

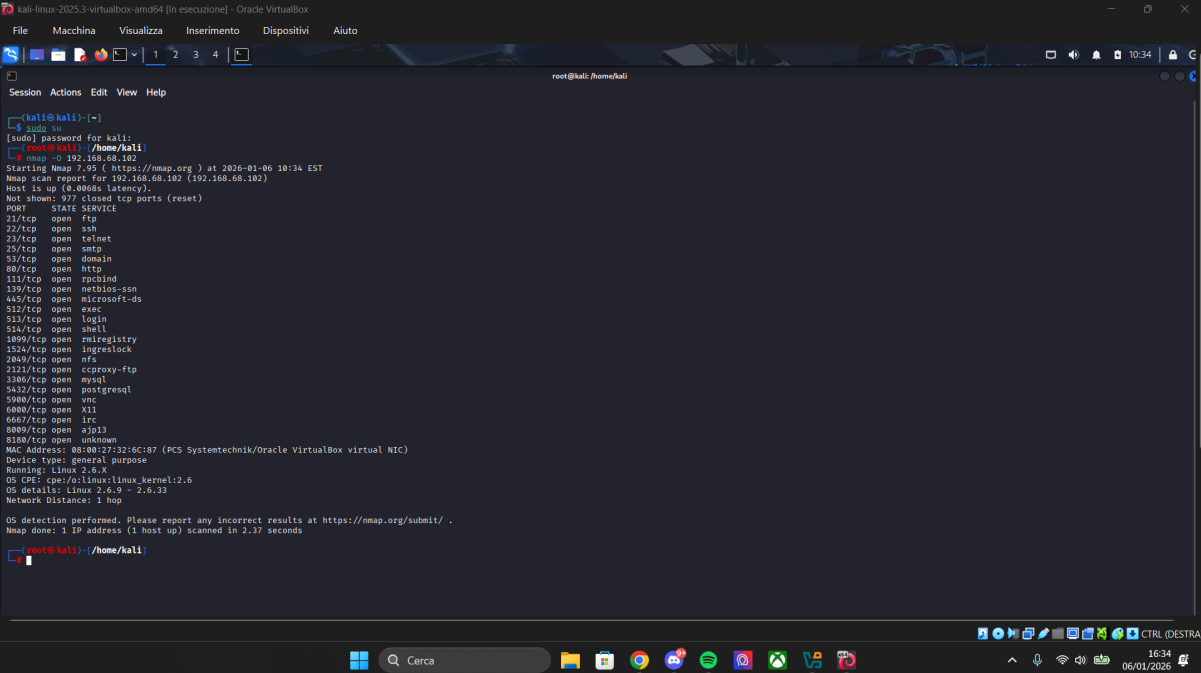
Nmap (Network Mapper) è uno strumento open-source estremamente potente e versatile per la scansione della rete e l'identificazione dei dispositivi e dei servizi. Le sue funzionalità principali includono:

- 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.



