

# Esercizio Epicode 25.10.2023

## Scansione di rete con Nmap

### 1) Macchina Metasploitable

Come prima cosa abbiamo scansionato con Nmap, utilizzando l'opzione **-O**, il sistema operativo per poter controllare con quale tipo di dispositivo abbiamo a che fare. La scansione ci riporterà ad una macchina virtuale con SO Metasploitable. Inoltre mostra quali porte sono aperte con il relativo servizio.

```
(christian@kali)-[~]
$ sudo nmap -O 192.168.50.101
[sudo] password for christian:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:27 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00029s 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: 08:00:27:30:59:23 (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 14.60 seconds
```

Subito dopo aver eseguito lo scan dell'SO ho provato a utilizzare due comandi (-sS e -sT), una invia i pacchetti solo in SYN (poco invasiva) e l'altra in SYN/SYN-ACK/ACK (molto invasiva). Con Nmap -sT posso avere una scansione delle porte molto più dettagliata.

```
(christian@kali)-[~]
$ sudo nmap -sS 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:29 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00013s 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: 08:00:27:30:59:23 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.18 seconds

(christian@kali)-[~]
$ sudo nmap -sT 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:31 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00043s 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
MAC Address: 08:00:27:30:59:23 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.20 seconds
```

Alla fine per avere una scansione dettagliata andremo a vedere la versione dell'SO del dispositivo, questo dato sarà fondamentale per le prossime fasi del PT

```
(christian@kali)-[~]
$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:34 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00019s latency).
Not shown: 977 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)
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  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)
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
MAC Address: 08:00:27:30:59:23 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CP
E: 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 65.69 seconds
```

## 2) Macchina Windows 7

Se su Windows andremo a utilizzare gli stessi comandi utilizzati per Metasploitable, i dati ricavati saranno pochi o nulli. Questo perché il Firewall di Windows non ci farà passare il ping della macchina Kali da cui utilizziamo Nmap. Da qui possiamo prendere 2 vie o disattivare il firewall di Windows per far passare tutti i pacchetti, oppure utilizzare il comando -Pn che ci disattiva il ping e fa passare solo il protocollo TCP.

```
(christian@kali)-[~]
$ sudo nmap -O 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:37 CEST
Nmap scan report for 192.168.50.102
Host is up (0.00055s latency).
Not shown: 991 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
MAC Address: 08:00:27:99:82:30 (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 (98%), Microsoft Windows Embedded Standard 7 (98%), Microsoft Windows 7 Professional or Windows 8 (97%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (97%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (96%), Microsoft Windows Server 2008 R2 or Windows 8.1 (95%), Microsoft Windows Server 2008 SP1 (94%), Microsoft Windows 7 (94%), Microsoft Windows 8.1 R1 (92%), Microsoft Windows 7 SP1 (92%)
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 27.04 seconds
```