## Unità 2 - S5-L5

**21/10/2025**


# Alessandro Pietro Salerno


# Report di Security Assessment: Scansione Rete Target (Fase 1)

---

## 1. Introduzione

Il presente report documenta le attività di scansione e analisi condotte in conformità con l'esercizio richiesto. L'obiettivo di questa attività è simulare la Fase 2 **(Service Enumeration and Scanning)** di un Penetration Test.

Questa fase è fondamentale per identificare la superficie di attacco, enumerare i servizi esposti e rilevare le firme dei sistemi operativi dei target designati. I dati raccolti sono critici per la successiva fase di analisi delle vulnerabilità.

Le attività sono state condotte in un ambiente di laboratorio isolato (Rete Interna, subnet `192.168.50.0/24`) utilizzando la macchina Kali Linux (`192.168.50.10`) come postazione di attacco.

## 2. Metodologia e Fasi Operative

L'analisi è stata condotta seguendo una metodologia strutturata, applicando diverse tecniche di scansione Nmap per raccogliere informazioni in modo progressivo. Le fasi operative eseguite sul target primario (Metasploitable) sono state:

1. **OS Fingerprinting (`-O`):** Rilevamento del sistema operativo per determinare la piattaforma target.

2. **SYN Scan (`-sS`):** Scansione delle porte "stealth" (half-open) per un'enumerazione rapida e discreta delle porte TCP aperte.

3. **TCP Connect Scan (`-sT`):** Scansione delle porte "full-connect" per enumerare le porte TCP aperte e confrontare i risultati e il comportamento rispetto alla scansione SYN.

4. **Version Detection (`-sV`):** Identificazione precisa del software e delle versioni in esecuzione sui servizi esposti.

## 3. Analisi dei Risultati - Target 1: Metasploitable

I seguenti risultati sono stati ottenuti sul target primario.

- **Indirizzo IP Target:** `192.168.50.3`

### 3.1. Fase 1: OS Fingerprinting

È stata eseguita una scansione Nmap per il rilevamento del sistema operativo.

- **Comando Eseguito:** `sudo nmap -O 192.168.50.3`
- **Risultato Principale:** Il sistema operativo target è stato identificato come **`Linux 2.6.X`** (con dettagli che suggeriscono un kernel tra `Linux 2.6.9` e `2.6.33`).

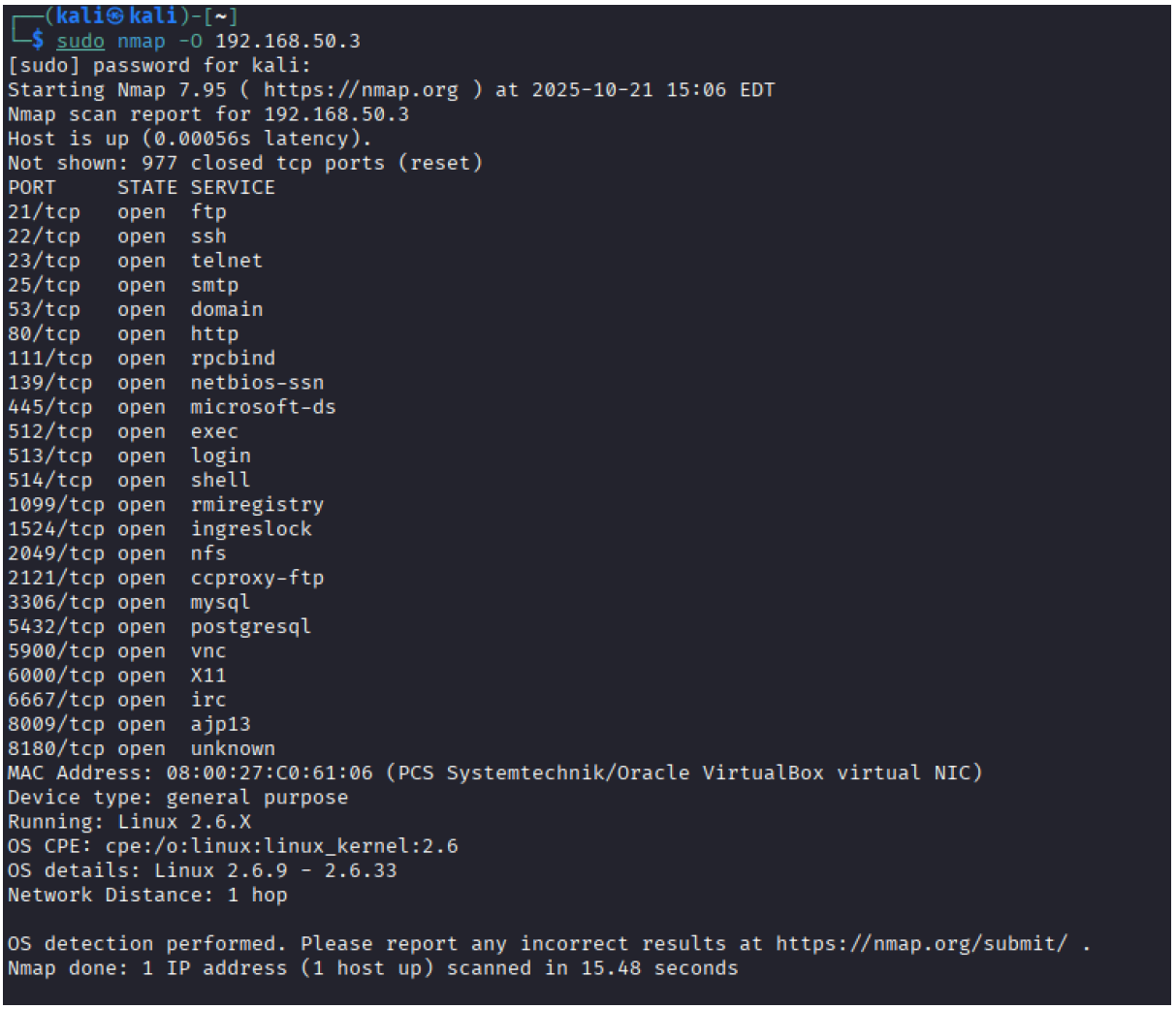
  Questo indica un sistema operativo datato, potenziale portatore di vulnerabilità note.

