S5-L2

Relazione: Tecniche di scansione con Nmap

Introduzione

Nmap (Network Mapper) è uno strumento di scansione di rete open-source, progettato principalmente per scopi di sicurezza e ampiamente usato sia dai professionisti della sicurezza informatica che dagli amministratori di rete. Creato inizialmente da Gordon Lyon (conosciuto anche come Fyodor), Nmap è oggi uno degli strumenti di analisi della rete più affidabili e versatili, con funzionalità che vanno oltre la semplice scoperta delle porte aperte.

Funzionalità Principali di Nmap:

Oltre alle scansioni di base, Nmap offre molte altre funzionalità avanzate:

1. \*\*Scansione delle Porte\*\*: È possibile effettuare scansioni su specifiche porte o su tutto l'intervallo di porte disponibili. Nmap rileva se una porta è aperta, chiusa o filtrata da un firewall.

2. \*\*Identificazione dei Servizi e delle Versioni\*\*: Utilizzando l’opzione `-sV`, Nmap può identificare i servizi esatti in esecuzione su ogni porta e spesso anche le loro versioni. Questo è particolarmente utile per identificare le versioni obsolete o vulnerabili di software in esecuzione su server e dispositivi di rete.

3. \*\*OS Detection\*\*: L'\*\*OS Fingerprinting\*\* (`-O`) è una tecnica che consente di dedurre il sistema operativo del target in base a come risponde ai pacchetti. Nmap usa un database di fingerprint per confrontare le risposte del target e determinarne il sistema operativo.

4. \*\*Scansioni di Tipo Avanzato\*\*:

- \*\*TCP SYN Scan\*\* (`-sS`): Veloce e stealth, non completa il "three-way handshake" TCP, evitando spesso di essere rilevato.

- \*\*TCP Connect Scan\*\* (`-sT`): Completa la connessione TCP, utile quando non si hanno permessi elevati per fare Syn Scan.

- \*\*UDP Scan\*\* (`-sU`): Scansiona le porte UDP, generalmente più lenta rispetto alla scansione TCP ma utile per trovare servizi UDP come DNS o DHCP.

- \*\*Xmas e Null Scan\*\*: Tecniche di scansione per bypassare firewall o rilevare se una porta è filtrata, inviando pacchetti non convenzionali.

5. \*\*NSE - Nmap Scripting Engine\*\*: Una delle funzionalità più potenti di Nmap è l'NSE, che permette di eseguire script per compiti specifici, come la verifica di vulnerabilità, la scoperta di servizi di rete o anche attacchi brute-force.

Gli script NSE sono raggruppati in categorie (ad es., vuln per vulnerabilità, auth per autenticazione, ecc.), e permettono di personalizzare le scansioni in base agli obiettivi di analisi.

6. \*\*Scansioni Distribuite\*\*: Con l'opzione `-iL`, Nmap permette di caricare una lista di target da un file, permettendo di effettuare scansioni su larga scala su reti complesse o segmenti di rete differenti.

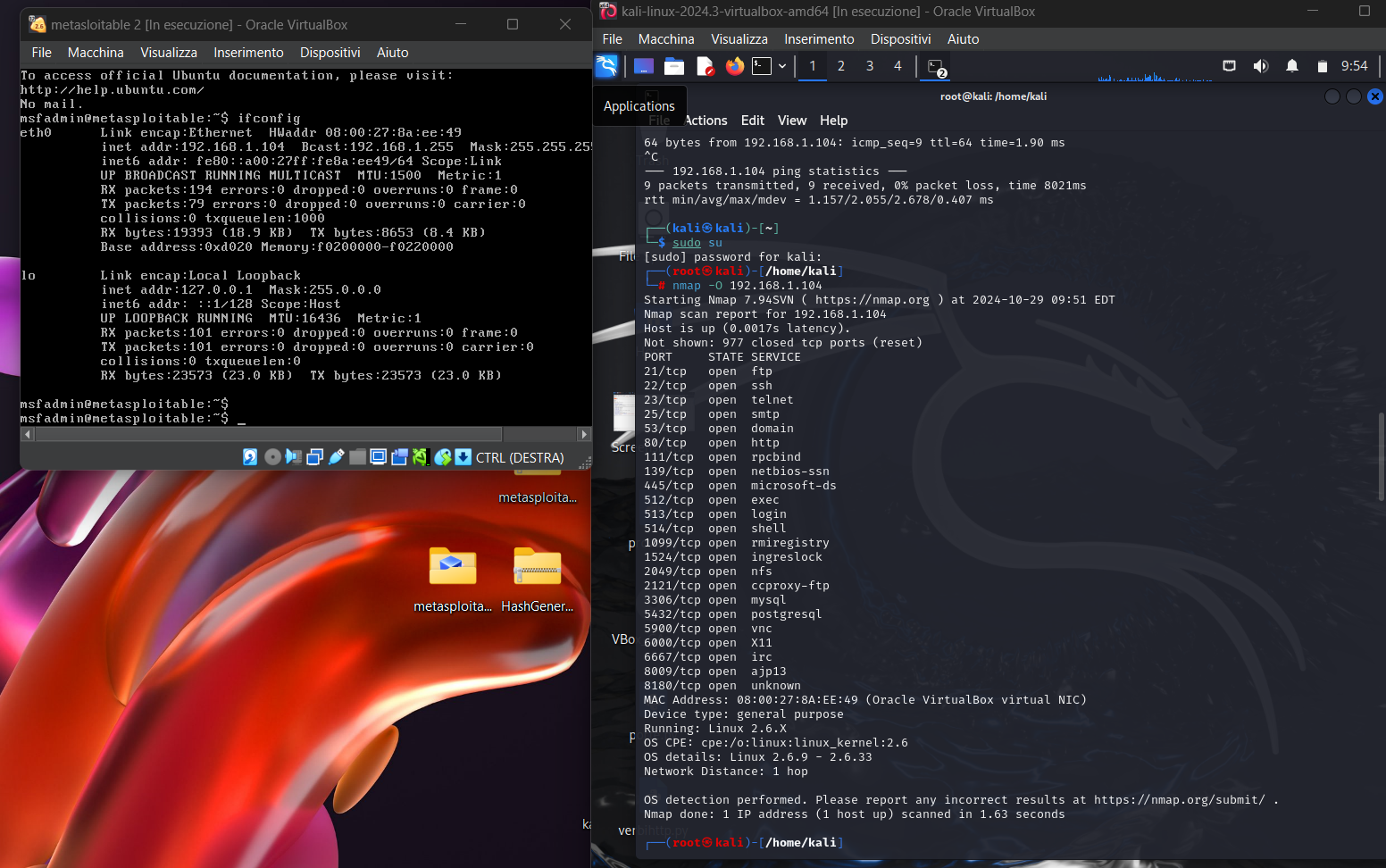
7. \*\*Aggiornamenti del Database dei Fingerprint e delle Versioni\*\*: Nmap viene aggiornato regolarmente per includere nuovi sistemi operativi, servizi e vulnerabilità nel suo database. Questo permette di identificare anche tecnologie recenti e le loro versioni.

