Floriana Feminò

23/11/2022

TECNICHE DI SCANSIONE CON NMAP

	Macchine Target
SYN Scan	**Metasploitable**
TCP Connect Scan	**Metasploitable**
Version Detection	**Metasploitable**
OS Fingerprint	**Metasploitable, Windows 7**

Macchine target:

- **Metasploitable**
- **Windows 7**

Tecniche di scansione utilizzate:

- **SYN Scan** (*Stealth Scan*)
- **TCP Connect Scan**
- **Version Detection**
- **OS Fingerprint**

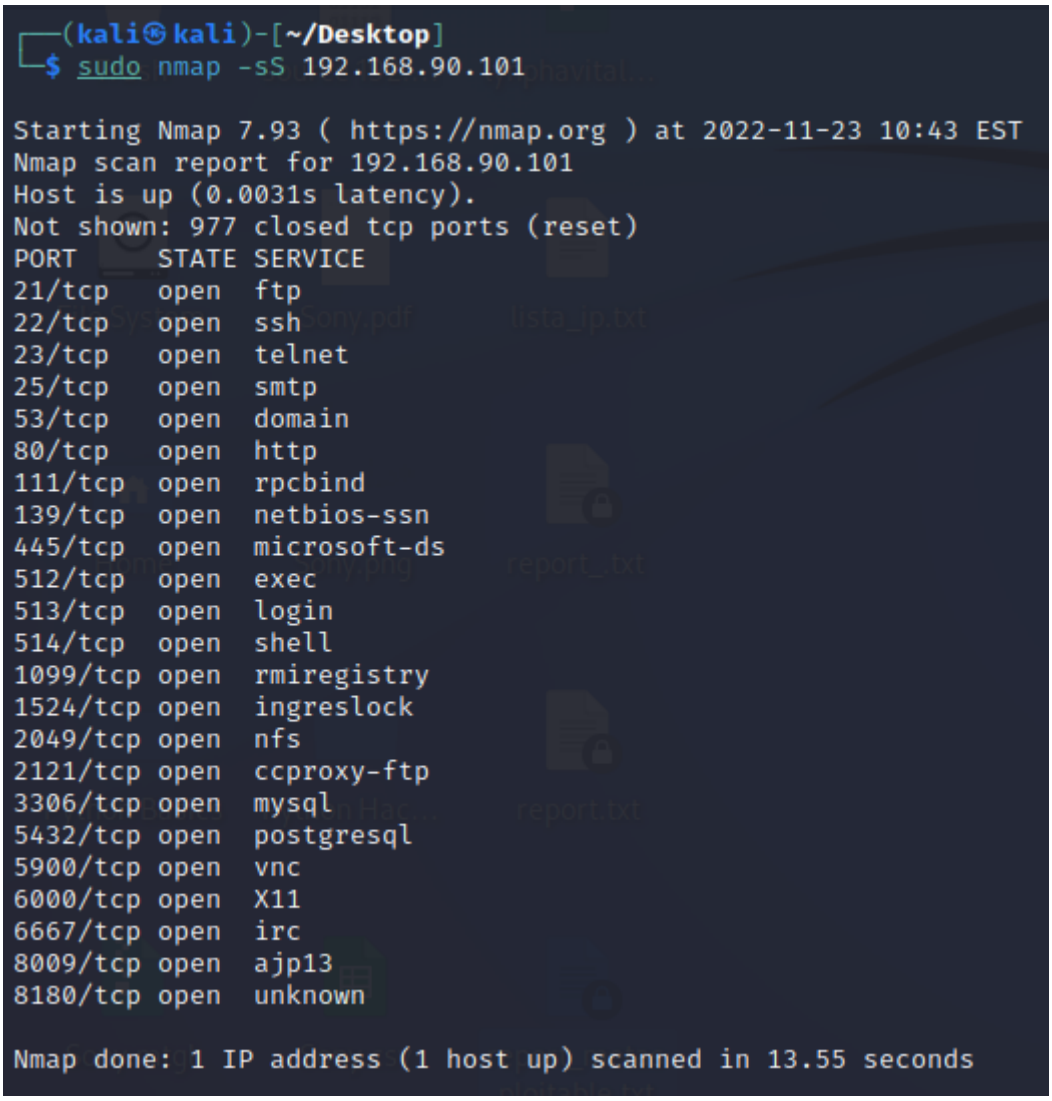
Scanning machine: Kali

➔ Tutte e 3 le macchine coinvolte nei test si trovano su rete interna e rispondono positivamente alle echo requests (ping).