---

La scasione OS fingerprint ha dunque identificato il sistema operativo , ed ha inoltre riportato ulteriori informazioni come : il tipo di dispositivo ("general purpose"), la distanza di rete (numero di hop , ovvero attraverso quanti router sono passati i pacchetti di rete TCP, UDP , ICMP , della scansione prima di arrivare a destinazione) .
Oltre alle informazione enunciate , lo screenshot che allego , ne riporta altre.

“La scansione OS fingerprint ha richiesto per inviare alcuni pacchetti raw specifici i privilegi di root . Questa informazione ci sarà utile per capire la

scansione successiva ed utile per comprendere alcune delle differenze tra la SYN scan e la TCP connect. “




### 3.2. Fase 2: SYN Scan (Stealth)

È stata eseguita una scansione SYN per enumerare le porte TCP aperte.

- **Comando Eseguito:** `sudo nmap -sS 192.168.50.3`

- **Risultato Principale:** La scansione ha identificato **23 porte TCP aperte**, indicando una superficie di attacco molto ampia. Nmap ha

riportato che le restanti 977 porte scansionate erano nello stato "closed (reset)" , dunque Nmap ha la certezza al 100% che su quella porta **non c'è nessun servizio in ascolto**. Ha ottenuto questa certezza perché il sistema operativo target (Metasploitable) gli ha risposto direttamente con un pacchetto **RST (Reset)**.

“ altri stati di porte che abbiamo visto a lezione sono :

**`open` (SYN/ACK):**

- Nmap invia **SYN** alla porta.
- Il servizio che è in ascolto risponde: **SYN/ACK** ("Sì! Sono aperto e pronto a parlare!").
- Nmap sa che è aperta. (Poi invia un RST per essere "stealth" e non completare la connessione).

**`closed “reset”` (RST):**

- Nmap invia **SYN** alla porta
- L'OS (non un servizio) risponde: **RST** ("No! Non c'è nessuno qui. Vattene.").
- Nmap sa che è chiusa.

**`filtered` (Nessuna risposta):**

- Nmap invia **SYN** alla porta.
- Un **firewall** tra Nmap e il target vede il pacchetto, sa che non è permesso e lo **scarta** in silenzio.
- Nmap non riceve *nulla* indietro (né SYN/ACK né RST). Dopo un po' (timeout), Nmap si arrende e dice: "Non ho ricevuto risposta. La porta è probabilmente `filtered`." “

La cansione SYN è chiamata "half-open" perché invia un pacchetto SYN, aspetta un SYN/ACK (porta aperta) o RST (porta chiusa), ma se riceve SYN/ACK invia subito un RST invece di completare l'handshake con un ACK.

