Tecniche di scansione con Nmap

Giuseppe Gigliotti
gius199874@gmail.com

November 11, 2025

Indice

1 Descrizione:

Questo esercizio è diviso in due fasi. Nella prima chiede di effettuare le scansioni fatte nell'esercizio precedente con Nmap sul target Windows con indirizo IP 192.168.51.102 con Windows Firewall abilitato e disabilitato. (OS fingerprint,Syn Scan - TCP connect, trovate differenze tra i risultati della scansioni TCP connect e SYN? - Version detection) Esse infatti si trovano su "reti diverse" avendo la kali (la nostra macchina attaccante) sull'indirizzo IP 192.168.50.100. Per fare ciò abbiamo utilizzato una terza macchina PFSENSE (già configurata), utilizzando come router per far comunicare le due macchine. Finite le scansioni e raccolte le informazioni richieste dalla traccia:

- IP
- Sistema Operativo
- porte aperte
- servizi in ascolto con versione
- descrizione dei servizi

Alla fine di questa prima fase si può spostare il target Windows nella stessa rete dell attaccante e ripetere le scansioni con Windows Firewall abilitato e disabilitato per passare alla seconda fase. La seconda fase (facoltativa) richiedeva di modificare le impostazioni di rete, portando il nostro target sulla stessa rete della kali, quindi la macchina windows, avrà indirizzo 192.168.50.102.

2 FASE 1: RETE DIVERSA

- Target: 192.168.51.102 (windows 10)
- Attaccante 192.168.50.100 (kali)
- Macchina di supporto 192.168.50.1 (Pfsense)

2.1 FIREWALL DISATTIVATO:

2.1.1 OS Fingerprint

```
nmap -O 192.168.51.102
```

Output:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-08 21:58 CET
Nmap scan report for 192.168.51.102
Host is up (0.0016s 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/submi
Nmap done: 1 IP address (1 host up) scanned in 3.08 seconds
```

2.1.2 Syn Scan

```
nmap -sS -v 192.168.51.102
```

Aggiunto il flag -v per far visualizzare al meglio che si trattasse dello Stealth Scan

Output:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-08 22:09 CET
Initiating Ping Scan at 22:09
Scanning 192.168.51.102 [4 ports]
Completed Ping Scan at 22:09, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:09
Completed Parallel DNS resolution of 1 host. at 22:09, 0.01s elapsed
Initiating SYN Stealth Scan at 22:09
```

```
Scanning 192.168.51.102 [1000 ports]
Discovered open port 139/tcp on 192.168.51.102
Discovered open port 80/tcp on 192.168.51.102
Discovered open port 135/tcp on 192.168.51.102
Discovered open port 3389/tcp on 192.168.51.102
Discovered open port 8080/tcp on 192.168.51.102
Discovered open port 445/tcp on 192.168.51.102
Discovered open port 13/tcp on 192.168.51.102
Discovered open port 8009/tcp on 192.168.51.102
Discovered open port 19/tcp on 192.168.51.102
Discovered open port 9/tcp on 192.168.51.102
Discovered open port 17/tcp on 192.168.51.102
Discovered open port 2103/tcp on 192.168.51.102
Discovered open port 1801/tcp on 192.168.51.102
Discovered open port 2107/tcp on 192.168.51.102
Discovered open port 7/tcp on 192.168.51.102
Discovered open port 2105/tcp on 192.168.51.102
Discovered open port 8443/tcp on 192.168.51.102
Discovered open port 5432/tcp on 192.168.51.102
Completed SYN Stealth Scan at 22:09, 1.35s elapsed (1000 total ports)
Nmap scan report for 192.168.51.102
Host is up (0.0014s 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

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.50 seconds
           Raw packets sent: 1018 (44.768KB) | Rcvd: 1001 (40.100KB)
```

2.1.3 TCP connect

```
nmap -sT 192.168.51.102
```

Output:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-08 22:10 CET
Nmap scan report for 192.168.51.102
Host is up (0.0013s 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

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
```

2.1.4 Version Detection