1. Scansioni su Metasploitable

1.1 SYN Scan

Avviamo la Syn Scan sull'indirizzo IP di Metasploitable eseguendo il comando **sudo nmap -sS 192.168.90.101**



Questo tipo di scansione viene anche definita ***Stealth Scan***, in quanto è molto più discreta della TCP Connect: quest'ultima effettua una scansione approfondita ed aggressiva poiché mira ad una connessione completa con la porta target, completando tutti gli step della Three-way handshake (SYN, SYN/ACK, ACK); la SYN Scan, invece, è meno tracciabile dai dispositivi di monitoraggio del traffico di rete (come Firewall) in quanto punta a verificare solamente lo stato della/e porta/e (= aperta o chiusa) dell'host inviando pacchetti di traffico con flag SYN e, alla eventuale risposta positiva di quest'ultimo (SYN/ACK), chiude di fatto la connessione inviando un pacchetto di reset (RST) della stessa.

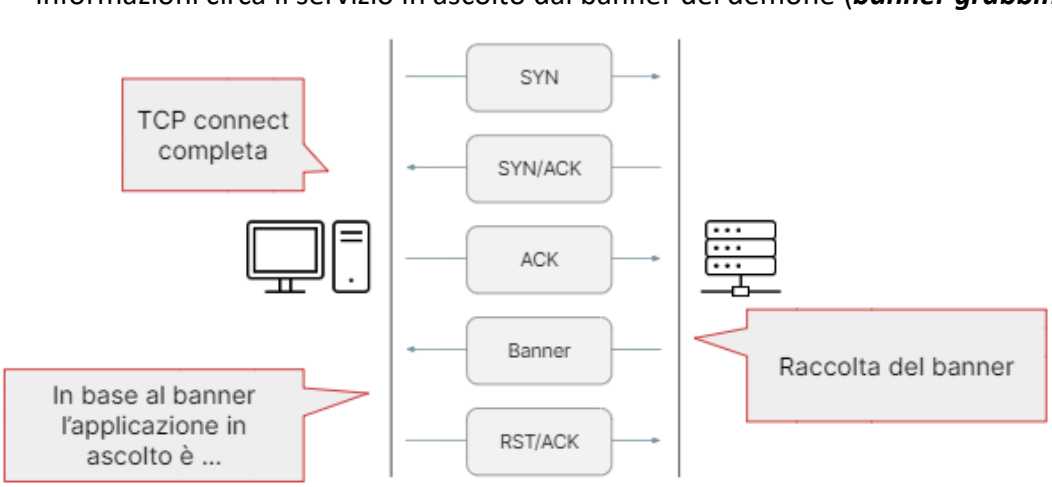
1.2 TCP Connect Scan

Avviamo la TCP Connect Scan eseguendo il comando **sudo nmap -sT 192.168.90.101**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sT 192.168.90.101
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 10:45 EST
Nmap scan report for 192.168.90.101
Host is up (0.010s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 13.56 seconds
```

1.3 Version Detection

La Version Detection è una scansione di tipo TCP Connect con aggiunta di specifici **test per la rilevazione dei servizi in ascolto** su una porta. Come la già menzionata scansione TCP Connect, è facile da rilevare perché genera molto traffico di rete. Durante una scansione Version Detection, Nmap esegue prima una TCP Connect e poi recupera informazioni circa il servizio in ascolto dal banner del demone (***banner grabbing***):



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV 192.168.90.101
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 11:00 EST
Nmap scan report for 192.168.90.101
Host is up (0.0070s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  rpcbind
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 54.27 seconds
```

1.4 OS Fingerprint

Questo tipo di scansione è in grado di restituire in output anche dettagli sul **sistema operativo** utilizzato dalla macchina target. Scelgo di effettuarla in 2 modi:

- eseguendo il comando **sudo nmap -O 192.168.90.101**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -O -oN report_metasploitable.txt 192.168.90.101

