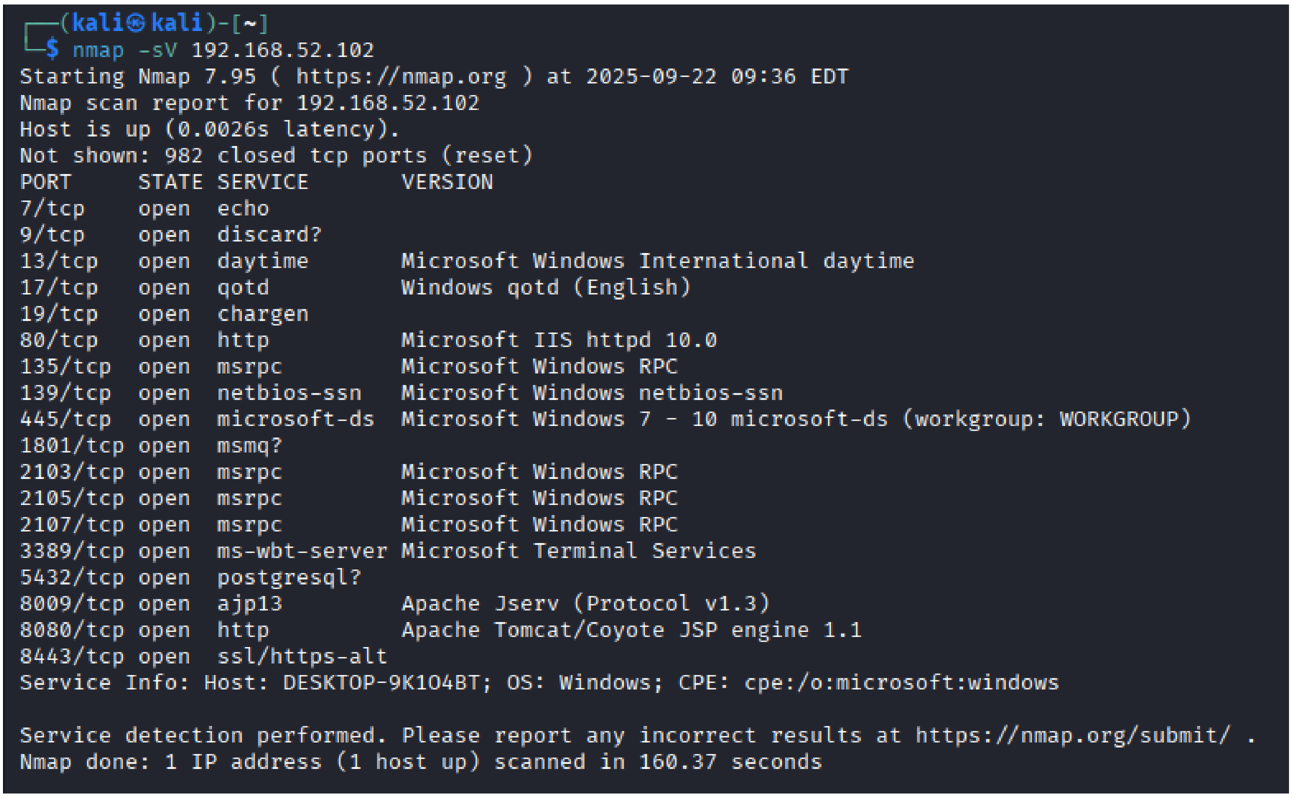
```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.52.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 10:01 EDT
Nmap scan report for 192.168.52.102
Host is up (0.0031s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
8443/tcp open  https-alt

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

1.5 Version detection

nmap -sV 192.168.52.102

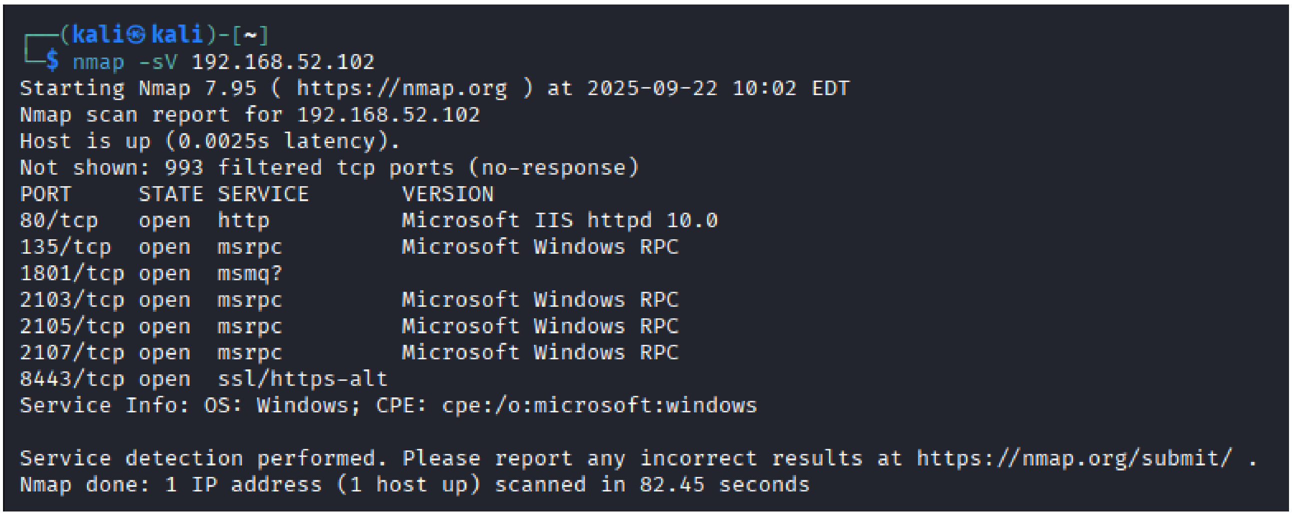
Firewall disattivato



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.52.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 09:36 EDT
Nmap scan report for 192.168.52.102
Host is up (0.0026s 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
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 160.37 seconds
```

Firewall attivo



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.52.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 10:02 EDT
