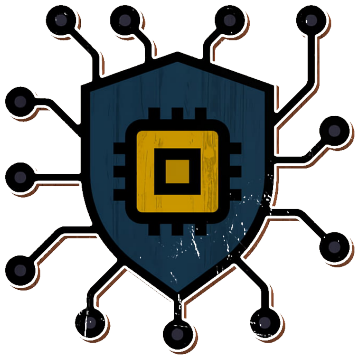


W11D4

Scansione dei servizi con Nmap su Target Windows [LAN3]

&

[Facoltativo] Scansione nella stessa rete [LAN1]

1 Introduzione

- Questo report documenta le scansioni effettuate con Nmap sul target Windows con il Windows Firewall abilitato e disabilitato, come richiesto dalla traccia dell'esame

- Le scansioni sono state eseguite inizialmente sulla rete LAN3 [IP 192.168.52.102], per la parte facoltativa sulla rete LAN1 [IP 192.168.50.102] dopo aver spostato il target nella stessa rete dell'attaccante

- L'obiettivo è identificare le porte aperte, i servizi attivi e il sistema operativo del target, confrontando i risultati con e senza firewall e in diverse configurazioni di rete

- La rete è stata correttamente configurata con pfSense per garantire la connettività tra l'attaccante e il target

2 Configurazione della macchina

Le scansioni sono state condotte in un ambiente virtuale configurato su **VirtualBox**, macchine:

❍ Attaccante

- **Nome** Kali Linux
- **IP** 192.168.50.100
- **Rete** LAN1 [192.168.50.0/24]
- **Descrizione** Sistema operativo basato su Debian, utilizzato per eseguire le scansioni con Nmap, Kali è configurato come macchina attaccante.

❍ Target

- **Nome** Windows
- **IP iniziale** 192.168.52.102 [LAN3]
- **IP facoltativo** 192.168.50.102 [LAN1, per la parte facoltativa]
- **Rete iniziale** LAN3 [192.168.52.0/24]
- **Rete facoltativa** LAN1 [192.168.50.0/24]
- **Descrizione** Macchina Windows [identificata come Windows 10 1507-1607] utilizzata come target delle scansioni, il Windows Firewall è stato riattivato con il comando netsh advfirewall set allprofiles state on per le scansioni iniziali e disabilitato per la seconda serie con netsh advfirewall set allprofiles state off

❍ Router/Firewall

- **Nome** pfSense

⇒ **Interfacce**

- WAN 192.168.1.172/24
- LAN1 192.168.50.1/24 [rete di Kali e target nella parte facoltativa]

- LAN2 192.168.51.1/24 [rete di Metasploitable, non utilizzata in questo esame]

- LAN3: 192.168.52.1/24 [rete iniziale di Windows]

- **Descrizione** pfSense gestisce il routing e il firewalling tra le reti, le regole di pfSense sono state configurate per consentire il traffico tra LAN1 e LAN3 e successivamente su LAN1, permettendo al target di rispondere al ping

3 Metodologia

Le scansioni sono state eseguite utilizzando **Nmap** su Kali Linux [192.168.50.100], tipi di scansione utilizzati:

3.1 Ping Scan [-sn Verifica se il target è attivo]

3.2 SYN Scan [-sS Scansione stealth TCP per identificare le porte aperte]

3.3 SYN Scan [-sU Scansione delle porte UDP]

2.4 Service Scan [-sV Rilevamento dei servi e delle loro versioni]

2.5 OS Detection [-O Identificazione del sistema operativo]

4 Scansioni con Windows Firewall [abilitato] [LAN3]

- In questa sezione, il target Windows [192.168.52.102] è nella rete LAN3 con il firewall abilitato [netsh advfirewall set allprofiles state on]

