Report di Scansioni Nmap

1. Introduzione

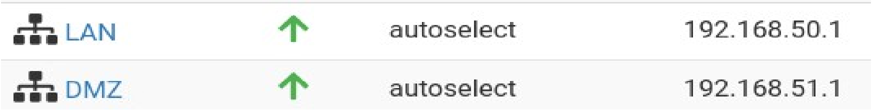
Effettuare scansioni sul target(Windows 10) con il firewal acceso e con I firewall spento.
- **Scenario Uno:** target e attaccante su due reti diverse, il target ha il firewall **acceso**.
- **Scenario Due:** target e attaccante su due reti diverse, il target ha il firewall **spento**.
- **Scenario facoltativo:** target e attaccante sulla stessa rete, con firewall acceso/spento.

2. Configurazione dell’ Ambiente

2.1 Ambiente di Rete

- **Macchina Firewall:**

- Sistema operativo:	pfSense - CE
- RETE 1:	192.168.50.0/24
- RETE 2:	192.168.51.0/24
- DNS:	epic-pfsense.epicode



LAN	↑	autoselect	192.168.50.1
DMZ	↑	autoselect	192.168.51.1

- **Macchina Attaccante:**

- Sistema operativo:	Kali Linux
- IP:	192.168.50.100
- DNS:	epic-kali.epicode

- **Macchina Target:**

- Sistema operativo:	Metasploitable - Linux
- IP LAN:	192.168.51.102
- IP DMZ:	192.168.50.102
- DNS:	epic-win10.epicode

2.2 Strumenti Utilizzati

- Nmap v7.95
- Hypervisor: Vmware ESXi

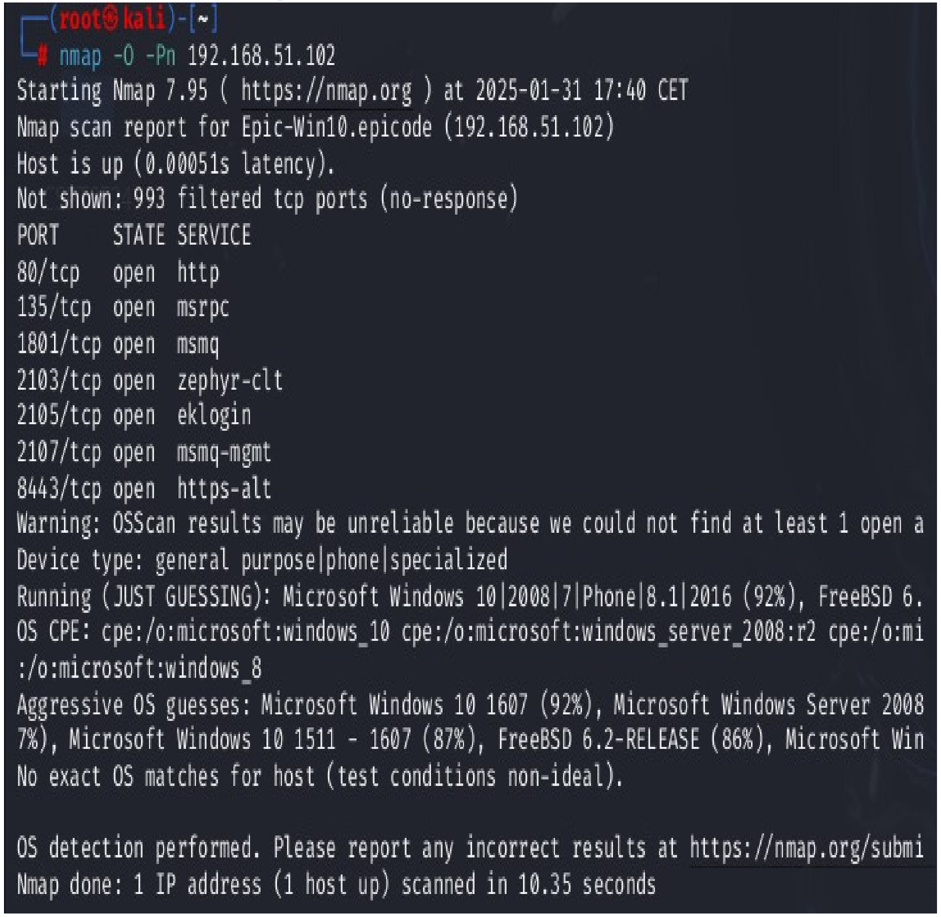
3. Scenario 1: Scansione Su Rete DMZ (Rete Separata)

3.1 OS Fingerprint

Con il firewall attivo sono costretto a utilizzare il flag -Pn per saltare la fase di rilevamento host in quanto il firewall non mi consente di portare a termine la scansione.

Comandi utilizzati:

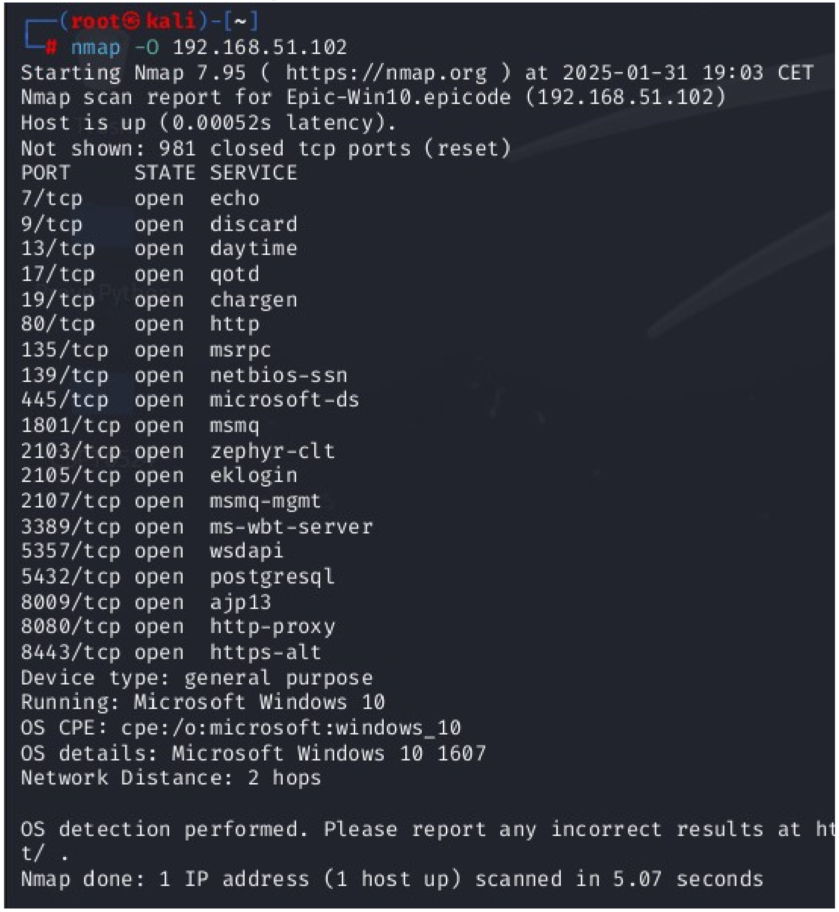
- Firewall ON (Figura 1) nmap -O -Pn 192.168.51.102



```
┌──(root㉿kali)-[~]
└─# nmap -O -Pn 192.168.51.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-31 17:40 CET
Nmap scan report for Epic-Win10.epicode (192.168.51.102)
Host is up (0.00051s 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 a
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 10|2008|7|Phone|8.1|2016 (92%), FreeBSD 6.
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:mi
:/o:microsoft:windows_8
Aggressive OS guesses: Microsoft Windows 10 1607 (92%), Microsoft Windows Server 2008
7%), Microsoft Windows 10 1511 - 1607 (87%), FreeBSD 6.2-RELEASE (86%), Microsoft Win
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submi
Nmap done: 1 IP address (1 host up) scanned in 10.35 seconds
```