Nmap scan report for 192.168.52.102
Host is up (0.0025s 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
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 82.45 seconds
```

2 Tecniche di scansione con Nmap sulla stessa rete

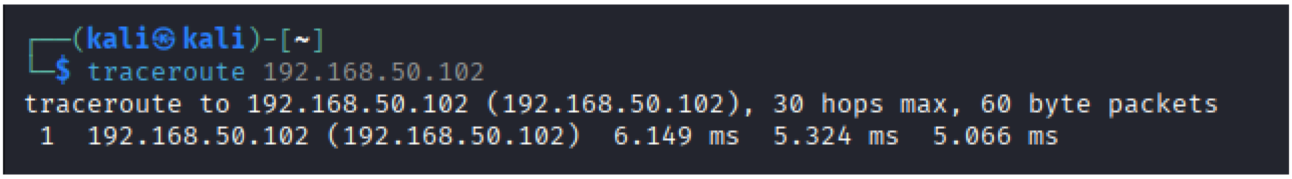
2.1 Configurazione di rete

Kali: 192.168.50.101

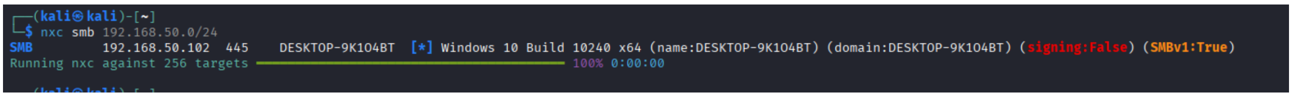
Windows: 192.168.50.102

Le due macchine stanno sulla stessa rete 192.168.50.0/24

Ognuna delle scansioni verrà eseguita sul target Windows, prima con il firewall disattivato e poi con il firewall attivo.



```
┌──(kali㉿kali)-[~]
└─$ traceroute 192.168.50.102
traceroute to 192.168.50.102 (192.168.50.102), 30 hops max, 60 byte packets
 1  192.168.50.102 (192.168.50.102)  6.149 ms  5.324 ms  5.066 ms
```

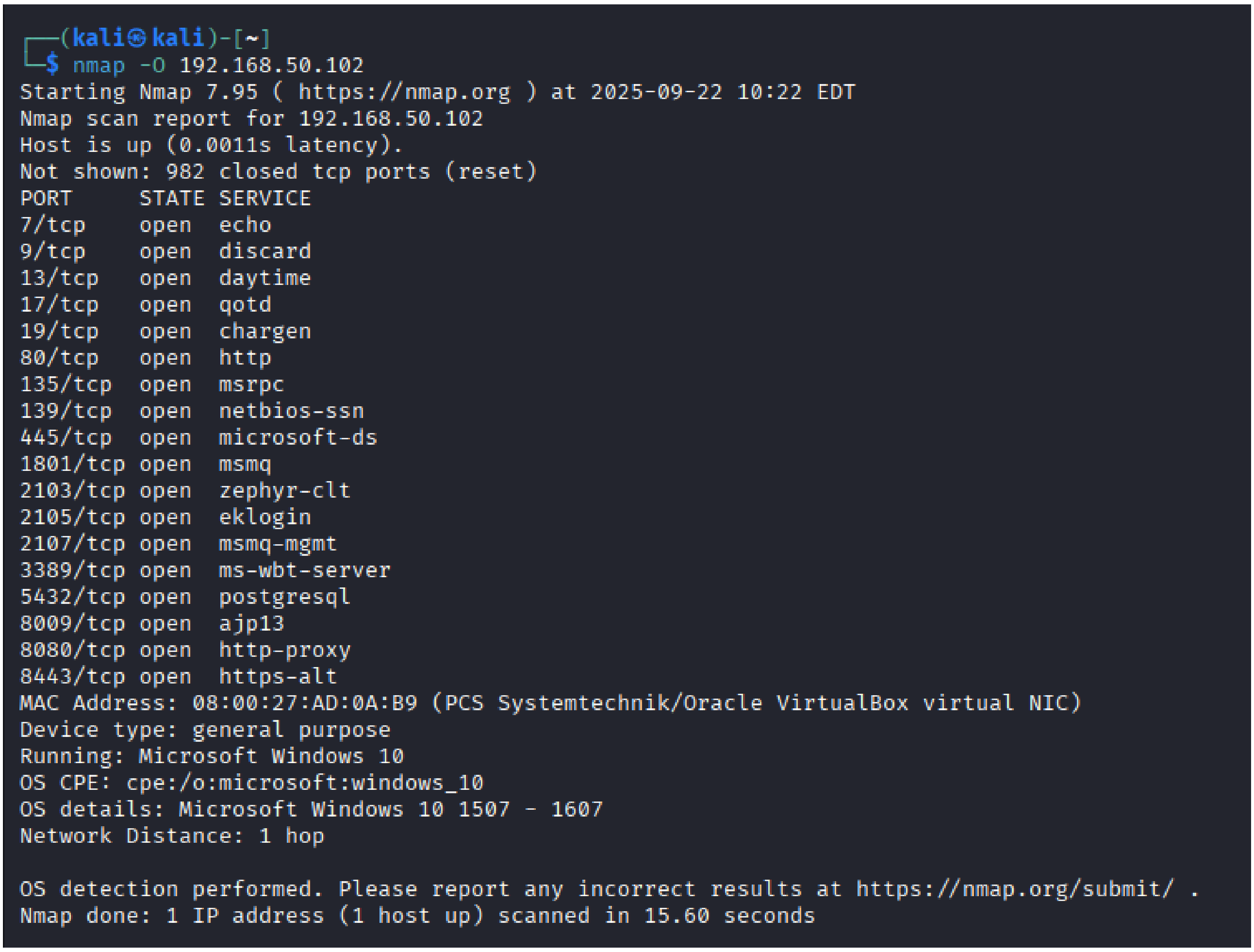


```
┌──(kali㉿kali)-[~]
└─$ nxc smb 192.168.50.0/24
