

Nmap (Network Mapper) è uno strumento open-source estremamente potente e versatile per la scansione della rete e l'identificazione dei dispositivi e dei servizi. Le sue funzionalità principali includono:

- Scansione degli Host: Identifica gli host attivi all'interno di una rete.
- Identificazione dei Servizi: Rileva i servizi in esecuzione su ciascun host, inclusi i numeri di porta e i protocolli.
- Rilevamento dei Sistemi Operativi: Utilizza varie tecniche di fingerprinting per determinare il sistema operativo in esecuzione su un host.
- Scansione delle Vulnerabilità: Può essere utilizzato per identificare potenziali vulnerabilità nei dispositivi e nei servizi rilevati.

Svolgimento

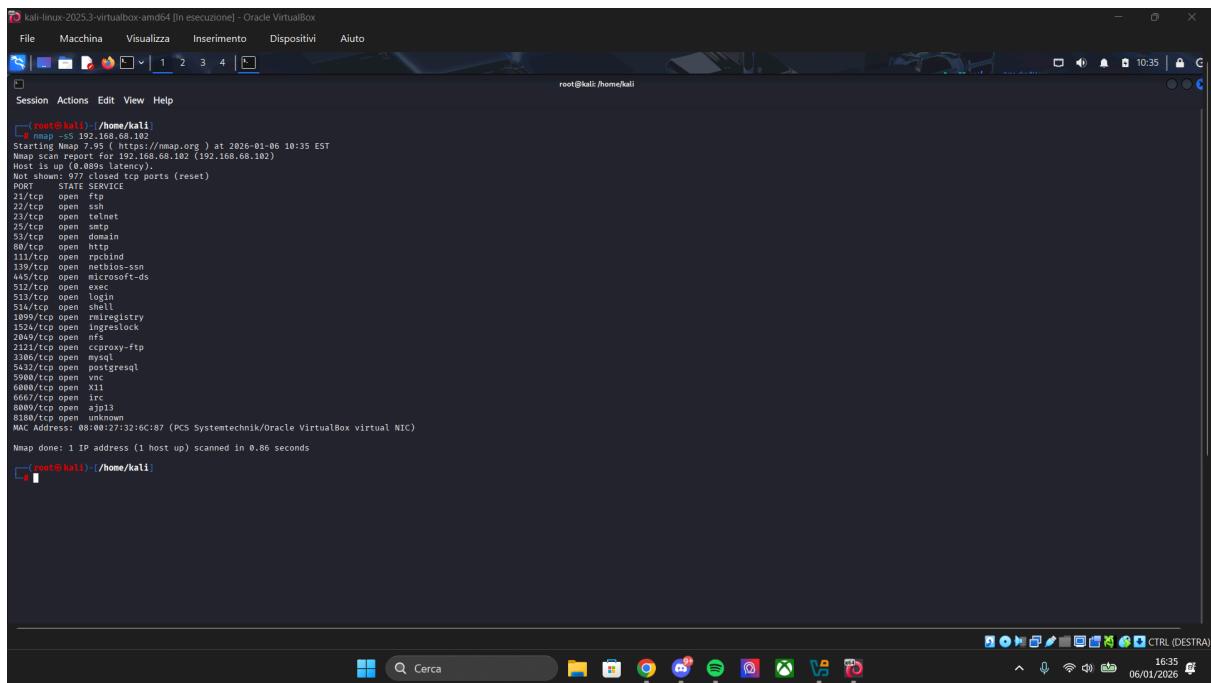
Abbiamo aperto la nostra macchina virtuale e la nostra metasploitable e abbiamo usato il comando nmap.

Rilevamento del Sistema Operativo: nmap -O tentando di determinare il sistema operativo dell'host di destinazione 192.168.68.102. La scansione è avvenuta con successo.

```
[root@kali ~]# nmap -O 192.168.68.102
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 10:34 EST
Nmap scan report for 192.168.68.102 (192.168.68.102)
Host is up (0.0008s latency).
Nmap scan initiated 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  login
514/tcp   open  shell
1394/tcp  open  raw.registry
1524/tcp  open  sunrpc
2049/tcp  open  nfs
2323/tcp  open  tcpwrap-ftp
3100/tcp  open  unknown
5432/tcp  open  postgresql
5900/tcp  open  vnc
59000/tcp open  vnc
60000/tcp open  vnc
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:32:6C:87 (PC Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o: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 2.37 seconds
```

TCP SYN Scan: namp -sS Esegue una scansione "half-open", inviando pacchetti SYN e attendendo risposte SYN/ACK. e' uno scan meno invasivo perchè nmap non completa il 3-way-handshake, ma chiude la comunicazione inviando un pacchetto RST (reset). Tuttavia, riesce a recuperare informazioni sullo stato della porta. Utile in quanto genera meno entropia e «rumore» a livello di rete dal host di destinazione 192.168.68.102. La scansione è avvenuta con successo.



```
(root@kali) [/home/kali]
[+] Nmap 7.95 ( https://nmap.org ) at 2026-01-06 10:35 EST
Nmap scan report for 192.168.68.102 (192.168.68.102)
Host is up (0.089s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.86 seconds
root@kali:~#
```

The screenshot shows a terminal window titled 'kali-linux-2025.3-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox'. The terminal displays the output of an nmap -sS scan against the host 192.168.68.102. The scan results show various open ports on the target host, including common services like FTP, SSH, and MySQL. The terminal window is part of a desktop environment with a taskbar at the bottom containing icons for file, browser, and other applications. The status bar at the bottom right shows the date and time as 06/01/2026 and 16:35.