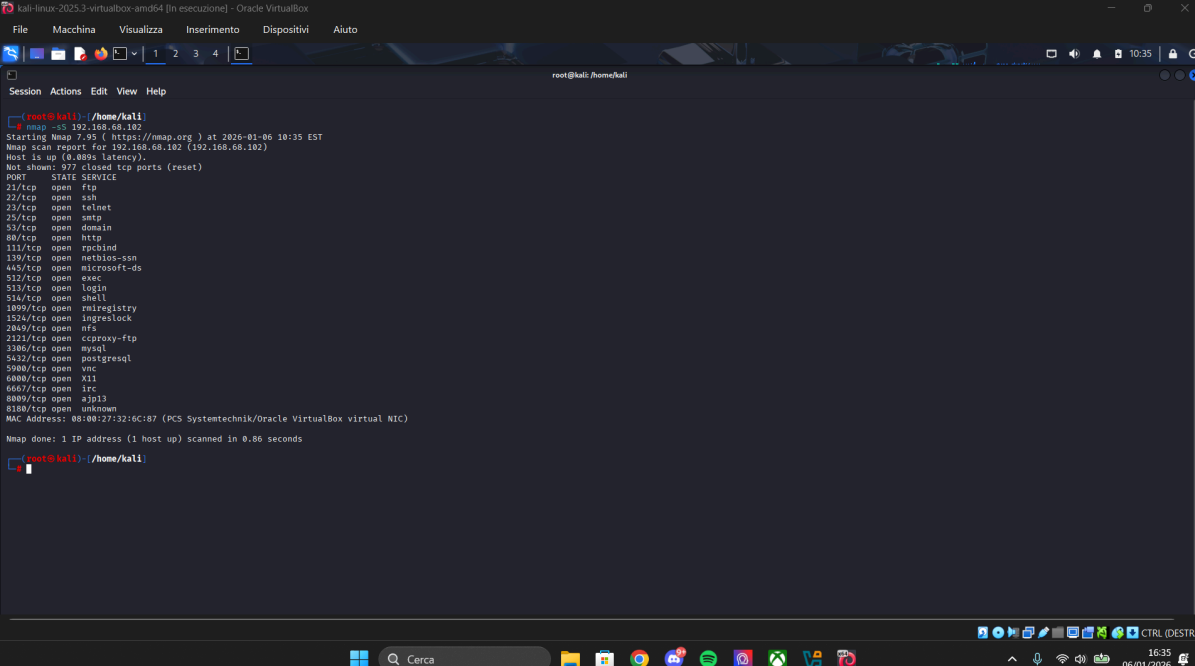
```
kali-linux-2025-3-virtualbox-amd64 [in esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

root@kali: /home/kali

(kali@kali)~$ sudo ss
[sudo] password for kali:
(kali@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 (0.800ms latency).
Not shown: 997 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
2386/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  x11
6667/tcp  open  ipc
8889/tcp  open  sftp
8100/tcp  open  unknown
MAC Address: 08:00:27:32:6C:87 (PCS Systemtechnik/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 2.37 seconds

(kali@kali)~$
```

TCP SYN Scan: nmap -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.



```
kali-linux-2023.3-virtualbox-ami04 [in esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

Session Actions Edit View Help

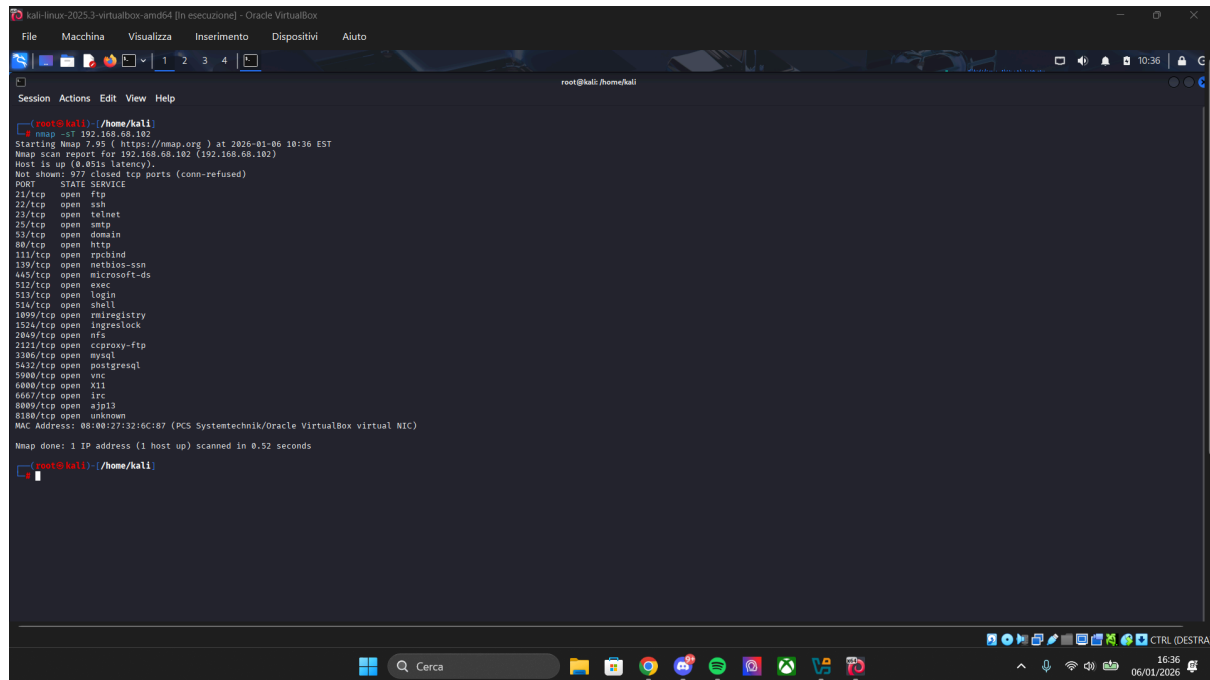
root@kali: /home/kali

root@kali:~# nmap -sS 192.168.68.102
Starting Nmap 7.99 ( https://nmap.org ) at 2020-01-06 10:35 EST
Nmap scan report for 192.168.68.102 (192.168.68.102)
Host is up (0.009s latency).
Not shown: 972 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  tuirglstry
1524/tcp  open  ingreslock
2849/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3386/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  x11
6667/tcp  open  irc
8080/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:32:6C:87 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds

root@kali:~#
```

