ESERCIZI S5/L2

Traccia: Tecniche di scansione con Nmap

Target 1: Metasploitable **(192.168.1.33)**
Target 2: Windows **(192.168.1.24)**

1. Analisi Target: Metasploitable

1.1. Identificazione Sistema Operativo (OS Fingerprint)

Per identificare il sistema operativo del target, ho utilizzato il comando ***sudo nmap -O***

- IP: 192.168.1.33
- OS Rilevato: Linux 2.6.X (Dettagli: Linux 2.6.9 - 2.6.33)

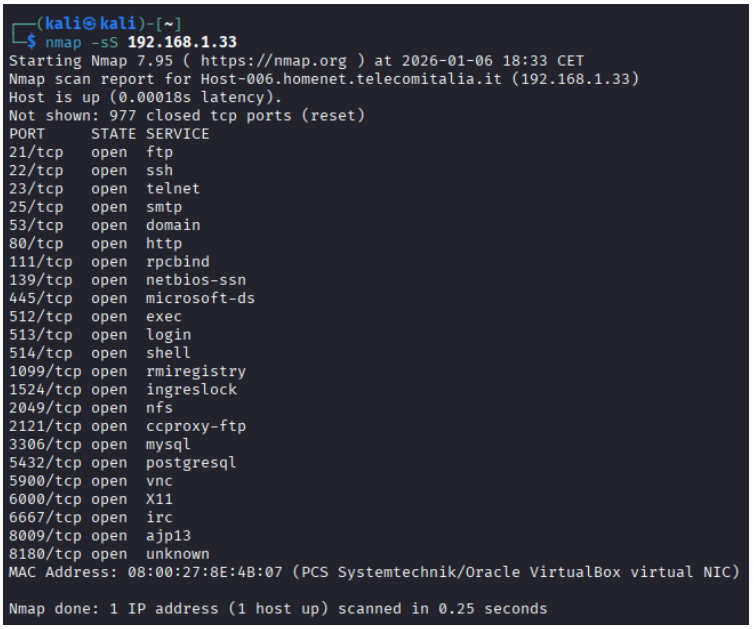
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.33
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 18:30 CET
Nmap scan report for Host-006.homenet.telecomitalia.it (192.168.1.33)
Host is up (0.00020s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
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: 08:00:27:8E:4B:07 (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 1.87 seconds
```

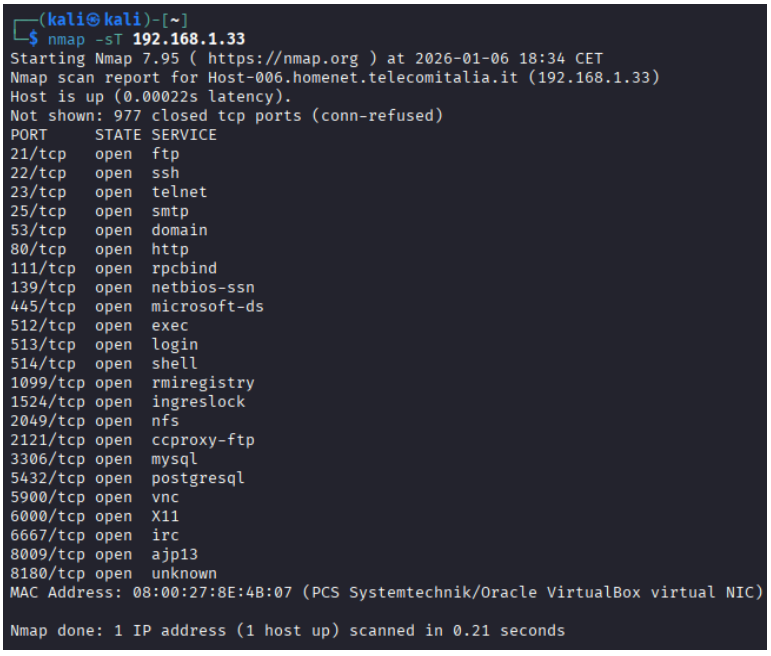
1.2. Confronto Tecniche di Scansione (SYN Scan vs TCP Connect)

Sono state eseguite due diverse tipologie di scansione per valutarne le differenze:

- **SYN Scan (`-sS`):** Eseguita in 0.25 secondi. È una scansione che non completa l'handshake TCP, risultando più veloce e meno invasiva nei log del target.



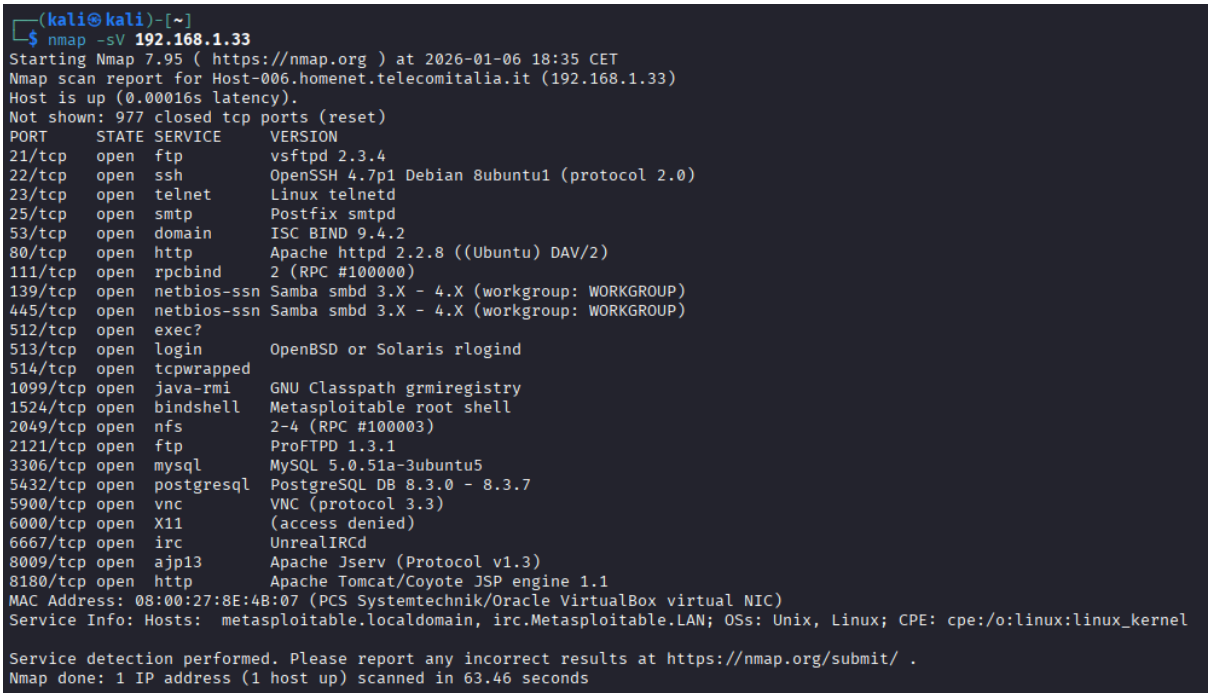
- **TCP Connect (`-sT`):** Eseguita in 0.21 secondi. Completa l'handshake TCP. In reti ampie è più lenta e facilmente tracciabile dai sistemi di IDS poiché stabilisce una connessione reale.



Differenze riscontrate: Entrambe hanno riportato correttamente le stesse porte aperte, ma lo stato dei pacchetti ignorati varia **(977 porte chiuse con** reset **per SYN, mentre TCP Connect le indica come** conn-refused**).**

1.3. Service & Version Detection

Attraverso il comando ***nmap -sV*** sono stati identificati i servizi attivi e le relative versioni, dato fondamentale per l'individuazione di vulnerabilità note.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.33
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 18:35 CET
Nmap scan report for Host-006.homenet.telecomitalia.it (192.168.1.33)
Host is up (0.00016s 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  X11         (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: 08:00:27:8E:4B:07 (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 63.46 seconds
```

