

# SCANSIONE DEI SERVIZI CON NMAP

La raccolta informazioni è una parte estremamente essenziale del penetration testing, sapere dove mettere le mani prima di un eventuale attacco, ovviamente con i dovuti permessi documentati su contratto da parte dell'ente.

Le azioni di scansione che eseguiremo fanno parte di quelle che possiamo definire tecniche attive di analisi, perchè andremo ad effettuare una interazione diretta con il nostro target, andando ad usare dei tool specifici per ottenere informazioni più dettagliate.

## Nmap

Per la scansione useremo NMAP che è uno strumento molto versatile e potente che ci permette di scansionare la rete e gli host, rilevare i dispositivi e sistemi operativi, trovare i servizi attivi e le vulnerabilità.

## OS fingerprint

Quello che andremo a fare è identificare il sistema operativo in esecuzione dell'host di destinazione. attraverso la kali con NMAP andiamo ad analizzare la metaspotable. per avere informazioni dettagliate sull'infrastruttura di rete.

Andremo ad usare un opzione chiamata OS fingerprint usando il comando nmap O invieremo una serie di pacchetti specifici all'host analizzandone le risposte e confrontandole con un database di firme per identificare il sistema operativo.

Al termine dell'esecuzione ci fornisce una ricognizione dettagliata, una valutazione delle vulnerabilità e di un identificazione del sistema operativo

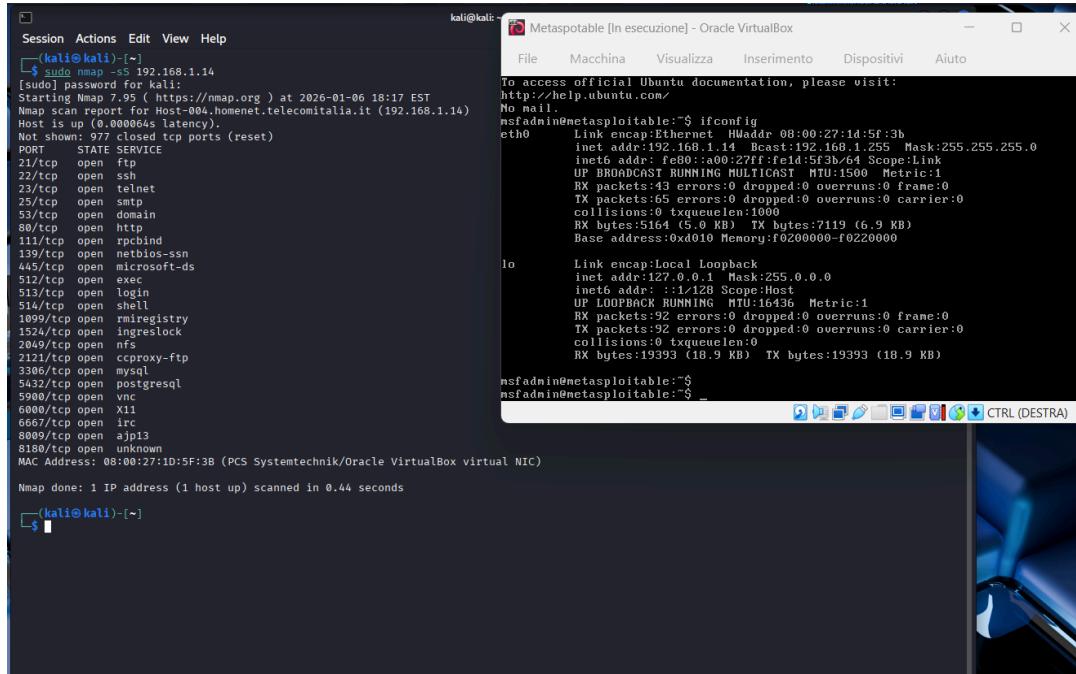
```
(kali㉿kali)-[~]
$ sudo nmap -O 192.168.1.14
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 17:55 EST
Nmap scan report for Host-004.homenet.telecomitalia.it (192.168.1.14)
Host is up (0.00034s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
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  cccproxy-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: 08:00:27:1D:5F:3B (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 8.21 seconds

(kali㉿kali)-[~]
```

## SYN Scan

Andremo ad utilizzare un metodo di scansione delle porte chiamato SYN scan, con il comando -sS questo scanner andrà a iniziare un canale 3-way-handshake con il target ma senza completarlo inviando per ultimo un pacchetto di reset e ricavando comunque informazioni sullo stato delle porte con i dati scambiati inizialmente, questo metodo è più discreto in quanto non faccia rilevare del tutto la scansione.