TCP Connect Scan: nmap -sT Esegue una scansione che stabilisce connessioni TCP complete. E' uno scan invasivo perchè 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.



```
kali-linux-2025.3-virtualbox-amd64 [in esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

root@kali: /home/kali

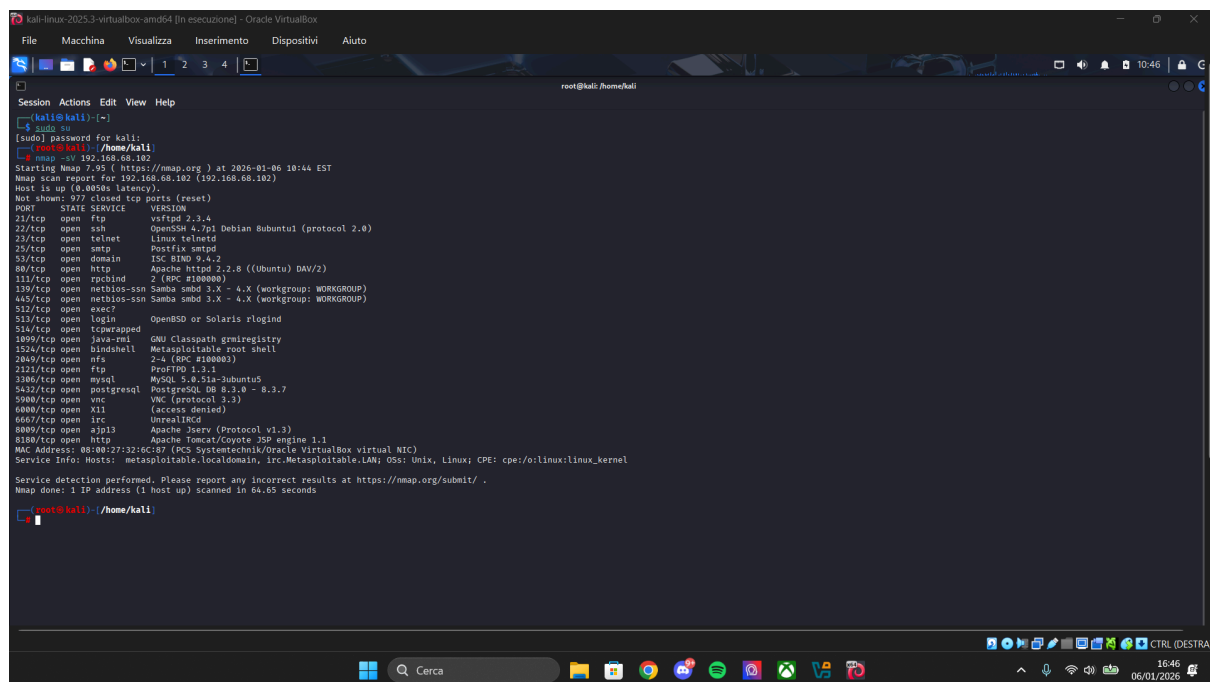
Session  Actions  Edit  View  Help

root@kali: /home/kali
$ nmap -sT 192.168.68.102
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 10:30 EST
Nmap scan report for 192.168.68.102 (192.168.68.102)
Host is up (0.051s latency).
Not shown: 972 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  tmirgistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-ftp
3386/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  x11
6667/tcp  open  irc
8080/tcp  open  ajp13
8180/tcp  open  http
MAC Address: 08:00:27:32:6C:87 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds

root@kali: /home/kali
```

