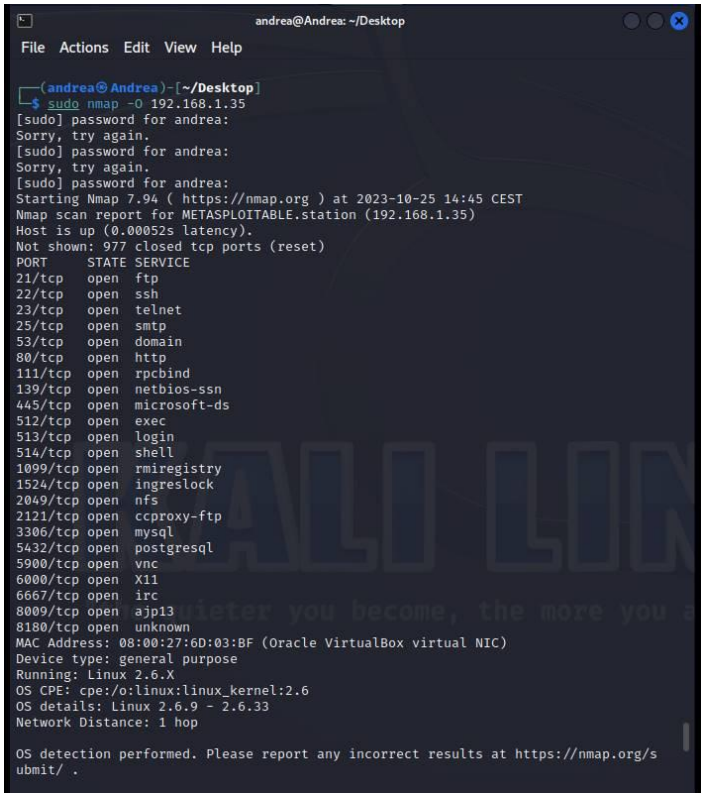
Settimana 5 Esercizio 3

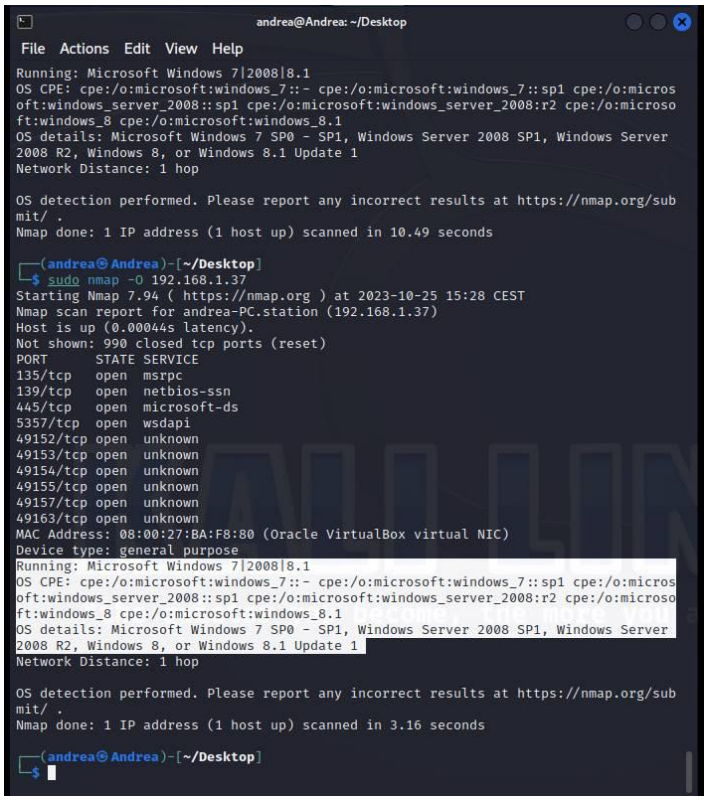
Utilizzo di NMAP

Oggi andremo a prendere dimestichezza con le scansioni tramite il tool NMAP.
Esso rappresenta un'ottima risorsa da utilizzare per effettuare mapping di rete per l'enumerazione dei servizi e la scansione degli host target: il mapping ci permette di conoscere dettagliatamente gli obbiettivi prima del pentest, di rendere quest'ultimo efficiente e di creare un ambiente di lavoro organizzato.