[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 10:34 EST
Nmap scan report for 192.168.90.101
Host is up (0.0025s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded), Linux 2.6.20 - 2.6.24 (Ubuntu 7.04 - 8.04)
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 16.44 seconds
```

In questo caso ho scelto di creare un piccolo report di riepilogo dei dati ottenuti in output alla scansione, quindi ho aggiunto lo switch -oN seguito dal nome del file di testo da creare (report_metasploitable.txt)

OS info

- avvalendomi della feature **NMAP Scripting Engine (NSE)**. Grazie ad essa, è possibile eseguire piccoli script per automatizzare alcuni task di rete. Dalla directory /usr/share/nmap/scripts scelgo di utilizzare **smb-os-discovery.nse** il cui scopo è provare a determinare la versione dell'os di un sistema target a partire dal banner del servizio SMB, e lo eseguo con il comando

nmap 192.168.90.101 --script smb-os-discovery

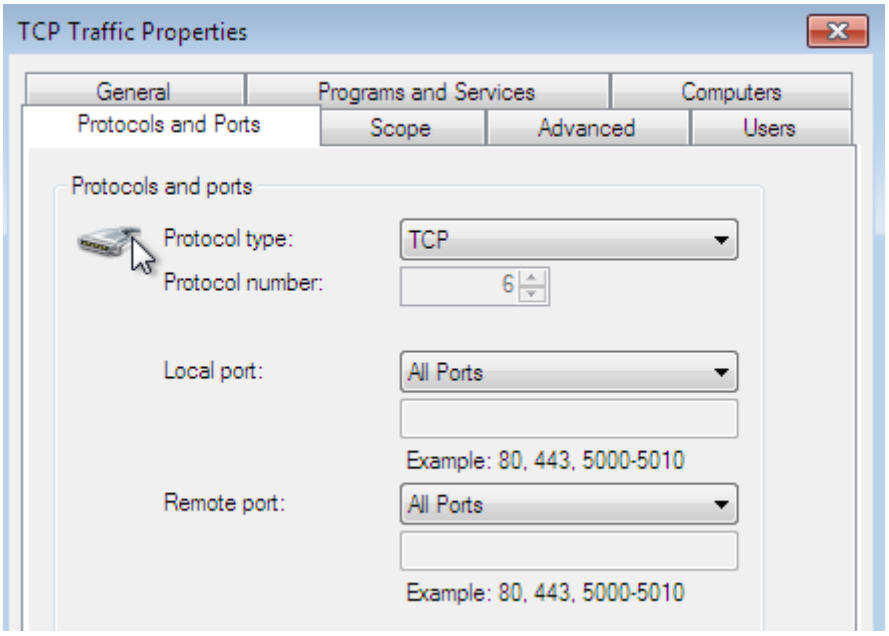
```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap 192.168.90.101 --script smb-os-discovery
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 21:35 CET
Nmap scan report for 192.168.90.101
Host is up (0.013s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2022-11-23T15:35:22-05:00

Nmap done: 1 IP address (1 host up) scanned in 14.23 seconds
```

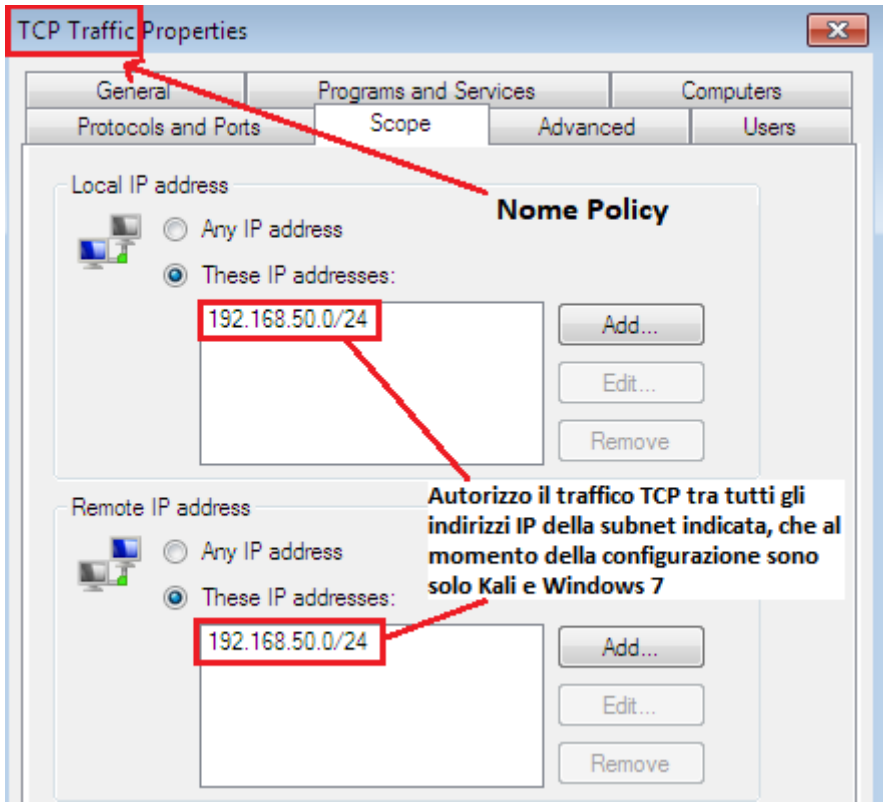
2. OS Fingerprint su Windows 7

Proviamo ad eseguire questa scansione su Windows 7, ma senza prima impostare una policy sul Firewall che permetta il traffico TCP proveniente da Kali, i risultati sono i seguenti:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -O 192.168.50.102
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 10:24 EST
Nmap scan report for 192.168.50.102
Host is up (0.00095s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:C8:46:D5 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

Procediamo dunque a creare tale policy dalle impostazioni del Firewall in Windows 7.





Adesso riproviamo la scansione eseguendo il comando **sudo nmap -O 192.168.50.102**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -O 192.168.50.102
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 12:30 EST
Nmap scan report for 192.168.50.102
Host is up (0.0011s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:C8:46:D5 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:win
dows_7 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Embedded Standard 7, Microsoft Windows Ph
one 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop
```

