

# SCANSIONE DEI SERVIZI CON NMAP

## TASK

- Metaspitable: (IP 192.168.50.101)
  - OS fingerprint
  - Syn Scan
  - TCP connect
  - Version detection
- Windows: (IP 192.168.50.102)
  - OS fingerprint

## ANALISI E VALUTAZIONI

Iniziamo nello scansionare Metaspitable con Nmap:

- `nmap -O 192.168.50.101`

```
(kali@kali)-[/usr/share/nmap/scripts]
$ sudo nmap -O 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 08:10 EST
Nmap scan report for 192.168.50.101
Host is up (0.00073s 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
MAC Address: 08:00:27:7B:21:1D (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
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 18.19 seconds
```

Per creare il suo report in automatico basta usare il comando `<nmap -oN "nome_file" -O 192.168.50.101>`:

```
File Edit Search View Document Help
~/Desktop/Nmap_report/Finger_print_Meta [Read Only] - Mousepad

Finger_print_Windows

1 # Nmap 7.92 scan initiated Wed Nov 23 09:48:40 2022 as: nmap -oN Finger_print_Meta -O 192.168.50.101
2 Nmap scan report for 192.168.50.101
3 Host is up (0.0015s latency).
4 Not shown: 977 closed tcp ports (reset)
5 PORT      STATE SERVICE
6 21/tcp    open  ftp
7 22/tcp    open  ssh
8 23/tcp    open  telnet
9 25/tcp    open  smtp
10 53/tcp    open  domain
11 80/tcp    open  http
12 111/tcp   open  rpcbind
13 139/tcp   open  netbios-ssn
14 445/tcp   open  microsoft-ds
15 512/tcp   open  exec
16 513/tcp   open  login
17 514/tcp   open  shell
18 1099/tcp  open  rmiregistry
19 1524/tcp  open  ingreslock
20 2049/tcp  open  nfs
21 2121/tcp  open  ccproxy-ftp
22 3306/tcp  open  mysql
23 5432/tcp  open  postgresql
24 5900/tcp  open  vnc
25 6000/tcp  open  Xi11
26 6667/tcp  open  irc
27 8009/tcp  open  ajp13
28 8180/tcp  open  unknown
29 MAC Address: 08:00:27:7B:21:1D (Oracle VirtualBox virtual NIC)
30 Device type: general purpose
31 Running: Linux 2.6.X
32 OS CPE: cpe:/o:linux:linux_kernel:2.6
33 OS details: Linux 2.6.9 - 2.6.33
34 Network Distance: 1 hop
35
36 OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
37 # Nmap done at Wed Nov 23 09:48:56 2022 -- 1 IP address (1 host up) scanned in 18.52 seconds
38
```

- `nmap -F -sS 192.168.50.101`

```
(kali@kali)-[/usr/share/nmap/scripts]
$ sudo nmap -F -sS 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 08:30 EST
Nmap scan report for 192.168.50.101
Host is up (0.0080s latency).
Not shown: 82 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
513/tcp   open  login
514/tcp   open  shell
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  Xi11
8009/tcp  open  ajp13
MAC Address: 08:00:27:7B:21:1D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.93 seconds
```

Ho usato -F per andare a scansionare le 100 porte più utilizzate e quindi una scansione più restrittiva

- nmap -F -sT 192.168.50.101

```
(kali㉿kali)-[/usr/share/nmap/scripts]
$ sudo nmap -F -sT 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 08:31 EST
Nmap scan report for 192.168.50.101
Host is up (0.0058s latency).
Not shown: 82 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
513/tcp   open  login
514/tcp   open  shell
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
8009/tcp  open  ajp13
MAC Address: 08:00:27:7B:21:1D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.83 seconds
```

La differenza tra -sS e -sT sta proprio nel fatto che per le porte chiuse in una c'è "RESET" nell'altra "CONN-REFUSED". Per quest'ultima(-sT) il three-way-handshake è completato per le porta aperte, a differenza delle porte chiuse.

