

Scansione con NMAP della macchina Meta

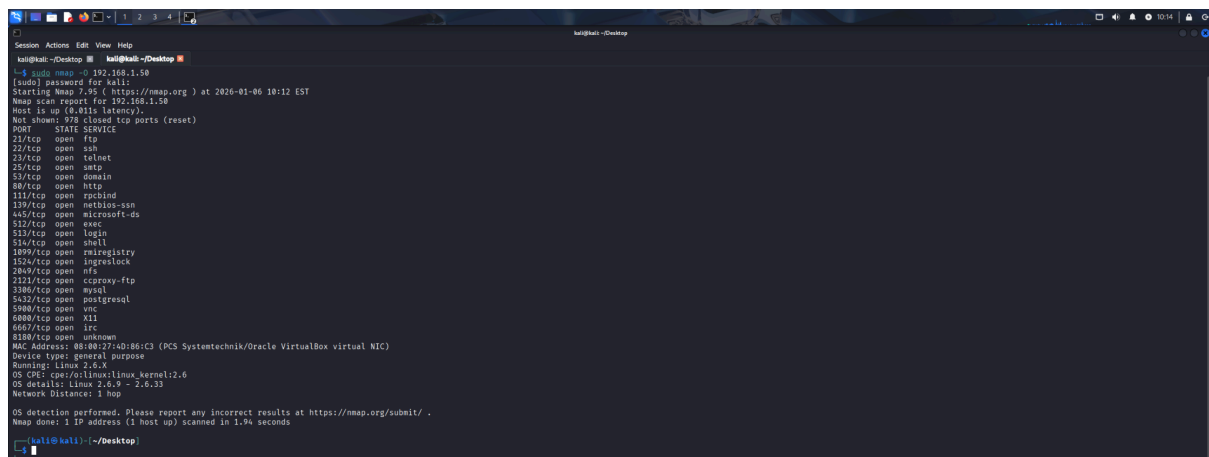
IP Meta:192.168.20.2

```
No mail.
msfadmin@metasploitable:~$ ipconfig
-bash: ipconfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4d:86:c3
          inet addr:192.168.20.2  Bcast:192.168.20.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe4d:86c3/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:61 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:4382 (4.2 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:110 errors:0 dropped:0 overruns:0 frame:0
          TX packets:110 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:22873 (22.3 KB)  TX bytes:22873 (22.3 KB)

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

Scansione per capire quale sistema operativo utilizza Meta



```
kali@kali:~/Desktop
kali@kali:~/Desktop
kali@kali:~/Desktop$ sudo nmap -O 192.168.1.50
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 10:12 EST
Nmap scan report for 192.168.1.50
Host is up (0.011 latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
30/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
119/tcp   open  metabase-svn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
516/tcp   open  shell
1899/tcp  open  nmap-registry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-ftp
2160/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6080/tcp  open  x11
6667/tcp  open  irc
9180/tcp  open  unknown
MAC Address: 08:00:27:4D:86:C3 (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 - 2.6.32
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 1.94 seconds

kali@kali:~/Desktop$
```

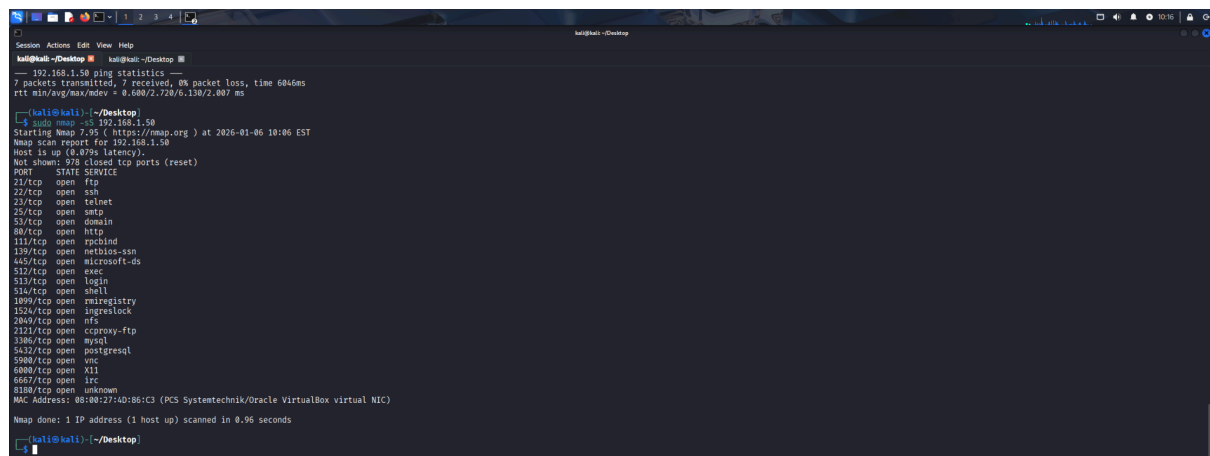
Per capire quale OS utilizza Meta usiamo nmap con il flag -O. Come si può evidenziare dallo screen il sistema operativo che usa Meta è Linux 2.6.9 - 2.6.33.

Ora vogliamo effettuare una scansione Syn Scan. Questo tipo di scansione ci permette di individuare porte aperte senza stabilire una connessione TCP completa, cioè non completa il three-way-handshake. E' una scansione che fa meno rumore perchè:

- Non completa la connessione
- Non crea una sessione applicativa
- Molti servizi non registrano la connessione nei log applicativi
- Rimane rilevabile da firewall e sistemi IDS/IPS

Requisiti richiesti:

- Richiede privilegi di root
- Usa pacchetti TCP raw
- E' più veloce e più "stealth" di -sT