Iniziamo con la scansione su Metasploiable come target andando ad usare vari comandi a seconda del tipo di scansione:

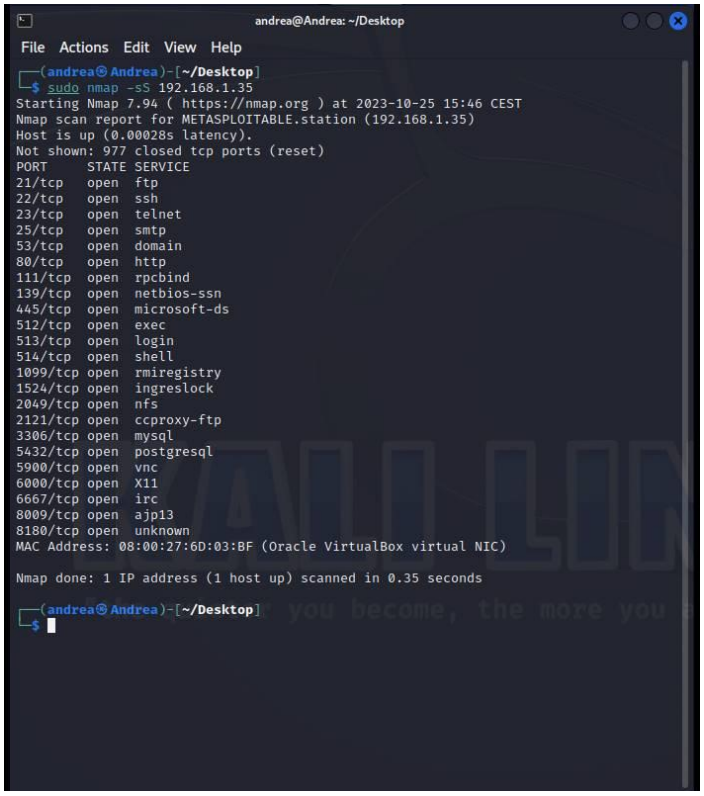
1. OS Fingerprint: questo comando serve per determinare il sistema operativo della macchina target attraverso la dicitura *'nmap -O <IP target>'*. Con esso possiamo notare (come in figura 1) che oltre alla descrizione delle porte aperte e dei protocolli associati ad esse ci mostra anche il dettaglio del sistema operativo di quell'IP 192.168.1.35 con tutte le versioni.



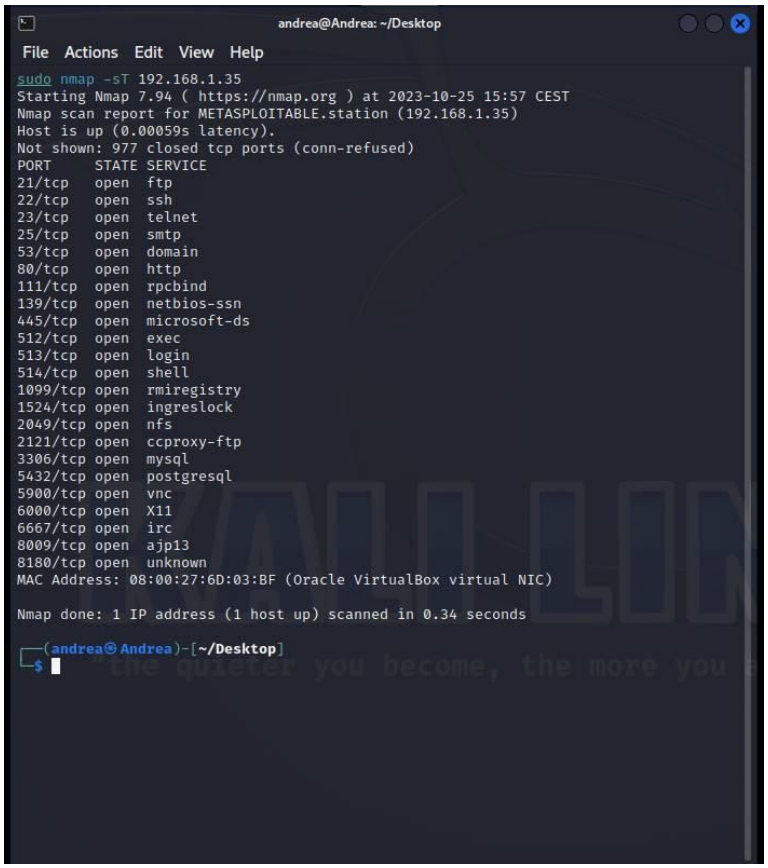


È possibile eseguire la stessa scansione verso una macchina Windows con IP 192.168.1.37; la grande differenza sta nell'andare ad impostare il firewall di Windows in modo tale che il nostro IP di Kali possa comunicare con esso impostando la regola.
Anche qui possiamo notare che ci fornisce i dettagli inerenti al sistema operativo Windows.

