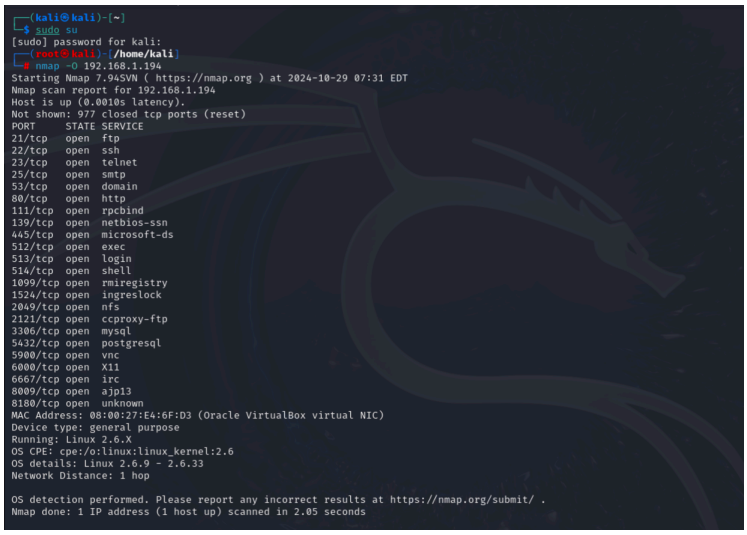
ESERCITAZIONE S5/L2

TRACCIA: Tecniche di scansione con Nmap
È stato richiesto allo studente di effettuare le seguenti scansioni sul target Metasploitable: OS fingerprint, Syn Scan, TCP connect, Version detection e di trovare differenze tra i risultati della scansioni TCP connect e SYN
E la seguente sul target Windows: OS fingerprint.

SVOLGIMENTO

Ho svolto l'esercizio tramite l'utilizzo dello strumento nMap, network mapping, strumento open-source estremamente potente e versatile per la scansione della rete e l'identificazione dei dispositivi e dei servizi. Le sue funzioni principali sono quattro:

- Scansione degli Host: Identifica gli host attivi all'interno di una rete.
- Identificazione dei Servizi: Rileva i servizi in esecuzione su ciascun host
- Rilevamento dei Sistemi Operativi: Utilizza varie tecniche di fingerprinting per determinare il sistema operativo in esecuzione su un host.
- Scansione delle Vulnerabilità: Può essere utilizzato per identificare potenziali vulnerabilità.

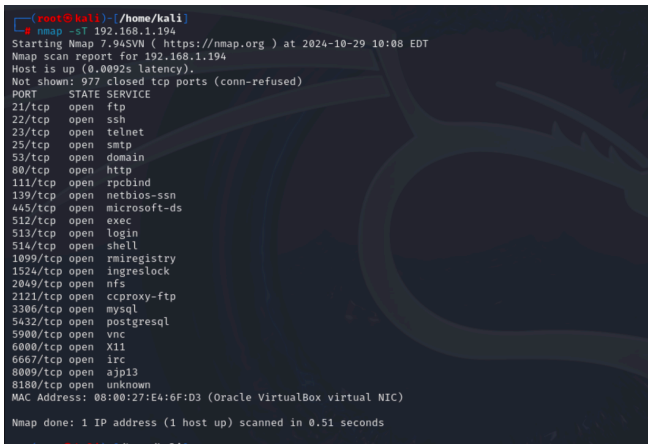


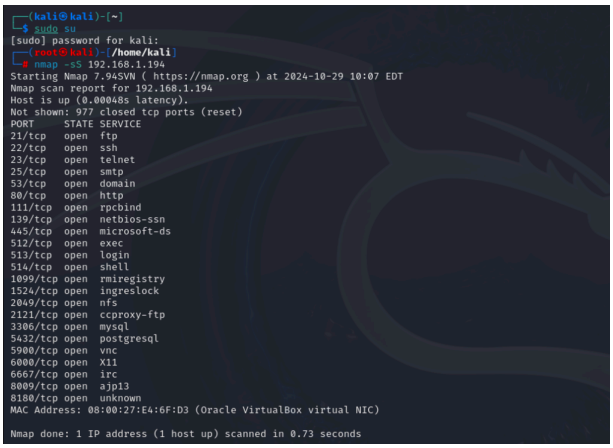
Prima di tutto ho recuperato l'indirizzo IP dalla macchina virtuale di Metasploitable2: 192.168.1.194.

Successivamente per lo svolgimento dell'esercizio, nel terminale della macchina di Kali Linux, ho utilizzato i comandi "nmap -O" per il rilevamento del Sistema Operativo, che ha la funzione di determinare il sistema operativo dell'host di destinazione.

