Mattia Montis

Scansione con NMAP

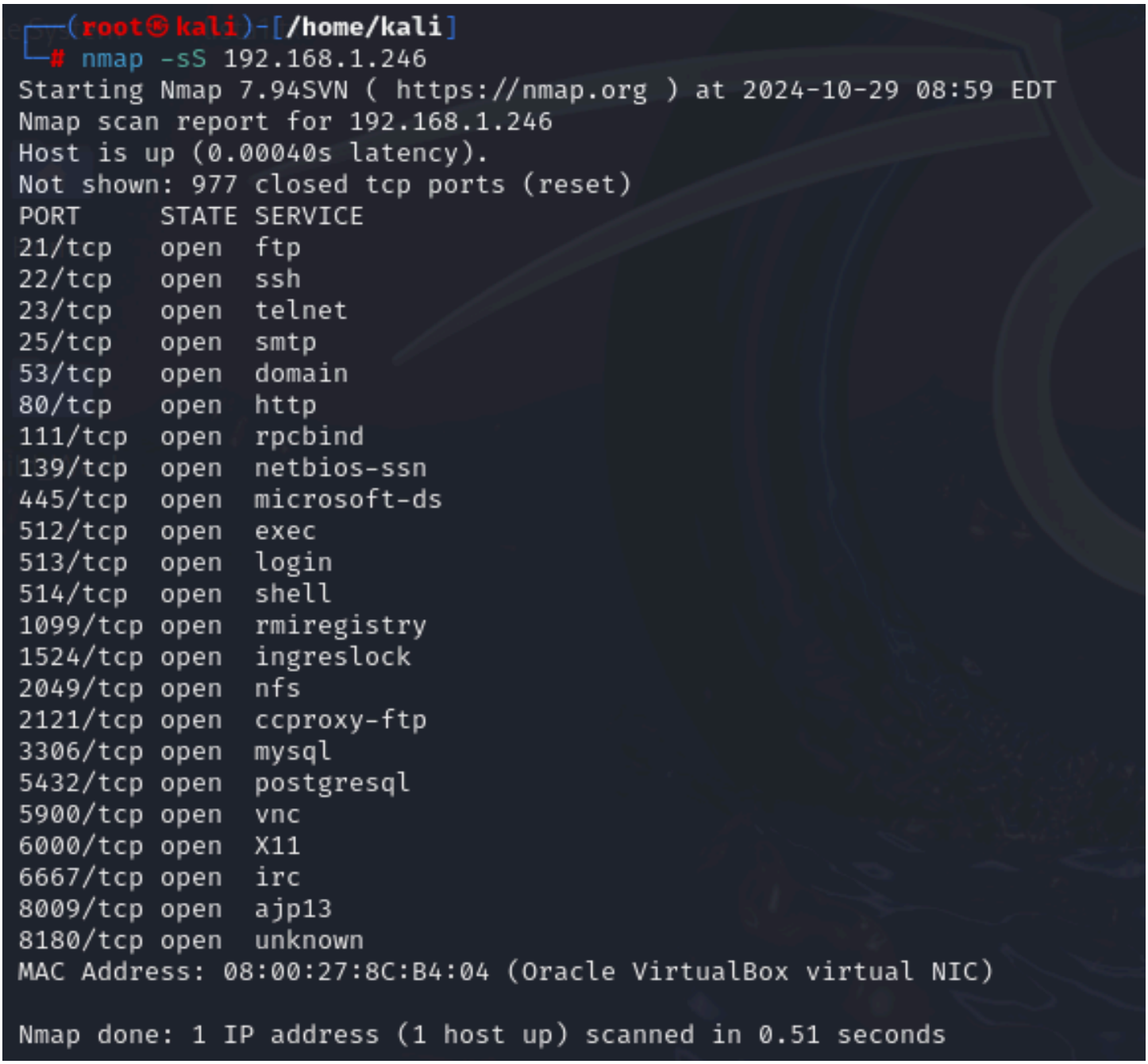
Di seguito sono riportati i risultati delle quattro scansioni eseguite da kali Linux sul sistema Metasploitable con Nmap. Le scansioni includono **Syn Scan**, **TCP Connect Scan**, **OS Fingerprint**, e **Version Detection**, con l'obiettivo di identificare informazioni chiave come IP, sistema operativo, porte aperte e servizi in ascolto con versioni.

1. **IP e Obiettivo**

- **IP Target:** 192.168.1.246
- **Host:** Metasploitable, una macchina virtuale vulnerabile usata per scopi di testing.

