In questo esercizio ho eseguito diverse tipologie di scansioni Nmap su una macchina Metasploitable residente sulla rete 192.168.50.0/24.
Lo scopo era confrontare il comportamento delle varie tecniche di scanning e raccogliere informazioni su:

- sistema operativo del target,
- porte aperte,
- servizi esposti,
- versioni software.

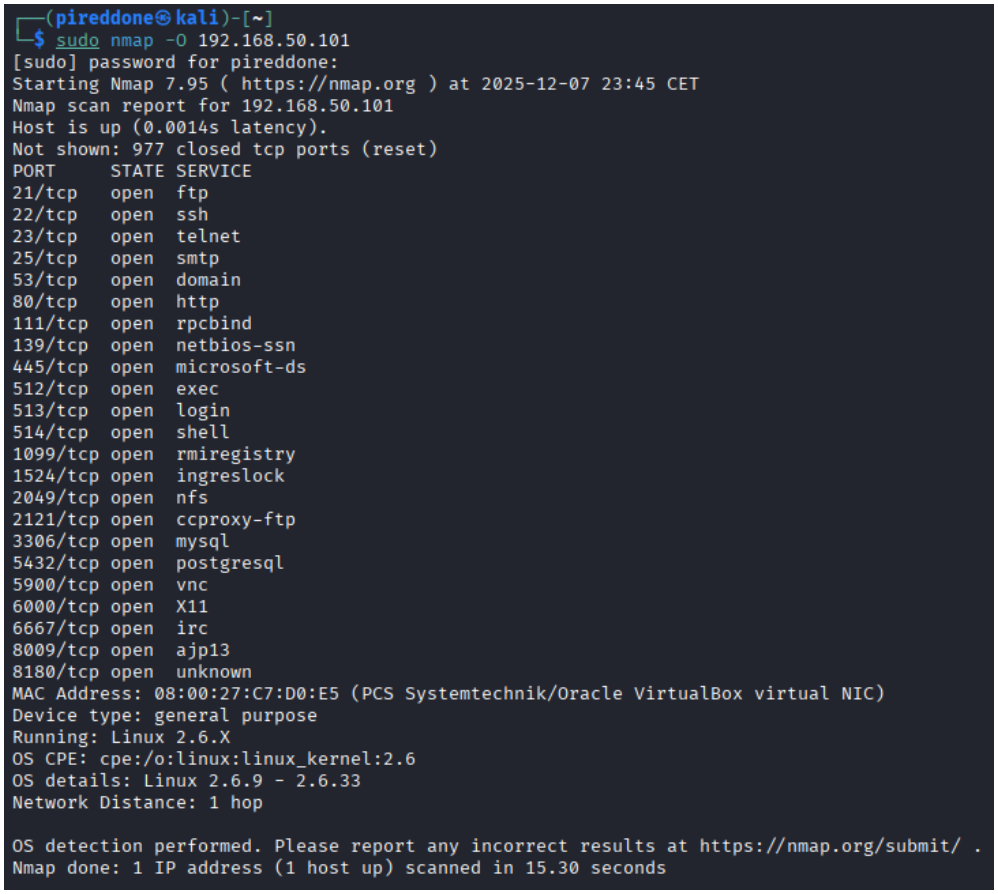
Metasploitable è una macchina deliberatamente vulnerabile, quindi rappresenta un ottimo ambiente di laboratorio.

🔸 1. OS FINGERPRINTING (-O)

La prima analisi ha avuto l'obiettivo di identificare il sistema operativo utilizzato dalla macchina target.

