Report S5/L2

Scansione Nmap

La traccia ci chiede di effettuare le seguenti scansioni utilizzando Nmap sul target Metasploitable:

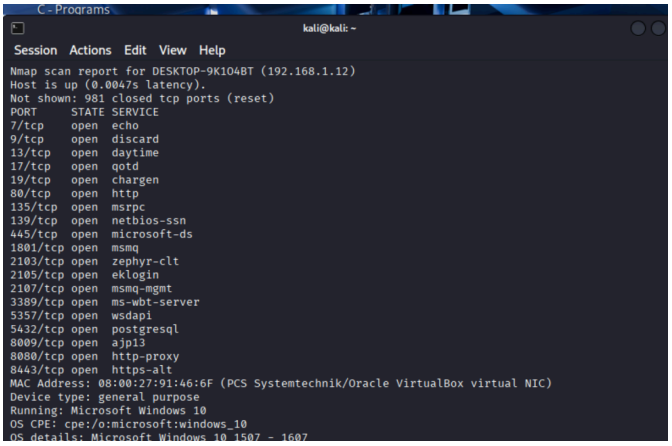
- OS fingerprint
- Syn Scan
- TCP connect - trovate differenze tra i risultati della scansione TCP connect e SYN?
- Version detection

Inoltre sul target Windows:
- OS fingerprint

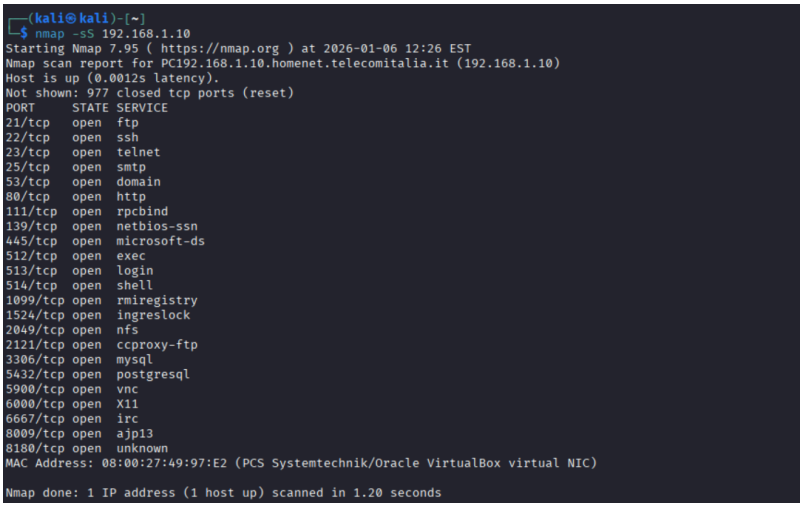
Nmap(Network Mapper):
è uno strumento open-source estremamente potente per la scansione della rete e l'identificazione dei dispositivi e dei servizi. Utilizzato nella fase 2 del Penetration Testing per la mappatura di rete:

- *Identificazione dei dispositivi*: Rilevare e identificare tutti i dispositivi collegati alla rete, inclusi client, server, router, switch e altri dispositivi di rete.
- *Rilevamento dei protocolli*: Determinare quali protocolli di rete vengono utilizzati dai dispositivi, come HTTP, HTTPS ecc.
- *Scansione delle Porte*: Identificare le porte aperte e i servizi in esecuzione su ciascun dispositivo
- *Analisi della Topologia:* Comprendere la disposizione e le interconnessioni tra i vari dispositivi nella rete.