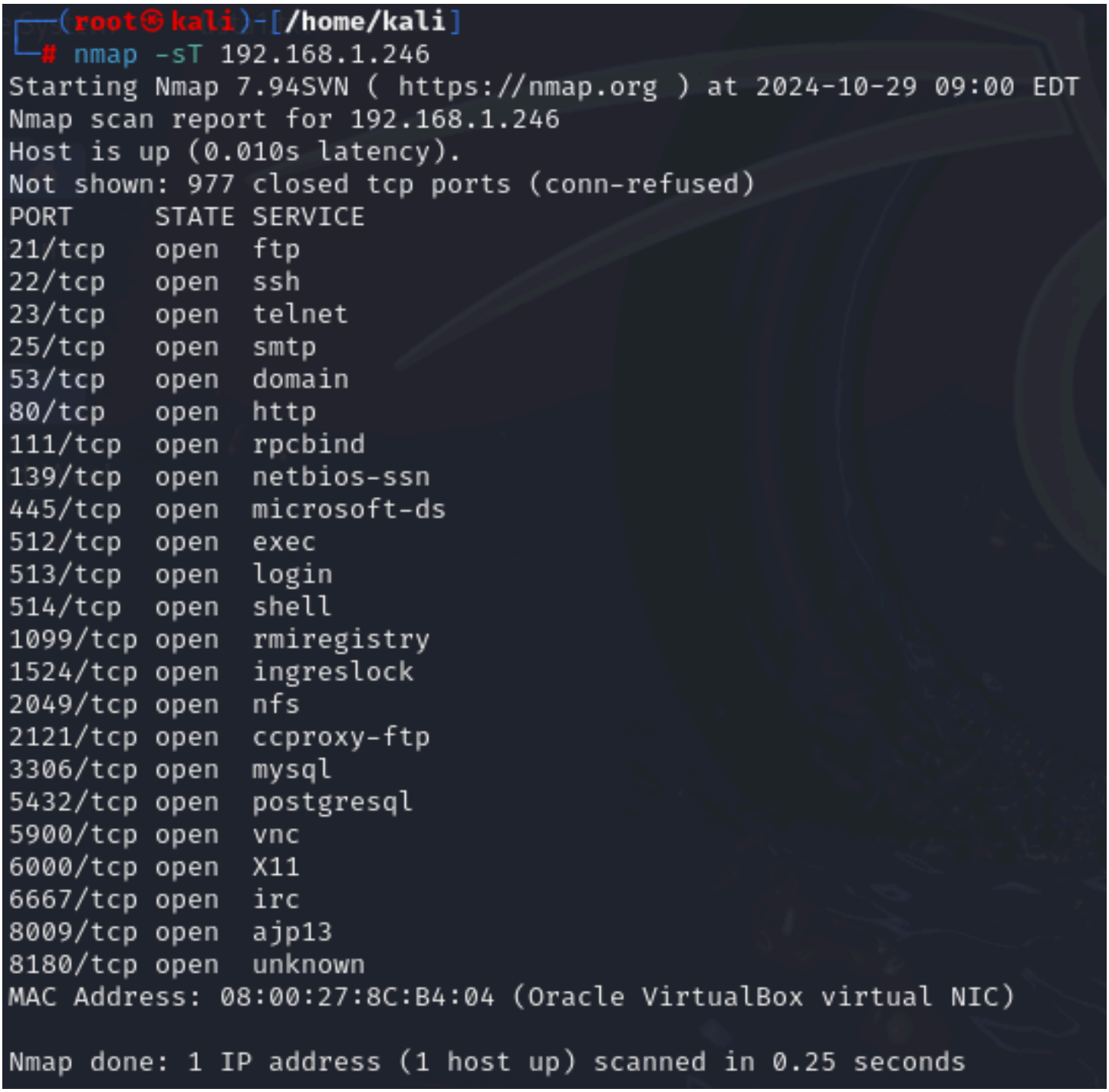
2. **Syn Scan (nmap -sS)**

- **Comando**: nmap -sS 192.168.1.246
- **Descrizione**: Questa scansione invia pacchetti SYN per identificare le porte aperte senza stabilire una connessione completa (metodo stealth).
- **Risultato**:
  - Ha rilevato diverse porte aperte (tra cui 21, 22, 23, 25, 80, 3306, ecc.) con servizi come FTP, SSH, Telnet, SMTP, HTTP, MySQL, ecc.
- **Nota**: La scansione è rapida e silenziosa, quindi è meno probabile che venga rilevata dal sistema di destinazione rispetto a una scansione completa.