TCP Connect Scan: namp -sT Esegue una scansione che stabilisce connessioni TCP complete. È uno scan invasivo perché nmap completa il 3-way-handshake, creando così il canale. Recupera info sullo stato della porta, ma crea più «rumore a livello network» ed è dunque una tecnica di scanning più identificabile e che su grosse reti potrebbe creare congestioni di rete dal host di destinazione 192.168.68.102. La scansione è avvenuta con successo.

```
(root@kali) /home/kali
[+] root@kali: ~
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 10:36 EST
Nmap scan report for 192.168.68.102 (192.168.68.102)
Host is up (0.051s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
MAC Address: 08:00:27:32:6C:87 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

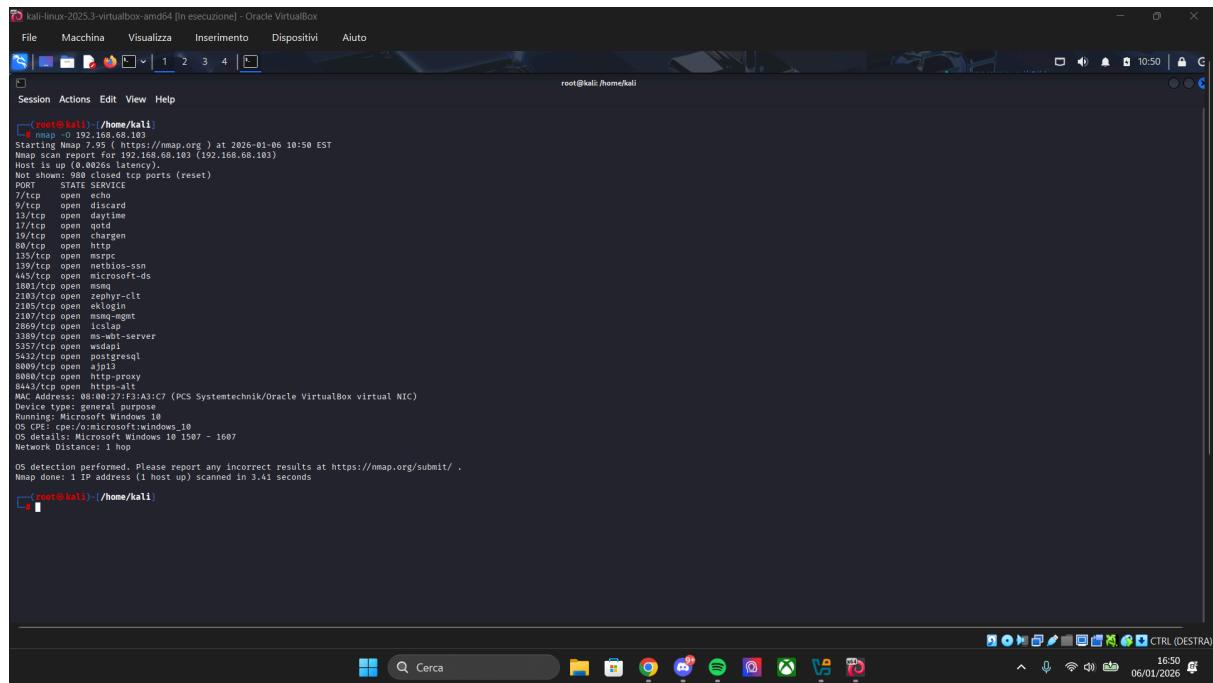
Rilevamento delle Versioni dei Servizi: nmap -sV Identifica i servizi in esecuzione e le loro versioni dell'host di destinazione 192.168.68.102. La scansione è avvenuta con successo.

```
[sudo] password for kali:
[+] root@kali: ~
[+] root@kali: /home/kali
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 10:44 EST
Nmap scan report for 192.168.68.102 (192.168.68.102)
Host is up (0.0536s latency).
Nmap done: 1 IP address (1 host up) scanned in 64.65 seconds
MAC Address: 08:00:27:32:6C:87 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 64.65 seconds
```

Abbiamo aperto la nostra macchina virtuale e la nostra metaploitable windows e abbiamo usato il comando nmap.

Rilevamento del Sistema Operativo: nmap -O tentando di determinare il sistema operativo dell'host di destinazione 192.168.68.103. La scansione è avvenuta con successo.



```
[root@kali ~]# nmap -O 192.168.68.103
Starting Nmap 7.91 ( https://nmap.org ) at 2026-01-06 10:50 EST
Nmap scan report for 192.168.68.103 (192.168.68.103)
Host is up (0.0026s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
7/tcp      open  echo
9/tcp      open  discard
13/tcp     open  nntp
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
1000/tcp   open  netbios-ssn
2083/tcp   open  sehpvr-clt
2105/tcp   open  eklogin
2107/tcp   open  msmq-mgmt
2139/tcp   open  ms-wbt-server
3389/tcp   open  ms-wbt-server
5357/tcp   open  wsdapi
5422/tcp   open  ms-ole-obj-ctrl
8009/tcp   open  aip13
8088/tcp   open  http-proxy
8443/tcp   open  https-alt
MAC Address: 00:0C:29:1A:3C:7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: 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 3.41 seconds
```