- Firewall OFF (Figura 2) nmap -O 192.168.51.102



```
┌──(root㉿kali)-[~]
└─# nmap -O 192.168.51.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-31 19:03 CET
Nmap scan report for Epic-Win10.epicode (192.168.51.102)
Host is up (0.00052s latency).
Not shown: 981 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
5357/tcp open  wsdapi
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 ht
t/ .
Nmap done: 1 IP address (1 host up) scanned in 5.07 seconds
```

Differenze:

- Si nota che nmap, sul firewall attivo scopre 7 porte rispetto alle 19 porte che vengono scoperte senza firewall.
- In entrambe le scansioni abbiamo ottenuto informazioni su sistema operativo target. Si vola
- Chiaramente si distingue in numero di hop effettuati tra reti diverse.
- Soprattutto si nota che il tempo di scansione senza firewall ha impiegato 5s rispetto ai 10s che ha scoperto solo 7 porte ma comunque importanti.

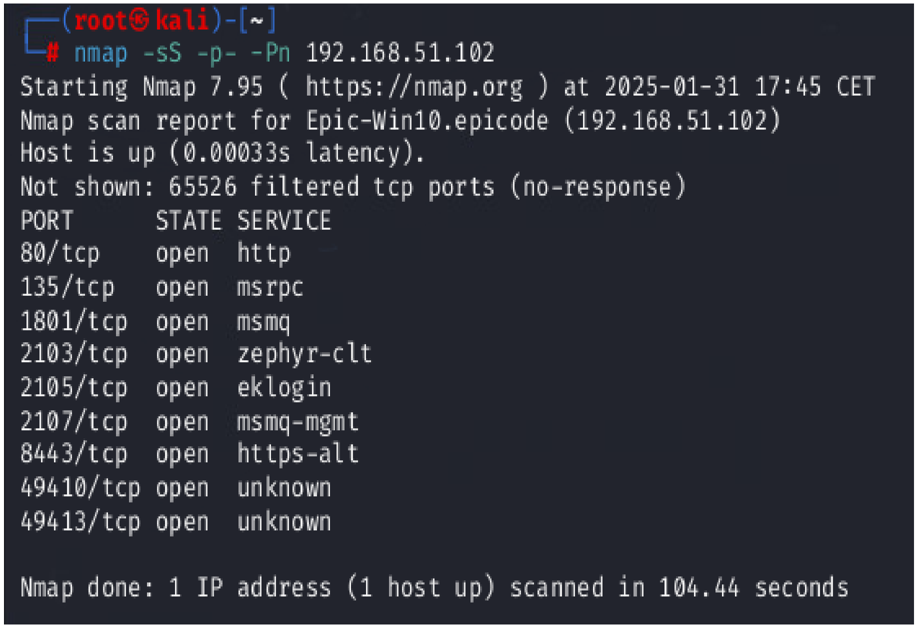
3.2 SYN Scan

Con il firewall attivo sono costretto a utilizzare il flag -Pn per saltare la fase di rilevamento host perchè il firewall me lo impedisce.

Comandi utilizzati:

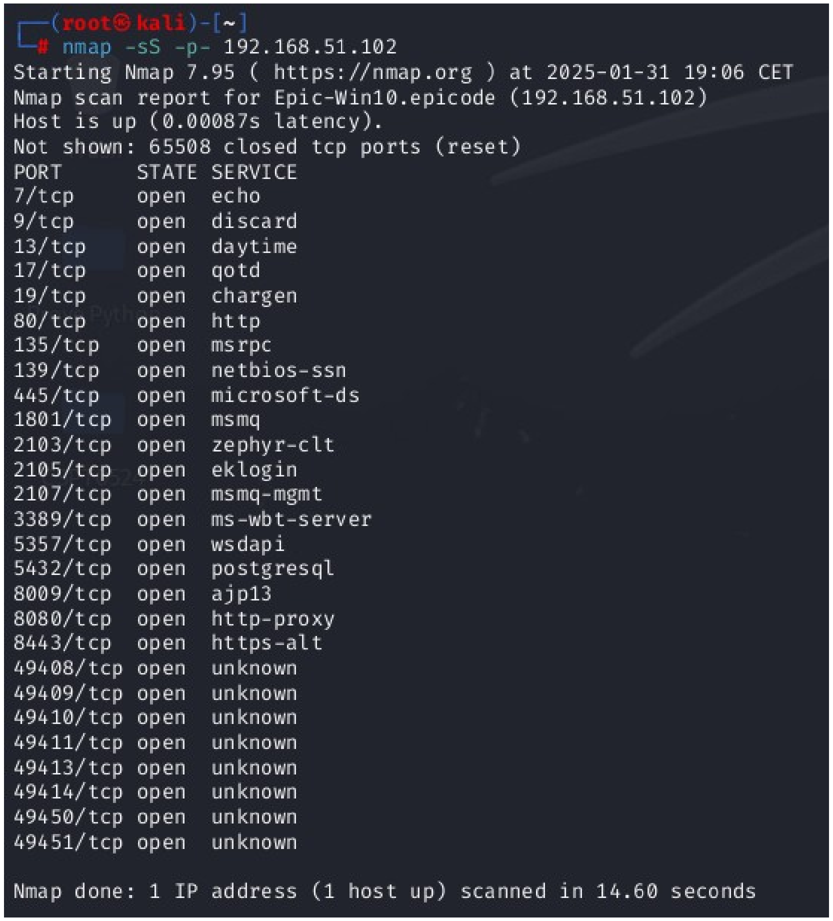
- **Firewall ON (Figura 1)** nmap -sS -p- -Pn 192.168.51.102

- **Firewall OFF (Figura 2)** nmap -sS -p- 192.168.51.102



```
┌──(root㉿kali)-[~]
└─# nmap -sS -p- -Pn 192.168.51.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-31 17:45 CET
Nmap scan report for Epic-Win10.epicode (192.168.51.102)
Host is up (0.00033s latency).
Not shown: 65526 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
49410/tcp open  unknown
49413/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 104.44 seconds
```



```
┌──(root㉿kali)-[~]
└─# nmap -sS -p- 192.168.51.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-31 19:06 CET
Nmap scan report for Epic-Win10.epicode (192.168.51.102)
Host is up (0.00087s latency).
Not shown: 65508 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
5357/tcp  open  wsdapi
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
49408/tcp open  unknown
49409/tcp open  unknown
49410/tcp open  unknown
49411/tcp open  unknown
49413/tcp open  unknown
49414/tcp open  unknown
49450/tcp open  unknown
49451/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 14.60 seconds
```