✓ Comando eseguito:

sudo nmap -O 192.168.50.101



✓ **Risultato**

Nmap ha identificato il sistema operativo come:

- **Linux 2.6.x**
- Probabilmente una distribuzione molto vecchia (come confermato da Metasploitable2)

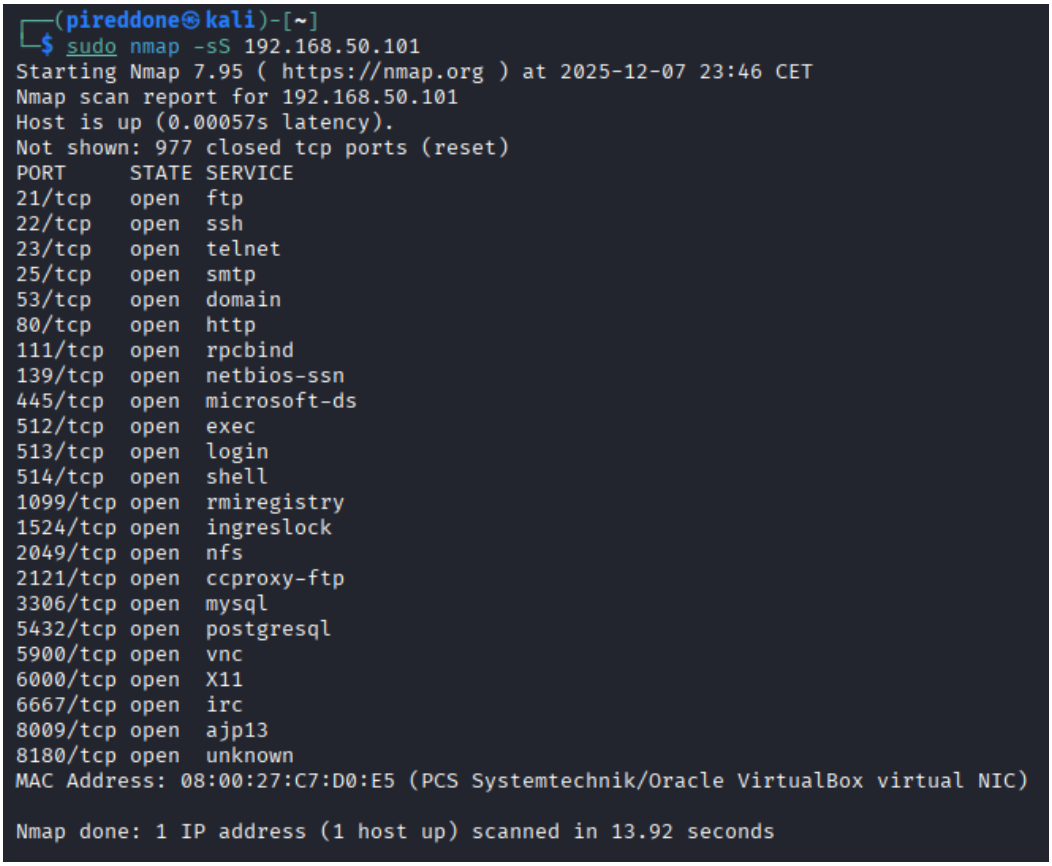
Sono emerse anche numerose porte aperte, segno che il sistema è volutamente esposto per l'esercitazione.

🔸 **2. SYN SCAN (-sS)**

Successivamente ho eseguito una SYN scan, conosciuta come “scansione stealth”.

✓ **Comando:**

sudo nmap -sS 192.168.50.101



✓ **Risultato**

La scansione ha rivelato un’ampia lista di porte aperte, tra cui:

- 21/tcp → FTP
- 22/tcp → SSH

- 23/tcp → Telnet
- 25/tcp → SMTP
- 80/tcp → HTTP
- 3306/tcp → MySQL
- 5432/tcp → PostgreSQL
- 5900/tcp → VNC
- Molti altri servizi legacy (IRC, RPC, NetBIOS, ecc.)

