

# Nmap



**Nmap (abbreviazione di "Network Mapper") è uno strumento open-source molto utilizzato per la scansione e l'analisi di reti. Creato inizialmente per la scoperta di host e il rilevamento di servizi su una rete, Nmap è diventato uno dei principali strumenti nel campo della sicurezza informatica e dell'amministrazione di rete.**

**Ecco alcune delle sue principali funzionalità:**

**Scansione delle porte:** Nmap può esaminare le porte di un dispositivo per verificare quali sono aperte, chiuse o filtrate, aiutando a identificare i servizi attivi su ciascuna porta.

**Rilevamento dei servizi:** può determinare quali servizi (ad esempio, HTTP, FTP, DNS) sono in esecuzione su una porta specifica e identificare la versione del software associato.

**Rilevamento del sistema operativo:** Nmap può analizzare le risposte dei dispositivi per fare un'ipotesi sul sistema operativo in uso, aiutando gli amministratori a ottenere un quadro dettagliato dell'infrastruttura di rete.

**Scoperta di host:** permette di identificare quali dispositivi sono attivi e connessi in una rete, cosa particolarmente utile per mappare grandi reti aziendali.

**Rilevamento di vulnerabilità:** Nmap può essere esteso tramite Nmap Scripting Engine (NSE), che include script predefiniti per il rilevamento di vulnerabilità e test di sicurezza.

# Identificazione sistema operativo

## Utilizzando il comando - O (OS Fingerprint)

L'OS fingerprinting è una tecnica usata per identificare il sistema operativo (OS) in esecuzione su un dispositivo remoto. Nmap, ad esempio, utilizza l'OS fingerprinting per analizzare i pacchetti di risposta del dispositivo a specifiche sonde, confrontandoli con un database di firme di vari sistemi operativi conosciuti.

In questo esempio la nostra cavia sarà il software di metasploitable2.

```
(root@Aluandr)-[/home/alessio]
# nmap -O 192.168.1.89
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 12:42 CET
Nmap scan report for 192.168.1.89
Host is up (0.0015s latency).
Not shown: 977 filtered tcp ports (no-response)
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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (95%), QEMU (92%), Bay Networks embedded (85%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (95%), QEMU user mode network gateway (92%), Bay
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.35 seconds
```

```
metasploit [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:dd:85:15
          inet addr:192.168.1.89  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fedd:8515/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:44 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5195 (5.0 KB)  TX bytes:7119 (6.9 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
```



# Scansione porte

## Utilizza comando sS (Syn Scan)

```
(root@Aluandr)-[/home/alessio]
# nmap -sS 192.168.1.89
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 12:43 CET
Nmap scan report for 192.168.1.89
Host is up (0.0067s latency).
Not shown: 977 filtered tcp ports (no-response)
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 4.46 seconds
```

La SYN scan è una tecnica di scansione per determinare quali porte sono aperte su un dispositivo senza stabilire una connessione completa. È anche conosciuta come half-open scan (scansione a metà), poiché non completa l'intero processo di handshake TCP.

Ecco come funziona una SYN scan:

Il client (in questo caso, Nmap) invia un pacchetto SYN alla porta di destinazione.

Se la porta è aperta, il server risponde con un pacchetto SYN-ACK.

Invece di completare il three-way handshake con un pacchetto ACK, Nmap interrompe la connessione inviando un pacchetto RST (Reset), così da non stabilire una connessione completa.

# Scansione completa delle porte

## Utilizza comando -sT (Tcp connect scan)

```
(root@Aluandr)-[/home/alessio]
# nmap -sT 192.168.1.89
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 12:44 CET
Nmap scan report for sT (127.0.0.1)
Host is up (0.0000040s latency).
rDNS record for 127.0.0.1: localhost
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
5432/tcp  open  postgresql

Nmap scan report for 192.168.1.89
Host is up (0.0058s latency).
Not shown: 977 filtered tcp ports (no-response)
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: 2 IP addresses (2 hosts up) scanned in 4.65 seconds
```

La TCP connect scan è una tecnica di scansione delle porte che utilizza il metodo di connessione standard di TCP per determinare lo stato delle porte su un dispositivo. A differenza della SYN scan, che non completa il processo di handshake TCP, la TCP connect scan stabilisce effettivamente una connessione completa. Questo avviene attraverso il three-way handshake di TCP, che consiste nei seguenti passaggi:

Il client invia un pacchetto SYN (synchronize) al server.

Il server risponde con un pacchetto SYN-ACK (synchronize-acknowledge) se la porta è aperta.

Il client invia un pacchetto ACK (acknowledge) per completare la connessione.

# Rilevamento delle versioni dei servizi

## Utilizza il comando -sV Banner(service/version detection)

```
(root@Aluandr)-[/home/alessio]
# nmap -sV 192.168.1.89
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 12:45 CET
Stats: 0:01:25 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 12:47 (0:00:04 remaining)
Nmap scan report for 192.168.1.89
Host is up (0.0067s latency).
Not shown: 977 filtered tcp ports (no-response)
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?
513/tcp   open  login?
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
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 143.83 seconds
```

Il comando -sV in Nmap viene utilizzato per eseguire il service/version detection. Questa opzione permette di identificare i servizi in esecuzione sulle porte aperte e, se possibile, di determinare anche la versione specifica di ciascun servizio. Questo è utile per raccogliere informazioni sui sistemi in rete e per valutare eventuali vulnerabilità.