SMB         192.168.50.102  445    DESKTOP-9K1O4BT  [*] Windows 10 Build 10240 x64 (name:DESKTOP-9K1O4BT) (domain:DESKTOP-9K1O4BT) (signing:False) (SMBv1:True)
Running nxc against 256 targets ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 100% 0:00:00
```

2.2 OS fingerprint

nmap -O 192.168.50.102

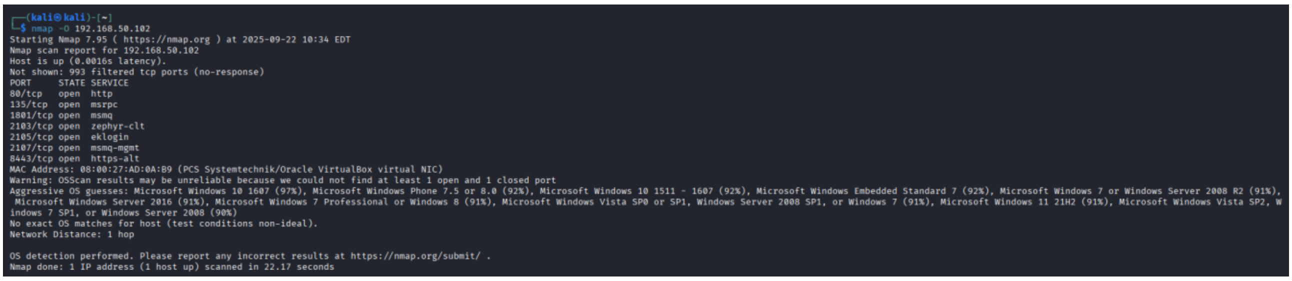
Firewall disattivato



```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 10:22 EDT
Nmap scan report for 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:AD:0A:B9 (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 15.60 seconds
```

Firewall attivo



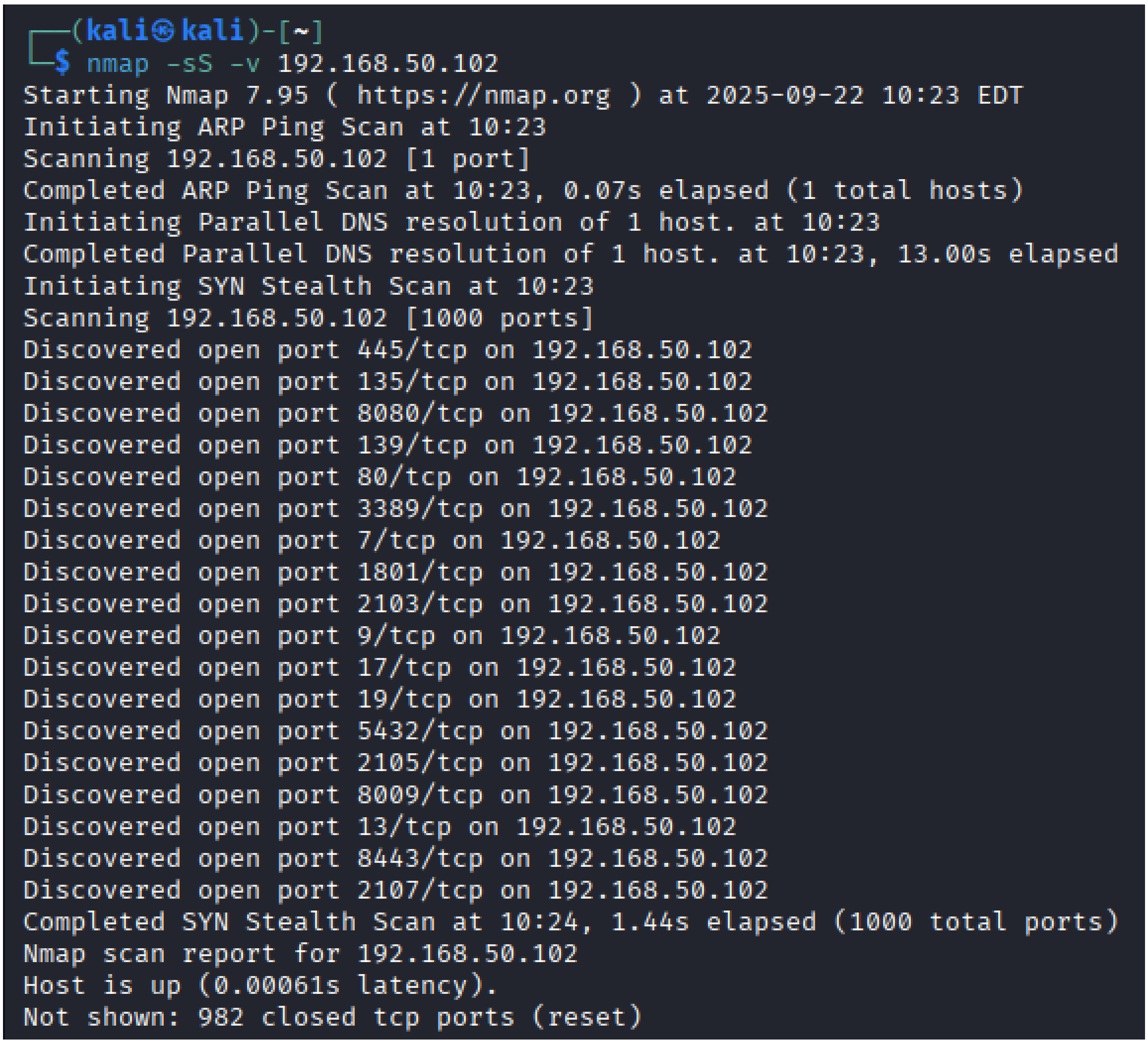
```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 10:34 EDT
Nmap scan report for 192.168.50.102
Host is up (0.0016s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
1801/tcp 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:AD:0A:B9 (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 (92%), Microsoft Windows 10 1511 - 1607 (92%), Microsoft Windows Embedded Standard 7 (92%), Microsoft Windows 7 or Windows Server 2008 R2 (91%),