- Verifica Ping ping -c 3 192.168.52.102

```
┌──(kali㉿kali)-[~]
└─$ ping -c 3 192.168.52.102
PING 192.168.52.102 (192.168.52.102) 56(84) bytes of data.
64 bytes from 192.168.52.102: icmp_seq=1 ttl=127 time=1.99 ms
64 bytes from 192.168.52.102: icmp_seq=2 ttl=127 time=2.33 ms
64 bytes from 192.168.52.102: icmp_seq=3 ttl=127 time=2.84 ms

── 192.168.52.102 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2025ms
rtt min/avg/max/mdev = 1.993/2.387/2.839/0.347 ms
```

4.1 Connectivity check

- Verifica connettività nmap -sn 192.168.52.102

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.52.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-20 03:49 EDT
Nmap scan report for 192.168.52.102
Host is up (0.0052s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

- Il target è attivo e raggiungibile, confermando che la configurazione di pfSesne consente il traffico

4.2 TCP SYN Scan

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -p- 192.168.52.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-20 03:49 EDT
Nmap scan report for 192.168.52.102
Host is up (0.0074s latency).
Not shown: 65509 filtered tcp ports (no-response)
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
49408/tcp open  unknown
49409/tcp open  unknown
49410/tcp open  unknown
49411/tcp open  unknown
49415/tcp open  unknown
49417/tcp open  unknown
49418/tcp open  unknown
49516/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 190.23 seconds
```

- Sono state rilevate 26 porte TCP aperte incluse porte comuni di Windows [135-139-445-3389] e altre insolite [7-9-13-17-19- 5432], questo suggerisce una configurazione permissiva del firewall o un sistema non standard

4.3 UDP Scan

❍ Verifica scansione UDP nmap -sU -p1-1000 192.168.52.102

```
┌──(kali㉿kali)-[~]
└─$ nmap -sU -p1-1000 192.168.52.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-20 03:53 EDT
Nmap scan report for 192.168.52.102
Host is up (0.0035s latency).
All 1000 scanned ports on 192.168.52.102 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 28.87 seconds
```

❍ Nessuna porta UDP aperta rilevata, tutte risultano [open|filtered] a causa del Firewall

4.4 Scanning Services

- Verifica delle porte specificate [7-9-13-17-19-80-135-139-445-1801-2103-2105-2107-3389-5432-8009-8080-8443-49408-49409-49410-49411-49415-49417-49418-49516] sono state selezionate perché identificate come aperte dalla scansione TCP SYN, garantendo un'analisi mirata dei servizi attivi

⇒ nmap -sV -p 7,9,13,17,19,80,135,139,445,1801,2103,2105,2107,3389,5432,8009,8080,8443,49408,49409,49410,49411,49415,49417,49418,49516 192.168.52.102

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 7,9,13,17,19,80,135,139,445,1801,2103,2105,2107,3389,5432,8009,8080,8443
,49408,49409,49410,49411,49415,49417,49418,49516 192.168.52.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-20 04:07 EDT
Stats: 0:02:12 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.15% done; ETC: 04:10 (0:00:05 remaining)
Nmap scan report for 192.168.52.102
Host is up (0.0054s latency).

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
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
49415/tcp open  msrpc         Microsoft Windows RPC
49417/tcp open  msrpc         Microsoft Windows RPC
49418/tcp open  msrpc         Microsoft Windows RPC
49516/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 160.24 seconds
```

- La scansione ha identificato servizi come Microsoft IIS [porta 80] RPC [135-2103-2105-2107-49408-49411-49415-49417-49418-49516] NetBIOS [139] SMB [445] RDP [3389] e Apache Tomcat [8080- 8009] La porta 5432 [PostgreSQL] e altre [7-9-13-17-19] suggeriscono una configurazione non standard