Come si può notare, la scansione adesso restituisce un'analisi dello stato delle porte – le 1000 più note, come da impostazione di default – più un guess di quale potrebbe essere il sistema operativo in uso dalla macchina, ipotizzando tra 5 OS (Windows 2000, Windows 8.1, Windows 7, Windows Phone e Windows Vista). Per provare a restringere il campo ed ottenere un feedback più fedele, eseguiamo di nuovo il fingerprint, ma cambiando alcuni parametri:

- Il **Timing**, ossia l'intervallo di tempo tra una richiesta TCP SYN e l'altra, affinchè il Firewall non sia subissato di richieste che spesso possono essere interpretate come anomale e quindi bloccate
- La **porta sorgente** (source port), affinchè la richiesta possa risultare proveniente da una porta nota (le scansioni hanno come impostazione di default l'invio di richieste TCP provenienti da porte randomizzate e non note) e quindi interpretabile come sicura dal Firewall

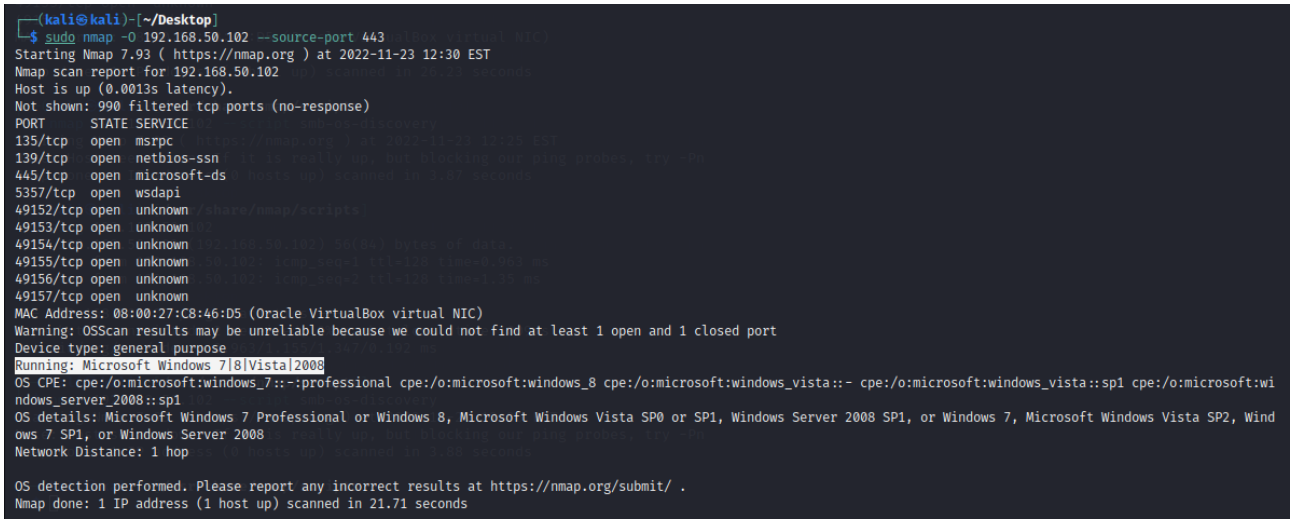
Proviamo quindi ad eseguire un OS fingerprint con timing **T2** (***polite scan***). Il timing di default per le scansioni nmap è T3, quindi parliamo di una scansione un po' più lenta rispetto alle tempistiche standard. Eseguiamo il comando

