W11D1 Pratica 1

Giacomo di Giacinto

EPICODE

Esercizio
Scansione dei servizi

Traccia: Tecniche di scansione con Nmap

Si richiede allo studente di effettuare le seguenti scansioni sul target **Metasploitable**:

- OS fingerprint
- Syn Scan
- TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?
- Version detection

Modificate le impostazioni di rete delle macchine virtuali per fare in modo che i due target siano sulla stessa rete.
A valle delle scansioni, per entrambi gli IP, è prevista la produzione di un **report** contenente le seguenti info (dove disponibili):

- IP
- Sistema Operativo
- Porte Aperte
- Servizi in ascolto con versione
- Descrizione dei servizi

https://www.poftut.com/nmap-output/

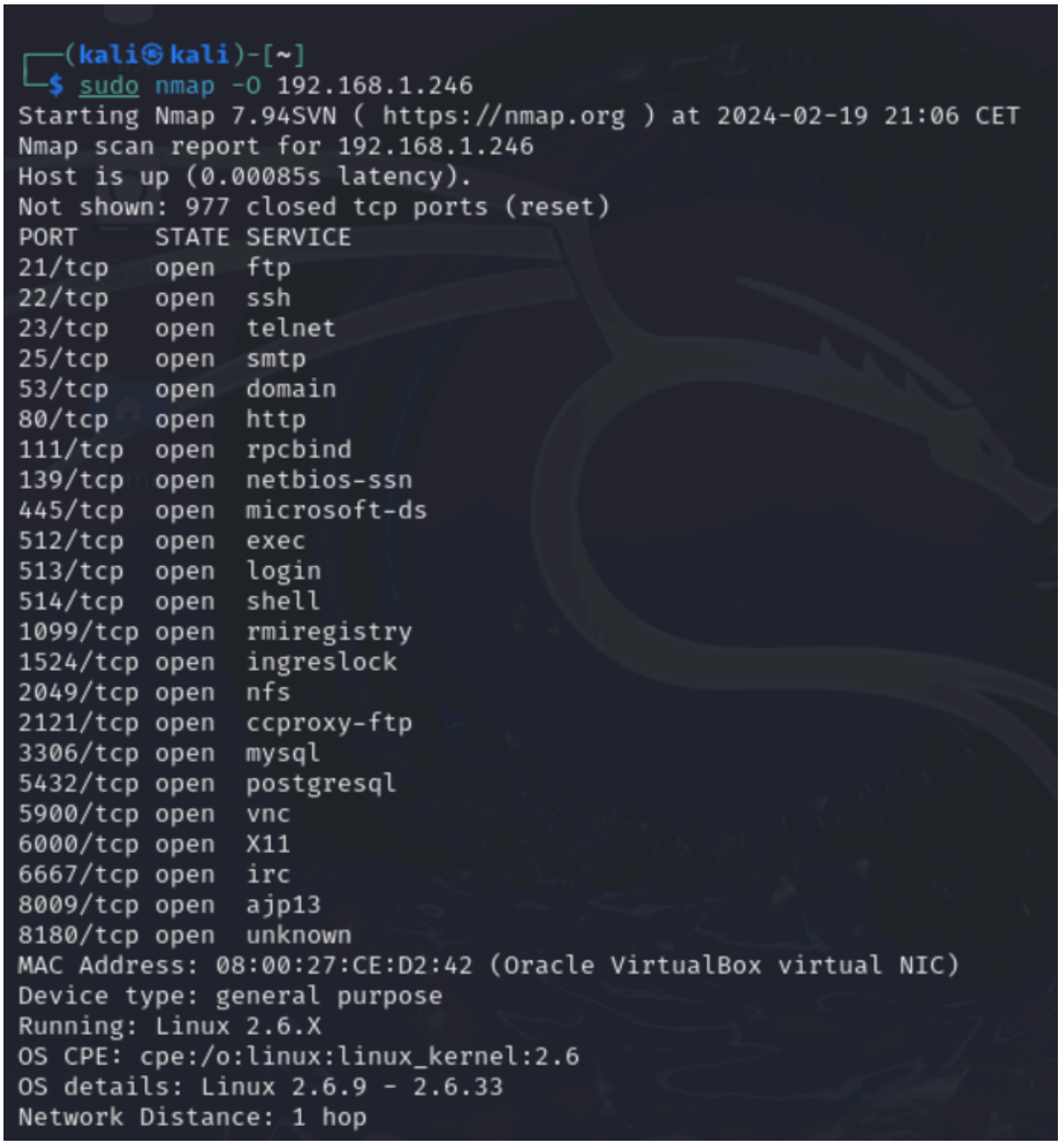
nmap -oN report1 IP

Di seguito elenco le scansioni sul target Metasploitable come da traccia dell'esercizio seguite da una breve descrizione delle funzioni peculiari della specifica richiesta.
Preciso che i due target si trovano sulla stessa rete.