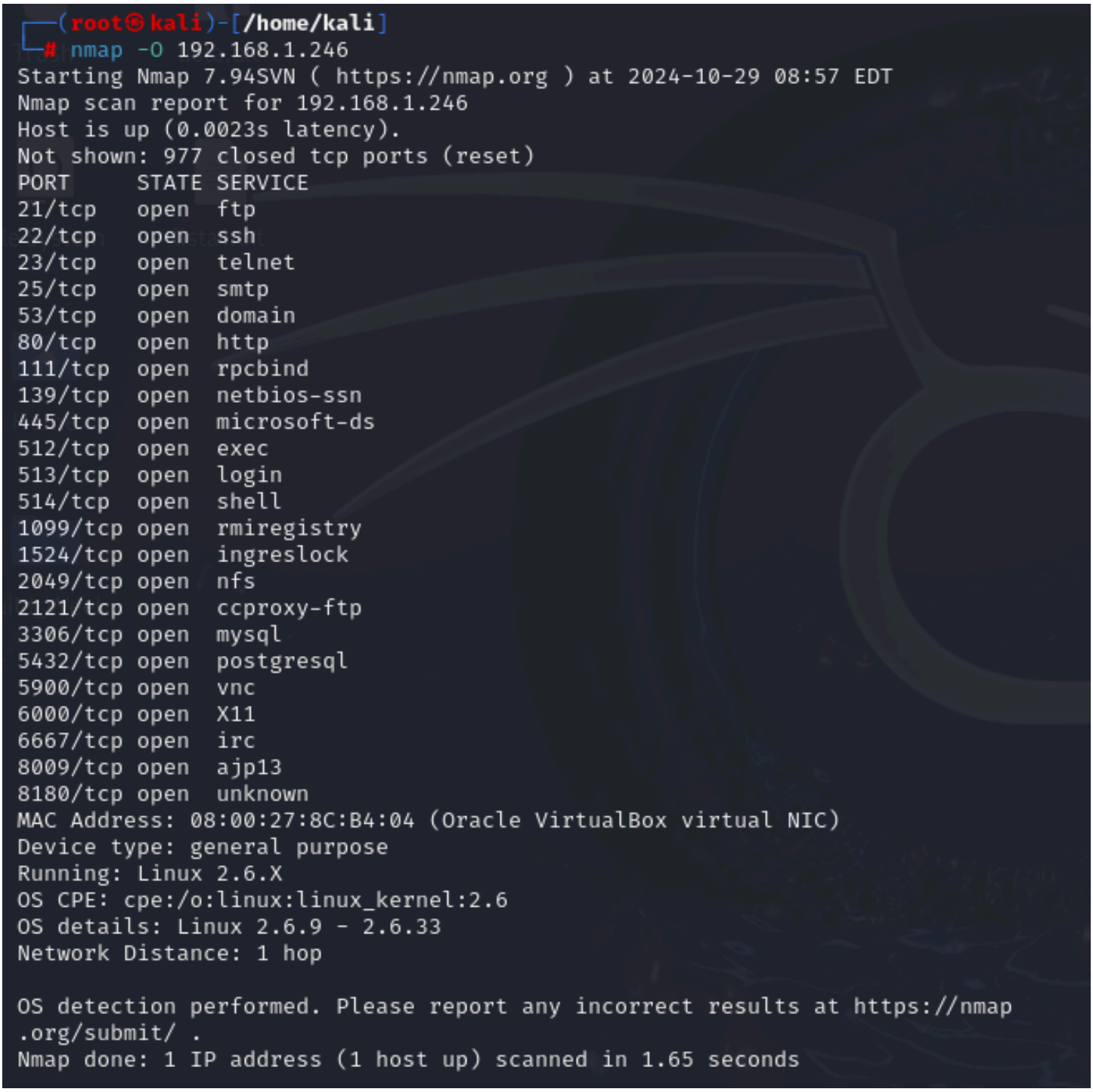
3. **TCP Connect Scan (nmap -sT)**

- **Comando**: nmap -sT 192.168.1.246
- **Descrizione**: La scansione TCP Connect esegue una connessione completa alle porte per testare se sono aperte o meno. È meno discreta rispetto alla Syn Scan, ma garantisce che il sistema di destinazione sia effettivamente in ascolto sulla porta.
- **Risultato**:
  - L'output mostra le stesse porte aperte rilevate nella Syn Scan, confermando la loro presenza. Servizi come FTP, SSH, Telnet, HTTP, MySQL sono nuovamente elencati.
- **Differenze rispetto alla Syn Scan**: Entrambe le scansioni rilevano le stesse porte aperte e servizi, ma la **TCP Connect Scan** stabilisce una connessione completa, il che significa che è più facilmente rilevabile da firewall e sistemi di monitoraggio.