“anche per questa scansione allego lo screenshot”

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 15:11 EDT
Nmap scan report for 192.168.50.3
Host is up (0.00083s 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:C0:61:06 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.50 seconds
```

### 3.3. Fase 3: TCP Connect Scan

È stata eseguita una scansione TCP Connect per validare i risultati precedenti.

- **Comando Eseguito:** `nmap -sT 192.168.50.3`
- **Risultato Principale:** La scansione ha confermato lo stesso identico elenco di **23 porte TCP aperte**. Le 977 porte chiuse sono state riportate come "closed (conn-refused)", una dicitura diversa da "reset" dovuta al differente meccanismo di scansione.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.50.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 15:19 EDT
Nmap scan report for 192.168.50.3
Host is up (0.0035s 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: 08:00:27:C0:61:06 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
```

## Differenze tra i due tipi di scansione

**Risultati:** Entrambe le scansioni (`-sS` e `-sT`) hanno prodotto un elenco identico di porte aperte.

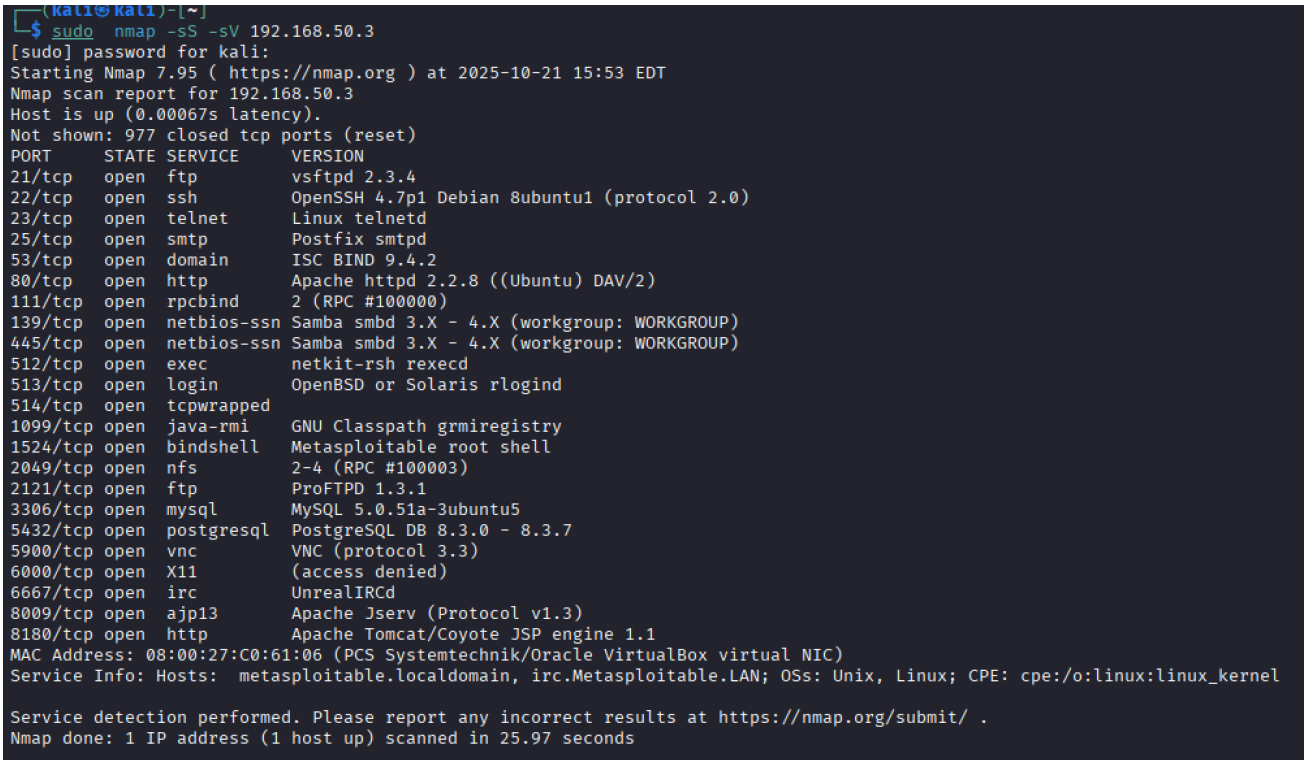
**Differenze Operative:** La scansione `-sS` ha richiesto privilegi `sudo` per creare pacchetti raw e non ha completato l'handshake TCP.

La scansione `-sT` non ha richiesto privilegi `sudo` poiché ha utilizzato la chiamata di sistema `connect()` per stabilire un handshake completo, rendendola più "rumorosa" e facilmente loggabile dalle applicazioni target.