```
nmap -sV 192.168.51.102
```

Output:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-08 22:16 CET
Nmap scan report for 192.168.51.102
Host is up (0.0015s 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: WORKGR
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
Service Info: Host: DESKTOP-9K104BT; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/
Nmap done: 1 IP address (1 host up) scanned in 159.70 seconds
```

2.2 FIREWALL ATTIVATO:

2.2.1 OS Fingerprint

```
nmap -O 192.168.51.102
```

Output:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-08 22:27 CET
Nmap scan report for 192.168.51.102
Host is up (0.0016s 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
Warning: OSScan results may be unreliable because we could not find at least 1 open an
Aggressive OS guesses: Microsoft Windows 10 1607 (97%), Microsoft Windows Phone 7.5 or
Microsoft Windows Embedded Standard 7 (93%), Microsoft Windows 10 1511 - 1607 (92%),
Microsoft Windows 7 or Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2
Microsoft Windows Server 2016 (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%)
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 8.49 seconds
```

2.2.2 Syn Scan

```
nmap -sS -v 192.168.51.102
```

Aggiunto il flag -v per far visualizzare al meglio che si trattasse dello Stealth Scan

Output:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-08 22:29 CET
Initiating Ping Scan at 22:29
Scanning 192.168.51.102 [4 ports]
Completed Ping Scan at 22:29, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:29
Completed Parallel DNS resolution of 1 host. at 22:29, 0.02s elapsed
Initiating SYN Stealth Scan at 22:29
Scanning 192.168.51.102 [1000 ports]
Discovered open port 3389/tcp on 192.168.51.102
Discovered open port 135/tcp on 192.168.51.102
Discovered open port 80/tcp on 192.168.51.102
Discovered open port 2103/tcp on 192.168.51.102
Discovered open port 2107/tcp on 192.168.51.102
Discovered open port 2105/tcp on 192.168.51.102
Discovered open port 1801/tcp on 192.168.51.102
Discovered open port 8443/tcp on 192.168.51.102
Completed SYN Stealth Scan at 22:29, 4.40s elapsed (1000 total ports)
```

```
Nmap scan report for 192.168.51.102
Host is up (0.0017s 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

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.54 seconds
           Raw packets sent: 1997 (87.844KB) | Rcvd: 10 (424B)
```

2.2.3 TCP connect

```
nmap -sT 192.168.51.102
```

Output:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-08 22:32 CET
Nmap scan report for 192.168.51.102
Host is up (0.0019s 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 4.56 seconds
```

2.2.4 Version Detection

```
nmap -sV 192.168.51.102
```

Output:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-08 22:33 CET
Nmap scan report for 192.168.51.102
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
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/s
Nmap done: 1 IP address (1 host up) scanned in 81.68 seconds
```

---

3 FASE 2: STESSA RETE

- Target: 192.168.50.102 (windows 10)
- Attaccante 192.168.50.100 (kali)

3.1 FIREWALL DISATTIVATO:

3.1.1 OS Fingerprint

```
nmap -O 192.168.50.102
```

Output:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-08 22:54 CET
Nmap scan report for windows (192.168.50.102)
Host is up (0.0011s 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
MAC Address: 08:00:27:67:DE:22 (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/submi
Nmap done: 1 IP address (1 host up) scanned in 2.84 seconds
```

3.1.2 Syn Scan