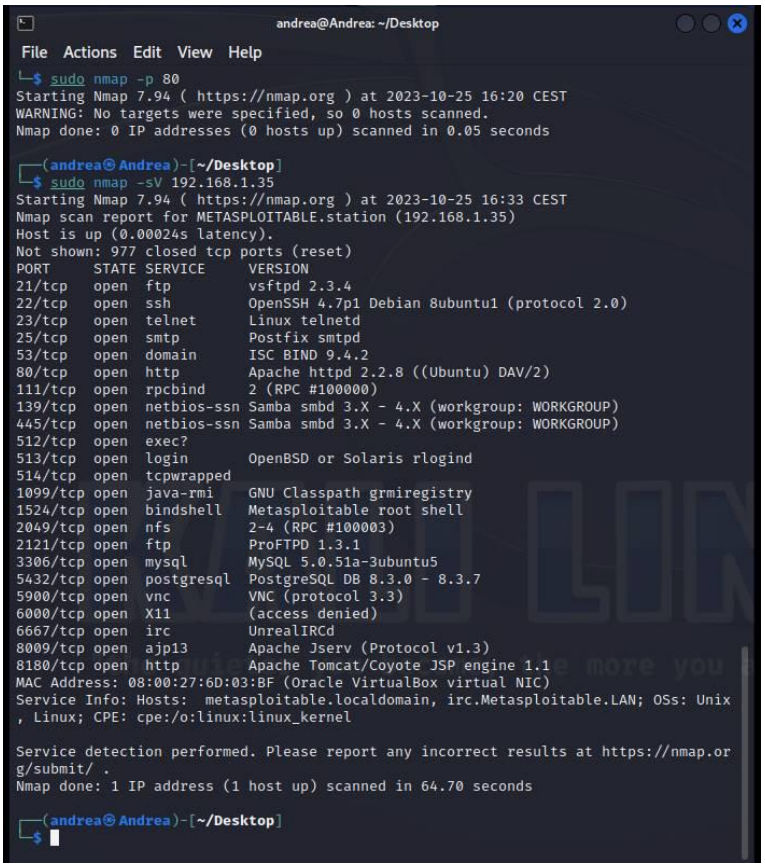
2. Syn Scan: tramite il comando *'nmap -sS <IP>'* riusciamo a capire quali porte sono aperte e quali servizi sono attivi su di esse. Rispetta solo il primo passaggio dell' HandShake SYN/ACK senza chiuderlo in modo tale da risultare più veloce e meno invasivo/rumoroso. Questo porta, tuttavia, ad un'accuratezza minore. Possiamo identificare servizi molto importanti e le relative porte predefinite come: 21 FTP, 22 SSH, 80 HTTP, 443 HTTPS.



3. TCP Connect: è, in poche parole, la conclusione del metodo di scansione precedente. Esso tramite comando *'nmap s-T <IP>'* va a concludere tutte le fasi dell' HandShake risultanto più invasivo rispetto al solo SYN. Aspetta di ricevere tutte le fasi e ciò porta a creare una latenza maggiore. Esso, tuttavia, è molto attendibile.



4. Version Detection: è un tipo di scansione chiamata anche *'banner grabbing'* che permette di recuperare informazioni inerenti al software su una determinata porta e alla sua versione. Questo ci permette di sperimentare in laboratorio virtuale le vulnerabilità e di verificarne l'attendibilità nel caso la porta predefinita sia stata cambiata (contromisura efficace).



Un altro comando molto utile è anche *'nmap <IP> --script smb-os-discovery'* che mostra le informazioni di un sistema operativo con un particolare script molto dettagliato che riporta anche i nomi utenti o del PC: