**NMAP**

**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.

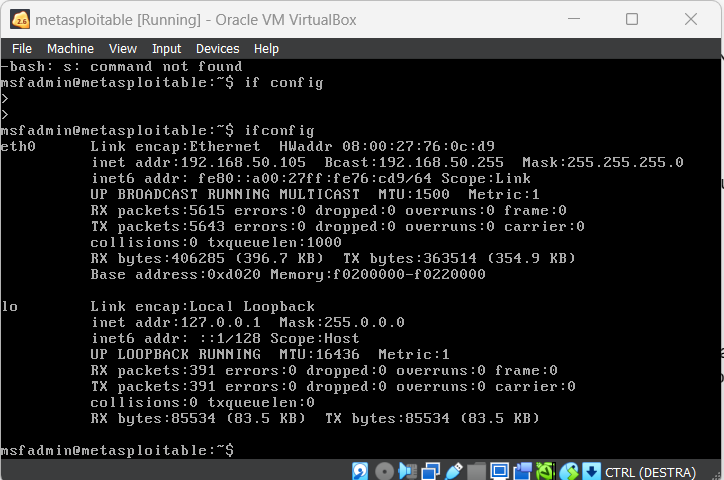
E la seguente sul target Windows 7: OS fingerprint

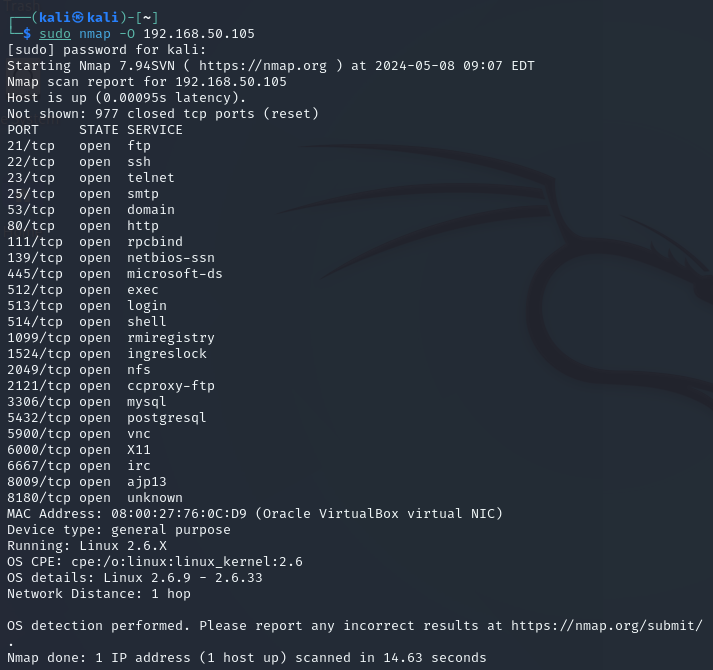
A valle delle scansioni è prevista la produzione di un report contenente le seguenti info (dove disponibili):   
IP.   
Sistema Operativo.   
Porte Aperte.   
Servizi in ascolto con versione.

Quesito extra (al completamento dei quesiti sopra): Quale potrebbe essere una valida ragione per spiegare il risultato ottenuto dalla scansione sulla macchina Windows 7? Che tipo di soluzione potreste proporre per continuare le scansioni?

Iniziamo con Kali e Meta.

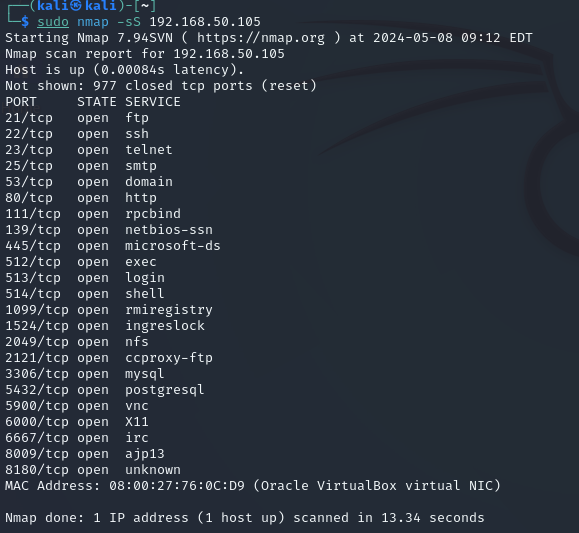
Per prima cosa usiamo NMAP per effettuare l’OS Fingerprinting sulla macchina meta con IP 192.168.50.105, tramite lo switch -O, che ci restituirà il sistema operativo del target.



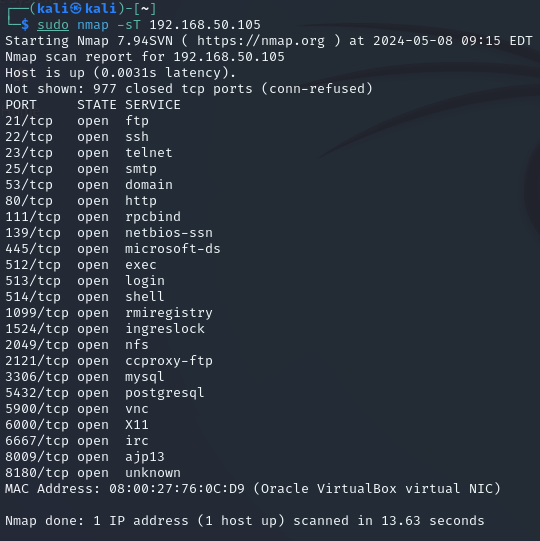


Test eseguito con successo, nmap ha analizzato i tempi di risposta del protocollo tcp e ha individuato il sistema operativo di Metasploitable, ovvero linux ver2.6.x.