## 3.4. Fase 4: Version Detection

È stata eseguita una scansione combinata `-sS -sV` per identificare le versioni specifiche del software in esecuzione sui servizi esposti.

- Comando Eseguito: `sudo nmap -sS -sV 192.168.50.3`
- Risultato Principale: La scansione ha fornito con successo le informazioni sulla versione per la maggior parte dei servizi aperti. Questi dati sono fondamentali per la successiva analisi delle vulnerabilità, in quanto legano un servizio a specifiche debolezze (CVE) note.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV 192.168.50.3
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 15:53 EDT
Nmap scan report for 192.168.50.3
Host is up (0.00067s 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 Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:C0:61:06 (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 25.97 seconds
```

## 3.5. Tabella Riepilogativa

La tabella seguente riassume tutti i dati raccolti sul target Metasploitable, integrando i risultati di tutte le fasi di scansione.

| PORTA | STATO | SERVIZIO (Identificato) | VERSIONE (da Fase 4: -sV) |
|---|---|---|---|
| 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) |

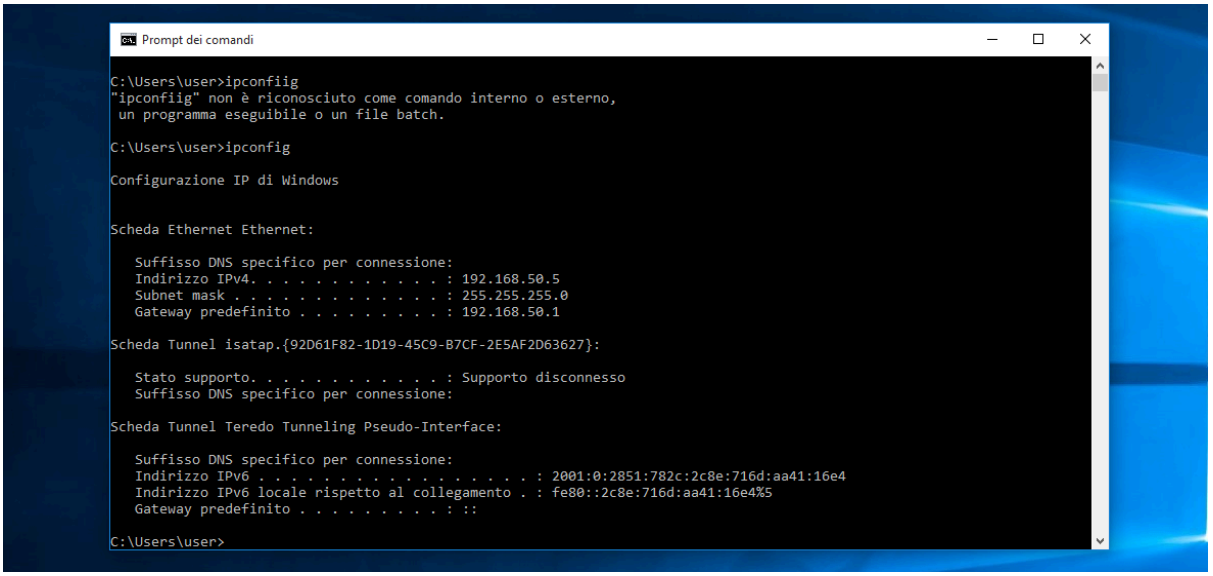
| | | | |
|---|---|---|---|
| 512/tcp | open | exec | netkit-rsh rexecd |
| 513/tcp | open | login | OpenBSD or Wu-ftpd rlogind |
| 514/tcp | open | shell | netkit-rsh rshd |
| 1099/tcp | open | rmiregistry | GNU Classpath grmiregistry |