1) OS fingerprint

Questa richiesta identifica le porte aperte del target, analizza le risposte, per mettere in evidenza il sistema operativo e la sua versione. Metasploitable ha come sistema operativo Linux alla versione 2.6.9 - 2.6.33 e dì seguito vediamo tutte le porte aperte con il relativo servizio a suo fianco.

- Il comando da utilizzare è sudo nmap -O <e l'IP target>

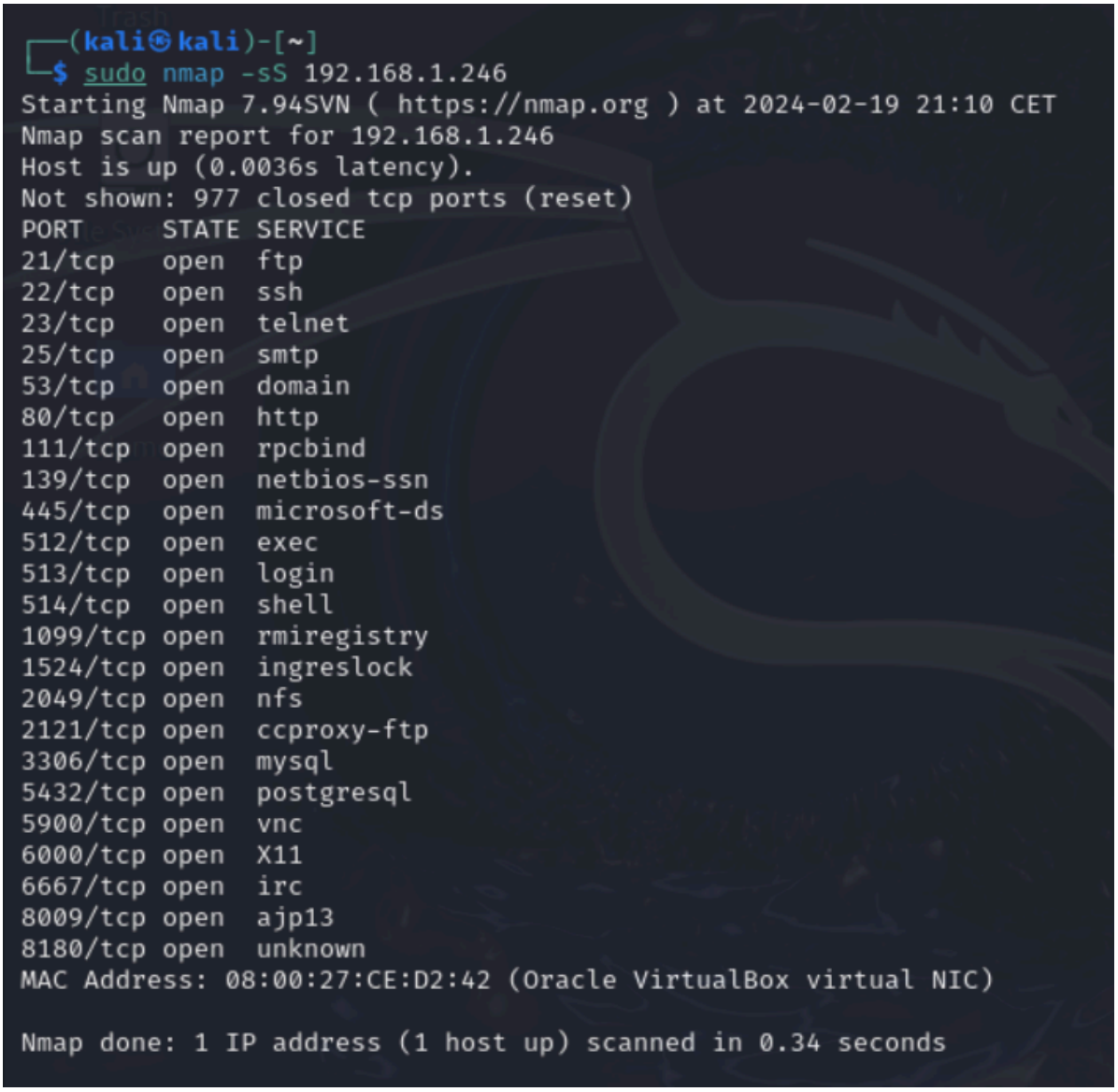


2) Syn scan

La scansione Syn è una scansione utilizzata per determinare le porte aperte di un indirizzo IP. La peculiarità di questa scansione sta nel fatto che la tecnica utilizzata è più silenziosa rispetto ad altri tipi di scansione .
Nella Syn scan il sistema invia i pacchetti con il flag Syn, se la porta è aperta il sistema risponde con un Syn/Ack, e la connessione si interrompe prima della risposta finale di Ack.
Se invece la porta è chiusa il sistema risponde con un Rst.