```
nmap -sS -v 192.168.50.102
```

Aggiunto il flag -v per far visualizzare al meglio che si trattasse dello Stealth Scan

Output:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-08 22:56 CET
Initiating ARP Ping Scan at 22:56
```

```
Scanning 192.168.50.102 [1 port]
Completed ARP Ping Scan at 22:56, 0.05s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 22:56
Scanning windows (192.168.50.102) [1000 ports]
Discovered open port 139/tcp on 192.168.50.102
Discovered open port 3389/tcp on 192.168.50.102
Discovered open port 445/tcp on 192.168.50.102
Discovered open port 8080/tcp on 192.168.50.102
Discovered open port 80/tcp on 192.168.50.102
Discovered open port 135/tcp on 192.168.50.102
Discovered open port 7/tcp on 192.168.50.102
Discovered open port 2103/tcp on 192.168.50.102
Discovered open port 8009/tcp on 192.168.50.102
Discovered open port 9/tcp on 192.168.50.102
Discovered open port 19/tcp on 192.168.50.102
Discovered open port 2107/tcp on 192.168.50.102
Discovered open port 5432/tcp on 192.168.50.102
Discovered open port 8443/tcp on 192.168.50.102
Discovered open port 1801/tcp on 192.168.50.102
Discovered open port 2105/tcp on 192.168.50.102
Discovered open port 13/tcp on 192.168.50.102
Discovered open port 17/tcp on 192.168.50.102
Discovered open port 5357/tcp on 192.168.50.102
Completed SYN Stealth Scan at 22:56, 1.61s elapsed (1000 total ports)
Nmap scan report for windows (192.168.50.102)
Host is up (0.00070s 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
MAC Address: 08:00:27:67:DE:22 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.73 seconds
           Raw packets sent: 1121 (49.308KB) | Rcvd: 1001 (40.104KB)
```

3.1.3 TCP connect

```
nmap -sT 192.168.50.102
```

Output:

```
nmap -sT 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-08 22:59 CET
Nmap scan report for windows (192.168.50.102)
Host is up (0.0018s latency).
Not shown: 981 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
MAC Address: 08:00:27:67:DE:22 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.41 seconds
```

3.1.4 Version Detection

```
nmap -sV 192.168.50.102
```

Output:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-08 23:00 CET
Nmap scan report for windows (192.168.50.102)
Host is up (0.00083s 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: WORKGR
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
MAC Address: 08:00:27:67:DE:22 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-9K104BT; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/
Nmap done: 1 IP address (1 host up) scanned in 159.17 seconds
```

3.2 FIREWALL ATTIVATO:

3.2.1 OS Fingerprint

```
nmap -O 192.168.50.102
```

Output:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-08 23:07 CET
Nmap scan report for windows (192.168.50.102)
Host is up (0.00073s 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: 08:00:27:67:DE:22 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open ar
Aggressive OS guesses: Microsoft Windows 10 1607 (97%),
Microsoft Windows Phone 7.5 or 8.0 (94%), Microsoft Windows 10 1511 - 1607 (92%),
Microsoft Windows Embedded Standard 7 (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 (9
Microsoft Windows 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/submit
Nmap done: 1 IP address (1 host up) scanned in 9.43 seconds
```

3.2.2 Syn Scan

```
nmap -sS -v 192.168.50.102
```

Aggiunto il flag -v per far visualizzare al meglio che si trattasse dello Stealth Scan

Output:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-08 23:09 CET
Initiating ARP Ping Scan at 23:09
Scanning 192.168.50.102 [1 port]
```

```
Completed ARP Ping Scan at 23:09, 0.05s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 23:09
Scanning windows (192.168.50.102) [1000 ports]
Discovered open port 3389/tcp on 192.168.50.102
Discovered open port 135/tcp on 192.168.50.102
Discovered open port 445/tcp on 192.168.50.102
Discovered open port 80/tcp on 192.168.50.102
Discovered open port 139/tcp on 192.168.50.102
Discovered open port 2103/tcp on 192.168.50.102
Discovered open port 1801/tcp on 192.168.50.102
Discovered open port 8443/tcp on 192.168.50.102
Discovered open port 5357/tcp on 192.168.50.102
Discovered open port 2107/tcp on 192.168.50.102
Discovered open port 2105/tcp on 192.168.50.102
Completed SYN Stealth Scan at 23:09, 4.44s elapsed (1000 total ports)
Nmap scan report for windows (192.168.50.102)
Host is up (0.00056s 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: 08:00:27:67:DE:22 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.60 seconds
           Raw packets sent: 1992 (87.632KB) | Rcvd: 14 (600B)
```

3.2.3 TCP connect