Poi eseguiamo una scansione Syn, per vedere se la macchina risponde.

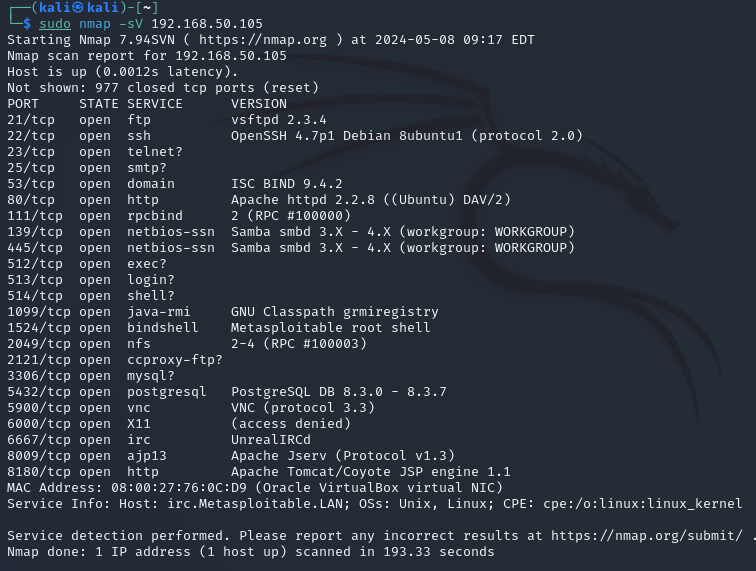


La macchina ha risposto e si è sincronizzata con il pacchetto SYN. Ora vediamo se ci sono differenze con un ciclo TCP completo.

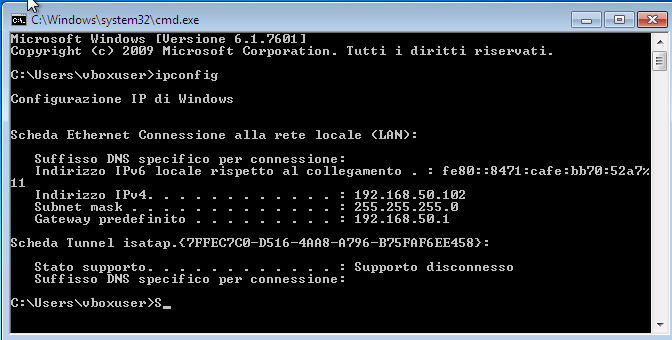


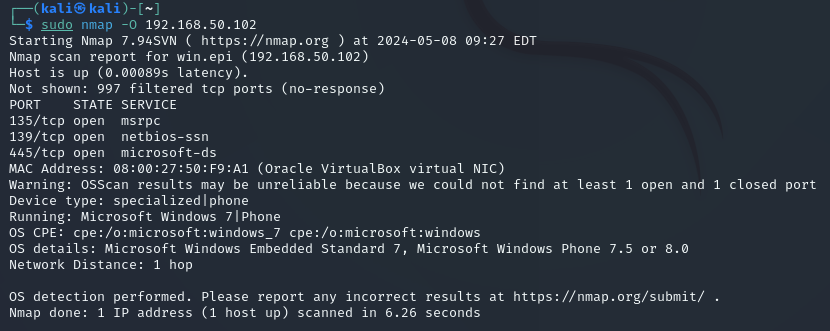
Come ci si aspettava, non ci sono differenze sostanziali se non qualche millesimo di secondo in più, dato che il ciclo completo effettua anche invio di SYN/ACK e di ACK.

Ora vediamo le versioni del software e dei servizi sulla macchina di meta, questo passaggio è molto utile per vedere le versioni del software sulle porte aperte, così da poter poi individuare possibili vulnerabilità.



Adesso passiamo all’ OS Fingerprinting della macchina Windows con IP 192.168.50.102





Come possiamo vedere, l’OS fingerprinting è avvenuto con successo ma nmap segnala che 997 porte siano filtrate, molto probabilmente vengono filtrate dal firewall di windows che è configurato di default.

Proviamo ad utilizzare uno dei metodi visti a lezione per aggirare il firewall di windows.

Utilizziamo la Sneaky scan del Timing di NMAP per cercare di aggirare il firewall.

sudo nmap -T1 192.168.50.102

Così facendo effettueremo una scansione lenta che però è anche meno invasiva e ha la possibilità di aggirare i sistemi di protezione come IDS, IPS e Firewall a difesa della macchina target. Ovviamente questo tipo di scansione non è una panacea che aggirerà tutti gli ostacoli: molto dipende dalla configurazione di difesa della macchina, se i dispositivi a protezione della rete sono sensibili, quasi sicuramente questo metodo non funzionerà.