4. **OS Fingerprint (nmap -O)**

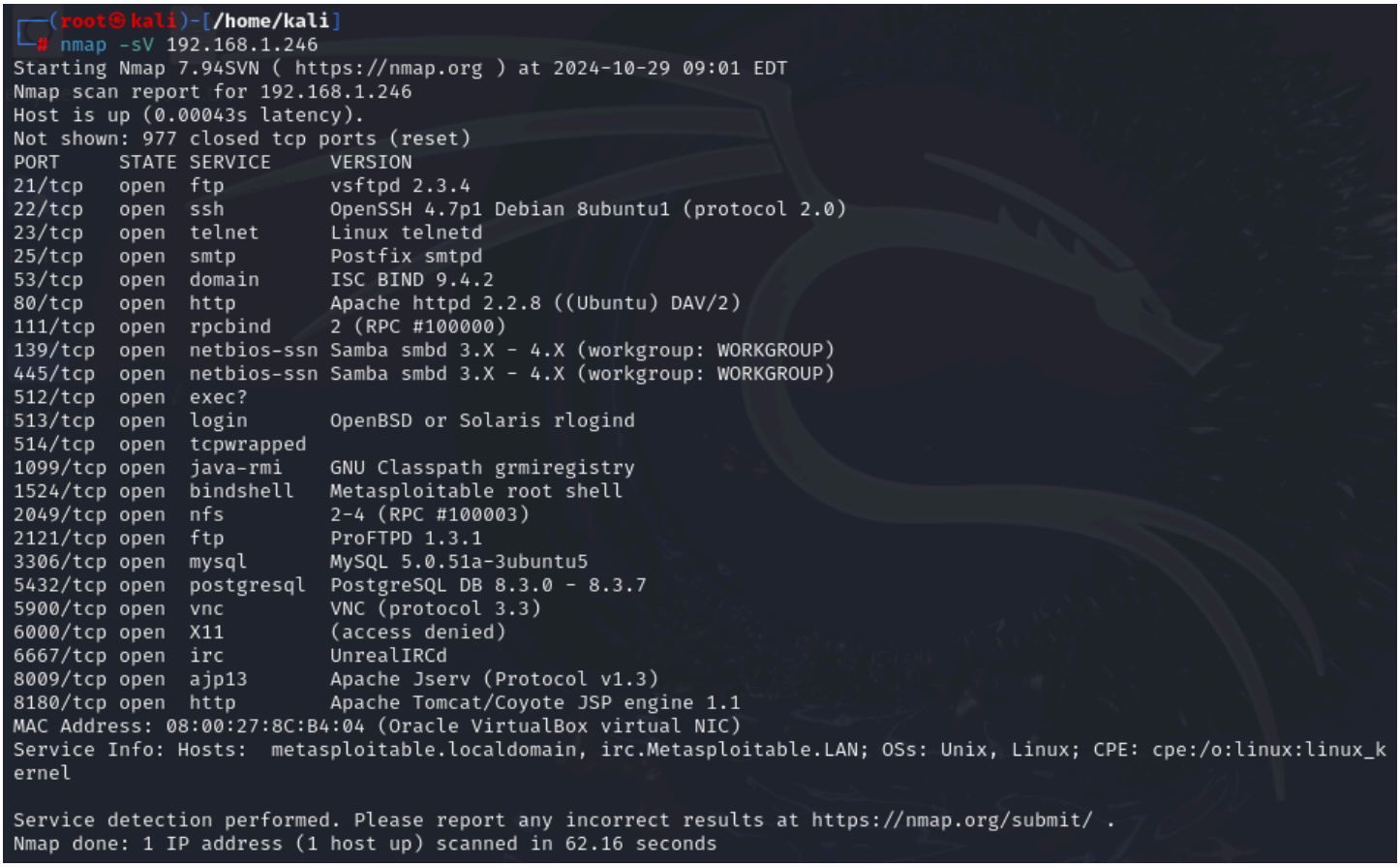
- **Comando**: nmap -O 192.168.1.246
- **Descrizione**: La scansione OS Fingerprint cerca di identificare il sistema operativo del target attraverso l'analisi di specifici pacchetti di rete.
- **Risultato**:
  - Sistema operativo identificato come **Linux 2.6.X.**
  - **Tipo di dispositivo**: General Purpose.
  - **Dettagli di rete**: Network Distance di 1 hop, indicando una connessione diretta tra la macchina Kali e Metasploitable.
- **Conclusione**: La macchina target utilizza una vecchia versione del kernel Linux, confermando che si tratta di una macchina di testing vulnerabile.