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.



```
kali-linux-2025.3-virtualbox-amd64 [in esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

root@kali: /home/kali

Session  Actions  Edit  View  Help

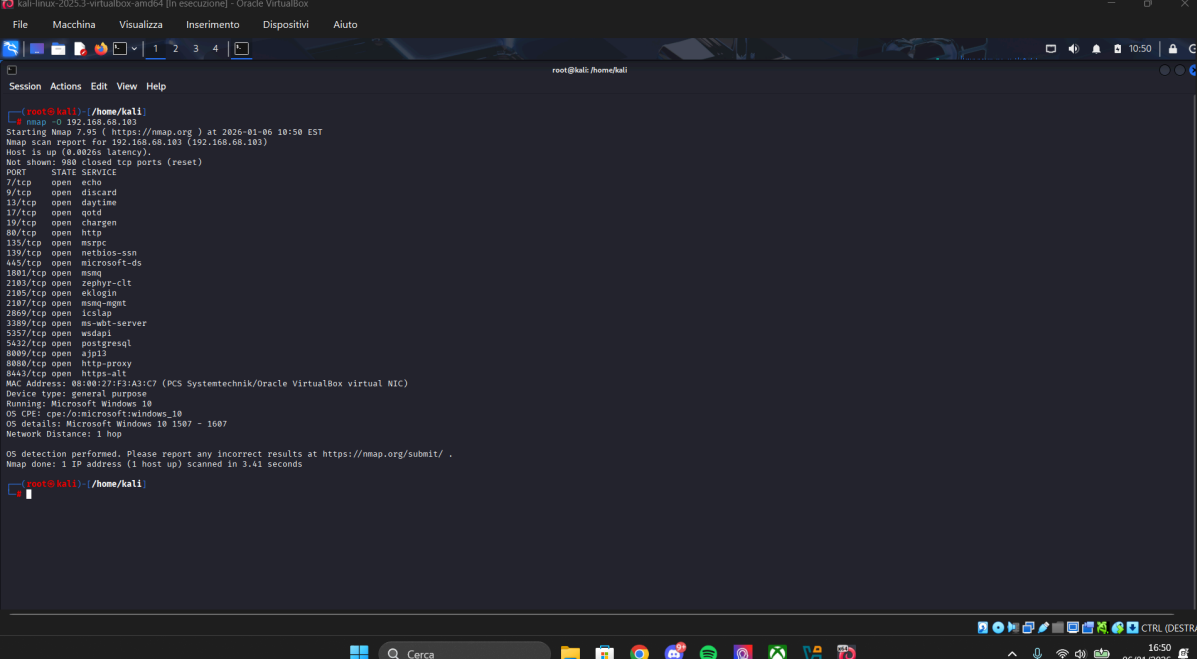
root@kali: /home/kali
$ sudo su
[sudo] password for kali:
root@kali: /home/kali
$ nmap -sV 192.168.68.102
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 10:44 EST
Nmap scan report for 192.168.68.102 (192.168.68.102)
Host is up (0.0050s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian Buntuntu (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/2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind        2 (rpcbind)
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           OpenBSD or Solaris rlogind
513/tcp   open  login          OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi       GNU Classpath gwiregistry
1524/tcp  open  bindshell      Metasploitable root shell
2049/tcp  open  nfs            2.x (RPC: rlm000)
2121/tcp  open  ftp            ProFTPD 1.3.1
3386/tcp  open  mysql          MySQL 5.0.51a-Debian
5432/tcp  open  postgresql     PostgreSQL 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
8080/tcp  open  ajp13          Apache Jserv (Protocol v1.3)
8180/tcp  open  http           Apache/2.2.8/Ubuntu/PHP engine 1.1
MAC Address: 08:00:27:32:6C:87 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploit.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 64.65 seconds

root@kali: /home/kali
```

Abbiamo aperto la nostra macchina virtuale e la nostra metasploitable 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.



```
kali-linux-2025.3-virtualbox-amd64 [in esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

root@kali: /home/kali

root@kali: /home/kali# nmap -O 192.168.68.103
Starting Nmap 7.95 ( 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: 980 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  sklogind
2107/tcp  open  msmq-mgmt
2809/tcp  open  iclslap
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
5432/tcp  open  postgresql
8080/tcp  open  ajp13
8088/tcp  open  http-proxy
8443/tcp  open  https-alt
MAC Address: 08:00:27:F3:A3:C7 (PCS Systemtechnik/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 3.41 seconds

root@kali: /home/kali#
```