4.5 Operating system detection

- Rilevazione Sistema Operativo nmap -O 192.168.52.102

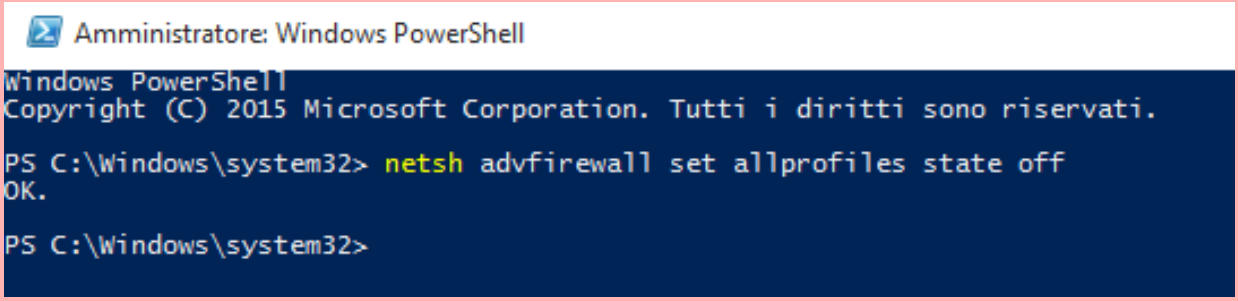
```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.52.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-20 04:12 EDT
Nmap scan report for 192.168.52.102
Host is up (0.0035s latency).
Not shown: 982 filtered tcp ports (no-response)
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   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
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 10.30 seconds
```

- Il rilevamento del SO è inaffidabile perché Nmap non ha trovato almeno una porta chiusa, tuttavia, le ipotesi indicano una versione di Windows [tipo Windows 10-Windows 7-Server 2016] coerente con i servizi rilevati

5 Scansioni con Windows Firewall [Disabilitato] [LAN3]

- In questa sezione, il Windows Firewall sul target [192.168.52.102] sarà disabilitato [netsh advfirewall set allprofiles state off]

- **DISATTIVAZIONE** Accedo al target Windows tramite RDP ed eseguo comando PowerShell [con provilegi amministrativi] netsh advfirewall set allprofiles state off



5.1 Connectivity check

❍ Verifica connettività nmap -sn 192.168.52.102

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.52.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-20 04:25 EDT
Nmap scan report for 192.168.52.102
Host is up (0.0025s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

❍ Il target è attivo e raggiungibile

5.2 TCP SYN Scan

❍ Verifica scansione TCP SYN nmap -sS -p- 192.168.52.102

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -p- 192.168.52.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-20 04:25 EDT
Nmap scan report for 192.168.52.102
Host is up (0.0028s latency).
Not shown: 65509 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
49408/tcp open  unknown
49409/tcp open  unknown
49410/tcp open  unknown
49411/tcp open  unknown
49415/tcp open  unknown
49417/tcp open  unknown
49418/tcp open  unknown
49516/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 3333.79 seconds
```

❍ Le stesse 26 porte TCP aperte rilevate con firewall abilitato, la differenza principale è che le porte non aperte sono ora [closed] [reset] invece di [filtered], confermando che il firewall è disabilitato

5.3 UDP Scan

❍ Verifica scansione UDP nmap -sU -p1-1000 192.168.52.102

```
┌──(kali㉿kali)-[~]
└─$ nmap -sU -p1-1000 192.168.52.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-20 05:21 EDT
Nmap scan report for 192.168.52.102
Host is up (0.0024s latency).
Not shown: 990 closed udp ports (port-unreach)
PORT    STATE         SERVICE
7/udp   open|filtered echo
9/udp   open|filtered discard
13/udp  open|filtered daytime
17/udp  open|filtered qotd
19/udp  open|filtered chargen
137/udp open          netbios-ns
138/udp open|filtered netbios-dgm
161/udp open|filtered snmp
500/udp open|filtered isakmp
520/udp open|filtered route