- nmap -F -sV 192.168.50.101

```
(kali㉿kali)-[/usr/share/nmap/scripts]
$ sudo nmap -F -sV 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 08:37 EST
Nmap scan report for 192.168.50.101
Host is up (0.0049s latency).
Not shown: 82 closed tcp ports (reset)
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      2 (RPC #100000)
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)
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
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)
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
MAC Address: 08:00:27:7B:21:1D (Oracle VirtualBox virtual NIC)
Service Info: Host: metasploitable.localdomain; 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 54.31 seconds
```

- `nmap 192.168.50.101 --script smb-os-discovery`

```
(kali㉿kali)-[/usr/share/nmap/scripts]
$ sudo nmap 192.168.50.101 --script smb-os-discovery
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 08:28 EST
Nmap scan report for 192.168.50.101
Host is up (0.0031s 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
MAC Address: 08:00:27:7B:21:1D (Oracle VirtualBox virtual NIC)

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: 2022-11-23T08:28:25-05:00

Nmap done: 1 IP address (1 host up) scanned in 16.09 seconds
```

Tale comando ci fornisce info più dettagliate riguardo all'Host (IP target), informazioni come Sistema operativo, il nome del computer...

Passiamo ora a Windows:

- `nmap -oN "nome_file" -O 192.168.50.102` (per ottenere il report)

```
File Edit Search View Document Help
~/Desktop/Finger_print_Windows [Read Only] - Mousepad

1 # Nmap 7.92 scan initiated Wed Nov 23 09:08:20 2022 as: nmap -oN Finger_print_Windows -T4 -O 192.168.50.102
2 Nmap scan report for 192.168.50.102
3 Host is up (0.00155 latency).
4 Not shown: 991 closed tcp ports (reset)
5 PORT      STATE SERVICE
6 135/tcp    open  msrpc
7 139/tcp    open  netbios-ssn
8 445/tcp    open  microsoft-ds
9 49152/tcp   open  unknown
10 49153/tcp   open  unknown
11 49154/tcp   open  unknown
12 49155/tcp   open  unknown
13 49156/tcp   open  unknown
14 49157/tcp   open  unknown
15 MAC Address: 08:00:27:ED:CD:61 (Oracle VirtualBox virtual NIC)
16 Device type: general purpose
17 Running: Microsoft Windows 7/2008/8.1
18 OS CPE: cpe:/o:microsoft:windows_7:- cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
19 OS details: Microsoft Windows 7 SP1 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
20 Network Distance: 1 hop
21
22 OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
23 # Nmap done at Wed Nov 23 09:08:38 2022 -- 1 IP address (1 host up) scanned in 19.69 seconds
24
```

- `nmap -sV 192.168.50.102`

```
(kali㉿kali)-[~/Desktop]
$ sudo nmap -sV 192.168.50.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 09:27 EST
Nmap scan report for 192.168.50.102
Host is up (0.00085s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
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)
49152/tcp  open  msrpc        Microsoft Windows RPC
49153/tcp  open  msrpc        Microsoft Windows RPC
49154/tcp  open  msrpc        Microsoft Windows RPC
49155/tcp  open  msrpc        Microsoft Windows RPC
49156/tcp  open  msrpc        Microsoft Windows RPC
49157/tcp  open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:ED:CD:61 (Oracle VirtualBox virtual NIC)
Service Info: Host: DOMENICO-PC; 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 76.47 seconds
```

Una cosa importante da notare è che questa scansione non sarebbe stata resa possibile se non avessimo prima disabilitato il firewall di Windows 7, di fatti l'errore sarebbe stato questo:

```
(kali㉿kali)-[~/Desktop]
$ sudo nmap -Pn -O 192.168.50.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 09:22 EST
Nmap scan report for 192.168.50.102
Host is up (0.00050s 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:ED:CD:61 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
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 43.99 seconds
```

Al fine di poter scansionare Windows una soluzione alternativa sarebbe potuta essere la creazione di una regola Firewall in grado di poter bypassare il sistema di difesa di Windows e quindi permettere solo per Kali la scansione.

Un'altra alternativa è “provare” con il comando `<nmap -T1 -p 139 192.168.50.102>` in quanto il T1 è un tempo più ambio per l’invio dei pacchetti, fondamentale per deviare il “problema” firewall di windows. Abbiamo inserito pertanto una porta target, la quale si può evincere dallo screen precedente che è aperta ed inserita solo una per permettere una scansione più veloce a causa proprio dello svantaggio del T1. Il risultato sarà pressocchè questo:

```
(kali@kali)-[/usr/share/nmap/scripts]
$ sudo nmap -T1 -p 139 192.168.50.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 11:00 EST
Nmap scan report for 192.168.50.102
Host is up.

PORT      STATE      SERVICE
139/tcp   filtered  netbios-ssn
MAC Address: 08:00:27:ED:CD:61 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 73.74 seconds
```

In effetti il risultato ottenuto è proprio la scansione della porta con stato però “filtered”.