Di seguito vediamo la lista delle porte aperte con il rispettivo servizio assegnato

- il comando da utilizzare è sudo nmap -sS <e l'IP target>

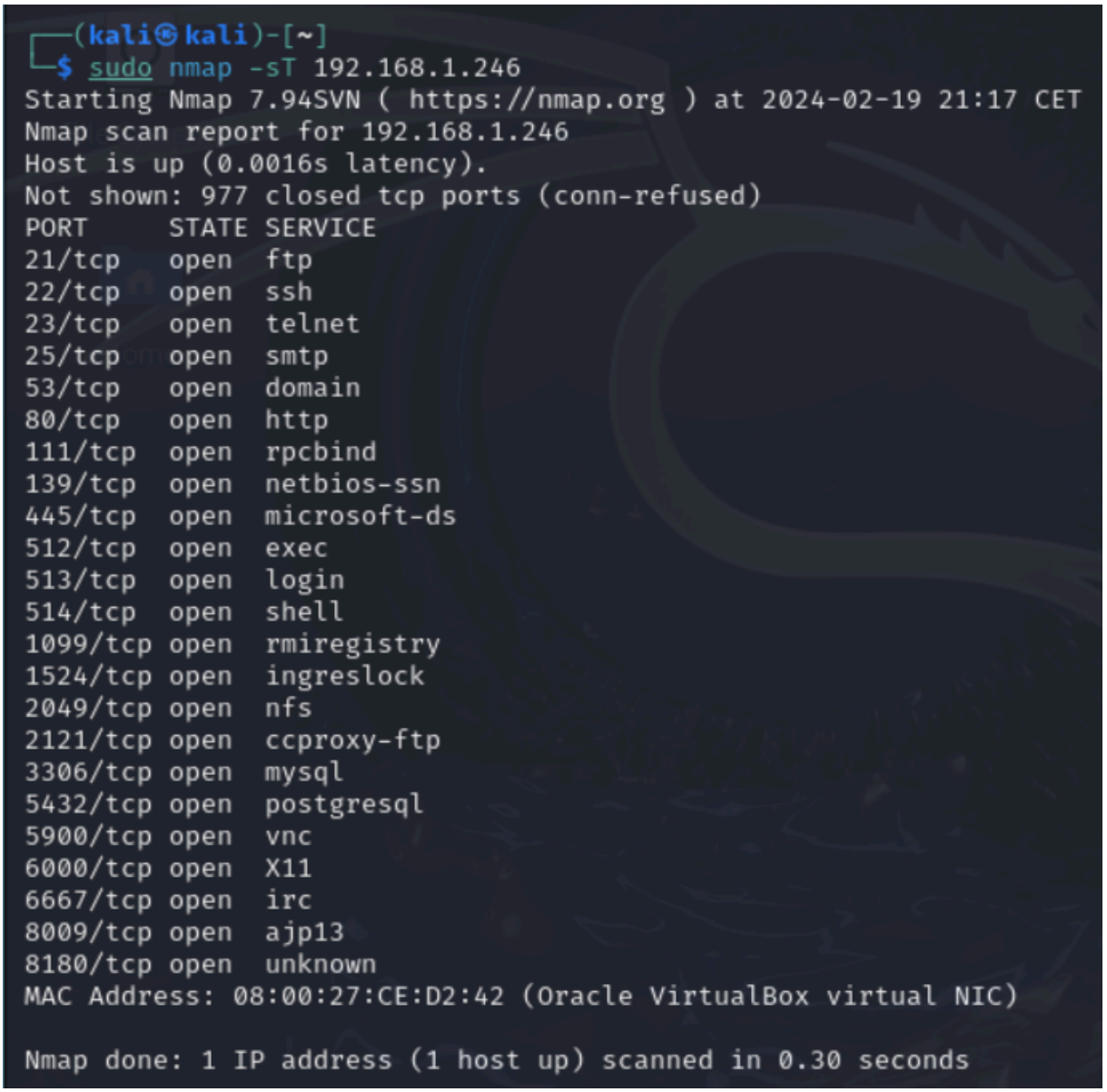


3) Tcp connect

Questa scansione a differenza della scansione Syn porta a termine la three-way-handshake e quindi porta a termine la domanda Syn, la risposta Syn/Ack e la chiusura della richiesta con Ack.
Questa scansione è meno silenziosa della precedente e potrebbe essere identificata da applicazioni che ascoltano il traffico della macchina target.

il risultato è lo stesso della precedente scansione, vengono indicate le porte e i loro servizi associati.

