EPICODE-CS0124
S5/L3 - Pratica

Flaviano Sedici

Pratica

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.

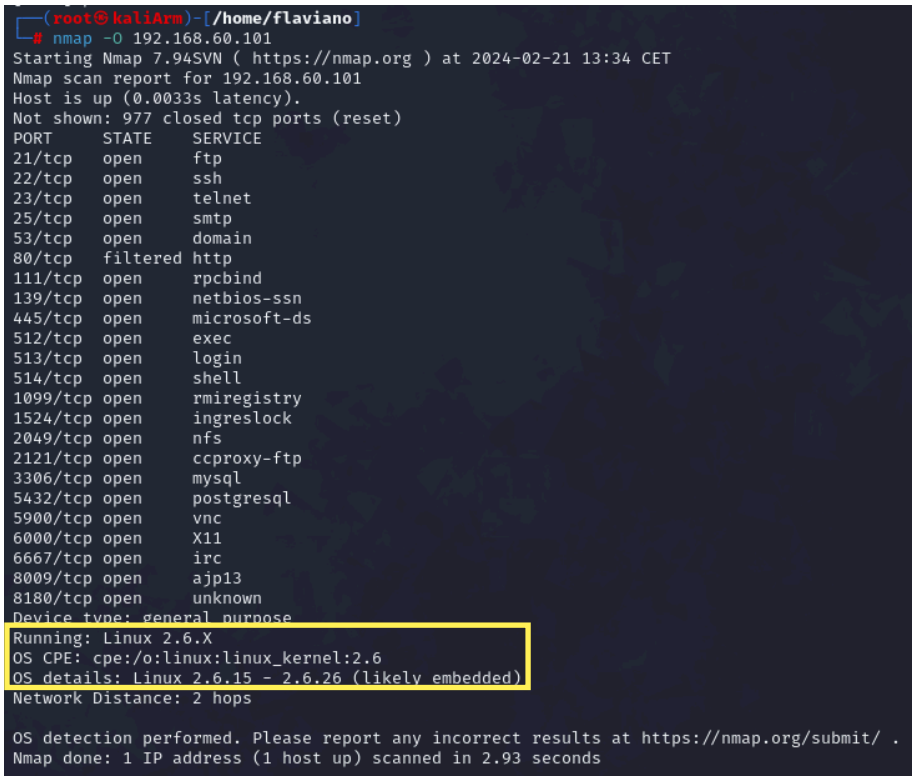
E la seguente sul target Windows 7:

- OS fingerprint.

---

1. Target Metasploitable (192.168.60.101)

1.1. OS Fingerprint

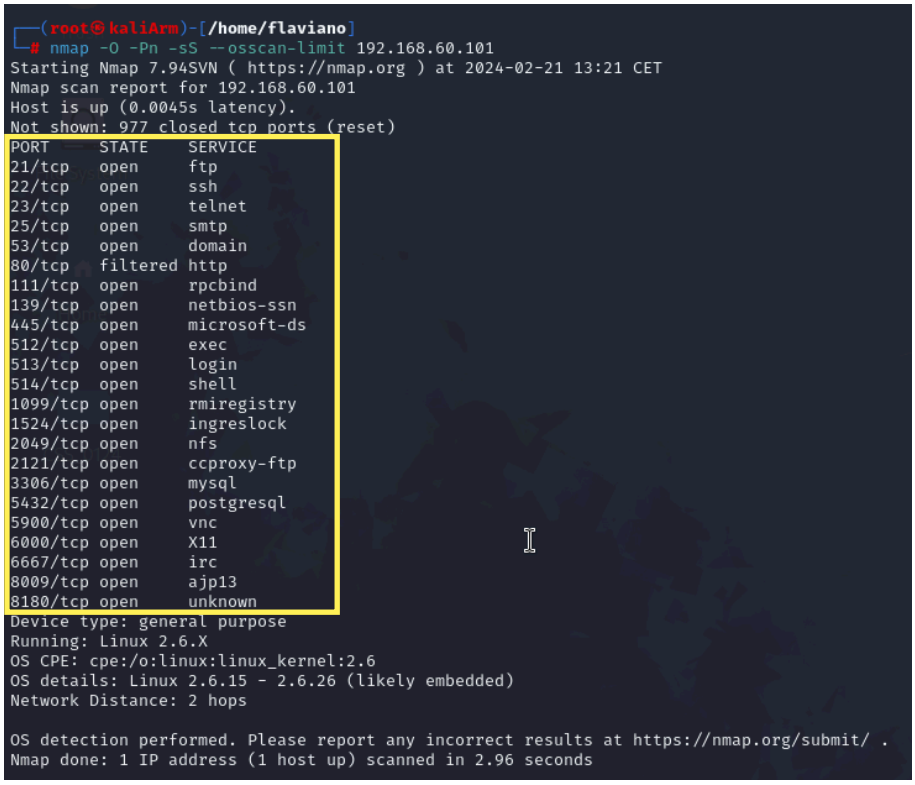


Sulla VM di Metasploitable è stato effettuato uno scan per il riconoscimento del SO, che ha restituito il sistema operativo nell'immagine.

1.2. Syn Scan

Per effettuare il SYN Scan è stato utilizzato il comando:

nmap -O -Pn -sS —osscan-limit 192.168.60.101



Si è utilizzato lo switch -sS per completare la richiesta ma è stato deciso di aggiungere anche gli switch -Pn per evitare di utilizzare il ping.

Inoltre è stato ampliato lo switch -O con lo switch —osscan-limit per rilevare eventuale differenze con —osscan-guess (vedi paragrafi successivi).

Lo switch -sS genera meno traffico e quindi ha minore probabilità di essere rilevato.

1.3. TCP Connect

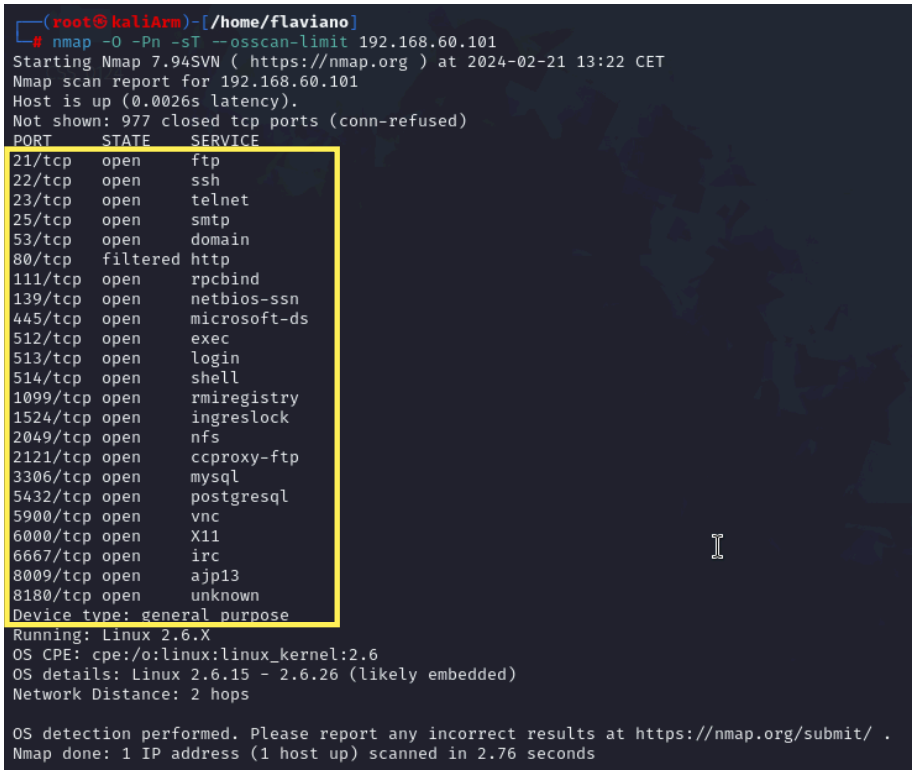
Per effettuare il TCP Connect è stato utilizzato il comando:

nmap -O -Pn -sT —osscan-limit 192.168.60.101

Si è utilizzato lo switch -sT per completare la richiesta ma è stato deciso di aggiungere anche gli switch -Pn per evitare di utilizzare il ping.

Inoltre è stato ampliato lo switch -O con lo switch —osscan-limit per rilevare eventuale differenze con —osscan-guess (vedi paragrafi successivi).

Come è possibile notare i risultati della scansione sono identici ma il tempo è inferiore di 0,2 secondi rispetto alla scansione effettuata con lo switch -sS, è più invasiva e nello stesso tempo leggermente più veloce con maggiore generazione di traffico (facilmente individuabile).



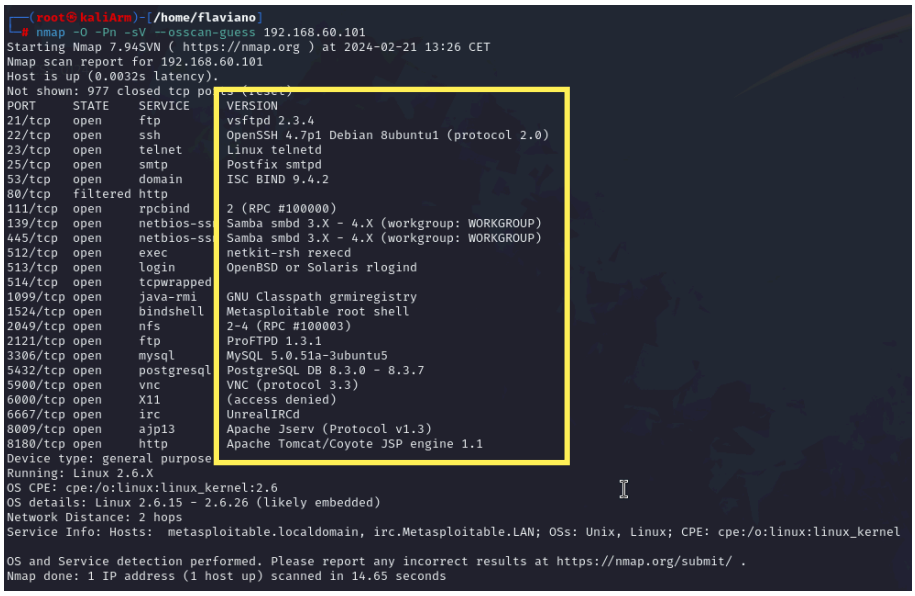
1.4. Version Detection

Per effettuare il Version Detection è stato utilizzato il comando:

nmap -O -Pn -sV —osscan-limit 192.168.60.101

Si è utilizzato lo switch -sV per completare la richiesta ma è stato deciso di aggiungere anche gli switch -Pn per evitare di utilizzare il ping.

Inoltre è stato ampliato lo switch -O con lo switch —osscan-guess e in questo caso non è stata rilevata alcuna differenza rispetto alla —osscan-limit.



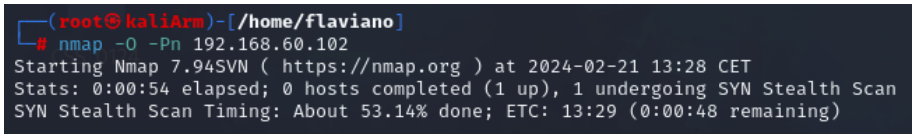
Come è possibile notare i risultati della scansione oltre che i dati aggiuntivi sul versionamento delle applicazioni collegate alle porte, ma il tempo di scansione è aumentato notevolmente fino a 14,65 secondi.

2. Windows 7 (192.168.60.102)

2.1. OS Fingerprint (Firewall)

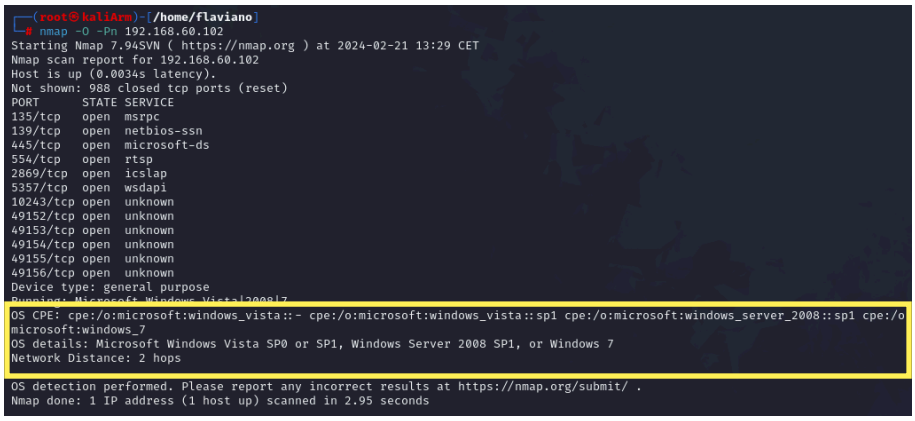
Eseguendo il comando per effettuare il discover del sistema operativo target, il firewall di Windows blocca lo scan di nmap.

Abbiamo inserito il comando -Pn per eludere il blocco del firewall di Windows sul ping.



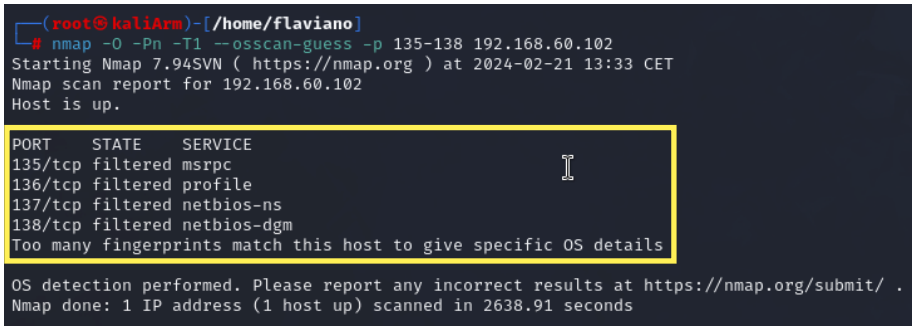
2.2. OS Fingerprint (no Firewall)

Eseguendo lo stesso comando avendo disabilitato il firewall di Windows, nmap restituisce dei risultati in breve tempo 2.95 secondi.



2.3. OS Fingerprint (Firewall) soluzioni alternative

Al fine di aggirare i controlli del firewall di Windows, è stato utilizzato lo switch -T1 per rallentare la frequenza della scansione di nmap in modo che il firewall non cataloghi la scansione come una possibile minaccia.



Il -Pn è stato aggiunto per evitare di effettuare il ping che normalmente viene bloccato dal firewall di Windows.

L'azione è stata circoscritta alle porte comprese tra la 135 e la 138 in modo da accelerare il processo di ricerca.

Come si evince dal test lo stato delle porte è comunque filtrato (quindi protetto da firewall) e nmap non riesce ad identificare il sistema operativo, oltre che ad impiegare 2.638 secondi.

La **porta 135** riporta comunque il servizio **msrpc** che è legato a **Microsoft Security Event Log su protocollo MSRPC** e possiamo quindi ragionevolmente ipotizzare che il sistema operativo sia Windows.

https://www.ibm.com/docs/it/dsm?topic=options-microsoft-security-event-log-over-msrpc-protocol