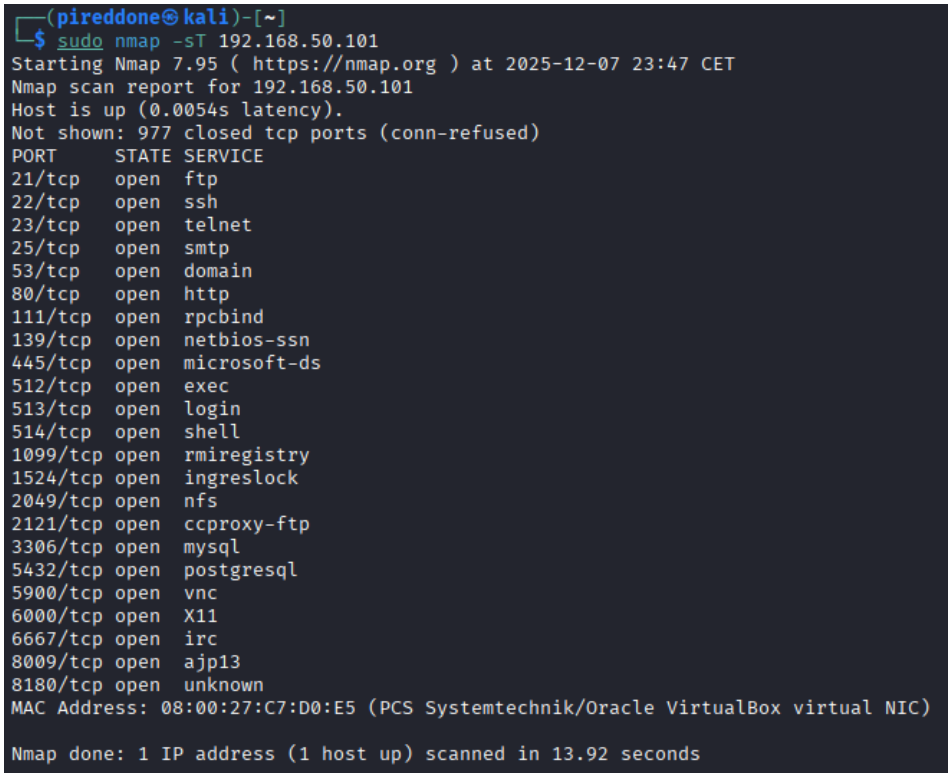
La SYN scan **non completa la connessione TCP**, quindi risulta meno "rumorosa" e spesso preferita nei pentest.

🔸 3. TCP CONNECT SCAN (-sT)

Ho poi eseguito la connect scan, che invece completa il three-way-handshake.

✓ Comando:

sudo nmap -sT 192.168.50.101



✓ Risultato

L'elenco delle porte aperte è praticamente identico alla SYN scan, ma:

- la connect scan è **più lenta**,
- è più facilmente rilevabile dai sistemi di logging,

- rappresenta il metodo “standard” se Nmap non ha privilegi elevati.

Breve confronto

Scansione	Caratteristica	Rumorosità	Privilegi richiesti
SYN (-sS)	Semi-stealth	Bassa	Root
TCP (-sT)	Connessione completa	Alta	Nessuno

🔸 4. VERSION DETECTION (-sV)

Infine ho eseguito una scansione per rilevare le versioni dei servizi in ascolto.

✓ Comando:

sudo nmap -sV 192.168.50.101

```
┌──(pireddone㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 23:48 CET
Nmap scan report for 192.168.50.101
Host is up (0.00060s 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?
514/tcp  open  shell       Netkit rshd
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:C7:D0:E5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux
_kernel
```

✓ Risultati principali

- **FTP** → vsftpd 2.3.4 (versione famosa per una backdoor)
- **SSH** → OpenSSH 4.7p1
- **HTTP** → Apache 2.2.8 + PHP 5.2.4
- **SMB** → Samba 3.x
- **MySQL** → MySQL 5.0.51a-3ubuntu5
- **PostgreSQL** → 8.3.0 - 8.3.7
- **Tomcat** → Coyote JSP engine 1.1

Tutte versioni obsolete, utili ai fini della didattica.

🔸 Conclusioni

Le varie scansioni hanno confermato che Metasploitable espone:

- un’ampia superficie di attacco,
- servizi privi di aggiornamenti,
- protocolli non cifrati (FTP, Telnet, SMTP, IRC),
- software soggetti a vulnerabilità note.

L’esercitazione ha permesso di capire come ogni modalità di scansione fornisca informazioni specifiche e come confrontarle per ottenere un quadro completo dell’host target.