Esercitazione W11D1 - Pratica 2

Nmap

Fabio Benevento - 16/01/2024

Traccia

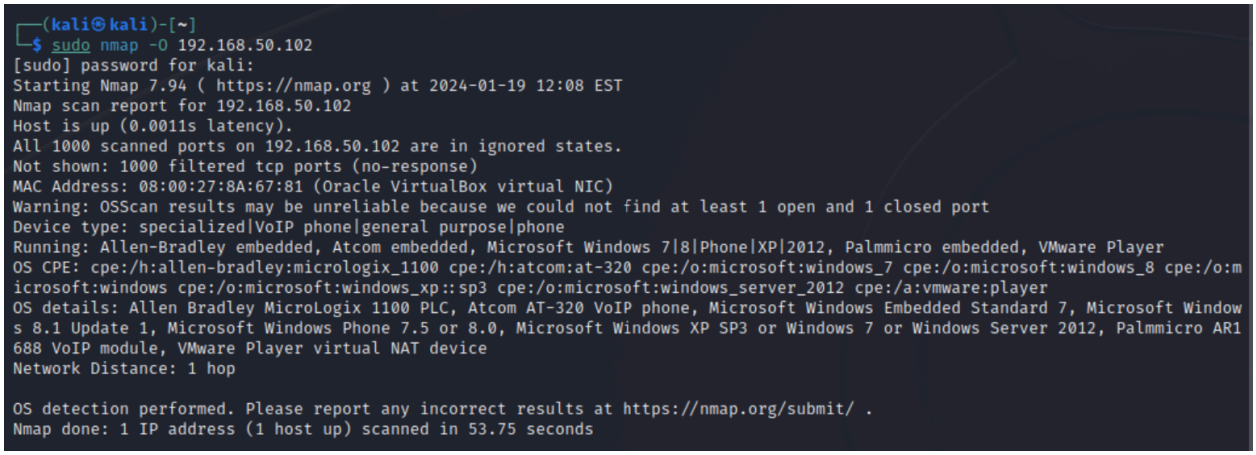
Si richiede allo studente di effettuare le seguenti scansioni sul target Windows 7:
- OS fingerprint
- Syn Scan
- Version detection

Implementazione

Nelle seguenti pagine sono illustrati i comandi utilizzati per ricavare le informazioni richieste.
Entrambe le macchine sono collocate sulla stessa sottorete (192.168.50.x) con indirizzi rispettivamente di 192.168.50.100 per Kali Linux e di 192.168.50.102 per Windows 7

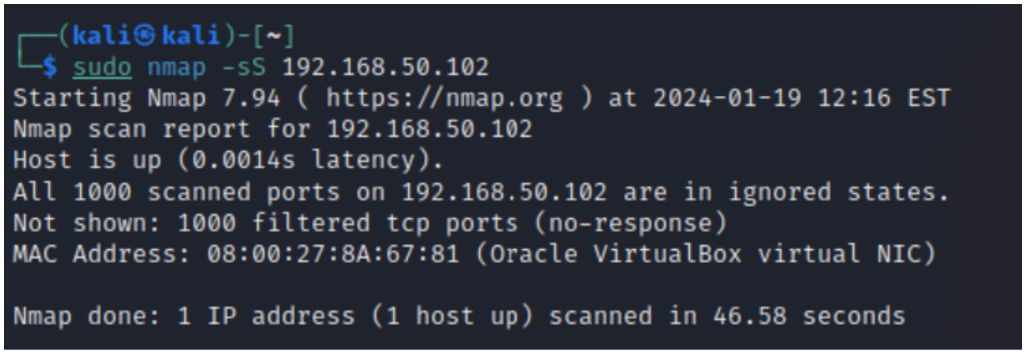
OS Fingerprinting (-O)

Tramite l'opzione -O è possibile individuare la versione del sistema operativo che viene stampata in basso al termine della scansione dei servizi come mostrato nell'immagine sottostante.



Syn Scan (-S)

Tramite l'opzione -S è possibile effettuare la scansione senza effettuare la connessione completa con three-way handshake



Version detection (-V)

Il seguente test non è stato condotto in quanto, come emerso con i precedenti comandi, non risultano porte aperte. Ciò potrebbe esser dovuto alla presenza di un firewall / IPS che blocca le richieste in ingresso. Per aggirare queste limitazioni andrebbero adottati metodi specifici che possono riuscire a bypassare il blocco.

Report finale

Di seguito il report in forma tabellare con le informazioni trovate

Fonte	Kali Linux - IP: 192.168.50.100		
Target	Windows 7 - IP: 192.168.50.102		
Tipo di scan	Nmap (varie modalità)		
Numero servizi trovati		nessuna porta esposta	
Porta	**Servizio**	**Versione**	**Descrizione**