Differenze:

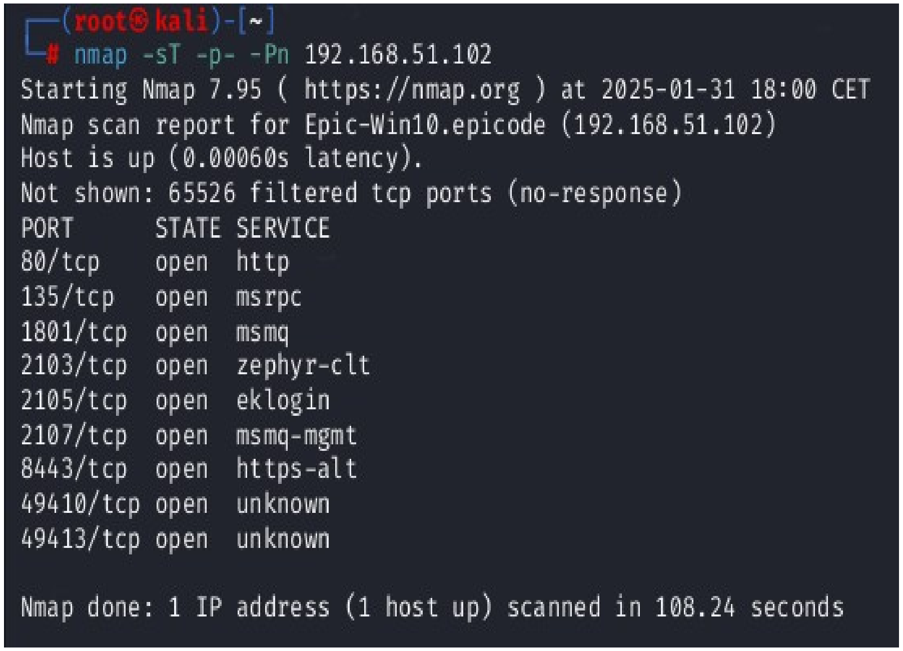
- I tempi di scansione questa volta mostrano differenze abbastanza grandi, quasi 100s
- Con Firewall Attivo, scopriamo 9 porte e come già visto impiega piu di 100s per eseguire la scansione
- Con Firewall Disattivo otteniamo più porte aperte oltre alla tempistica di 14s

3.3 TCP Connect Scan

Comandi utilizzati:

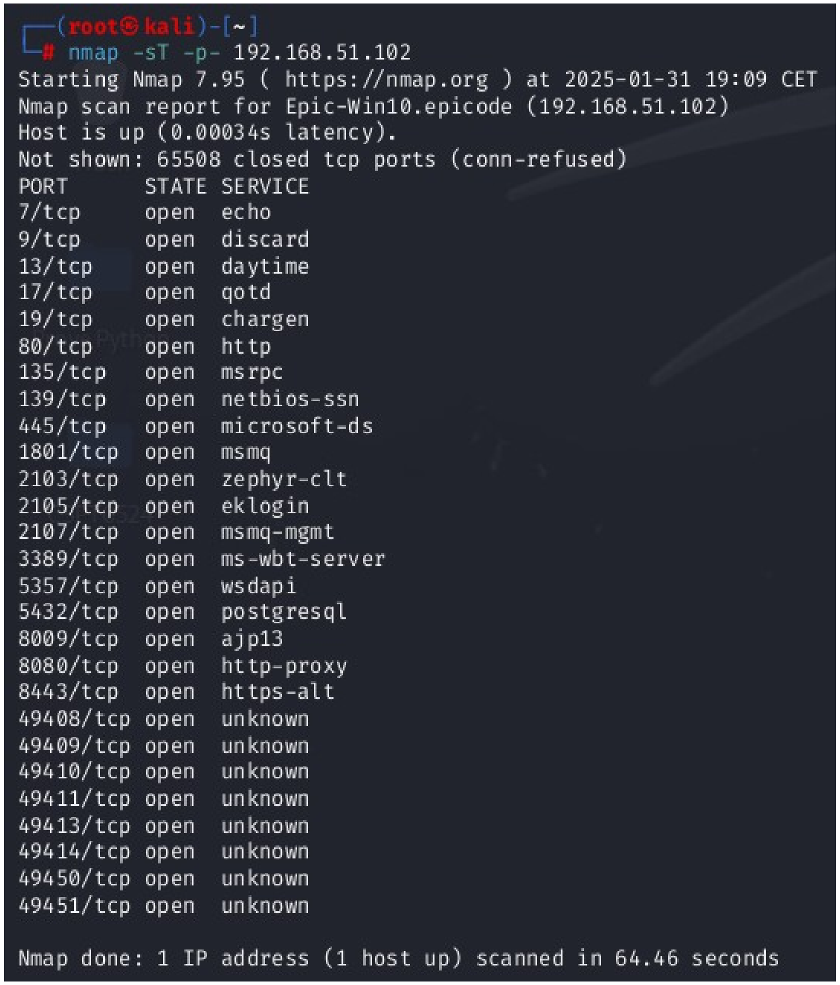
- Firewall ON (Figura 1) nmap -sT -p- -Pn 192.168.51.102

- Firewall OFF (Figura 2) nmap -sT -p- 192.168.51.102



```
┌──(root㉿kali)-[~]
└─# nmap -sT -p- -Pn 192.168.51.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-31 18:00 CET
Nmap scan report for Epic-Win10.epicode (192.168.51.102)
Host is up (0.00060s latency).
Not shown: 65526 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
49410/tcp open  unknown
49413/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 108.24 seconds
```



```
┌──(root㉿kali)-[~]
└─# nmap -sT -p- 192.168.51.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-31 19:09 CET
Nmap scan report for Epic-Win10.epicode (192.168.51.102)
Host is up (0.00034s latency).
Not shown: 65508 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
5357/tcp  open  wsdapi
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
49408/tcp open  unknown
49409/tcp open  unknown
49410/tcp open  unknown
49411/tcp open  unknown
49413/tcp open  unknown
49414/tcp open  unknown
49450/tcp open  unknown
49451/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 64.46 seconds
```

