

Introduzione

È uno scanner di rete. Nello specifico, **scansiona gli host della rete**.

Con nmap raccogliamo tutte le informazioni che riguardano i dispositivi nella rete, come:

- numero dei dispositivi
- tipologia dei dispositivi (web server, nas, eccetera)
- sistema operativo
- servizi attivi, ovvero le porte aperte dei protocolli di rete
- Le vulnerabilità (anche se lo strumento più adatto a questo scopo è Nessus)

Nelle prossime pagine, andiamo a scansionare due macchine virtuali: Metasploitable e Windows 10.

Scansione dei servizi con Nmap

Metasploitable

OS Fingerprint (-O): Tenta di determinare il sistema operativo dell'host di destinazione.

Nmap invia una serie di pacchetti specifici per osservare le risposte del servizio.

Queste risposte vengono poi confrontate con un database di firme conosciute per identificare il servizio e la sua versione.

```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)-[/home/kali]
# nmap -O 192.168.1.67
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 15:45 CET
Nmap scan report for 192.168.1.67
Host is up (0.016s 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:DC:92:34 (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 2.6.21 (97%), Linux 2.6.9 - 2.6.30 (97%), Linux 2.6.9 - 2.6.33 (97%), Linux 2.6.13 - 2.6.32 (97%), Linux 2.6.24 - 2.6.28 (96%), Linux 2.6.18 - 2.6.32 (96%), Linux 2.6.22 (embedded, ARM) (96%), Linux 2.6.22 - 2.6.23 (96%), Linux 2.6.18 (Debian 4, VMware) (96%), Linksys RV042 router (96%)
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 4.33 seconds
```

SYN Scan (-sS): una volta ricevuto il pacchetto SYN/ACK dalla macchina target, non conclude il 3-way-handshake, ma appurato che la porta è aperta chiude la comunicazione, evitando la creazione del canale e generando meno “rumore” a livello di rete.

Per chiudere la connessione, anziché inviare nella terza fase il pacchetto ACK, invia il pacchetto **RST (reset)**.

Non effettuerà il ping, bypassa il firewall, a discapito di un **risultato meno attendibile**.

```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)-[/home/kali]
# nmap -sS 192.168.1.67
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 15:47 CET
Nmap scan report for 192.168.1.67
Host is up (0.022s 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:DC:92:34 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds
```

TCP Scan (-sT): è il metodo di scansione più invasivo, in quanto per controllare se una porta è aperta o meno e recuperare informazioni sul servizio in ascolto, nmap completa tutti i passaggi del 3-way-handshake, stabilendo di fatto un canale.

Nmap effettuerà un **ping** e di conseguenza il risultato sarà più accurato

```
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[/home/kali]
# nmap -sT 192.168.1.67
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 15:48 CET
Nmap scan report for 192.168.1.67
Host is up (0.045s 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:DC:92:34 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.65 seconds
```

Version Detection (-sV): Identifica i servizi in esecuzione e le loro versioni.

```
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[/home/kali]
# nmap -sV 192.168.1.67
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 15:48 CET
Nmap scan report for 192.168.1.67
Host is up (0.024s 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 rshcd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
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:DC:92:34 (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 14.05 seconds
```

Windows

OS Fingerprint (-O):

```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)-[/home/kali]
# nmap -O 192.168.1.66
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 16:14 CET
Nmap scan report for 192.168.1.66
Host is up (0.0016s 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: 08:00:27:4B:6B:37 (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/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.92 seconds
```