2. Analisi Target: Windows

2.1. OS Fingerprint

Anche qui, come con il primo Target, per individuare il sistema operativo ho utilizzato il comando ***sudo nmap -O***

- IP: 192.168.1.24
- OS Rilevato: Microsoft Windows XP (Aggressive OS guesses: Windows 2000 SP4 o Windows XP SP2/SP3).

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.24
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 18:50 CET
Nmap scan report for windowsxp.homenet.telecomitalia.it (192.168.1.24)
Host is up (0.00025s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:5C:8D:1C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 2000 SP3/SP4 or Windows XP SP1/SP2 (97%), Microsoft Windows XP SP2 or SP3 (97%), Microsoft Windows 2000 SP0 - SP4 or Windows XP SP0 - SP1 (95%), Microsoft Windows 2000 SP4 or Windows XP SP1a (95%
), Microsoft Windows Server 2003 SP1 or SP2 or Windows XP SP1 (95%), Microsoft Windows 2000 SP4 (93%), Microsoft Windows XP Professional SP2 or Windows Server 2003 (93%), Microsoft Windows XP SP1 (93%), Microsoft Windows XP SP3 (92%), M
icrosoft Windows 2000 Server SP3 or SP4 (92%)
No exact OS matches for host (test conditions non-ideal).
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 9.52 seconds
```