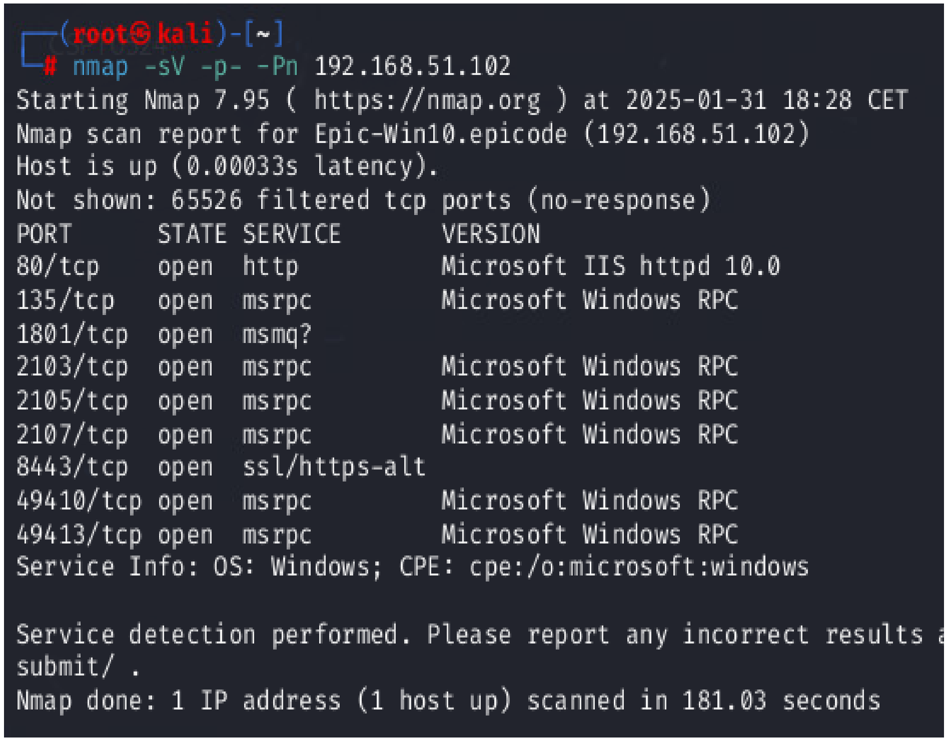
Differenze:

- Come già notato in precedenza I tempi di scansione variano, ma questa volta anche con Firewall Spento abbiamo impiegato più tempo per via delle connessioni TCP.
- Con Firewall Attivo, scopriamo 9 porte e come già visto impiega piu di 100s per eseguire la scansione.
- Con Firewall Disattivo otteniamo più porte aperte ma questa volta una tempistica piu lunga.

3.4 Version Detection

Comandi utilizzati:

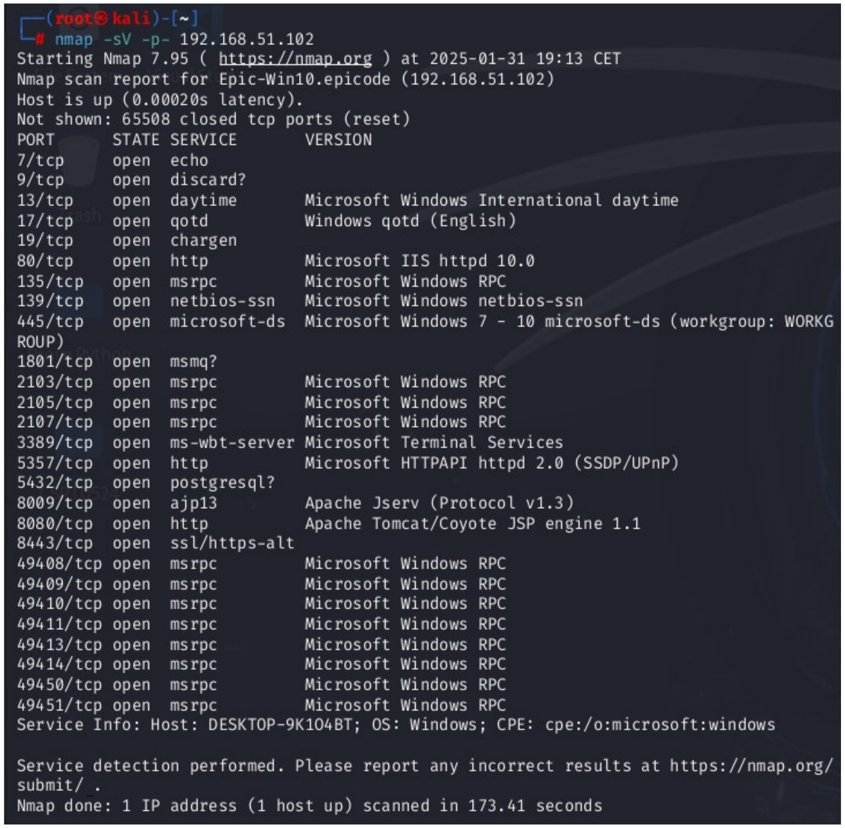
- **Firewall ON (Figura 1)** nmap -sV -p- -Pn 192.168.51.102



```
┌──(root㉿kali)-[~]
└─# nmap -sV -p- -Pn 192.168.51.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-31 18:28 CET
Nmap scan report for Epic-Win10.epicode (192.168.51.102)
Host is up (0.00033s latency).
Not shown: 65526 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
49410/tcp open  msrpc         Microsoft Windows RPC
49413/tcp open  msrpc         Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results a
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 181.03 seconds
```

- **Firewall OFF (Figura 2)** nmap -sV -p- 192.168.51.102



```
┌──(root㉿kali)-[~]
└─# nmap -sV -p- 192.168.51.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-31 19:13 CET
Nmap scan report for Epic-Win10.epicode (192.168.51.102)
Host is up (0.00020s latency).
Not shown: 65508 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: WORKG
ROUP)
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
5357/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
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
49408/tcp open  msrpc         Microsoft Windows RPC
49409/tcp open  msrpc         Microsoft Windows RPC
49410/tcp open  msrpc         Microsoft Windows RPC
49411/tcp open  msrpc         Microsoft Windows RPC
49413/tcp open  msrpc         Microsoft Windows RPC
49414/tcp open  msrpc         Microsoft Windows RPC
49450/tcp open  msrpc         Microsoft Windows RPC
49451/tcp open  msrpc         Microsoft Windows RPC
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 173.41 seconds
```

Differenze:

- Tempi di scansioni decisamente piu lunghi rispetto a scansioni SYN/TCP
- Con Firewall Attivo, scopriamo 9 porte con tipo di servizio e versione
- Con Firewall Disattivo otteniamo più porte aperte con servizi e versioni