Nmap done: 1 IP address (1 host up) scanned in 1123.52 seconds
```

❍ La porta 137/udp [NetBIOS Name Service] è aperta e altre porte [7- 9 - 13 - 17 - 19 - 138 - 161 - 500 - 520] sono [open|filtered] questo indica che il firewall disabilitato consente maggiore visibilità delle porte UDP rispetto a prima

5.4 Scanning Services

- Verifica delle porte TCP specificate [7 -9 - 13 - 17 - 19 - 80 - 135 - 139 - 445 - 1801 - 2103 - 2105 - 2107 - 3389 - 5432 - 8009 - 8080 - 8443 - 49408 - 49409 - 49410 - 49411 - 4941 - 49417 - 49418 - 49516] sono state selezionate perché identificate come aperte dalla scansione TCP SYN, garantendo un'analisi mirata dei servizi attivi

⇒ nmap -sV -p 7,9,13,17,19,80,135,139,445,1801,2103,2105,2107,3389,5432,8009,8080,8443,49408,49409,49410,49411,49415,49417,49418,49516 192.168.52.102

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 7,9,13,17,19,80,135,139,445,1801,2103,2105,2107,3389,5432,8009,8080,8443,49
408,49409,49410,49411,49415,49417,49418,49516 192.168.52.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-20 05:56 EDT
Nmap scan report for 192.168.52.102
Host is up (0.0075s latency).

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
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
49415/tcp open  msrpc         Microsoft Windows RPC
49417/tcp open  msrpc         Microsoft Windows RPC
49418/tcp open  msrpc         Microsoft Windows RPC
49516/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 159.76 seconds
```

- I servizi sono identici a quelli rilevati con firewall abilitato, indicando che il firewall non blocca queste porte TCP, i servizi includono IIS [80] RPC [135 - 2103 - 2105 - 2107 - 49408 - 49411 - 49415 - 49417 - 49418 - 49516] NetBIOS [139] SMB [445] RDP [3389] Apache Tomcat [8080 - 8009] PostgreSQL [5432]

5.5 Operating system detection

- Rilevazione Sistema Operativo nmap -O 192.168.52.102

```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.52.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-20 05:58 EDT
Nmap scan report for 192.168.52.102
Host is up (0.0039s 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 3.54 seconds
```

- Il rilevamento del SO è più accurato grazie alle porte chiuse rilevate [reset] Nmap identifica il sistema come Windows 10 1607, coerente con i servizi rilevati

6 [Facoltativa] Scansioni nella Stessa Rete (LAN1)

6.1 Scansione con Firewall [Abilitato]

- Il target Windows sarà spostato da LAN 3 sulla rete LAN1 con gateway [192.168.50.1/24] e IP [192.168.50.102]

- **ATTIVAZIONE** Accedo al target Windows tramite RDP ed eseguo comando PowerShell [con provilegi amministrativi] [netsh advfirewall set allprofiles state on]

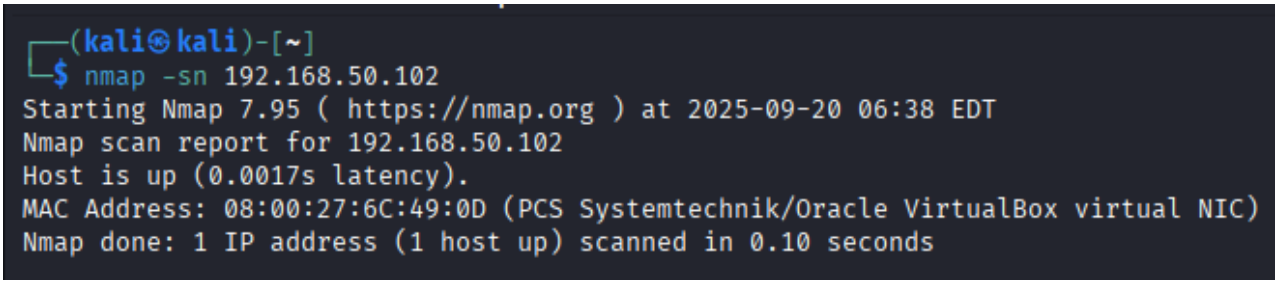
```
PS C:\Windows\system32> netsh advfirewall set allprofiles state on
OK.
```

