Report Scansione Metasploitable e WindowsXP

Indirizzi IP presi in esame:

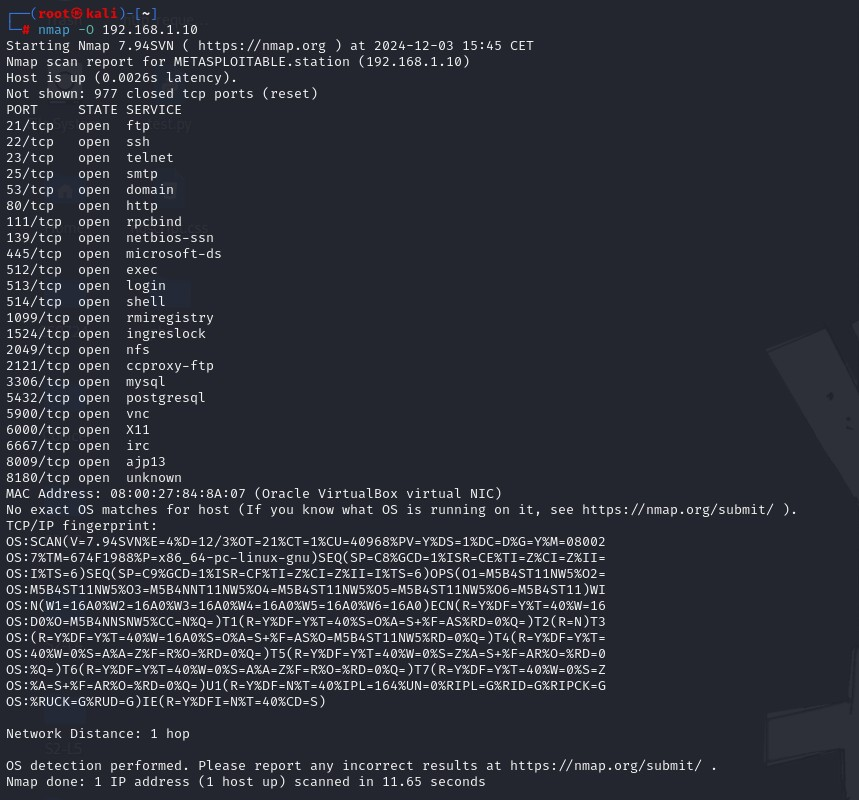
- Metasploitable = 192.168.1.10/24

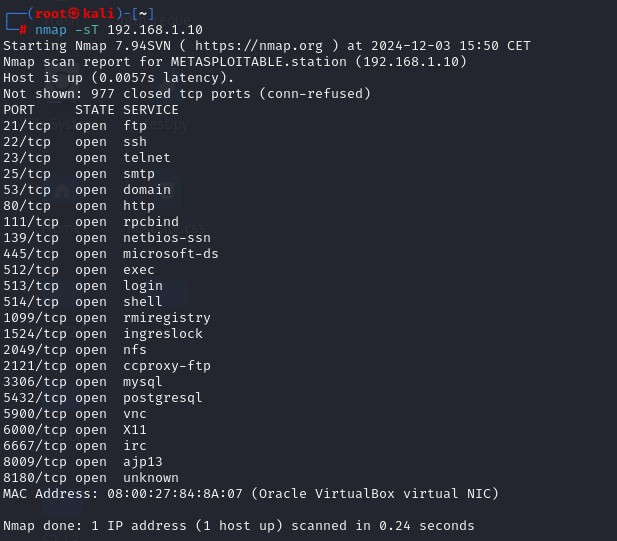
- WindowsXP = 192.168.1.15/24

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

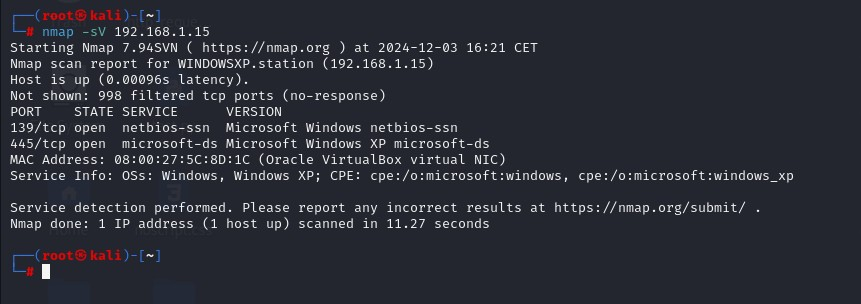
Descrizione generata automaticamente  
  
  
  
Infine, nmap -sV 192.168.1.10

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



EXTRA

Come extra ho testato lo switch -g che serve a selezionare una specifica porta da cui inviare i pacchetti  
in questo caso ho provato:

nmap -g 80 192.168.1.10  
Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente  
Immagine che contiene testo, schermata, numero, Carattere

Descrizione generata automaticamente

per quanto riguarda lo switch -f invece, serve a frammentare i pacchetti inviati per superare firewall e IDS che controllano in base alla grandezza dei pacchetti  
per esempio:   
nmap -f 192.168.1.10

Immagine che contiene testo, schermata, Carattere, design

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere, menu

Descrizione generata automaticamente

È corretto usare il comando -p U:53,T:200?  
il comando è corretto, e consente di scansionare le specifiche porte richieste con determinati protocolli , esempio:

nmap -sS -sU –p U:53,T:200 192.168.1.10

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Infine, il -D su nmap si utilizza principalmente per effettuare un decoy, ovvero mascherare l’indirizzo IP mandando diversi pacchetti da un IP selezionato dall’utente

Esempio:

nmap -D 192.168.1.6 192.168.1.10

Immagine che contiene testo, schermata

Descrizione generata automaticamente

Immagine che contiene testo, schermata, menu, Carattere

Descrizione generata automaticamente

Il comando -D RND:10 invece seleziona un numero di IP randomico con cui mascherare i pacchetti, in questo caso altri 10 IP generati casualmente  
  
esempio:

nmap -D RND:10

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere, documento

Descrizione generata automaticamente