NMAP

Traccia: 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:

- OS fingerprint.

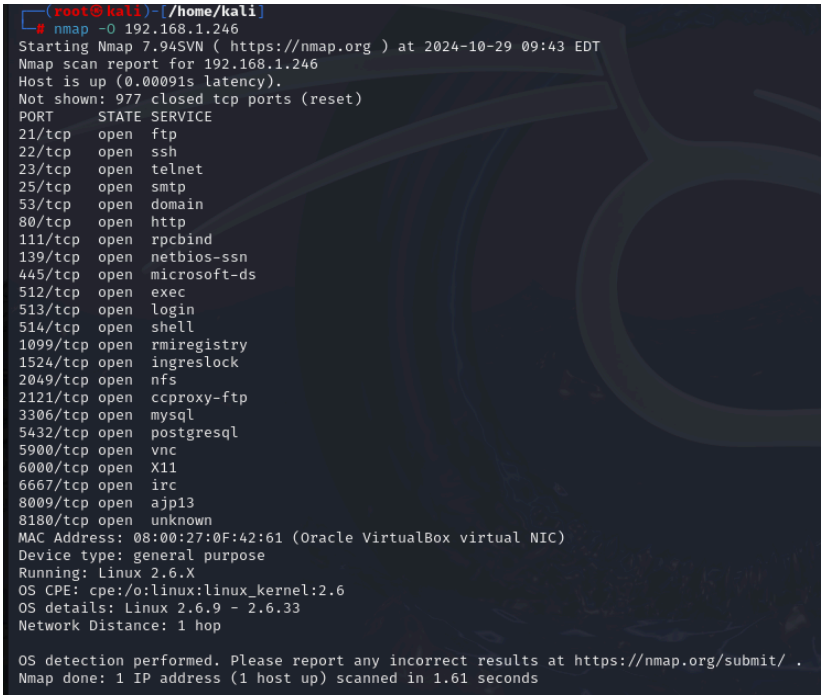
Oggi abbiamo imparato a conoscere il programma NMAP, uno strumento utile per la scansione e mappatura delle reti identificando le porte aperte, i dispositivi connessi, i servizi attivi e le vulnerabilità. E' spesso utilizzato in ambito di sicurezza informatica.

OS Fingerprint

Il primo comando che andremo ad analizzare sarà il comando OS Fingerprint, viene utilizzato su NMAP per identificare il sistema operativo di un dispositivo utilizzando l'indirizzo IP, ne analizza le risposte ricevute dai pacchetti inviati e confronta le informazioni con un database di firme di sistemi operativi conosciuti. Il comando che si utilizza sarà:

nmap -O [indirizzo IP]

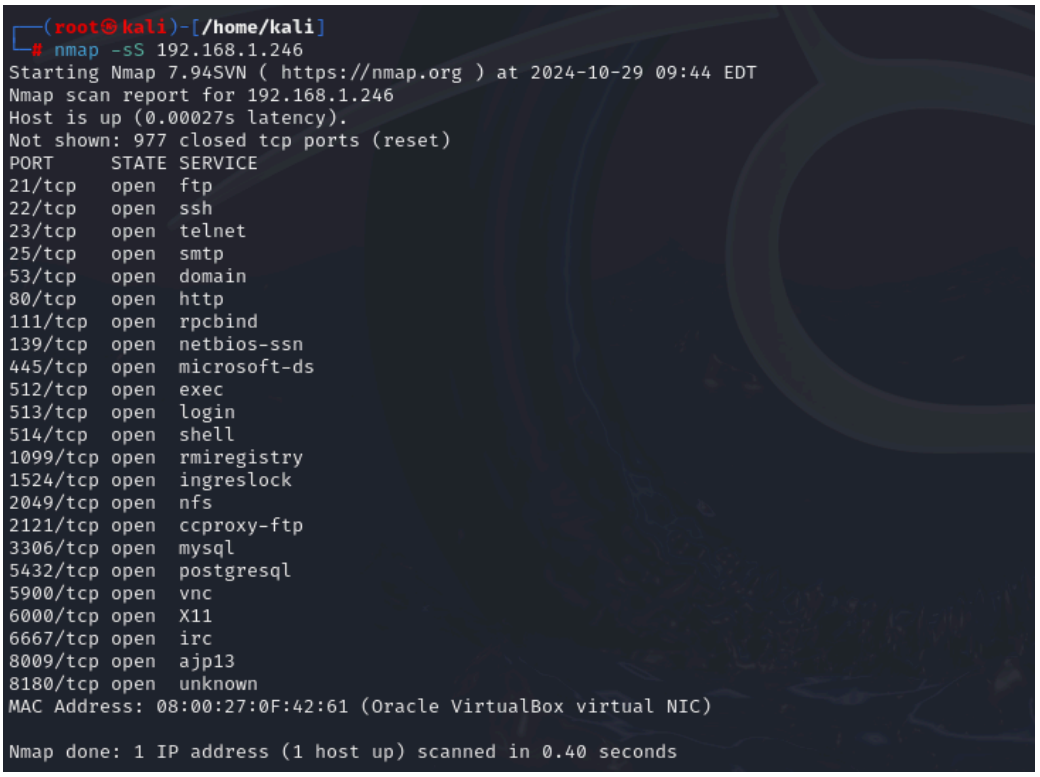
Qui lo abbiamo utilizzato inviando il comando dalla macchina Kali Linux, indirizzandolo alla macchina Metasploitable2.



Ciò che ci andrà a mostrare le informazioni rilevate tra cui l'elenco delle porte aperte, e nelle righe finali ci rivelerà quale è il sistema operativo della macchina Metasploitable2 presa in esame, ovvero Linux.

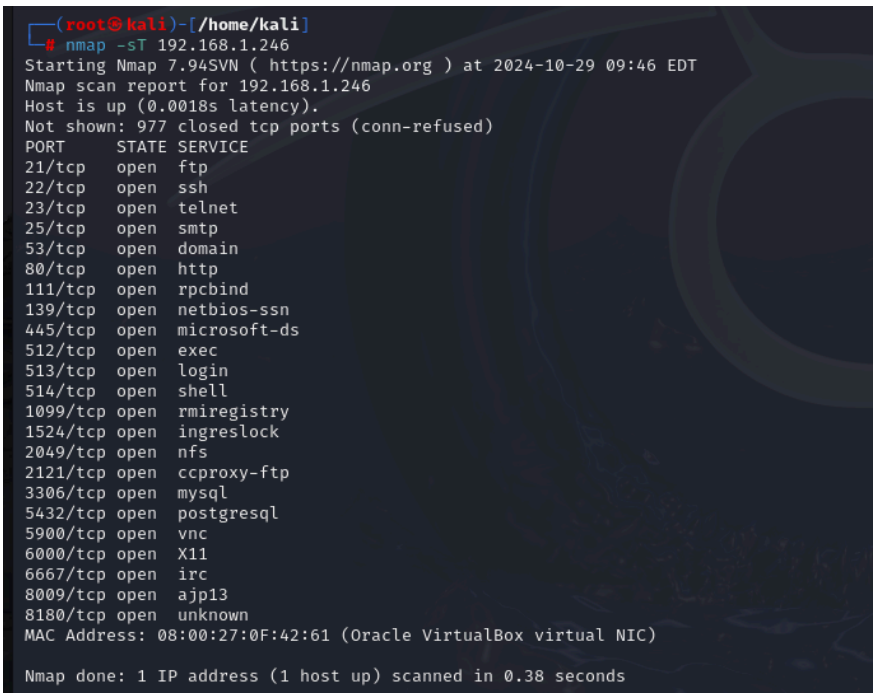
Syn Scan

Il secondo comando che siamo andati ad eseguire è il Syn Scan, ovvero una scansione meno invasiva, basata sul protocollo TCP, ma che non porta a termine il 3-hand-shake, limitandosi ad eseguire solo i primi 2 passaggi (Syn e Syn/Ack) per assicurarsi che la porta sia aperta. Il comando che verrà avviato sarà:
nmap -sS [indirizzo IP]
Questo tipo di scansione è più rapida e meno rilevabile dai firewall e sistemi di rilevamento delle intrusioni.



TCP Connect

Il terzo comando che andremo ad eseguire sarà il TCP Connect. Funziona in maniera analoga al Syn Scan, ma a differenza di questo, andrà a completare il 3-way-handshake in tutto e per tutto. Consente una analisi più completa delle porte aperte in quanto riesce a completare l'invio dei pacchetti. Il comando utilizzato è:
nmap -sT [indirizzo IP]
Rispetto a Syn Scan, questo metodo di scansione è facilmente rilevabile dal firewall o da sistemi di rilevamento delle intrusioni.