 Microsoft Windows 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%), Microsoft Windows Vista SP2, W
indows 7 SP1, or Windows Server 2008 (90%)
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 22.17 seconds
```

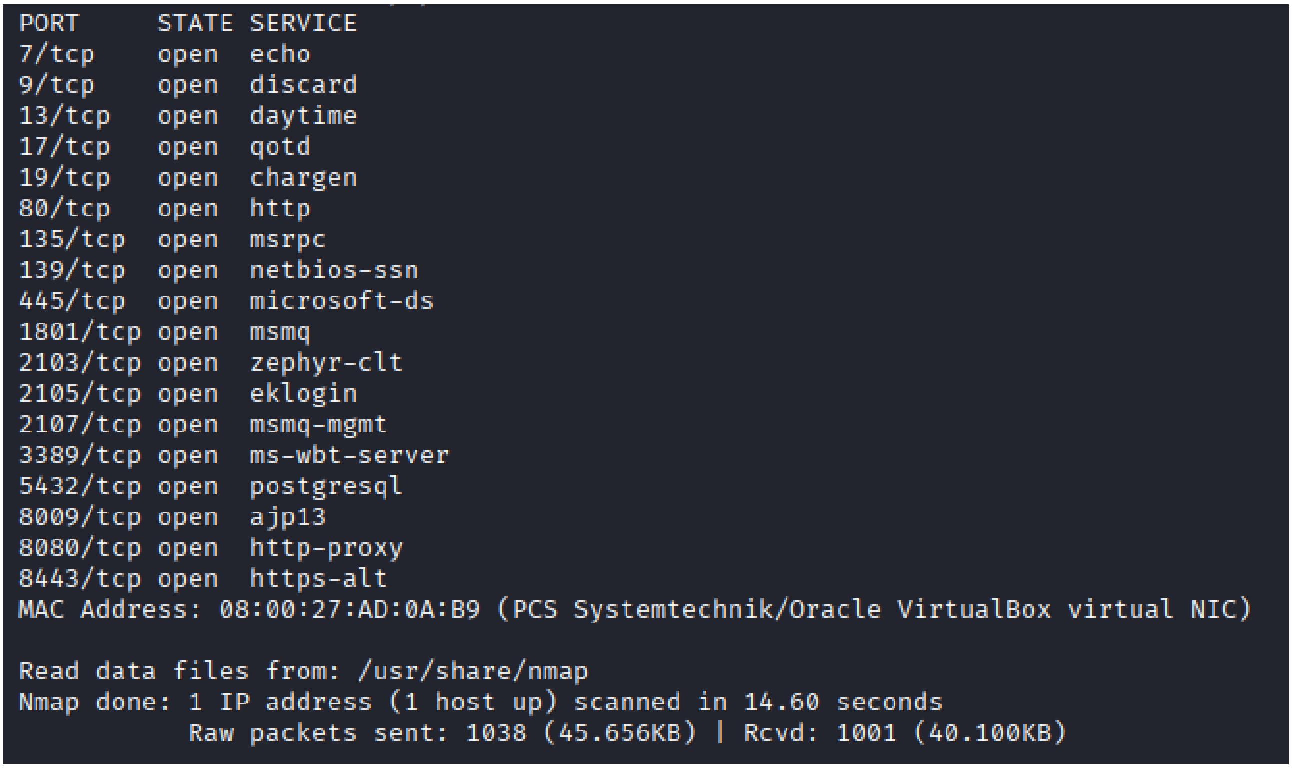
2.3 Syn scan

nmap -sS -v 192.168.50.102

Firewall disattivato



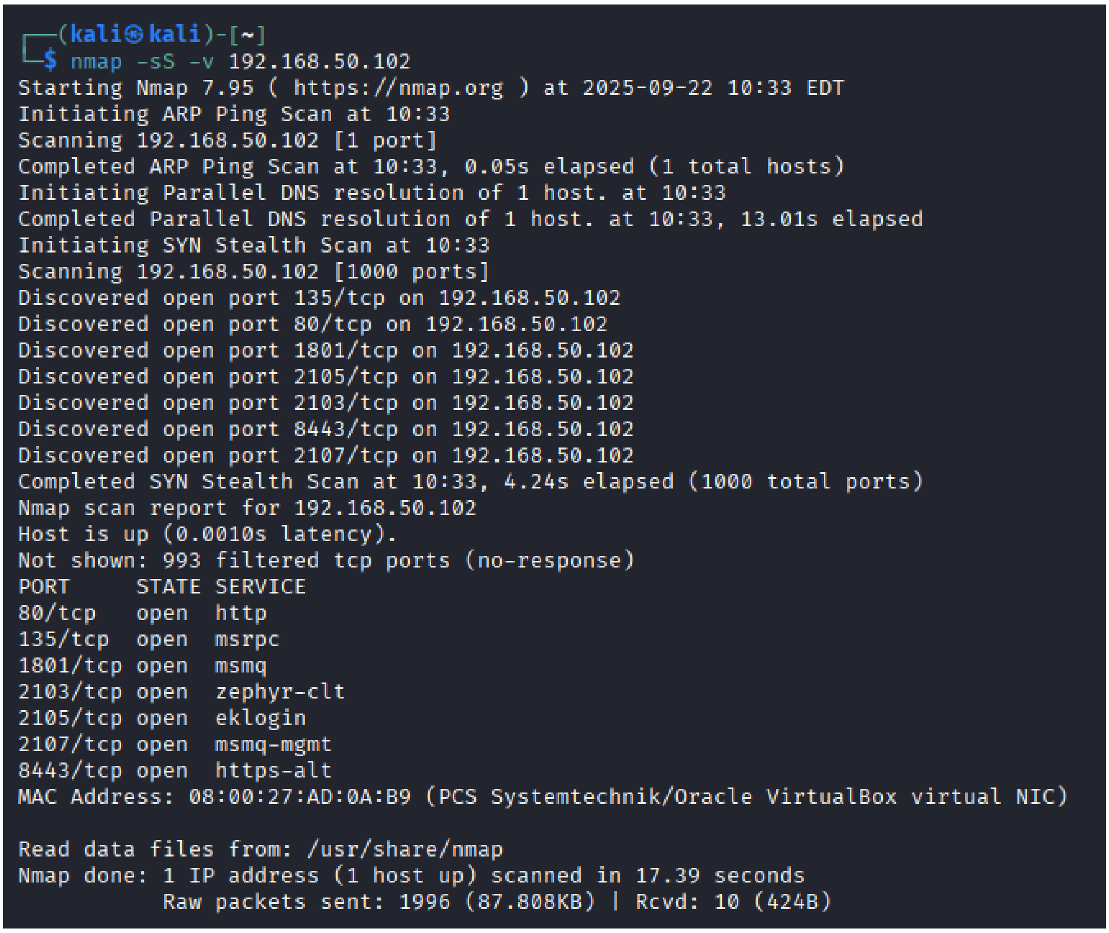
```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -v 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 10:23 EDT
Initiating ARP Ping Scan at 10:23
Scanning 192.168.50.102 [1 port]
Completed ARP Ping Scan at 10:23, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:23
Completed Parallel DNS resolution of 1 host. at 10:23, 13.00s elapsed
Initiating SYN Stealth Scan at 10:23
Scanning 192.168.50.102 [1000 ports]
