Scansione dei servizi su Windows

Le seguenti scansioni sono state fatte su host windows 10 (51.102) su subnet 192.168.51.0/24 da sorgente kali (50.100) su subnet 192.168.50.0/24, scansioni effettuate con FW Windows attivo.

OS Fingerprint → *nmap -O 192.168.51.102*

```
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
 1607 (92%), Microsoft Windows 10 1511 (91%), Microsoft Windows 7 or Windows Server 2008 R2 (91%), Microsoft Windows
s Server 2016 (91%), Microsoft Windows 7 Professional or Windows 8 (91%), Microsoft Windows Vista SP0 or SP1, Window
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 10.01 seconds
```

I risultati di OS Fingerprint potrebbero non essere affidabili, vengono riportati diversi sistemi con relativa percentuale di possibilità.

Syn Scan → *nmap -sS 192.168.51.102*

```
Nmap scan report for 192.168.51.102
Host is up (0.0071s 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

Nmap done: 1 IP address (1 host up) scanned in 6.26 seconds
```

Lo stato “992 **filtered** tcp ports” significa che Nmap non è riuscito a determinare se quelle porte sono **open** o **closed** perché il Windows Firewall ha bloccato i pacchetti. Le porte che risultano open sono quelle che hanno risposto e che corrispondono a una regola specifica di "allow".

TCP connect → *nmap -sT 192.168.51.102*

```
Nmap scan report for 192.168.51.102
Host is up (0.0070s 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

Nmap done: 1 IP address (1 host up) scanned in 6.06 seconds
```

Scansione che completa il 3-way-handshake, stesso output della scansione precedente.

Version detection → *nmap -sV 192.168.51.102*

```
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  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 109.79 seconds
```

La scansione è riuscita ad individuare le versioni dei servizi sulle porte open.

Disattivazione Windows Defender Firewall

Da questo momento nel report saranno riportate le stesse scansioni, con lo stesso target ma con Firewall Windows disattivato. Comando CMD per disabilitare tutti i profili FW:

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

OS Fingerprint → *nmap -O 192.168.51.102*

```
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 9.24 seconds
```

La scansione ha prodotto un output differente: ci sono più porte open, vengono riportati gli hops della comunicazione (2) ma soprattutto è stata rilevata una versione confermata del sistema operativo.

Syn Scan → *nmap -sS 192.168.51.102*

```
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

Nmap done: 1 IP address (1 host up) scanned in 1.12 seconds
```

Come visto già con la scansione di prima le porte open sono aumentate. Inoltre è diminuito il tempo impiegato per la scansione senza completamento del 3-way-handshake.

TCP connect → *nmap -sT 192.168.51.102*

```
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 1.10 seconds
```

In questa scansione con completamento del 3-way-handshake non è stata registrata nessuna variazione.

Version detection → *nmap -sV 192.168.51.102*

```
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  https-alt?
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 186.35 seconds
```

Sono stati rilevati le versioni di più servizi. Si può notare come all'aumentare delle porte open, di conseguenza anche dei servizi esposti, aumenti anche il tempo impiegato per la scansione.