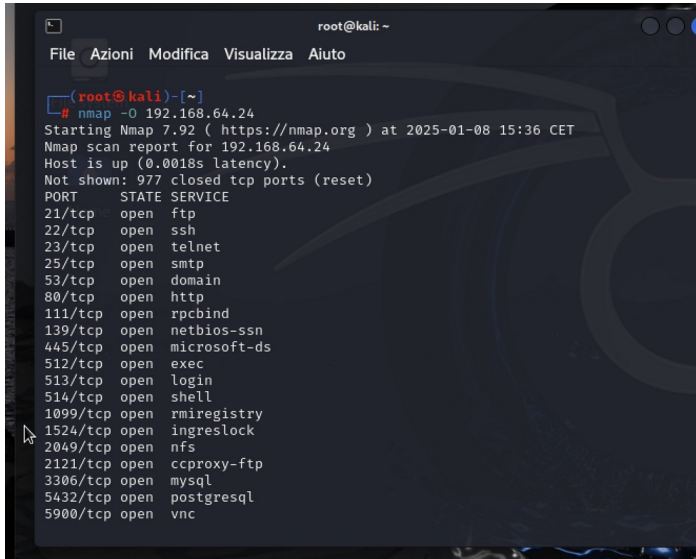


L'esercizio di oggi chideva di effettuare le seguenti scansioni sul target Metasploitable:

- OS fingerprint.
- Syn Scan.
- TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?
- Version detection.

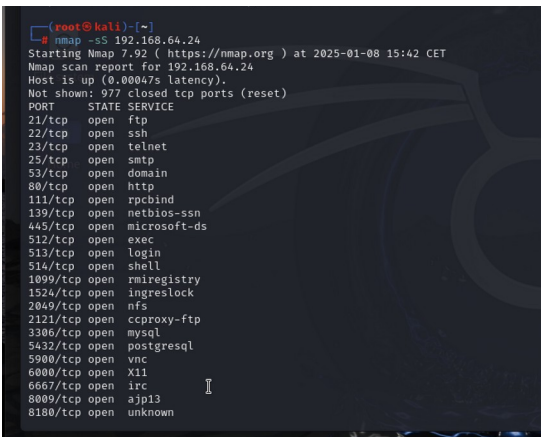
E la seguente sul target Windows:

- OS fingerprint.



```
(root@kali)-[~]
# nmap -O 192.168.64.24
Starting Nmap 7.92 ( https://nmap.org ) at 2025-01-08 15:36 CET
Nmap scan report for 192.168.64.24
Host is up (0.0018s 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
```

Iniziamo a fare una scansione con nmap su Linux, utilizzando il comando `nmap -O` (OS fingerprint), indirizzandola all'indirizzo IP di Metasploitable, come mostrato nell'immagine a sinistra



```
(root@kali)-[~]
# nmap -sS 192.168.64.24
Starting Nmap 7.92 ( https://nmap.org ) at 2025-01-08 15:42 CET
Nmap scan report for 192.168.64.24
Host is up (0.00047s 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
```

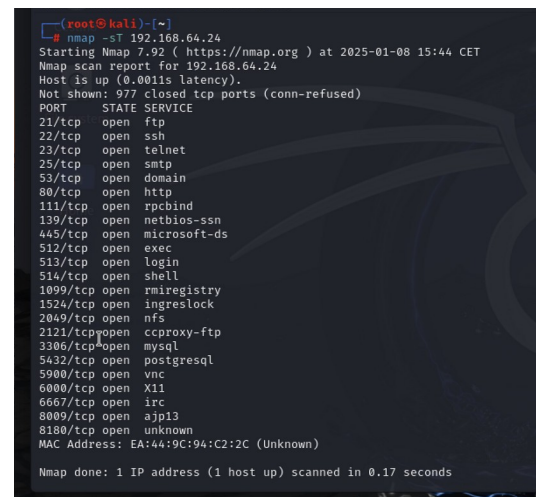
Il secondo comando è `-sS`, che viene utilizzato per eseguire una scansione SYN (SYN scan)

Il terzo comando è `-sT`, che corrisponde alla scansione TCP connect.

Le differenze sono :

-sS (SYN scan): Più veloce e discreta, ma meno completa.