Discovered open port 445/tcp on 192.168.50.102
Discovered open port 135/tcp on 192.168.50.102
Discovered open port 8080/tcp on 192.168.50.102
Discovered open port 139/tcp on 192.168.50.102
Discovered open port 80/tcp on 192.168.50.102
Discovered open port 3389/tcp on 192.168.50.102
Discovered open port 7/tcp on 192.168.50.102
Discovered open port 1801/tcp on 192.168.50.102
Discovered open port 2103/tcp on 192.168.50.102
Discovered open port 9/tcp on 192.168.50.102
Discovered open port 17/tcp on 192.168.50.102
Discovered open port 19/tcp on 192.168.50.102
Discovered open port 5432/tcp on 192.168.50.102
Discovered open port 2105/tcp on 192.168.50.102
Discovered open port 8009/tcp on 192.168.50.102
Discovered open port 13/tcp on 192.168.50.102
Discovered open port 8443/tcp on 192.168.50.102
Discovered open port 2107/tcp on 192.168.50.102
Completed SYN Stealth Scan at 10:24, 1.44s elapsed (1000 total ports)
Nmap scan report for 192.168.50.102
Host is up (0.00061s 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:AD:0A:B9 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 14.60 seconds
           Raw packets sent: 1038 (45.656KB) | Rcvd: 1001 (40.100KB)
```

Firewall attivo



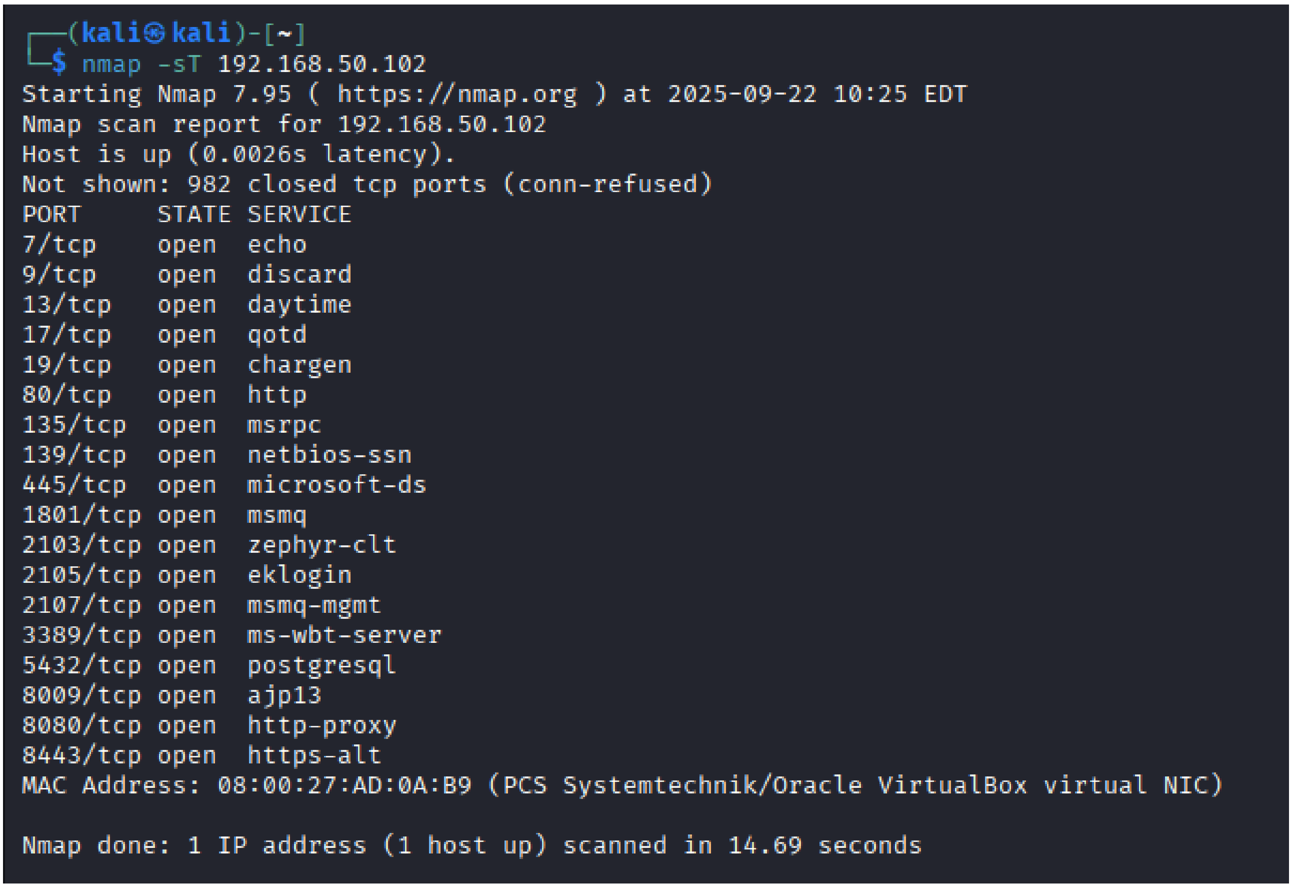
```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -v 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 10:33 EDT
Initiating ARP Ping Scan at 10:33
Scanning 192.168.50.102 [1 port]
Completed ARP Ping Scan at 10:33, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:33
Completed Parallel DNS resolution of 1 host. at 10:33, 13.01s elapsed
Initiating SYN Stealth Scan at 10:33
Scanning 192.168.50.102 [1000 ports]
Discovered open port 135/tcp on 192.168.50.102
Discovered open port 80/tcp on 192.168.50.102
Discovered open port 1801/tcp on 192.168.50.102
Discovered open port 2105/tcp on 192.168.50.102