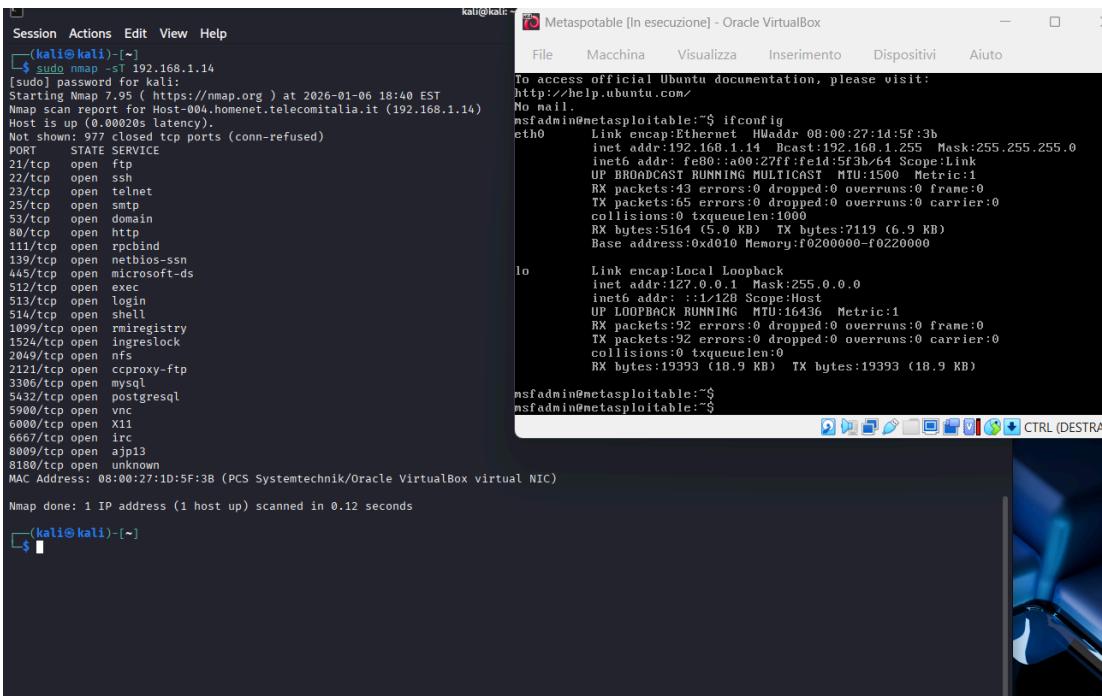


```
(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.1.14
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 18:17 EST
Nmap scan report for Host-004.homenet.telecomitalia.it (192.168.1.14)
Host is up (0.000s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
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: 08:00:27:1D:5F:3B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
```

## TCP connect scan

Il TCP connect scan è sempre un metodo di scansione delle porte fornito da NMAP a differenza del SYN questo metodo crea direttamente un canale 3-way-handshake completo per scansionare le porte e recuperare informazioni sul servizio in ascolto in modo più invasivo. **Il risultato resta di fatto invariato.**

