In questo esercizio ho analizzato il comportamento di un sistema operativo Windows 10 (IP: **192.168.50.102**) utilizzando Nmap in due contesti differenti:

1. **Con Windows Firewall attivo**
2. **Con Windows Firewall disattivato**

Lo scopo dell'esercitazione era osservare come il firewall influenzi la visibilità delle porte e dei servizi accessibili dall'esterno.
Ho eseguito quattro tipologie di scansione per ciascuna configurazione:

- OS Fingerprinting (-O)
- SYN Scan (-sS)
- TCP Connect Scan (-sT)
- Version Detection (-sV)

1. Scansioni con Windows Firewall ATTIVO

Con il firewall attivato, Windows applica politiche molto restrittive: la maggior parte delle porte appare come "filtered", segno che i pacchetti vengono bloccati in fase di filtro e non raggiungono i servizi interni.

✓ 1.1 OS Fingerprinting (-O)

La scansione mostra pochissime porte aperte e molti pacchetti filtrati.
Nmap ha difficoltà a riconoscere con precisione il sistema operativo a causa della scarsa superficie esposta.

```
┌──(pireddone㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.102
[sudo] password for pireddone:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 00:05 CET
Nmap scan report for 192.168.50.102
Host is up (0.0013s 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:F6:72:91 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed po
rt
Aggressive OS guesses: Microsoft Windows 10 1607 (97%), Microsoft Windows Phone 7.5 or 8.0 (94%), M
icrosoft Windows Embedded Standard 7 (93%), Microsoft Windows 10 1511 - 1607 (92%), Microsoft Windo
ws 7 or Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 or Windows 8.1 (91%), Micros
oft Windows Server 2016 (91%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Wind
ows 7 (91%), Microsoft Windows 11 21H2 (91%), Microsoft Windows Vista SP2, Windows 7 SP1, or Window
s Server 2008 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

✓ 1.2 SYN Scan (-sS)

Mostra solo poche porte aperte, principalmente servizi Windows di sistema:

- 80 (HTTP – IIS)
- 135 (MSRPC)
- 1801, 2103, 2105, 2107 (MSMQ)
- 3389 (RDP)
- 8443 (HTTPS-alt)

Il firewall filtra tutte le altre.

```
┌──(pireddone㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 00:07 CET
Nmap scan report for 192.168.50.102
Host is up (0.0013s 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:F6:72:91 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

✓ 1.3 TCP Connect Scan (-sT)

I risultati sono praticamente identici alla SYN scan.
La connect scan completa il three-way handshake, ma il firewall blocca comunque tutto ciò che non è esplicitamente consentito.

```
┌──(pireddone㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 00:08 CET
Nmap scan report for 192.168.50.102
Host is up (0.0023s 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:F6:72:91 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 17.93 seconds
```

✓ 1.4 Version Detection (-sV)

Con firewall attivo, alcune versioni vengono identificate, ma non tutte.

Servizi rilevati:

- **Microsoft IIS 10.0** (porta 80)
- **Microsoft RPC**
- **Terminal Services/RDP**
- **HTTPS-alt** configurato

```
┌──(piredd one㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 00:08 CET
Nmap scan report for 192.168.50.102
Host is up (0.0012s 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:F6:72:91 (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 94.09 seconds
```

2. Scansioni con Windows Firewall DISATTIVATO

Una volta disabilitato il firewall, la superficie di attacco è aumentata in modo significativo: il sistema risponde a molte più porte e servizi.

✓ 2.1 OS Fingerprinting (-O)

Con molte più porte aperte, Nmap riesce finalmente a identificare correttamente il sistema operativo:

- **Microsoft Windows 10**
- Versione compatibile con build 1507–1607

Molte porte addizionali risultano aperte, come:

- echo (7)
- daytime (13)
- QOTD (17)
- Chargen (19)

- 8000, 8009, 8080, 8443, ecc.

```
┌──(pireddone㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 00:13 CET
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:F6:72:91 (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 14.96 seconds
```

✓ 2.2 SYN Scan (-sS)

Mostra decine di porte aperte, inclusi:

- Servizi legacy (echo, discard, chargen, QOTD)
- Web server alternativi
- PostgreSQL su porta 5432
- Jserv (8009)
- Proxy HTTP (8080)

Windows risponde apertamente ai pacchetti SYN.

```
┌──(pireddone㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 00:14 CET
Nmap scan report for 192.168.50.102
Host is up (0.00094s 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:F6:72:91 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.89 seconds
```

✓ 2.3 TCP Connect Scan (-sT)

I risultati combaciano con la SYN scan:

- tutte le porte visibili
- connessioni accettate
- nessun filtraggio

```
┌──(pireddone㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 00:14 CET
Nmap scan report for 192.168.50.102
Host is up (0.0050s 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:F6:72:91 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.99 seconds
```

✓ 2.4 Version Detection (-sV)

Con il firewall spento, Nmap riesce a identificare:

- **Microsoft IIS 10**
- **Microsoft RPC**
- **Servizi Windows integrati**
- **Apache Jserv**
- **Apache Tomcat/Coyote JSP engine**
- **PostgreSQL**

La quantità di informazioni ottenute è molto maggiore rispetto alla configurazione precedente.

```
┌──(pireddone㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 00:15 CET
Nmap scan report for 192.168.50.102
Host is up (0.00066s 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:F6:72:91 (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 171.58 seconds
```

🔵 3. Confronto tra Windows con e senza Firewall

Elemento	Firewall ON	Firewall OFF
Porte visibili	Poche	Molte
Servizi rilevati	Limitati	Numerosi
OS detection	Inaccurata	Precisa
Superficie di attacco	Minima	Estesa
Rumorosità rete	Alta (molti “filtered”)	Bassa

✓ Considerazioni finali

- Il firewall attivo nasconde gran parte dell’host, rendendo difficile la ricognizione.
- Il firewall spento espone numerosi servizi che potrebbero essere potenziali vettori d’attacco.
- Lo scopo dell’esercizio è dimostrare quanto sia importante il firewall nella difesa perimetrale di un sistema Windows.

Conclusione

L’esercizio ha mostrato chiaramente come il Windows Firewall influenzi drasticamente i risultati delle scansioni.
Con il firewall attivo, l’host appare protetto e minimamente esposto; con il firewall disattivato, al contrario, emergono numerosi servizi che ampliano la superficie di attacco.