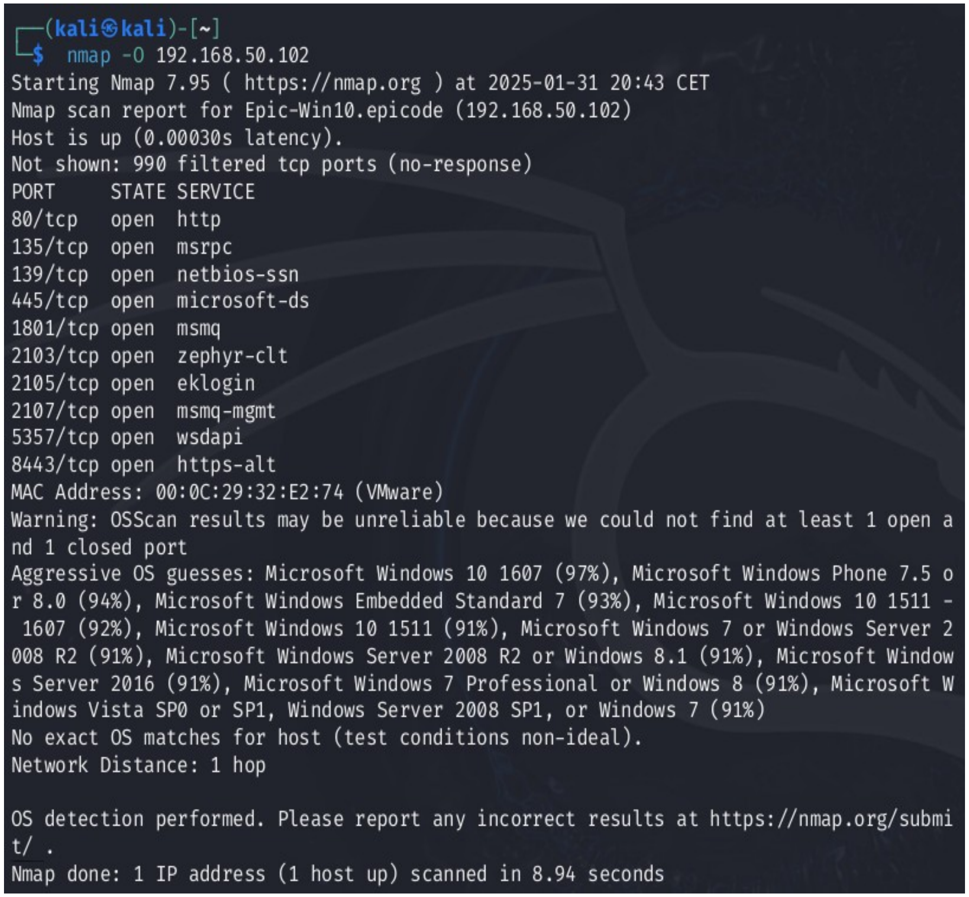
4. Scenario 2: Scansione Su Rete LAN (Stessa Rete)

4.1 OS Fingerprint

Comandi utilizzati:

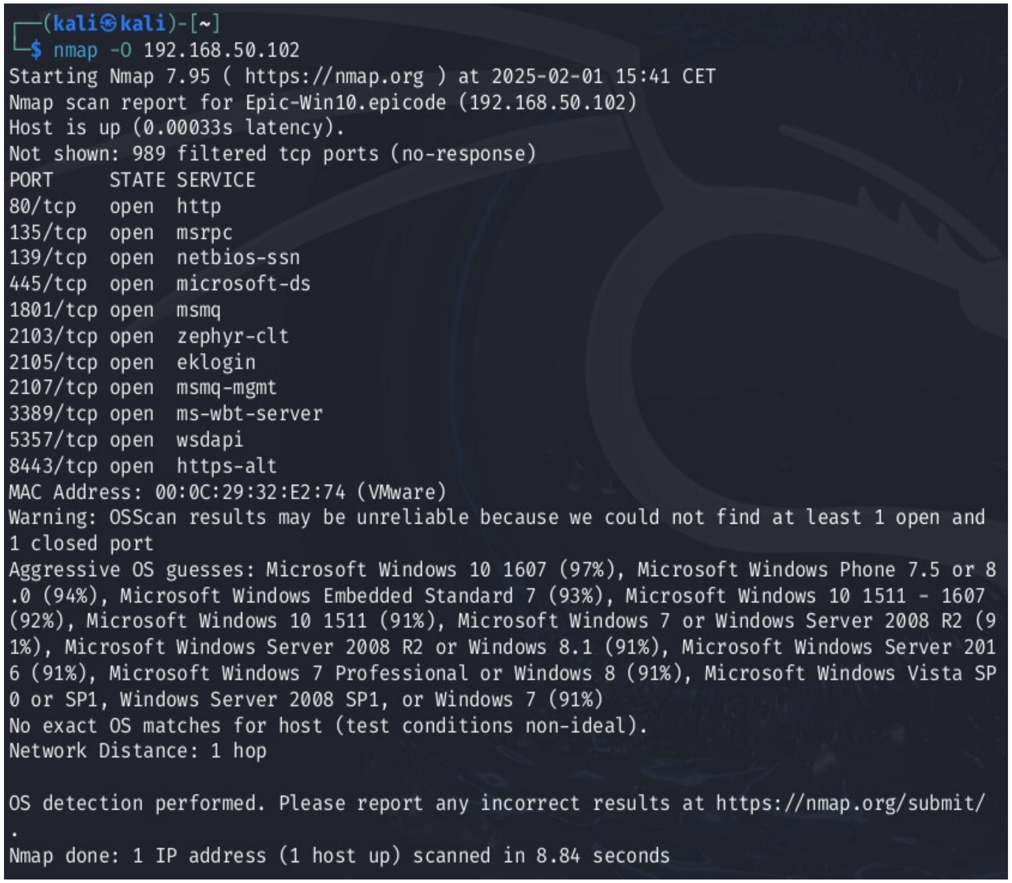
- Firewall ON (Figura 1) nmap -O 192.168.50.102

- Firewall OFF (Figura 2) nmap -O 192.168.50.102



```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-31 20:43 CET
Nmap scan report for Epic-Win10.epicode (192.168.50.102)
Host is up (0.00030s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT     STATE SERVICE
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
5357/tcp open  wsdapi
8443/tcp open  https-alt
MAC Address: 00:0C:29:32:E2:74 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open a
nd 1 closed port
Aggressive OS guesses: Microsoft Windows 10 1607 (97%), Microsoft Windows Phone 7.5 o
r 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 2
008 R2 (91%), Microsoft Windows Server 2008 R2 or Windows 8.1 (91%), Microsoft Window
s Server 2016 (91%), Microsoft Windows 7 Professional or Windows 8 (91%), Microsoft W
indows Vista SP0 or SP1, Windows Server 2008 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/submi
t/ .
Nmap done: 1 IP address (1 host up) scanned in 8.94 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-01 15:41 CET
Nmap scan report for Epic-Win10.epicode (192.168.50.102)
Host is up (0.00033s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT     STATE SERVICE
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
5357/tcp open  wsdapi
8443/tcp open  https-alt
MAC Address: 00:0C:29:32:E2:74 (VMware)
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 (9
1%), Microsoft Windows Server 2008 R2 or Windows 8.1 (91%), Microsoft Windows Server 201
6 (91%), Microsoft Windows 7 Professional or Windows 8 (91%), Microsoft Windows Vista SP
0 or SP1, Windows Server 2008 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 8.84 seconds
```