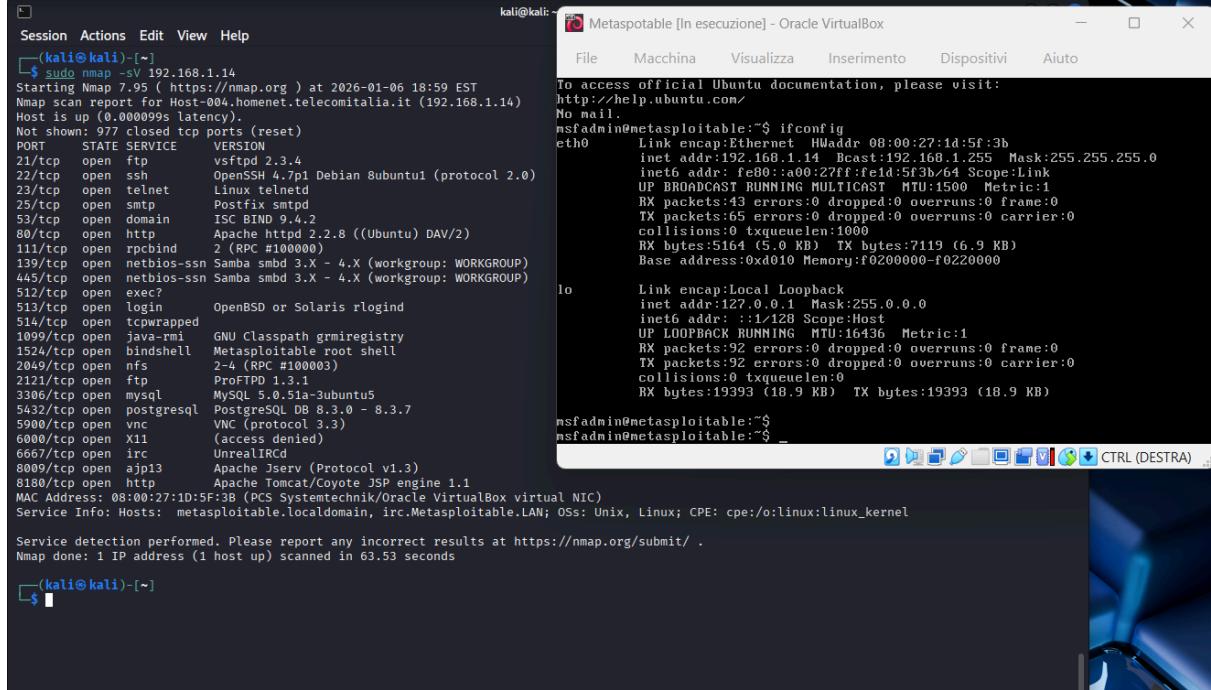


```
(kali㉿kali)-[~]
$ sudo nmap -sT 192.168.1.14
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 18:40 EST
Nmap scan report for Host-004.homenet.telecomitalia.it (192.168.1.14)
Host is up (0.000s latency).
Not shown: 977 closed tcp ports (comm-refused)
PORT      STATE 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: 08:00:27:1D:5F:3B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

## Version detection

Per scoprire i servizi e le relative versioni NMAP ci fornisce il comando nmap -sV che invia una serie di pacchetti di probe ai servizi sulle porte aperte e confronta le risposte con un database di firme per identificare il servizio e la versione in esecuzione.



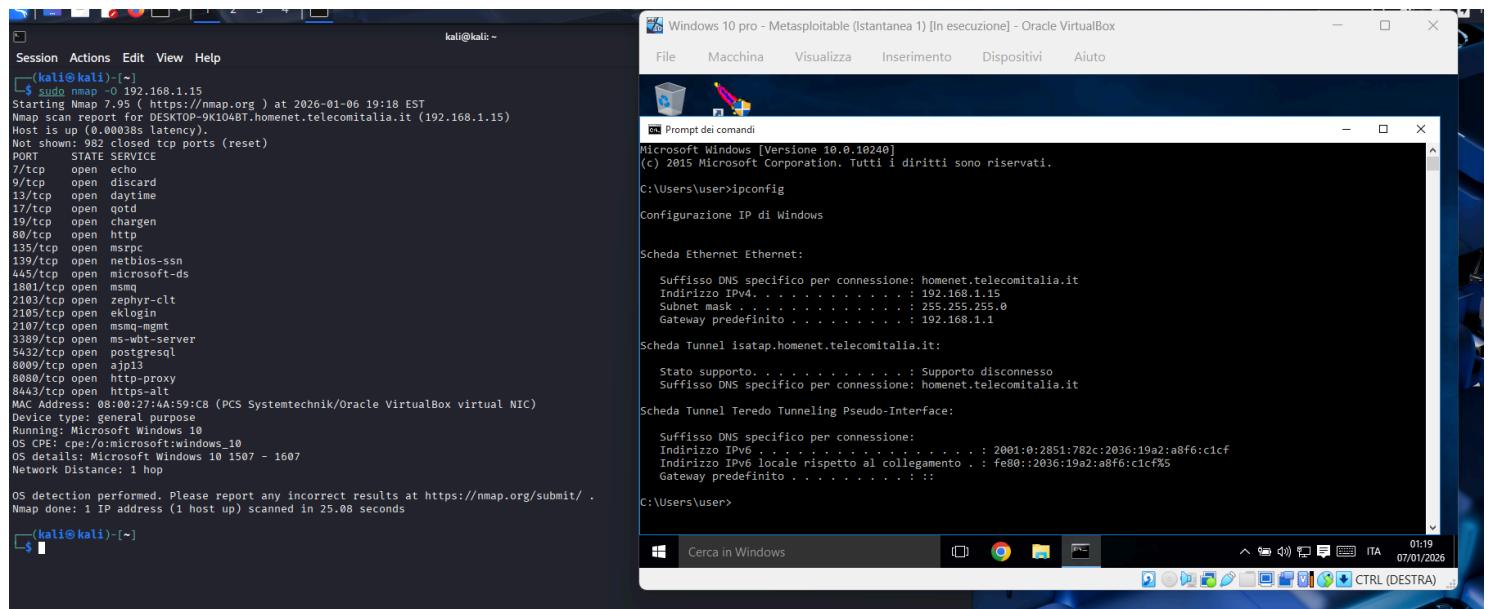
```
kali@kali:[~]
$ sudo nmap -sV 192.168.1.14
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 18:59 EST
Nmap scan report for Host-004.homenet.telecomitalia.it (192.168.1.14)
Host is up (0.00009s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  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?
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  vnc         (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: 08:00:27:10:5F:3B (PCS Systemtechnik/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 63.53 seconds

(kali㉿kali)-[~]
```

## OS fingerprint su windows

Andiamo ad analizzare l'infrastruttura di rete ed a identificare il sistema operativo di windows.



```
kali@kali:[~]
$ sudo nmap -O 192.168.1.15
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 19:18 EST
Nmap scan report for DESKTOP-9K104BT.homenet.telecomitalia.it (192.168.1.15)
Host is up (0.00038s latency).
Not shown: 982 closed tcp ports (reset)
PORT      STATE SERVICE
7/tcp      open  echo
9/tcp      open  discard
13/tcp     open  domain
17/tcp     open  gopher
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
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8000/tcp  open  http-proxy
8443/tcp  open  https-alt
MAC Address: 08:00:27:1A:59:C8 (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 25.08 seconds

(kali㉿kali)-[~]
```