- Verifica Ping ping -c 3 192.168.50.102

```
┌──(kali㉿kali)-[~]
└─$ ping -c 3 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=2.16 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=9.62 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=1.51 ms

── 192.168.50.102 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2079ms
rtt min/avg/max/mdev = 1.511/4.427/9.616/3.678 ms
```

6.1.1 Connectivity check

- Verifica connettività nmap -sn 192.168.50.102



- Il target è attivo e raggiungibile nella rete LAN1 con latenza ridotta [0.0017s] rispetto a LAN3 [0.0052s] suggerendo una comunicazione più diretta

6.1.2 TCP SYN Scan

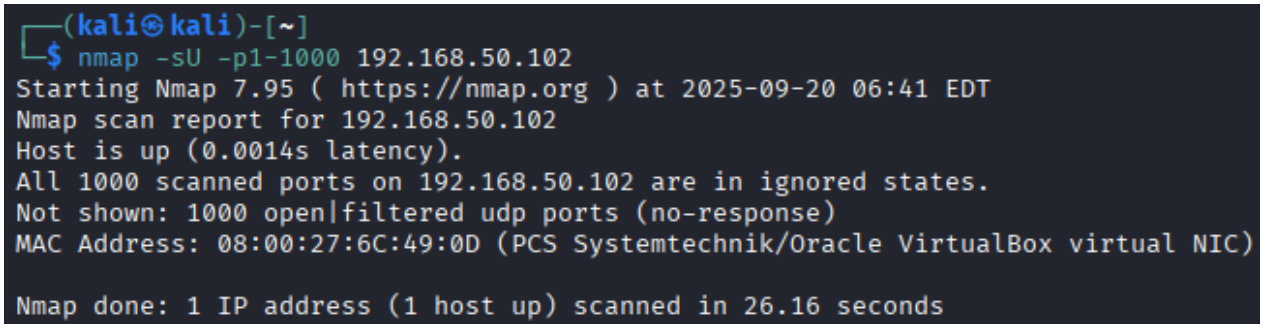
- Verifica scansione TCP SYN nmap -sS -p- 192.168.50.102

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -p- 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-20 06:38 EDT
Nmap scan report for 192.168.50.102
Host is up (0.0026s latency).
Not shown: 65509 filtered tcp ports (no-response)
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
49408/tcp open  unknown
49409/tcp open  unknown
49410/tcp open  unknown
49411/tcp open  unknown
49415/tcp open  unknown
49417/tcp open  unknown
49418/tcp open  unknown
49516/tcp open  unknown
MAC Address: 08:00:27:6C:49:0D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 122.99 seconds
```

- Le stesse 26 porte TCP aperte rilevate su LAN3 indicando che la configurazione del firewall è invariata, le porte non aperte sono [filtered] come su LAN3

6.1.3 UDP Scan

- Verifica scansione UDP nmap -sU -p1-1000 192.168.50.102



- Nessuna porta UDP aperta rilevata, tutte risultano [open|filtered] come su LAN3 con firewall abilitato

6.1.4 Scanning Services

- Verifica delle porte specificate [7 - 9 - 13 - 17 - 19 - 80 -135 - 139 - 445 - 1801 - 2103 - 2105 - 2107 - 3389 - 5432 - 8009 - 8080 - 8443 - 49408 - 49409 - 49410 - 49411 - 49415 - 49417 - 49418 - 49516] sono state selezionate perché identificate come aperte dalla scansione TCP SYN su LAN1

⇒ nmap -sV -p 7,9,13,17,19,80,135,139,445,1801,2103,2105,2107,3389,5432,8009,8080,8443,49408,49409,49410,49411,49415,49417,49418,49516 192.168.50.102

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 7,9,13,17,19,80,135,139,445,1801,2103,2105,2107,3389,5432,8009,8080,8443,49408,49409,49410,49411,49415,49417,49418,49516 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-20 06:55 EDT
Nmap scan report for 192.168.50.102
Host is up (0.0054s latency).

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
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
49415/tcp open  msrpc         Microsoft Windows RPC
49417/tcp open  msrpc         Microsoft Windows RPC
49418/tcp open  msrpc         Microsoft Windows RPC
49516/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 08:00:27:6C:49:0D (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 159.36 seconds
```