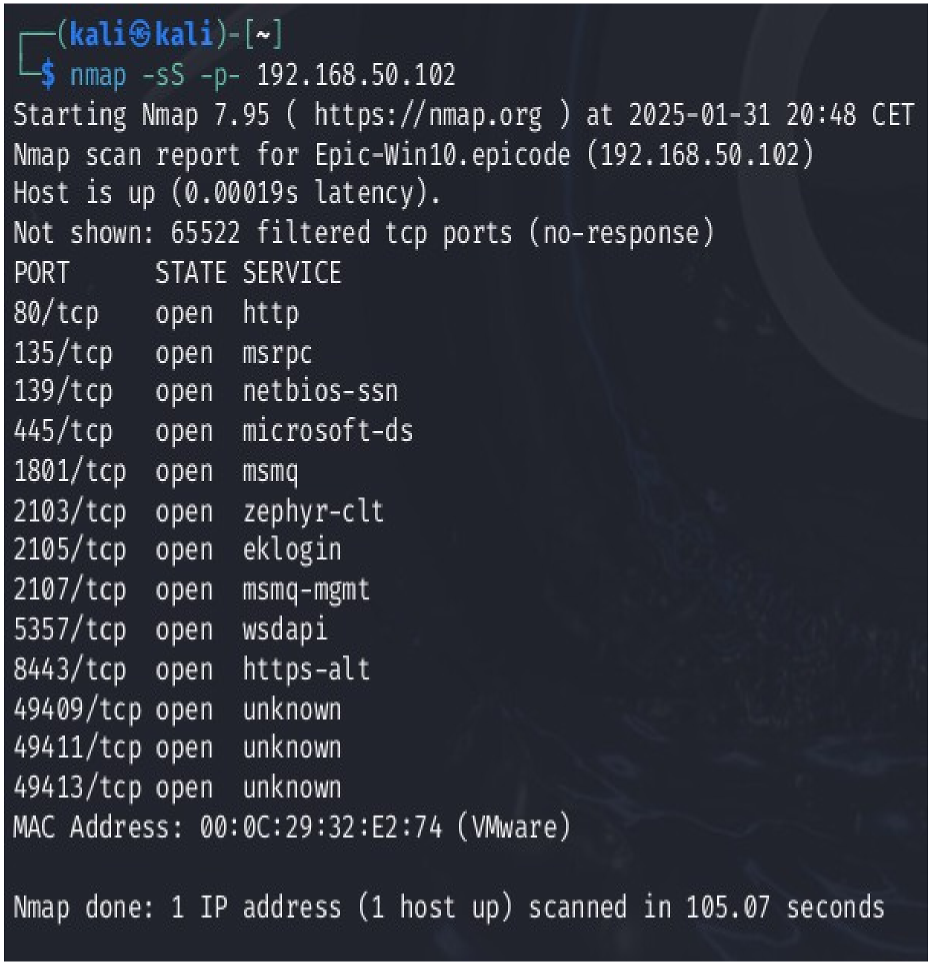
Differenze:

- Con il target nella stessa rete, i risultati cambiano, ma otteniamo il sistema operativo in entrambe le scansioni.
- Con Firewall Attivo, scopriamo 3 porte in più rispetto a una rete differente (7 porte)
- Con Firewall Disattivo otteniamo più porte aperte ma meno di una rete differente(mi aspettavo il contrario, vedi scenario 1)

4.2 SYN Scan

Comandi utilizzati:

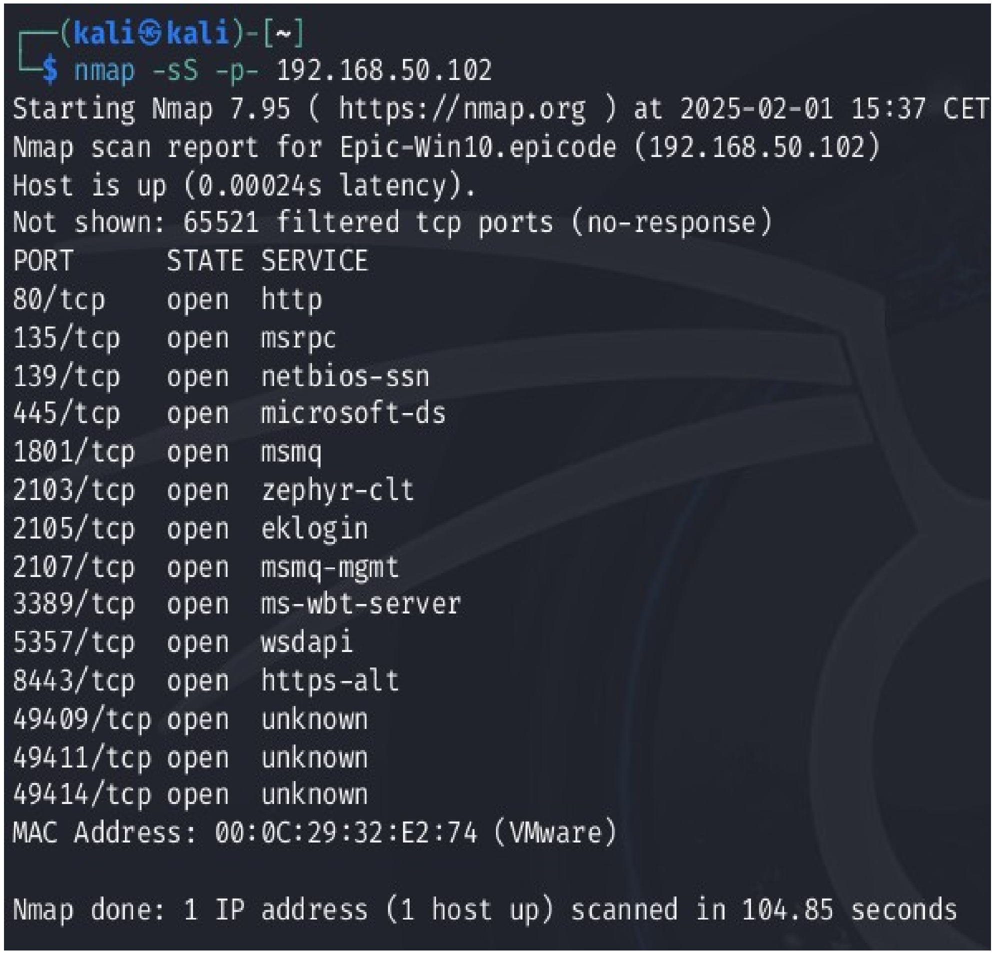
- **Firewall ON (Figura 1)** nmap -sS -p- 192.168.50.102



```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -p- 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-31 20:48 CET
Nmap scan report for Epic-Win10.epicode (192.168.50.102)
Host is up (0.00019s latency).
Not shown: 65522 filtered tcp ports (no-response)
PORT      STATE SERVICE
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
5357/tcp  open  wsdapi
8443/tcp  open  https-alt
49409/tcp open  unknown
49411/tcp open  unknown
49413/tcp open  unknown
MAC Address: 00:0C:29:32:E2:74 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 105.07 seconds
```

- **Firewall OFF (Figura 2)** nmap -sS -p- 192.168.50.102



```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -p- 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-01 15:37 CET
Nmap scan report for Epic-Win10.epicode (192.168.50.102)
Host is up (0.00024s latency).
Not shown: 65521 filtered tcp ports (no-response)
PORT      STATE SERVICE
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
5357/tcp  open  wsdapi
8443/tcp  open  https-alt
49409/tcp open  unknown
49411/tcp open  unknown
49414/tcp open  unknown
MAC Address: 00:0C:29:32:E2:74 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 104.85 seconds
```