```
nmap -sT 192.168.50.102
```

Output:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-08 23:10 CET
Nmap scan report for windows (192.168.50.102)
```

```
Host is up (0.0024s 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: 08:00:27:67:DE:22 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.24 seconds
```

3.2.4 Version Detection

```
nmap -sV 192.168.50.102
```

Output:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-08 23:12 CET
Nmap scan report for windows (192.168.50.102)
Host is up (0.00059s 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: WORKGRO
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
MAC Address: 08:00:27:67:DE:22 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-9K104BT; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/s
Nmap done: 1 IP address (1 host up) scanned in 80.88 seconds
```

4 RIEPILOGO INFORMAZIONI RACCOLTE

4.1 Informazioni Generali trovate

- Target IP: 192.168.50.102
- Hostname: DESKTOP-9K1O4BT
- Sistema Operativo: Windows 10 Build 1607
- MAC Address: 08:00:27:67:DE:22
- Workgroup SMB: WORKGROUP

4.2 Porte e Servizi Identificati

4.2.1 SCENARIO 1: FIREWALL OFF - STESSA RETE

Porte aperte: 18

Porta	Servizio	Descrizione	Versione/Dettagli
7	echo	Echo service	Standard TCP service
9	discard	Discard service	Non identificato precisamente
13	daytime	Daytime service	Microsoft Windows International daytime
17	qotd	Quote of the Day	Windows qotd (English)
19	chargen	Character Generator	Standard TCP service
80	http	Web server	**Microsoft IIS httpd 10.0**
135	msrpc	Microsoft RPC	Microsoft Windows RPC
139	netbios-ssn	NetBIOS Session Service	Microsoft Windows netbios-ssn
445	microsoft-ds	SMB File Sharing	Microsoft Windows 7-10 (workgroup: WORKGROUP)
1801	msmq	Microsoft Message Queue	Non identificato precisamente
2103	zephyr-clt	RPC service	Microsoft Windows RPC
2105	eklogin	RPC service	Microsoft Windows RPC
2107	msmq-mgmt	MSMQ Management	Microsoft Windows RPC
3389	ms-wbt-server	Remote Desktop Protocol	**Microsoft Terminal Services**
5432	postgresql	PostgreSQL Database	Non identificato precisamente
8009	ajp13	Apache JServ Protocol	**Apache Jserv (Protocol v1.3)**
8080	http-proxy	Apache Tomcat	**Apache Tomcat/Coyote JSP engine 1.1**
8443	https-alt	HTTPS Alternative	HTTPS alternativo

4.2.2 SCENARIO 2: FIREWALL ON - STESSA RETE

- **Porte aperte: 8**
- **Porte filtrate: 992** (risposta: no-response)

Porta	Stato	Servizio
80	open	http
135	open	msrpc
1801	open	msmq
2103	open	zephyr-clt
2105	open	eklogin
2107	open	msmq-mgmt
3389	open	ms-wbt-server
8443	open	https-alt

4.2.3 SCENARIO 3: FIREWALL OFF - RETI DIVERSE

Porte aperte: 19

NUOVA PORTA RILEVATA:

Porta	Servizio	Versione
5357	wsdapi	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

Nota: WSD (Web Services for Devices) è un servizio Windows per discovery di dispositivi, probabilmente ha regole di visibilità diverse tra reti.

4.2.4 SCENARIO 4: FIREWALL ON - RETI DIVERSE

- **Porte aperte: 8**
- **Porte filtrate: 992** (risposta: no-response)

Porta	Stato	Servizio
80	open	http
135	open	msrpc
1801	open	msmq
2103	open	zephyr-clt
2105	open	eklogin
2107	open	msmq-mgmt
3389	open	ms-wbt-server
8443	open	https-alt

5 CONCLUSIONI:

Alla fine delle due fasi abbiamo trovato una netta differenza tra le scansioni con il firewall accesso e il firewall chiuso. In particolare per quanto riguarda la scansione con il flag -O diminuisce la precisione di indviduare il OS della macchina target. Inoltre abbiamo analizzato i risultati delle porte con il firewall accesso (riduce le porte visibili) che con in firewall spento.