Discovered open port 2103/tcp on 192.168.50.102
Discovered open port 8443/tcp on 192.168.50.102
Discovered open port 2107/tcp on 192.168.50.102
Completed SYN Stealth Scan at 10:33, 4.24s elapsed (1000 total ports)
Nmap scan report for 192.168.50.102
Host is up (0.0010s 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:AD:0A:B9 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 17.39 seconds
           Raw packets sent: 1996 (87.808KB) | Rcvd: 10 (424B)
```

2.4 TCP connect

nmap -sT 192.168.50.102

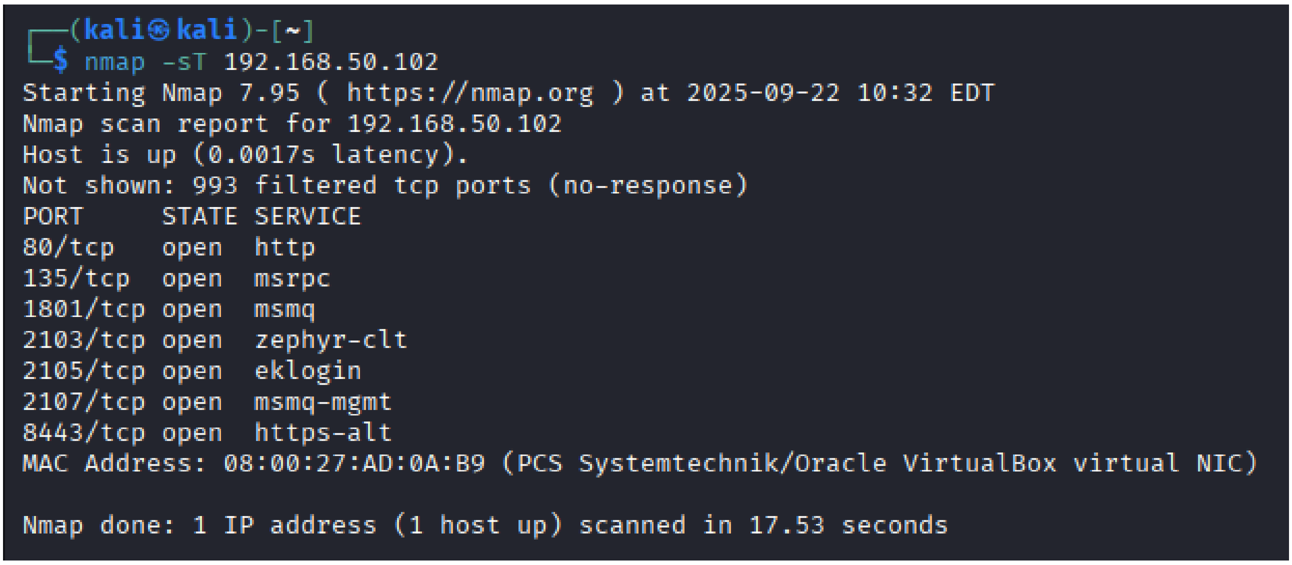
Firewall disattivato



```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 10:25 EDT
Nmap scan report for 192.168.50.102
Host is up (0.0026s 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:AD:0A:B9 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.69 seconds
```

Firewall attivo



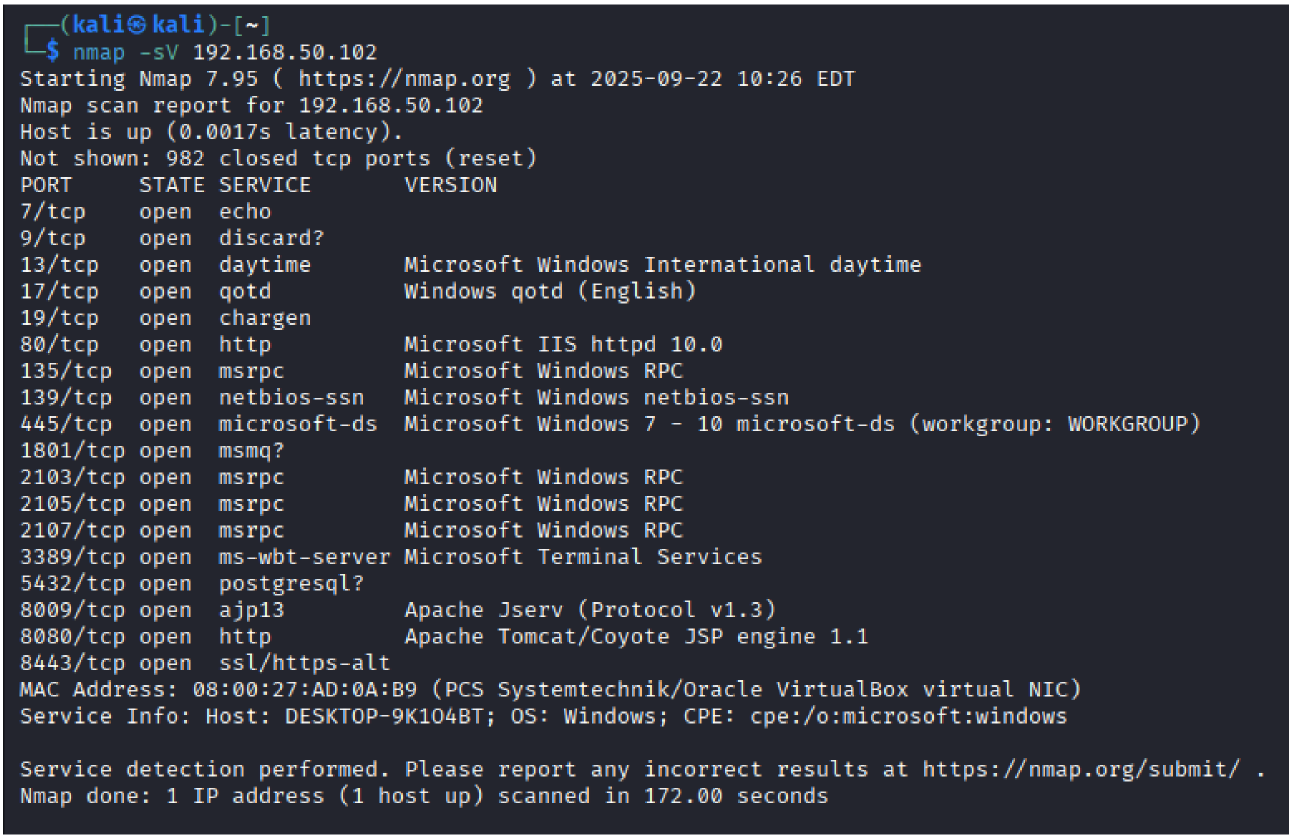
