S5/L3

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.

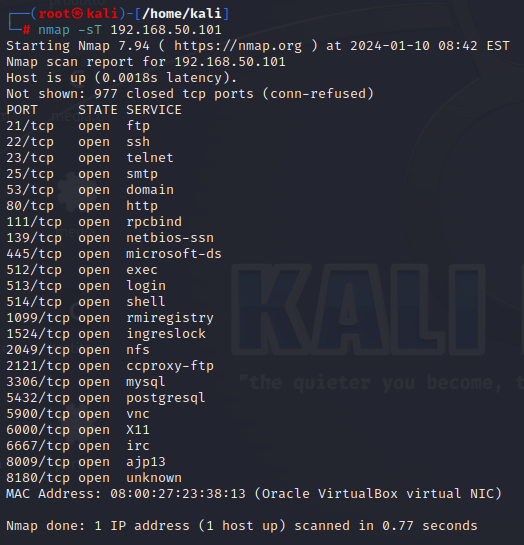
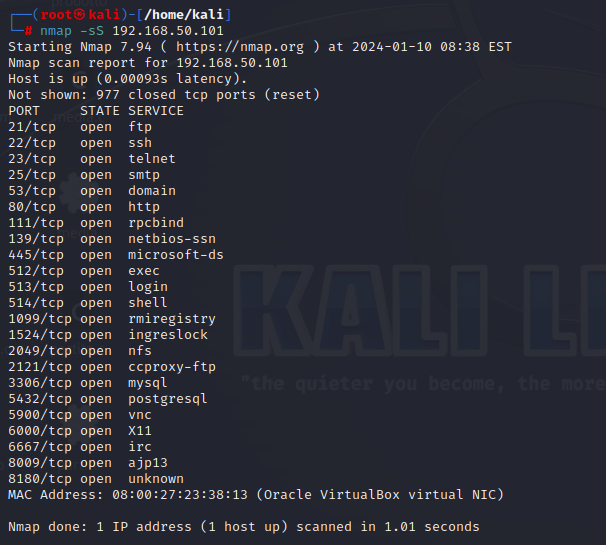
● Porte Aperte.

● 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?

Per prima cosa apriamo il terminale di Kali Linux e utilizziamo Nmap, ovvero uno strumento open source utilizzato per avere una mappa della scansione della rete e dei servizi e come target scriviamo l’IP di metasploitable 192.168.50.101

SYN SCAN: TCP CONNECT:



Il syn scan (-sS), è un metodo di scansione meno invasivo, una volta ricevuto il pacchetto dal target, non conclude il 3-way-handshake; ma solo il SYN. Perciò chiude la comunicazione una volta che è riuscito comunque a recuperare informazioni sullo stato della porta (open).

Il tcp connect (-sT), è un metodo più invasivo e completa tutti i passaggi del 3-way-handshake.

In questo caso non notiamo differenze tra i due metodi, ma in generale, con il metodo -sT abbiamo più informazioni sicure e affidabili, anche se creiamo più rumore a livello di network.

Come porte aperte e il servizio, tra quelle conosciute troviamo:

21 – ftp 🡪 protocollo di trasferimento file

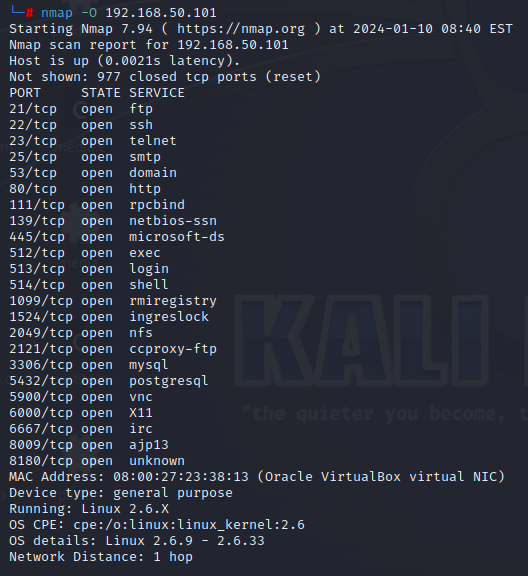
22 – ssh 🡪 protocollo che mi permette di stabilire una connessione remota e sicura

23 – telnet 🡪 protocollo che mi permette di stabilire una connessione remota ma non sicura

25 – smtp 🡪 protocollo per la trasmissione di email

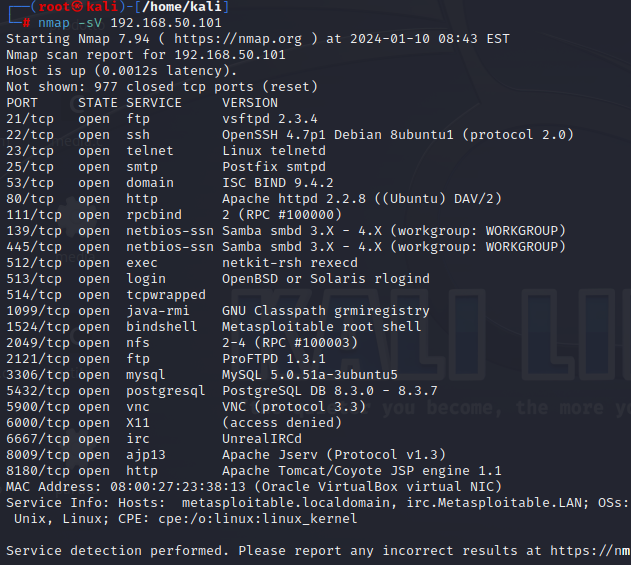
80 – http 🡪 protocollo per la trasmissione dati su internet

OS FINGER PRINT



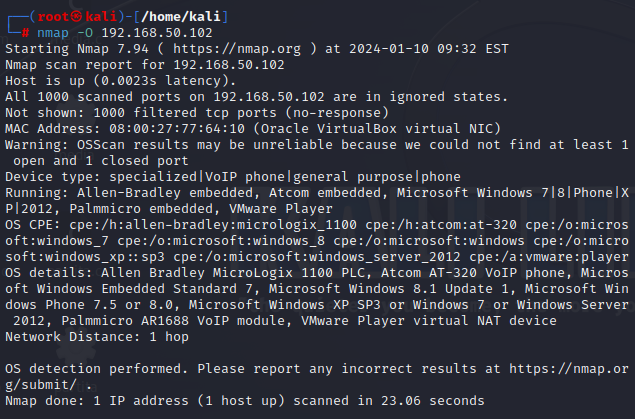
Questo comando (-O),in aggiunta ci identifica il sistema operativo (Linux), il kernel… ispezionando i pacchetti di risposta ricevuti. È un tipo di scansione aggressiva.

VERSION DETECTION



Questo comando (-sV) mi permette di identificare i servizi attivi sulle porte aperte e la loro versione, tramite quello che viene chiamato “banner grabbing”. In questo caso nmap esegue una prima TCP connect e poi tramite la cattura del banner risale alla loro versione, è meno aggressivo di -A.

Vediamo adesso l’OS fingerprint su Windows7, utilizzano il suo IP target 192.168.50.102



In questo caso non vediamo nessun risultato in quanto windows7 di base ha un suo firewall di protezione, per aggirare il problema potremmo creare una nuova regola.