Report Scansione Metasploitable e WindowsXP

Indirizzi IP presi in esame:

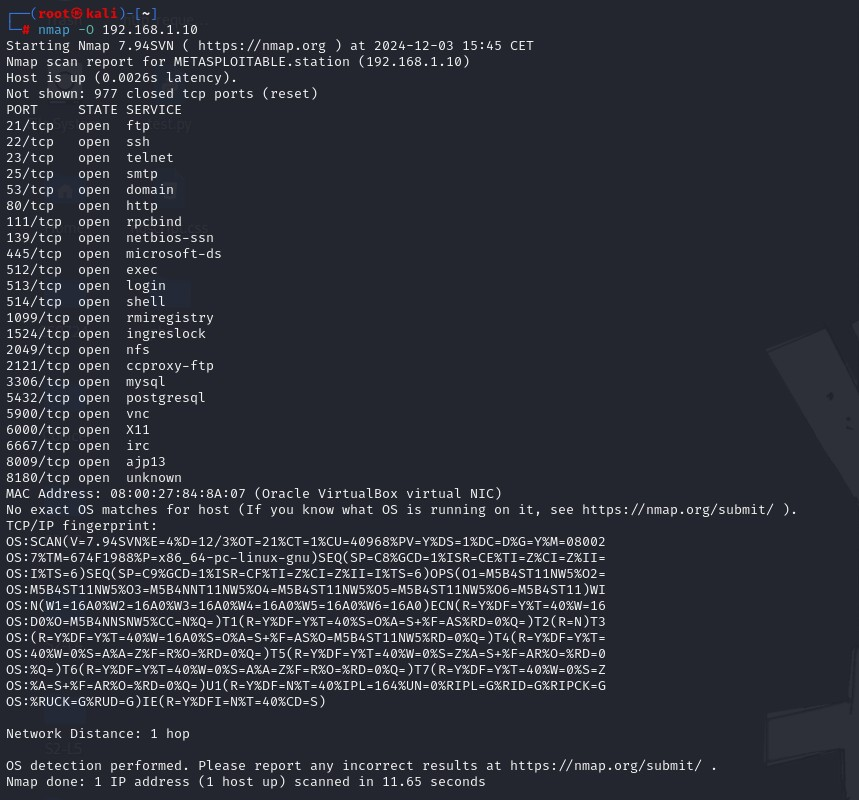
- Metasploitable = 192.168.1.10/24

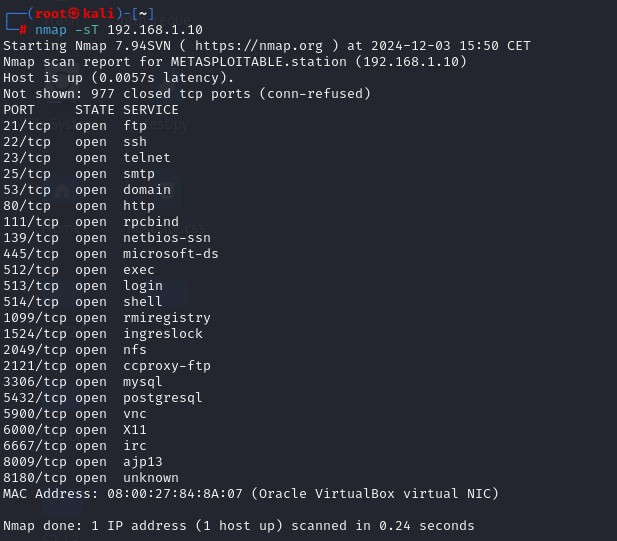
- WindowsXP = 192.168.1.15/24

Le scansioni effettuate sono state le seguenti:

per quanto riguarda la Metasploitable:

nmap -O 192.168.1.10 per trovare l’OS Fingerprint



Nmap -sT 192.168.1.10 per quanto riguarda la ricerca e scansione TCP connect  
  


Inoltre, nmap -sS 192.168.1.10, che a differenza della scansione TCP Connect, risulta piú stealth perché rifiuta immediatamente la connessione “al ritorno” invece di effettuare un three way handshake e restituire un RST in seguito.   
  
Immagine che contiene testo, schermata

Descrizione generata automaticamente  
  
  
  
Infine, nmap -sV 192.168.1.10

Immagine che contiene testo, schermata

Descrizione generata automaticamente

Per quanto riguarda la macchina WindowsXP invece, ho eseguito soltanto come da consegna la scansione dell’OS Fingerprint.

nmap -sV 192.168.1.15