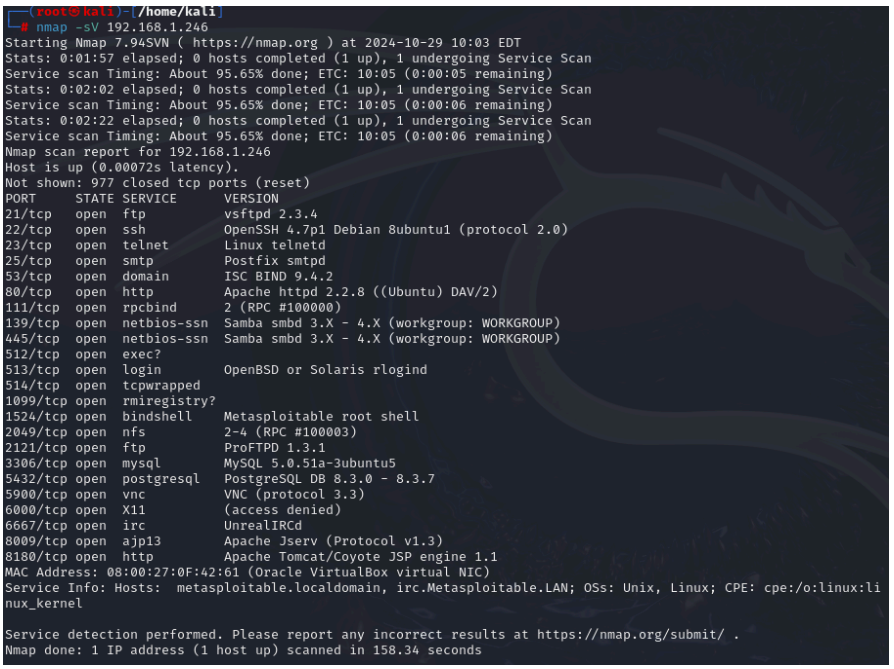


Version Detection

L'ultimo comando che andremo a vedere è Version Detection, questo comando serve ad identificare i servizi in esecuzione sulle porte aperte di un host, inviando richieste specifiche ai servizi e analizzando le risposte ricevute per identificare le porte aperte e le applicazioni e versioni specifiche attive su di esse. Il comando eseguito sarà:

nmap -sV [indirizzo IP]

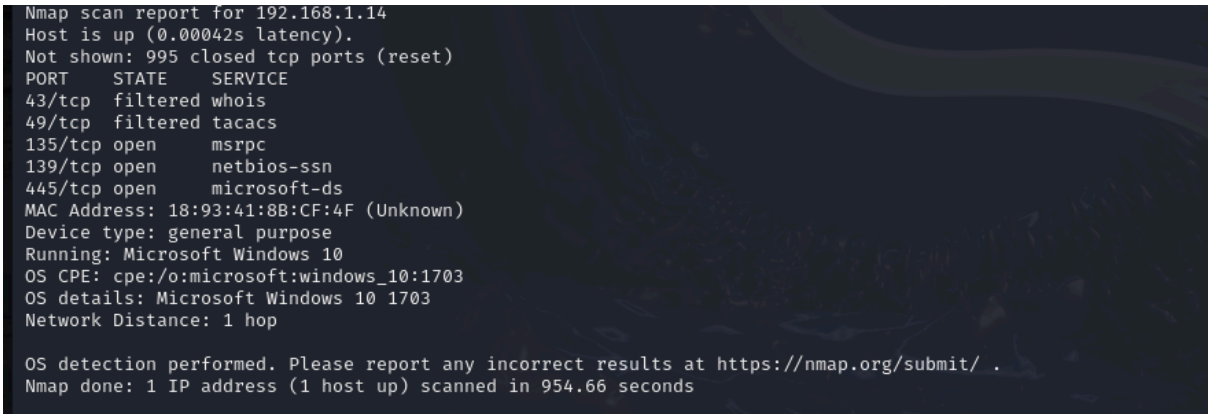
L'obiettivo di questo comando è quello di identificare le vulnerabilità e mappare la rete in maniera efficiente tramite un report dettagliato.



OS Fingerprint su Windows

Infine siamo andati ad eseguire il comando OS Fingerprint anche sulla macchina reale Windows per testarne l'efficacia.

Recuperando l'indirizzo IP della macchina reale siamo andati ad eseguire nuovamente il comando OS Fingerprint. L'output che ne abbiamo ottenuto è il seguente:



Nelle righe finali il report rileverà un sistema operativo Microsoft Windows 10, con aperte le porte 135, 139, 445, con le porte 43 e 49 aperte, ma con restrizioni.