5. **Version Detection (nmap -sV)**

- **Comando**: nmap -sV 192.168.1.246
- **Descrizione**: La Version Detection analizza le porte aperte per identificare versioni specifiche dei servizi in esecuzione.
- **Risultato**:
  - Ha rilevato informazioni dettagliate su molti servizi:
    - **FTP**: vsftpd 2.3.4
    - **SSH**: OpenSSH 4.7p1
    - **HTTP**: Apache httpd 2.2.8
    - **MySQL**: MySQL 5.0.51a

    - Altri servizi come Samba, PostgreSQL, VNC e IRC sono stati rilevati con versioni specifiche.
- **Utilità**: Questa scansione è fondamentale per l'identificazione delle versioni, utile per individuare vulnerabilità specifiche associate a ciascun servizio.



Differenze tra Syn Scan e TCP Connect scan

Nel network Scanning, il **Syn Scan e TCP Connect scan** sono due scansioni per visionare quale porte sono aperte in sistema target. La differenza principale è nel modo a cui avviene la scansione, cioè all'interazione con il protocollo **TCP.**

1. TCP Connect Scan (o Full Connect Scan)

- Metodo: Nel **TCP Connect Scan**, l'intero processo di handshaking a tre vie (Three-Way Handshake) del protocollo **TCP** viene completato. Questo significa che:
    - Il client invia un pacchetto **SYN** alla porta target.
    - Se la porta è aperta, il server risponde con un pacchetto **SYN-ACK.**
    - Il client invia quindi un pacchetto **ACK** per completare la connessione.
- Vantaggi: Poiché si realizza una connessione completa, è una scansione che non richiede privilegi particolari. Questo tipo di scansione può essere effettuato anche da un utente non root.
- Svantaggi: È più lenta e facilmente rilevabile dai sistemi di sicurezza come firewall, poiché ogni connessione è registrata nei log di sistema, risultando in più evidenti tracce dell'attività di scansione.

2. SYN Scan (o Half-Open Scan)

- Metodo: Nel **SYN Scan**, il client non completa l'intero processo di handshaking. La sequenza è la seguente:
  - Il client invia un pacchetto **SYN** alla porta target.
  - Se la porta è aperta, il server risponde con un pacchetto **SYN-ACK**.
  - Invece di rispondere con un **ACK**, il client invia un pacchetto RST (Reset) per interrompere la connessione.
- Vantaggi: Questo metodo evita di completare la connessione, riducendo le tracce. Risulta quindi meno rilevabile dai sistemi di sicurezza rispetto al TCP Connect Scan ed è generalmente più veloce.

Conclusioni

Le scansioni hanno identificato un sistema operativo Linux obsoleto con numerosi servizi e porte aperte, che riflette un ambiente vulnerabile ideale per scopi di testing e formazione. Le informazioni sulle versioni dei servizi indicano che il sistema è esposto a molteplici potenziali vulnerabilità note.

OS fingerprint verso windows

Per identificare il sistema operativo del mio portatile partendo dalla macchina virtuale Kali Linux su VirtualBox, ho dovuto prima impostare la scheda di rete di Kali su "Bridge". Successivamente, ho verificato tramite terminale che entrambe le macchine fossero sulla stessa rete; per farlo, ho forzato l'inserimento dell'indirizzo IPv4 di Kali.

Una volta accertato che entrambe le macchine si trovavano sulla stessa rete, ho disabilitato il firewall di Windows Defender per la rete locale. Questo passaggio è stato fondamentale per testare la comunicazione con un ping.

Infine, ho eseguito il comando da terminale Kali: **nmap -O {IP target}** per effettuare una scansione di fingerprinting del sistema operativo del target.

Dall’output ricavo le seguenti informazioni, il sistema operativo (Windows 10 versione 1703), le porte aperte e servizi attivi, l’indirizzo IP e MAC e la distanza tra dall’host (in questo caso siamo su rete locale quindi 1 hop).

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.1.245
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 10:08 EDT
Nmap scan report for MSI.homenet.telecomitalia.it (192.168.1.245)
Host is up (0.00060s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: F8:FE:5E:9A:FA:1F (Unknown)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1703
OS details: Microsoft Windows 10 1703
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 2.73 seconds
```