

Esercizio W11D4

- Eseguire scansione nmap su Windows con Firewall attivo:
Per eseguire la scansione con la rilevazione del sistema operativo e le versioni in uso dei servizi attivi uso il flag -sV e -O ed ottengo il seguente risultato:

```
➥ sudo nmap -sV -O 192.168.50.102 -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-03 04:52 EST
Stats: 0:01:17 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 81.82% done; ETC: 04:53 (0:00:13 remaining)
Nmap scan report for 192.168.50.102
Host is up (0.0018s latency).
Not shown: 989 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: WORKGROUP)
1801/tcp  open  msmq?          Microsoft Windows RPC
2103/tcp  open  msrpc          Microsoft Windows RPC
2105/tcp  open  msrpc          Microsoft Windows RPC
2107/tcp  open  msrpc          Microsoft Windows RPC
3389/tcp  open  ssl/ms-wbt-server?
5357/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8443/tcp  open  ssl/https-alt
MAC Address: 08:00:27:16:3B:0C (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 Phone 7.5 or 8.0 (92%), Microsoft Windows 10 1511 - 1607 (92%), Microsoft Windows Embedded Standard 7 (92%), Microsoft Windows 10 1607 (91%), Microsoft Windows 10 1511 (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, Windows 7 SP1, or Windows Server 2008 (90%), Microsoft Windows Server 2008 R2 or Windows 8.1 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: DESKTOP-9K104BT; OS: Windows; CPE: cpe:/o:microsoft:windows
```

- Eseguire la scansione nmap su Windows con Firewall disattivo:
Per eseguire la scansione, uso i comandi come sopra, ed ottengo il seguente risultato:

```
➥ sudo nmap -sV -O 192.168.50.102 -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-03 10:56 CET
Nmap scan report for 192.168.50.102
Host is up (0.0019s latency).
Not shown: 981 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?          Microsoft Windows RPC
2103/tcp  open  msrpc          Microsoft Windows RPC
2105/tcp  open  msrpc          Microsoft Windows RPC
2107/tcp  open  msrpc          Microsoft Windows RPC
3389/tcp  open  ssl/ms-wbt-server?
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
MAC Address: 08:00:27:16:3B:0C (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
Service Info: Host: DESKTOP-9K104BT; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Dalle 2 scansioni si nota come disattivando il firewall in Windows vengono mostrate ulteriori porte aperte e come si sia determinato con certezza il sistema operativo.
Le porte aperte adesso sono 19 contro le 11 della scansione con il firewall attivo.