- I servizi sono identici a quelli rilevati su LAN3, includendo IIS [80] RPC [135 - 2103 - 2105 - 2107 - 49408 - 49411 - 49415 - 49417 - 49418 - 49516] NetBIOS [139] SMB [445] RDP [3389] Apache Tomcat [8080 - 8009] PostgreSQL [5432]

6.1.5 Operating system detection

- Rilevazione Sistema Operativo nmap -O 192.168.50.102

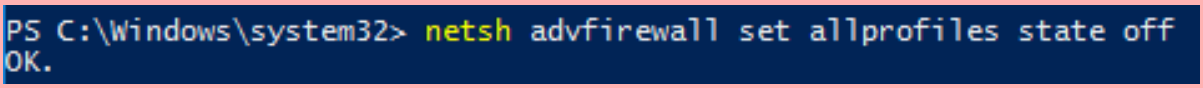
```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-20 06:58 EDT
Nmap scan report for 192.168.50.102
Host is up (0.0017s latency).
Not shown: 982 filtered tcp ports (no-response)
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   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: 08:00:27:6C:49:0D (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 Embed
ded Standard 7 (93%), Microsoft Windows 10 1511 - 1607 (92%), Microsoft Windows 10 1511 (91%), Microsoft Windows 7 or Win
dows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 or Windows 8.1 (91%), Microsoft Windows Server 2016 (91%), Mi
crosoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (91%), Microsoft Windows Vista SP2, Windows 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 8.99 seconds
```

- Il rilevamento del SO è inaffidabile per mancanza di una porta chiusa, ma ipotizza Windows 10 1607, coerente con i risultati su LAN3, la rete LAN1 ha una distanza di 1 hop [vs 2 hops su LAN3] indicando una comunicazione più diretta

6.2 Scansione con Firewall [Disabilito]

- In questa sezione, il Windows Firewall sul target [192.168.50.102] sarà disabilitato [netsh advfirewall set allprofiles state off]

- **DISATTIVAZIONE** Accedo al target Windows tramite RDP ed eseguo comando PowerShell [con provilegi amministrativi] netsh advfirewall set allprofiles state off



6.2.1 Connectivity check

Verifica connettività nmap -sn 192.168.50.102

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-20 07:12 EDT
Nmap scan report for 192.168.50.102
Host is up (0.0013s latency).
MAC Address: 08:00:27:6C:49:0D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

- Il target è attivo e raggiungibile nella rete LAN1, con latenza ridotta [0.0013s]

6.2.2 TCP SYN Scan

- Verifica scansione TCP SYN nmap -sS -p- 192.168.50.102

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -p- 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-20 07:12 EDT
Nmap scan report for 192.168.50.102
Host is up (0.0096s latency).
Not shown: 65509 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
49408/tcp open  unknown
49409/tcp open  unknown
49410/tcp open  unknown
49411/tcp open  unknown
49415/tcp open  unknown
49417/tcp open  unknown
49418/tcp open  unknown
49516/tcp open  unknown
MAC Address: 08:00:27:6C:49:0D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 27.90 seconds
```

- Le stesse 26 porte TCP aperte rilevate su LAN3 con firewall disabilitato, le porte non aperte sono “closed” [reset] confermando che il firewall è disabilitato, la scansione è stata più veloce [27.90s vs 3333.79s su LAN3] probabilmente per la rete più diretta

6.2.3 UDP Scan

- Verifica scansione UDP nmap -sU -p1-1000 192.168.50.102