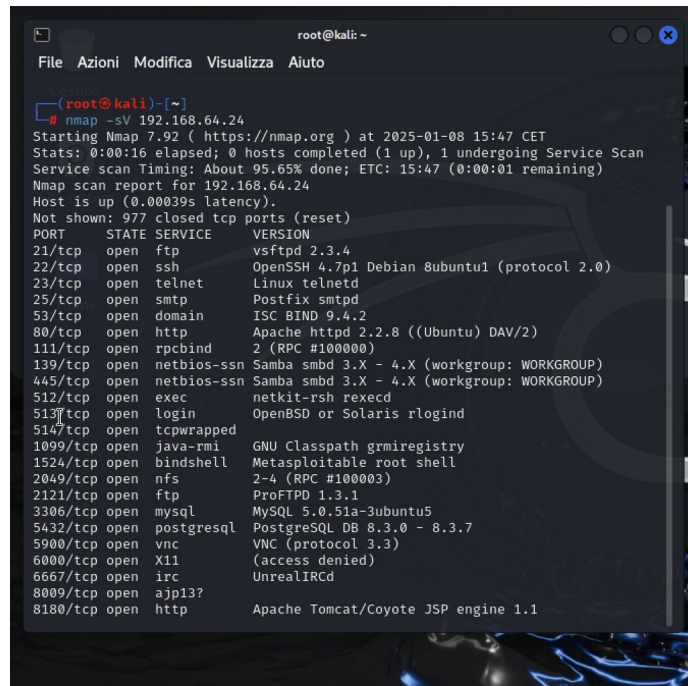
-sT (TCP connect scan): Più facile da rilevare, ma completa.



```
(root@kali)-[~]
# nmap -sT 192.168.64.24
Starting Nmap 7.92 ( https://nmap.org ) at 2025-01-08 15:44 CET
Nmap scan report for 192.168.64.24
Host is up (0.0011s latency).
Not shown: 977 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  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: EA:44:9C:94:C2:2C (Unknown)

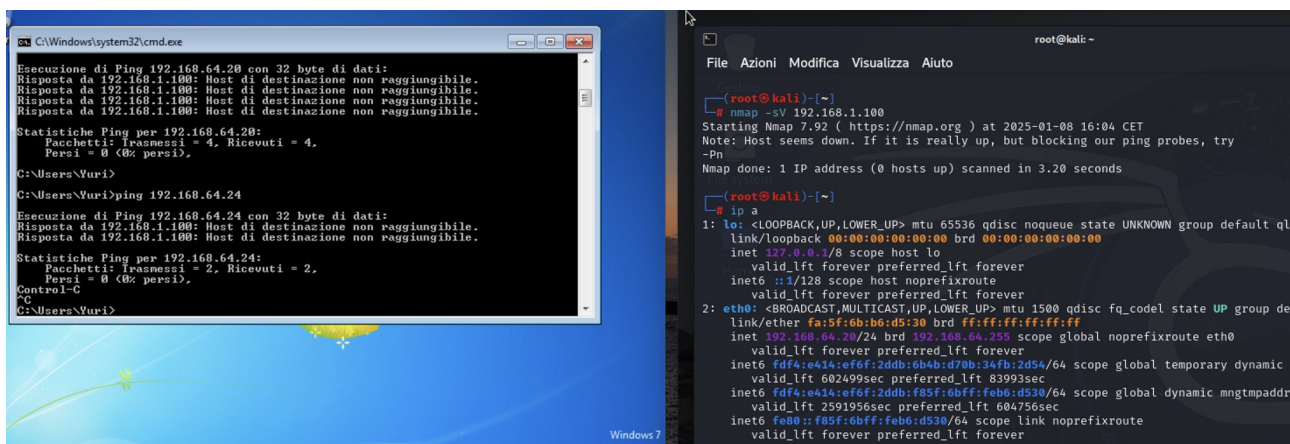
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

L'ultimo comando è la Version Detection, ovvero -sV, che identifica le versioni dei servizi su porte aperte.



```
root@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
root@kali: ~  
# nmap -sV 192.168.64.24  
Starting Nmap 7.92 ( https://nmap.org ) at 2025-01-08 15:47 CET  
Stats: 0:00:16 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 95.65% done; ETC: 15:47 (0:00:01 remaining)  
Nmap scan report for 192.168.64.24  
Host is up (0.00039s 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         netkit-rsh rexecd  
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  X11          (access denied)  
6667/tcp  open  irc          UnrealIRCd  
8009/tcp  open  ajp13?       Apache Tomcat/Coyote JSP engine 1.1  
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
```

Infine, lo stesso comando viene utilizzato per indirizzare Windows 7 da Linux.



```
C:\Windows\system32\cmd.exe  
Esecuzione di Ping 192.168.64.20 con 32 byte di dati:  
Risposta da 192.168.1.100: Host di destinazione non raggiungibile.  
Risposta da 192.168.1.100: Host di destinazione non raggiungibile.  
Risposta da 192.168.1.100: Host di destinazione non raggiungibile.  
Risposta da 192.168.1.100: Host di destinazione non raggiungibile.  
Statistiche Ping per 192.168.64.20:  
Pacchetti: Trasmessi = 4, Ricevuti = 4,  
Persi = 0 (0% persi).  
C:\Users\Vuri>  
C:\Users\Vuri>ping 192.168.64.24  
Esecuzione di Ping 192.168.64.24 con 32 byte di dati:  
Risposta da 192.168.1.100: Host di destinazione non raggiungibile.  
Risposta da 192.168.1.100: Host di destinazione non raggiungibile.  
Statistiche Ping per 192.168.64.24:  
Pacchetti: Trasmessi = 2, Ricevuti = 2,  
Persi = 0 (0% persi).  
Control-C  
^C  
C:\Users\Vuri>  
Windows 7  
0.0.0.0  
  
root@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
root@kali: ~  
# nmap -sV 192.168.1.100  
Starting Nmap 7.92 ( https://nmap.org ) at 2025-01-08 16:04 CET  
Note: Host seems down. If it is really up, but blocking our ping probes, try  
-Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 3.20 seconds  
  
root@kali: ~  
# ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether fa:5f:0b:b6:d5:30 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.64.20/24 brd 192.168.64.255 scope global noprefixroute eth0  
        valid_lft forever preferred_lft forever  
    inet6 fd4a:e414:ef6f:2ddb:6b4b:d70b:34fb:2d54/64 scope global temporary dynamic  
        valid_lft 602499sec preferred_lft 83993sec  
    inet6 fd4a:e414:ef6f:2ddb:f85f:6bff:feb6:d530/64 scope global dynamic mngtmpaddr  
        valid_lft 2591956sec preferred_lft 604756sec  
    inet6 fe80::f85f:6bff:feb6:d530/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever
```