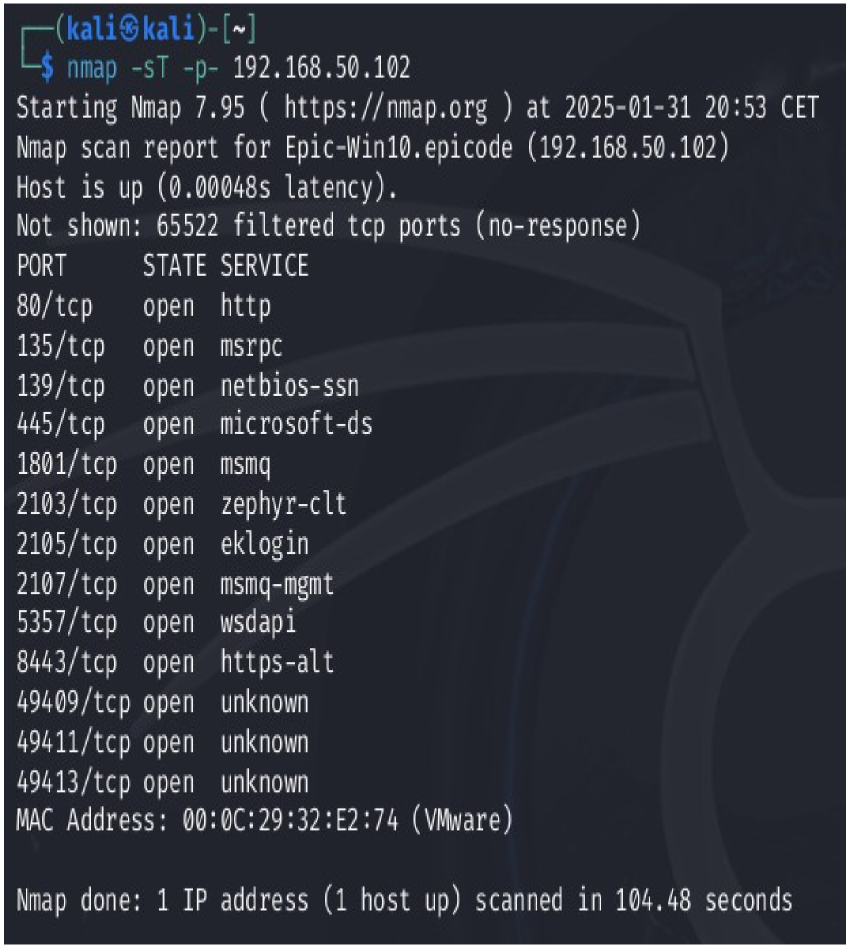
Differenze:

- Stessi risultati, ma senza firewall otteniamo la porta 3389
- Con Firewall Attivo abbiamo la porta 49 413
- Con Firewall Disattivo abbiamo la porta 49 414

3.3 TCP Connect Scan

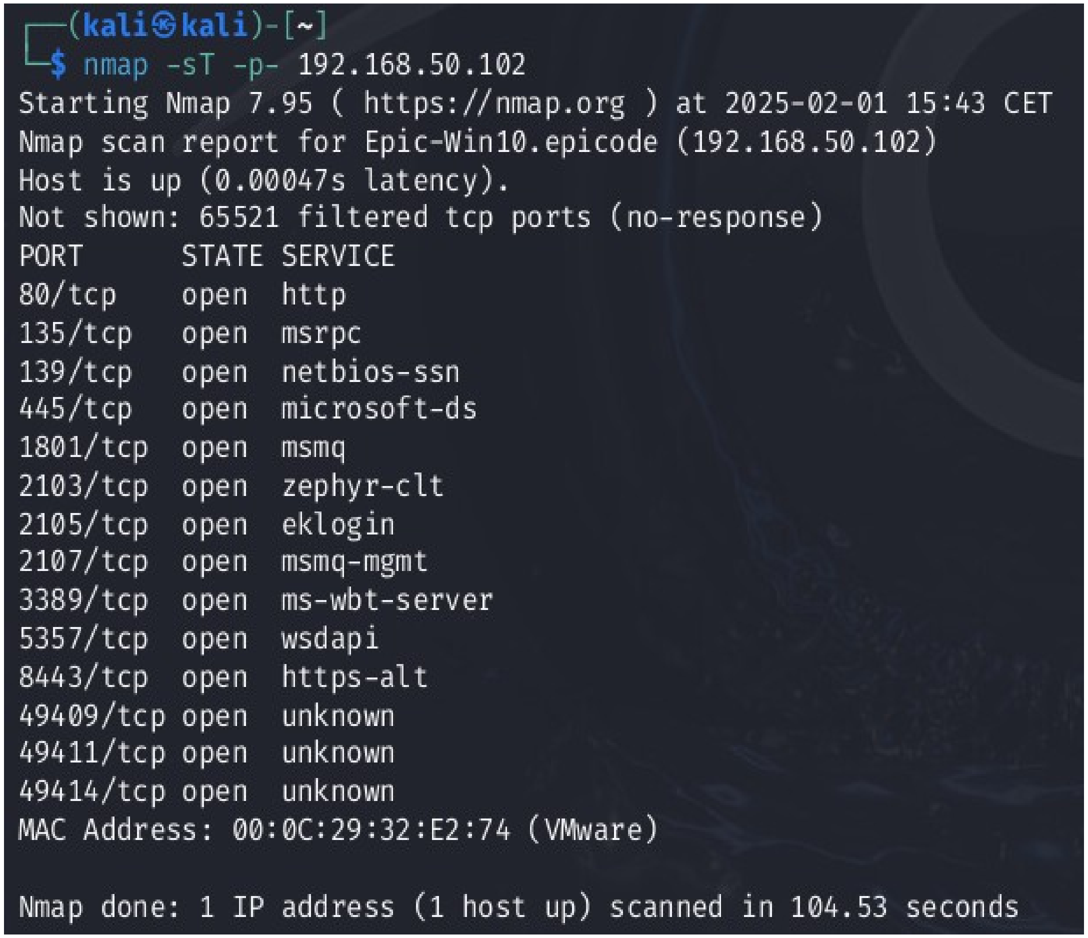
Comandi utilizzati:

- **Firewall ON (Figura 1)** nmap -sT -p- 192.168.50.102
- **Firewall OFF (Figura 2)** nmap -sT -p- 192.168.50.102



```
┌──(kali㉿kali)-[~]
└─$ nmap -sT -p- 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-31 20:53 CET
Nmap scan report for Epic-Win10.epicode (192.168.50.102)
Host is up (0.00048s latency).
Not shown: 65522 filtered tcp ports (no-response)
PORT      STATE SERVICE
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
5357/tcp  open  wsdapi
8443/tcp  open  https-alt
49409/tcp open  unknown
49411/tcp open  unknown
49413/tcp open  unknown
MAC Address: 00:0C:29:32:E2:74 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 104.48 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -sT -p- 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-01 15:43 CET
Nmap scan report for Epic-Win10.epicode (192.168.50.102)
Host is up (0.00047s latency).
Not shown: 65521 filtered tcp ports (no-response)
PORT      STATE SERVICE
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
5357/tcp  open  wsdapi
8443/tcp  open  https-alt
49409/tcp open  unknown
49411/tcp open  unknown
49414/tcp open  unknown
MAC Address: 00:0C:29:32:E2:74 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 104.53 seconds
```