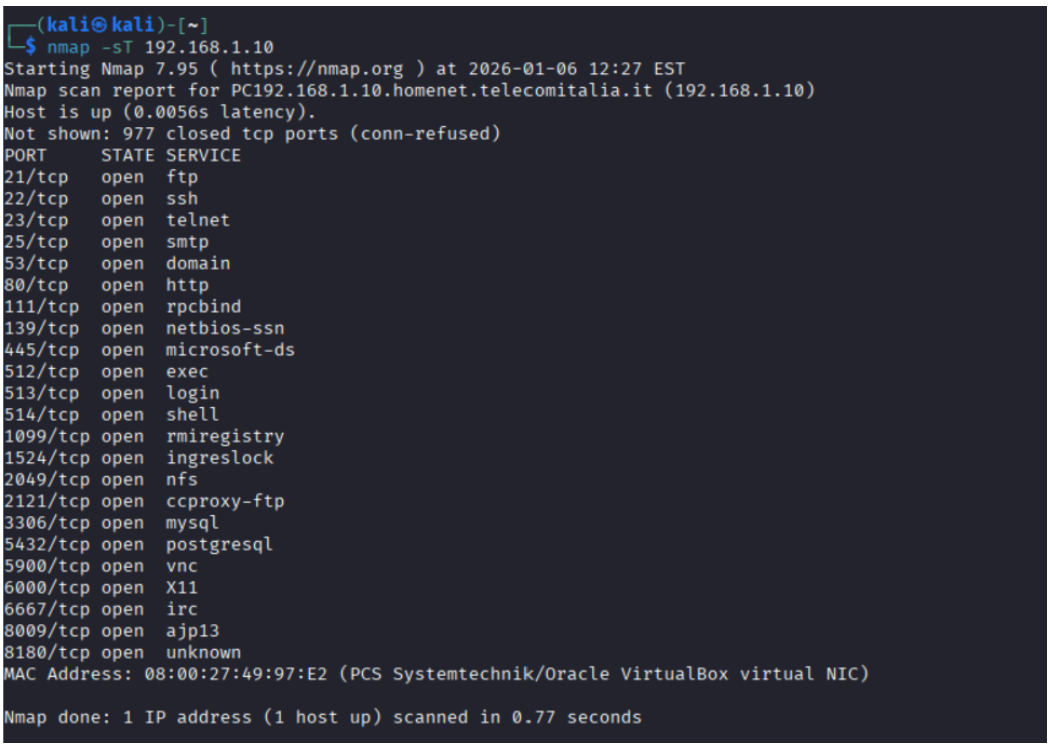
-Test sulla Metasploitable:
OS fingerprint
nmap -O 192.168.1.12 (analizza come risponde la rete per capire il sistema operativo dell'Host)



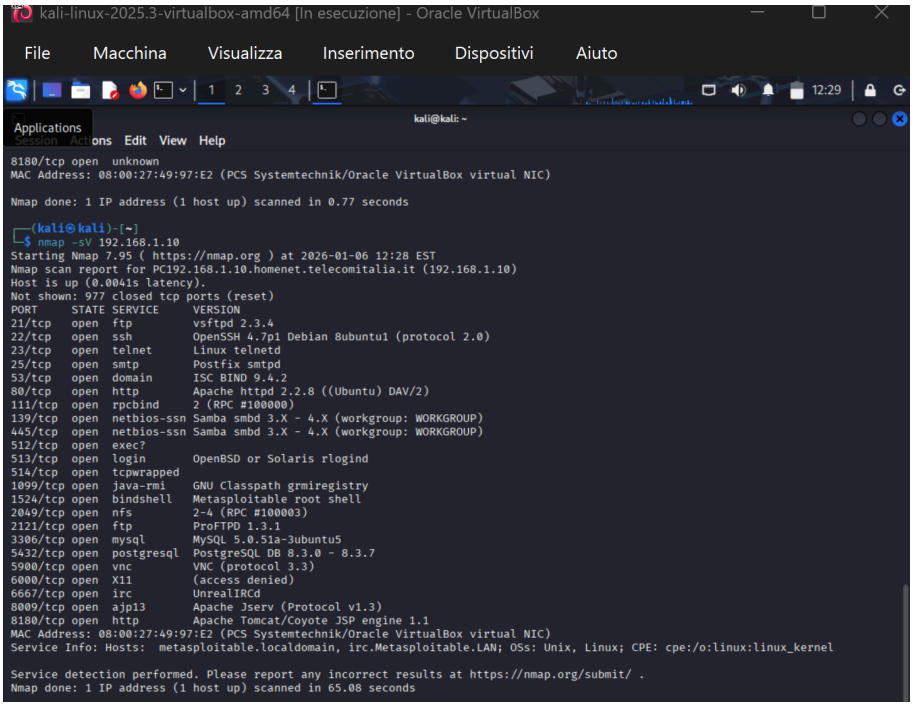
- **Test SYN SCAN :**
nmap -sS 192.168.1.10 (La **SYNSCAN** non chiude la connessione).
Però le differenze tra **-sS e -sT** evidenti non ci sono se guardiamo il risultato dell'operazione di scansione.



- Test TCP Connect:
nmap -sT 192.168.1.10



- Test Version Detection:
nmap -sV 192.168.1.10 questo comando serve per vedere la versioni dei servizi tramite le porte aperte



- Test target Windows:
nmap -O 192.168.1.12