```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 10:32 EDT
Nmap scan report for 192.168.50.102
Host is up (0.0017s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
1801/tcp 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:AD:0A:B9 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 17.53 seconds
```

2.5 Version detection

nmap -sV 192.168.50.102

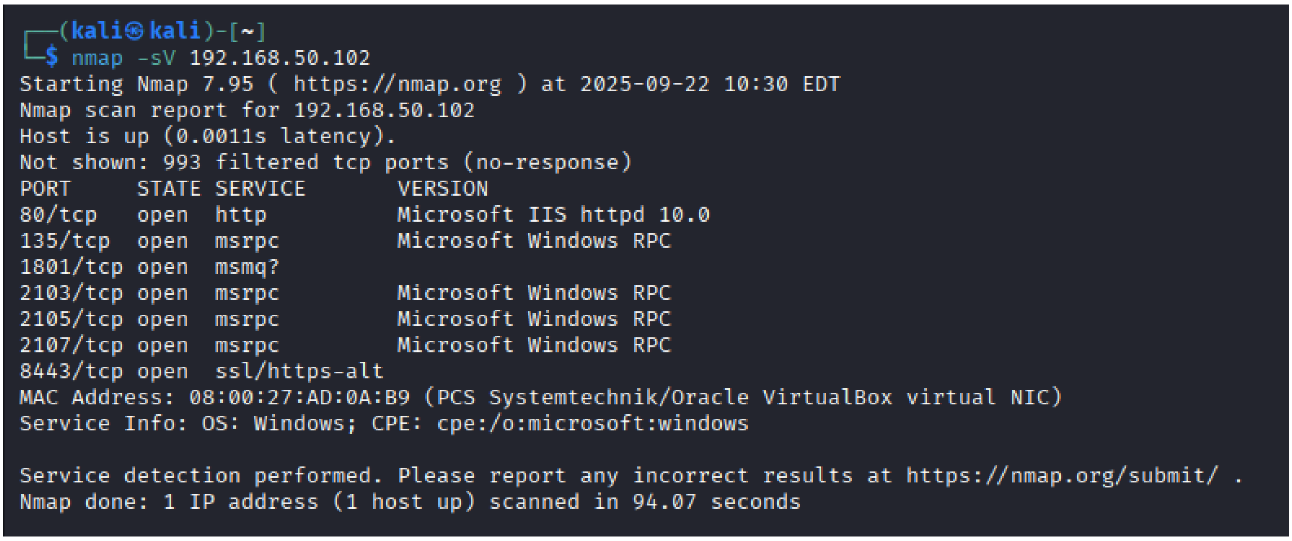
Firewall disattivato



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 10:26 EDT
Nmap scan report for 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:AD:0A:B9 (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 172.00 seconds
```

Firewall attivo



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 10:30 EDT
Nmap scan report for 192.168.50.102
Host is up (0.0011s 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:AD:0A:B9 (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 94.07 seconds
```