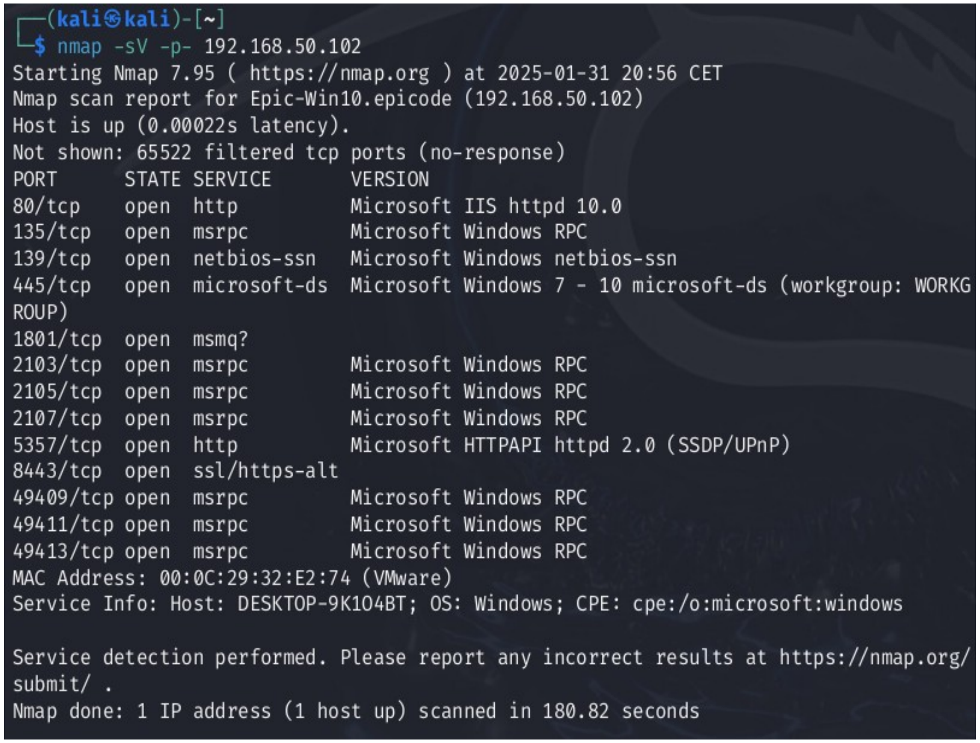
Differenze:

- Anche qui otteniamo la porta 3389 senza firewall.
- Con Firewall Attivo abbiamo la porta 49 413
- Con Firewall Disattivo abbiamo la porta 49 414

3.4 Version Detection

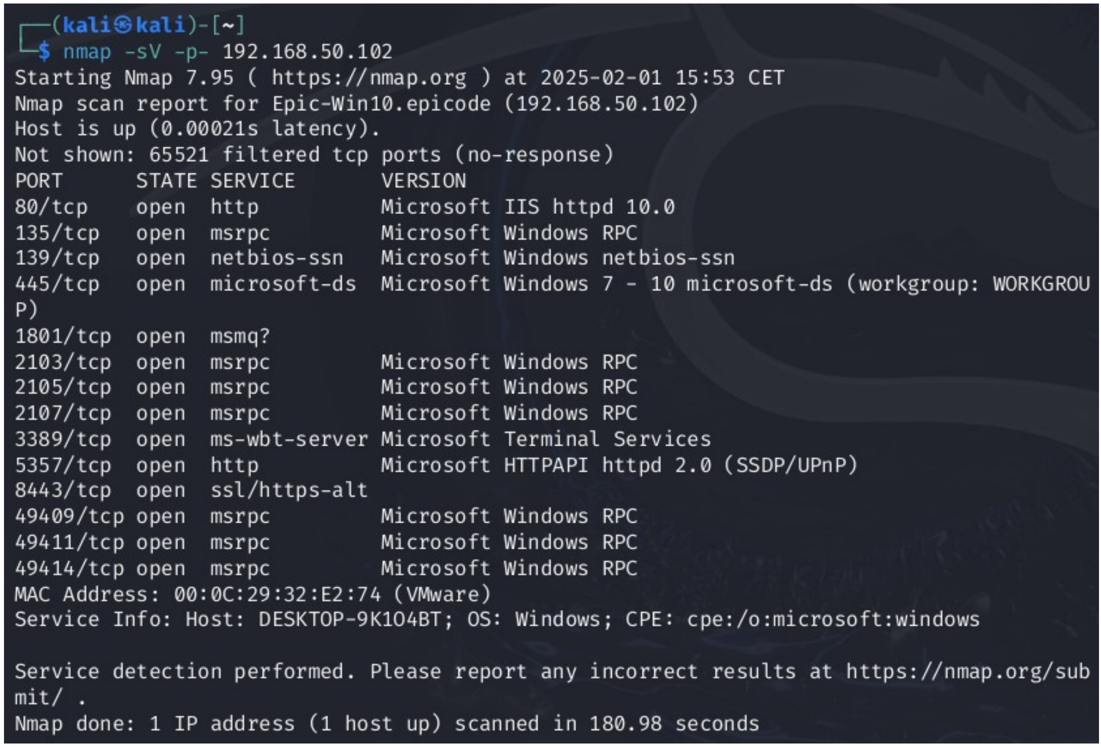
Comandi utilizzati:

- **Firewall ON (Figura 1)** nmap -sV -p- 192.168.50.102 - **Firewall OFF (Figura 2)** nmap -sV -p- 192.168.50.102



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p- 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-31 20:56 CET
Nmap scan report for Epic-Win10.epicode (192.168.50.102)
Host is up (0.00022s latency).
Not shown: 65522 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
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKG
ROUP)
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
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8443/tcp  open  ssl/https-alt
49409/tcp open  msrpc        Microsoft Windows RPC
49411/tcp open  msrpc        Microsoft Windows RPC
49413/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:32:E2:74 (VMware)
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 180.82 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p- 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-01 15:53 CET
Nmap scan report for Epic-Win10.epicode (192.168.50.102)
Host is up (0.00021s latency).
Not shown: 65521 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
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROU
P)
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
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8443/tcp  open  ssl/https-alt
49409/tcp open  msrpc        Microsoft Windows RPC
49411/tcp open  msrpc        Microsoft Windows RPC
49414/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:32:E2:74 (VMware)
Service Info: Host: DESKTOP-9K1O4BT; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 180.98 seconds
```

Differenze:

- Anche qui otteniamo la porta 3389 senza firewall.
- Con Firewall Attivo abbiamo la porta 49 413
- Con Firewall Disattivo abbiamo la porta 49 414

5. Conclusioni

- Se il firewall è attivo, otteniamo meno porte e servizi, al contrario senza firewall otteniamo piu informazioni, si notano I tempi di scansione e soprattutto si notano porte differenti tra firewall acceso e spento.

Francesco Rinaldi