Il **sistema operativo** risulta: Linux 2.6.9 - 2.6.33

Una volta trovato il Sistema Operativo vengono effettuati i comandi di identificazione dei Servizi, nello specifico, TCP Connect che esegue una scansione che stabilisce connessioni TCP (nmap -sT) e SYN Scan, che esegue una scansione "half-open", inviando pacchetti SYN e attendendo risposte SYN/ACK (nmap -sS).



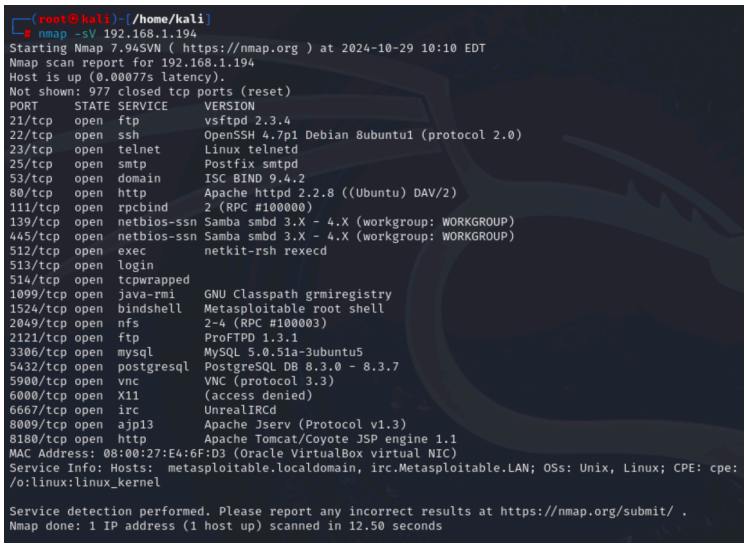


Nell'immagine a sinistra comando nmap -sT, a destra invece nmap -sS

ESERCITAZIONE S5/L2

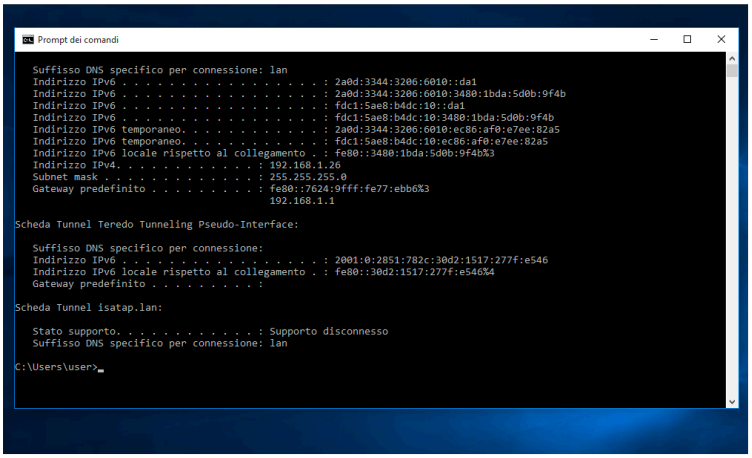
La differenza tra SYN Scan e TCP Connect, sta nella comunicazione. Come possiamo vedere nelle immagini precedenti prima delle porte appaiono, in quella di sinistra la voce "conn-refused" mentre in quella di destra "reset". La sostanziale differenza è proprio che nel caso del SYN Scan non viene completata 3-way-handshake, chiudendo la comunicazione con un pacchetto RST (reset), risultando meno invasivo generando meno rumore al livello di rete.

Infine con lo strumento "nmap -sV" sono state individuate le versioni dei servizi attivi.
Porte aperte: Sono state individuate 22 porte aperte.



Versioni e servizi attivi:
- Porta 21, si riferisce al servizio FTP versione vsftpd 2.3.4
- Porta 22, si riferisce al servizio SSH versione OpenSSH 4.7p1 Debian Subuntu1 (protocollo 2.0)
- Porta 23, si riferisce al servizio TELNET versione Linux telnetd
- Porta 25, si riferisce al servizio SMTP versione postfix smtpd
- Porta 139, si riferisce al servizio Netbois-ssn versione Samba smbd 3.X, 4.X (workgroup: WORKGROUP)

Come esercizio bonus, utilizzando come target Windows, bisognava determinare il Sistema Operativo con il comando "nmap -O" sempre dal terminale terminale di Kali



Nella prima immagine, è stato recuperato l'indirizzo IP, con il comando ipconfig,
Nella seconda invece tramite il comando sopracitato è risultato il sistema operativo: Microsoft Windows 10.