| 1524/tcp | open | ingreslock | Ingreslock service 1.11 |
| 2049/tcp | open | nfs | 2-4 (RPC #100003) |
| 2121/tcp | open | ccproxy-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 |

---

## 4. Target 2: Windows

- **Indirizzo IP Target:** 192.168.50.5

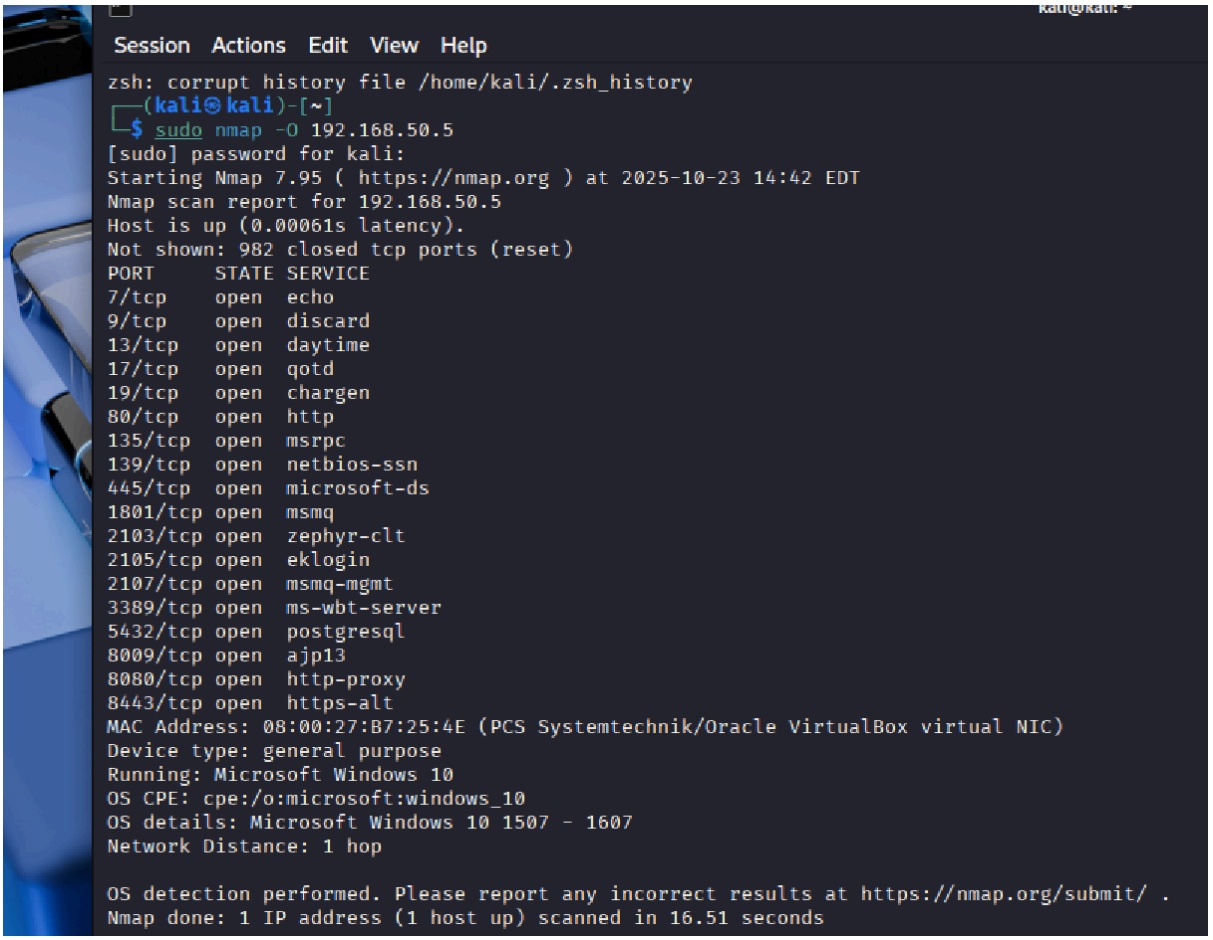



### 4.1. OS Fingerprinting (Target Windows)

È stata eseguita la scansione Nmap (-O) per il rilevamento del sistema operativo sul target Windows, come richiesto dall'esercizio.

**Comando Eseguito:** `sudo nmap -O 192.168.50.5`

- **Risultato Principale:** La scansione ha identificato con successo il sistema operativo come `Microsoft Windows 10`. I dettagli aggiuntivi forniti da Nmap (`OS details: Microsoft Windows 10 1507 - 1607`) suggeriscono un intervallo della versione più specifico.




---

## 5. Conclusioni

Le attività di scansione previste dall'esercizio sono state **completate con successo** su entrambi i target designati.

1. **Su Metasploitable (`192.168.50.3`):** È stato identificato un sistema obsoleto : **`Linux 2.6.X`** con una superficie di attacco molto ampia (23 porte TCP aperte).

   Le scansioni hanno rivelato versioni software specifiche per i servizi esposti (es. `vsftpd 2.3.4`, `Apache 2.2.8`, `MySQL 5.0.51a`), fornendo dati essenziali per una successiva analisi delle vulnerabilità.

2. **Su Windows (`192.168.50.5`):** È stato identificato correttamente un sistema **`Microsoft Windows 10`**. La scansione OS fingerprint ha inoltre rivelato 18 porte aperte.