- il comando da utilizzare è sudo nmap -sT <e l'IP target>

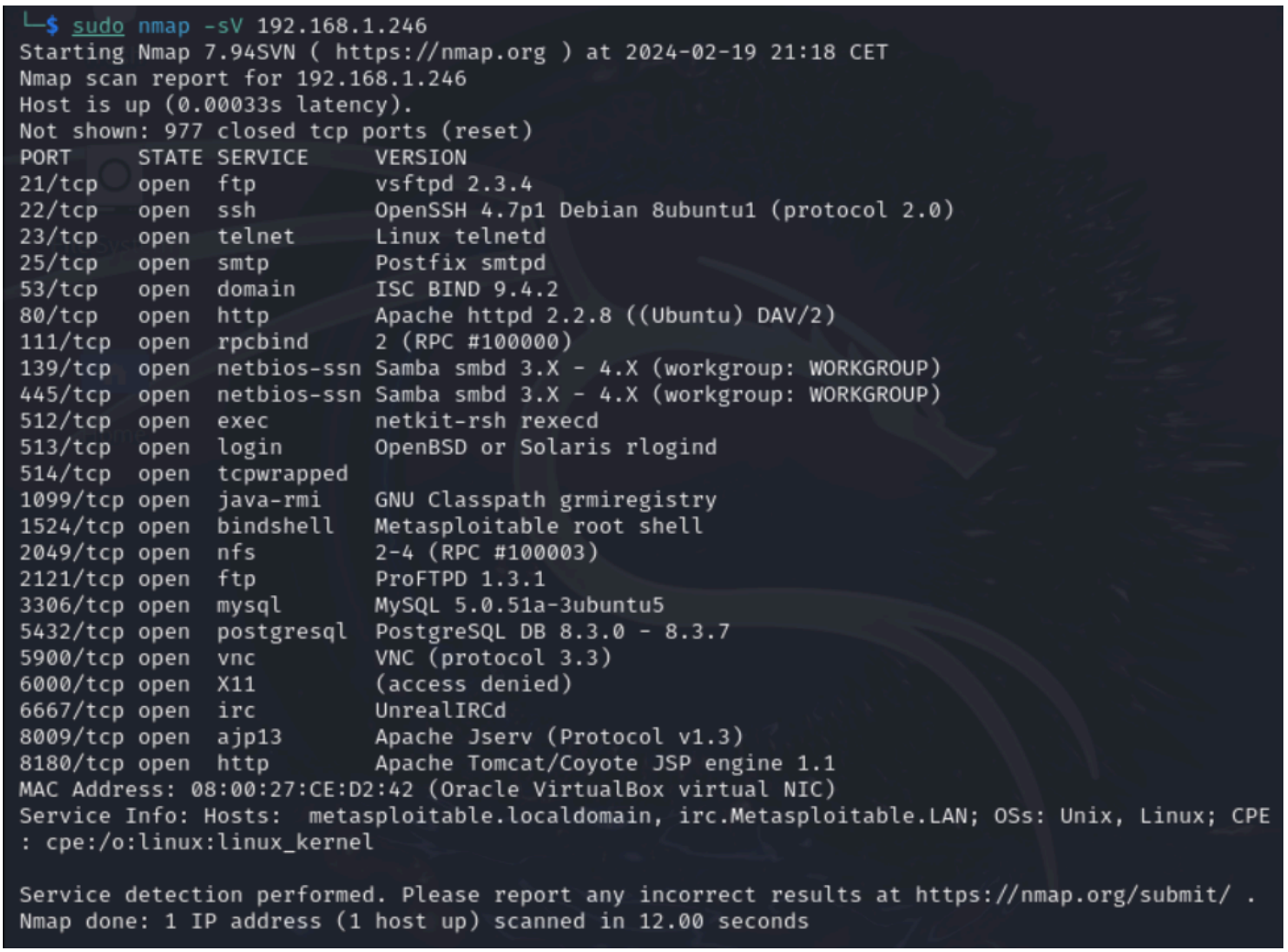


4) Version detection

Questo tipo di scansione è la più invasiva e oltre a stabilire i three-way-handshake recupera anche le informazioni relative al servizio in ascolto dal banner del demone.

Il risultato è simile alle scansioni sopra riportate, viene integrata anche la versione di ogni singolo servizio di ogni porta aperta

- il comando da utilizzare è sudo nmap -sV <e l'IP target>



Per concludere posso sostenere che queste tecniche di scansione sono simili ma ognuna differisce per qualche piccola peculiarità, in base alla casistica che mi troverò ad affrontare opterò per la soluzione più idonea al momento.