```
┌──(kali㉿kali)-[~]
└─$ nmap -sU -p1-1000 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-20 07:15 EDT
Nmap scan report for 192.168.50.102
Host is up (0.0014s latency).
Not shown: 990 closed udp ports (port-unreach)
PORT    STATE         SERVICE
7/udp   open          echo
9/udp   open|filtered discard
13/udp  open          daytime
17/udp  open          qotd
19/udp  open          chargen
137/udp open          netbios-ns
138/udp open|filtered netbios-dgm
161/udp open|filtered snmp
500/udp open|filtered isakmp
520/udp open|filtered route
MAC Address: 08:00:27:6C:49:0D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1078.02 seconds
```

- Le porte 7/udp, 13/udp, 17/udp, 19/udp, e 137/udp sono aperte, altre [9 - 138 - 161 - 500 - 520] sono [open|filtered], rispetto a LAN3, le porte 7- 13 - 17 - 19 sono passate da [open|filtered] a [open] indicando maggiore visibilità delle porte UDP con firewall disabilitato su LAN1

6.2.4 Scanning Services

- Verifica delle porte specificate [7 - 9 - 13 - 17 - 19 - 80 - 135 - 139 - 445 - 1801 - 2103 - 2105 - 2107 - 3389 - 5432 - 8009 - 8080 - 8443 - 49408 - 49409 - 49410 - 49411 - 49415 - 49417 - 49418 - 49516] sono state selezionate perché identificate come aperte dalla scansione TCP SYN su LAN1 con firewall disabilitato

⇒ nmap -sV -p 7,9,13,17,19,80,135,139,445,1801,2103,2105,2107,3389,5432,8009,8080,8443,49408,49409,49410,49411,49415,49417,49418,49516 192.168.50.102

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 7,9,13,17,19,80,135,139,445,1801,2103,2105,2107,3389,5432,8009,8080,8443,49408,49409,49410,49411,49415,49417,49418,
49516 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-20 07:50 EDT
Nmap scan report for 192.168.50.102
Host is up (0.0074s latency).

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
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
49415/tcp open  msrpc         Microsoft Windows RPC
49417/tcp open  msrpc         Microsoft Windows RPC
49418/tcp open  msrpc         Microsoft Windows RPC
49516/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 08:00:27:6C:49:0D (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 159.13 seconds
```

- I servizi sono identici a quelli rilevati su LAN3 e LAN1 con firewall abilitato, includendo IIS [80] RPC [135 - 2103 - 2105 - 2107 - 49408 - 49411 - 49415 - 49417 - 49418 - 49516] NetBIOS [139] SMB [445] RDP [3389] Apache Tomcat [8080 - 8009] PostgreSQL [5432]

6.2.5 Operating system detection

- Rilevazione Sistema Operativo nmap -O 192.168.50.102

```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-20 07:53 EDT
Nmap scan report for 192.168.50.102
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
MAC Address: 08:00:27:6C:49:0D (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 2.97 seconds
```

- Il rilevamento del SO identifica Windows 10 1507-1607 con maggiore accuratezza grazie alle porte chiuse rilevate (reset)

7 Risultati e Confronto

7.1 Firewall Abilitato [LAN3]

- **Ping Scan**: Host attivo [0.0052s latency]
- **TCP SYN**: 26 porte aperte [7 - 9 - 13 - 17 - 19 - 80 - 135 - 139 - 445 - 1801 - 2103 - 2105 - 2107 - 3389 - 5432 - 8009 - 8080 - 8443 - 49408 - 49411 - 49415 - 49417 - 49418 - 49516]
- **UDP Scan**: Nessuna porta aperta, tutte [open|filtered]
- **Service Scan**: Servizi includono IIS [80] RPC [135 - 2103 - 2105 - 2107 - 49408 - 49411 - 49415 - 49417 - 49418 - 49516] NetBIOS [139] SMB [445] RDP [3389] Apache Tomcat [8080 - 8009] PostgreSQL [5432]
- **OS Detection**: Ipotesi di Windows 10, 7, o Server [inaffidabile per mancanza di porte chiuse]
- **Tempi di scansione**: [TCP SYN 190.23s] [UDP: 28.87s] [Service Scan: 160.24s] [OS Detection: 10.30s]

