



# **EPICODE**

**Progetto Alessandro Moscetti 25/10**



```
(kali㉿kali)-[~]  
$ nmap -sn 192.168.50.*  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:19 CEST  
Nmap scan report for 192.168.50.100  
Host is up (0.000047s latency).  
Nmap scan report for 192.168.50.101  
Host is up (0.0056s latency).  
Nmap done: 256 IP addresses (2 hosts up) scanned in 19.68 seconds
```

Tramite l'opzione di nmap 'sn' siamo andati a controllare gli host attivi tramite ping. Utilizzando il carattere '\*' nell'ip target sono andato a scansionare tutti gli ip compresi tra il 192.168.50.0 e il 192.168.50.255. Sapendo che '192.168.50.100' è il nostro ip sulla rete, sappiamo di conseguenza l'ip della macchina target.

```
[sudo] password for kali:
(root@kali)-[/home/kali]
# nmap -sS 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:23 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00022s 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:E6:33:5F (Oracle VirtualBox virtual NIC)
```

Tramite l'opzione di nmap 'sS' siamo andati a effettuare un Syn scan sull'ip trovato in precedenza. Questa opzione è il metodo meno invasivo perchè non completa la 3-way-handshake ma si interrompe alla ricezione del syn/ack, ma potrebbe di conseguenza non essere accurata al 100%. Nell'output possiamo notare le varie porte aperte con il relativo servizio e il MAC Address dell'host.

```
(root@kali)-[/home/kali]
# nmap -sT 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:25 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0016s 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:E6:33:5F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.47 seconds
```

Tramite l'opzione di nmap 'sT' siamo andati a effettuare una scansione TCP Connect sull'ip. Questa opzione è più invasiva e lenta della precedente, ma più affidabile.

Possiamo notare che non ci sia differenza tra gli output con le opzioni 'sS' e 'sT'.  
La differenza sta nell'affidabilità degli output e il 'rumore' creato dalle scansioni.

```
(root@kali)-[/home/kali]
# nmap -Pn -O 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:30 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00083s 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:E6:33:5F (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 14.64 seconds
```

Per la fase di Os fingerprint siamo andati ad utilizzare l'omonima opzione con '-O' implementato da '-Pn' per non inviare ulteriori ping nella scansione.

Così facendo siamo andati a vedere il sistema operativo dell'host in questo caso 'Linux 2.6.X'.

```

(root@kali)-[/home/kali]
# nmap -sV -sT 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 (0.0016s 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      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:E6:33:5F (Oracle VirtualBox virtual NIC)
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 65.88 seconds

```

Tramite l'opzione 'sV' siamo andati a effettuare una Version detection.

Con questa opzione andiamo a vedere anche la versione e dettagli dei servizi, per il resto è a tutti gli effetti come la scansione TCP Connect.

Andando ad effettuare lo stesso esercizio con la nostra macchina Windows non troveremo alcun risultato senza disattivare o aggirare il Firewall del sistema operativo.



```
(root@kali)-[/home/kali]
# nmap -sS 192.168.50.103
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 16:33 CEST
Nmap scan report for 192.168.50.103
Host is up (0.00057s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49159/tcp  open  unknown
MAC Address: 08:00:27:80:3E:92 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.85 seconds
```

Ripetendo i passaggi troveremo le informazioni della macchina Windows.  
In questa immagine l'output con l'opzione Syn scan.

```
(root@kali)-[/home/kali]
# nmap -sT 192.168.50.103
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 16:34 CEST
Nmap scan report for 192.168.50.103
Host is up (0.0011s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49159/tcp  open  unknown
MAC Address: 08:00:27:80:3E:92 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.41 seconds
```

In questa immagine l'output con l'opzione di scansione TCP Control su macchina Windows.

```
(root@kali)-[/home/kali]
# nmap -Pn -O 192.168.50.103
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 16:35 CEST
Nmap scan report for 192.168.50.103
Host is up (0.0011s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49159/tcp  open  unknown
MAC Address: 08:00:27:80:3E:92 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
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 15.44 seconds
```

In questa immagine l'output con l'opzione di scansione Os fingerprint con cui scopriamo il sistema operativo in uso dalla macchina Windows.

```
(root@kali)-[/home/kali]
# nmap -sV -sT 192.168.50.103
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 16:36 CEST
Nmap scan report for 192.168.50.103
Host is up (0.00100s latency).
Not shown: 991 closed tcp ports (conn-refused)
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
49159/tcp  open  msrpc           Microsoft Windows RPC
MAC Address: 08:00:27:80:3E:92 (Oracle VirtualBox virtual NIC)
Service Info: Host: WINDOWS7; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submi
Nmap done: 1 IP address (1 host up) scanned in 73.82 seconds
```

In questa immagine l'output con l'opzione '-sV' per effettuare la scansione della versione dei servizi sulla macchina Windows.

**Grazie per l'attenzione.**