```
kali@kali:~/Desktop$ sudo nmap -sS 192.168.1.50
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 10:06 EST
Nmap scan report for 192.168.1.50
Host is up (0.079s latency).
Not shown: 678 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  raieregistry
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
8180/tcp  open  unknown
NMC Address: 00:00:27:40:B6:C3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.96 seconds
```

Ora effettuiamo una scansione Nmap con il flag -sT, detta TCP Connect Scan.

Questa tipologia di scansione utilizza la chiamata di sistema connect() per stabilire una connessione TCP completa con il target, completando il three-way handshake (SYN, SYN-ACK, ACK).

La scansione -sT consente di individuare le porte TCP aperte, chiuse o filtrate ed è la modalità utilizzata da Nmap quando non sono disponibili privilegi di root.

A differenza della SYN Scan (-sS), la TCP Connect Scan genera una connessione reale verso il servizio remoto, risultando più rumorosa e generalmente registrata nei log applicativi del sistema target.

```
Session Actions Edit View Help
kali@kali:~/Desktop
--- 192.168.1.50 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6046ms
rtt min/avg/max/ndev = 0.600/2.720/6.130/2.007 ms

kali@kali:~/Desktop
$ sudo nmap -sS 192.168.1.50
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 10:06 EST
Nmap scan report for 192.168.1.50
Host is up (0.079s latency).
Not shown: 578 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  nmapregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8180/tcp  open  unknown
MAC Address: 08:00:27:AD:B6:C3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.96 seconds

kali@kali:~/Desktop
```

Considerazioni di sicurezza

La TCP Connect Scan è meno stealth rispetto alla SYN Scan, ma garantisce maggiore affidabilità nei risultati, in quanto utilizza il normale stack TCP del sistema operativo.

Per questo motivo viene spesso utilizzata in contesti di test autorizzati e di analisi preliminare della superficie di attacco.

Ora facciamo una Version Detection utilizzando il flag `-sV` per capire quali servizi sono in ascolto sulle porte, individuare la versione software.

E' importante perchè permette di correlare i servizi a vulnerabilità note.

```
Session Actions Edit View Help
kali@kali:~/Desktop
--- 192.168.1.50 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6046ms
rtt min/avg/max/ndev = 0.600/2.720/6.130/2.007 ms

kali@kali:~/Desktop
$ sudo nmap -sV 192.168.1.50
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 10:29 EST
Nmap scan report for 192.168.1.50
Host is up (0.0829s latency).
Not shown: 578 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 6ubuntu1 (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 (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  tpcwrapped
1099/tcp  open  java-rmi     GNU Classpath gmicregistry
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 8.1.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8180/tcp  open  unknown
MAC Address: 08:00:27:AD:B6:C3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: hosts: metasploitable.localdomain, irc:Metasploitable.LAN, OS: 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 100.58 seconds

kali@kali:~/Desktop
```

La scansione `-sV` interagisce attivamente con i servizi individuati, inviando specifiche sonde applicative per ottenere informazioni dettagliate come il nome del servizio, la versione del software e, in alcuni casi, il sistema operativo o il banner del servizio.

La Version Detection ha ampliato l'analisi della superficie di attacco, permettendo di passare dalla semplice individuazione delle porte aperte all'identificazione puntuale dei servizi e delle versioni installate.

Considerazioni di sicurezza

L'identificazione delle versioni dei servizi rappresenta un passaggio critico per un attaccante, in quanto consente di associare i software rilevati a vulnerabilità pubbliche note (CVE). Tuttavia, trattandosi di una scansione più invasiva rispetto a una semplice port scan, può essere rilevata e registrata nei log del sistema target.

Scansione con NMAP della macchina Windows

```
Prompt dei comandi
Microsoft Windows [Versione 10.0.18240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\User>ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione: homenet.telecomitalia.it
    Indirizzo IPv4 . . . . . : 192.168.1.65
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.1

Scheda Tunnel Teredo Tunneling Pseudo-Interface:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 . . . . . : 2001:0:2851:782c::c2:128c:a011:6553
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::cc2:128c:a011:6553%5
    Gateway predefinito . . . . . :

Scheda Tunnel Isatap.homenet.telecomitalia.it:

    Stato supporto . . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione: homenet.telecomitalia.it

C:\Users\User>
```

IP Windows 192.168.1.65

Scansione per capire quale sistema operativo utilizza Windows

```
Session: Actions Edit View Help
kali@kali:~/Desktop
└─$ sudo nmap -i 192.168.1.65
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 10:47 EST
Nmap scan report for DESKTOP-9K1048T.homenet.telecomitalia.it (192.168.1.65)
Host is up (0.00073s 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  qdmd
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  msqm
2183/tcp  open  zephyr-clt
2185/tcp  open  exlogin
2187/tcp  open  msqm-ngat
3389/tcp  open  ms-wbt-server
5357/tcp  open  endap1
5432/tcp  open  postgresql
8089/tcp  open  ejb3
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
NIC: address: 08:00:27:98:27:62 (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 1.41 seconds

kali@kali:~/Desktop
```

Per capire quale sistema operativo utilizza questa macchina windows abbiamo utilizzato il flag -O. Come si può osservare dallo screen il sistema operativo che utilizza windows è windows_10.