7.2 Firewall Disabilitato [LAN3]

- **Ping Scan**: Host attivo [0.0025s latency]
- **TCP SYN**: Stesse 26 porte aperte, porte non aperte [closed] (reset)
- **UDP Scan**: Porta 137/udp aperta, porte 7 - 9 - 13 - 17 - 19 - 138 - 161 - 500 - 520 [open|filtered]
- **Service Scan**: Servizi identici a firewall abilitato
- **OS Detection**: Windows 10 1607 identificato con maggiore accuratezza
- **Tempi di scansione**: [TCP SYN 3333.79s “più lungo, probabilmente per condizioni di rete”] [UDP 1123.52s] [Service Scan 159.76s] [OS Detection: 3.54s]

7.3 Firewall Abilitato [LAN1]

- **Ping Scan**: Host attivo [0.0017s latency]
- **TCP SYN**: Stesse 26 porte aperte, porte non aperte [filtered]
- **UDP Scan**: Nessuna porta aperta, tutte [open|filtered]
- **Service Scan**: Servizi identici a LAN3
- **OS Detection**: Ipotesi di Windows 10 1607 [inaffidabile per mancanza di porte chiuse]
- **Tempi di scansione**: [TCP SYN 122.99s] [UDP 26.16s] [Service Scan 159.36s] [OS Detection 8.99s]

7.4 Firewall Disabilitato [LAN1]

- **Ping Scan**: Host attivo [0.0013s latency]
- **TCP SYN**: Stesse 26 porte aperte, porte non aperte [closed] (reset)
- **UDP Scan**: Porte 7 - 13 - 17 - 19 - 137/udp aperte, porte 9 - 138 - 161 - 500 - 520 [open|filtered]
- **Service Scan**: Servizi identici a LAN3 e LAN1 con firewall abilitato
- **OS Detection**: Windows 10 1507-1607 identificato con maggiore accuratezza
- **Tempi di scansione**: [TCP SYN 27.90s] [UDP 1078.02s] [Service Scan 159.13s] [OS Detection 2.97s]

8 Conclusioni

- Con il firewall abilitato, il target espone 26 porte TCP su entrambe le reti [LAN3 e LAN1] suggerendo una configurazione permissiva o non standard [tipo PostgreSQL, servizi di test come echo, qotd]

- Disabilitare il firewall su LAN3 e LAN1 aumenta la visibilità delle porte UDP [tipo 137/udp aperta su entrambe, 7 - 13 - 17 - 19/udp aperte su LAN1] e conferma le porte TCP aperte, con porte non aperte rilevate come [closed] invece di [filtered] migliorando l'accuratezza del rilevamento del SO Windows 10 1507-1607]

- Spostare il target su[LAN1 non ha modificato le porte TCP aperte, ma ha ridotto la latenza [0.0013-0.0017s vs 0.0025-0.0052s] e la distanza di rete [1 hop vs 2 hops] indicando una comunicazione più diretta senza filtri significativi di pfSense

- La configurazione non standard [tipo porte 7, 9, 13, 17, 19, 5432] indica un sistema di test con software aggiuntivo [tipo Apache Tomcat, PostgreSQL]

- Le scansioni su LAN1 sono state significativamente più veloci [tipo TCP SYN 27.90-122.99s vs 190.23-3333.79s su LAN3] probabilmente per la rete più diretta

Consigli fondametali

- Configurare il firewall per limitare l'esposizione di porte non necessarie [tipo 7 - 9 - 13 - 17 - 19] e monitorare i servizi non standard [tipo PostgreSQL, Tomcat]

- Verificare la configurazione di rete per ottimizzare i tempi di scansione su LAN3