sudo nmap -O -T2 192.168.50.102

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -O -T2 192.168.50.102
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 10:28 EST
Nmap scan report for 192.168.50.102
Host is up (0.0011s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:C8:46:D5 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7
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 928.72 seconds
```

Come si vede, il feedback relativo all'OS presenta adesso un margine ristretto a 3 (Windows Vista, Windows 2008 e Windows 7).

Proviamo adesso ad impostare come source port della scansione la **443** (https): eseguiamo il comando **sudo nmap -O 192.168.50.102 --source-port 443**



Questa volta la scansione suggerisce 4 possibili OS: uno in più rispetto alla precedente scansione con timing T2, ma uno in meno rispetto alla prima scansione con parametri di timing e source port invariati.

Impostando come source port la **80** (http), otteniamo invece lo stesso risultato della scansione con timing T2: la eseguiamo con il comando **sudo nmap -O 192.168.50.102 --source-port 80**

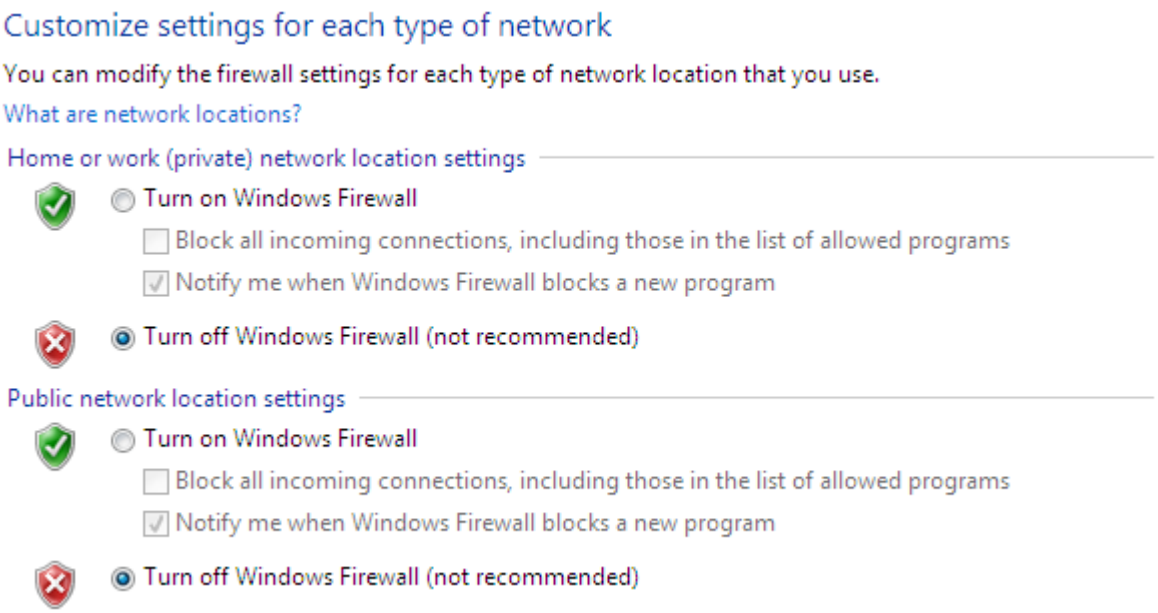
Proviamo adesso a ripetere la scansione mantenendo la stessa source port ma settando il timing a **T1** (***sneaky scan***):

sudo nmap -O -T1 192.168.50.102 --sourceport 80

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -O -T1 192.168.50.102 --source-port 80
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 12:42 EST
Nmap scan report for 192.168.50.102
Host is up (0.0016s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:C8:46:D5 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
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 33494.67 seconds
```

Come si vede, in questo caso il timing della scansione ridotto a T1 non ha prodotto una maggiore precisione nei risultati ottenuti.

Ne ricaviamo che per questo test è consigliato impostare il timing a T2 o cambiare solo la source port in 80, poiché questi due settaggi producono nella scansione gli stessi risultati che si avrebbero disattivando completamente il Firewall, come verificato nelle figure seguenti:




```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -O 192.168.50.102
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-24 04:11 CET
Nmap scan report for 192.168.50.102
Host is up (0.0012s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:C8:46:D5 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7
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 26.80 seconds
```