Scansione su Target Metasploitable

1. OS Fingerprint

La scansione dell’impronta del sistema operativo (OS fingerprinting) è fondamentale per identificare il tipo di sistema operativo in esecuzione sul target. Utilizzando il comando:

nmap -O <target\_IP>

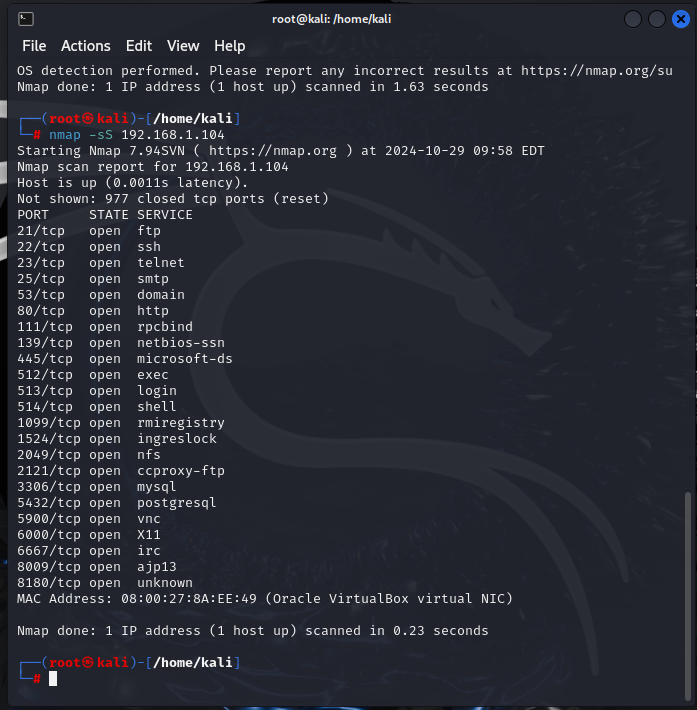


il tool analizza una serie di caratteristiche della rete per dedurre l'OS. Su Metasploitable, Nmap ha rilevato correttamente che il sistema operativo era basato su Linux, fornendo dettagli come la versione del kernel (solitamente una versione vecchia di Linux, dato che Metasploitable è un ambiente vulnerabile creato per scopi educativi).

2. Syn Scan

Il Syn Scan, noto anche come "TCP SYN Scan" o "half-open scan," è uno dei metodi di scansione più utilizzati perché è rapido e stealth. Il comando è:

nmap -sS <target\_IP>

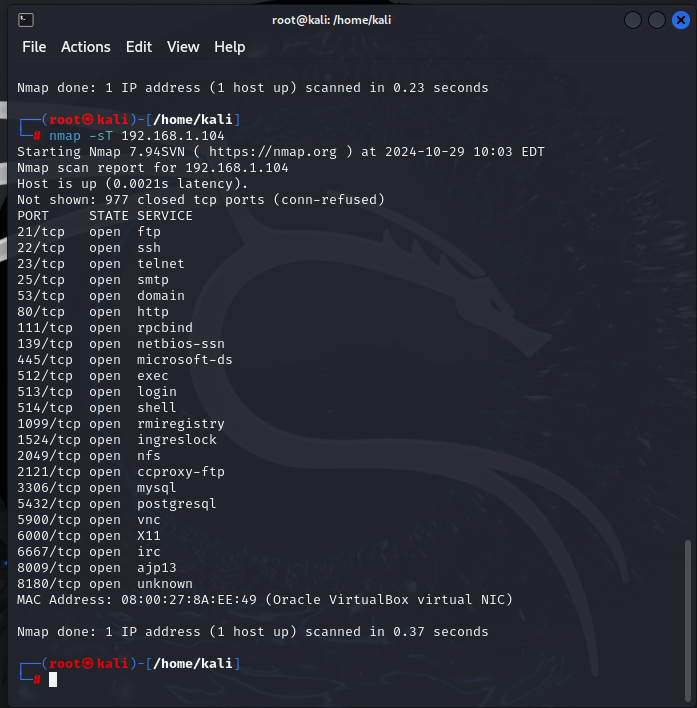


In questa modalità, Nmap invia pacchetti SYN alle porte del target, cercando di identificare quali porte sono aperte. \*\*Metasploitable\*\* ha restituito diverse porte aperte (es. 22, 80, 139, 445), rivelando i servizi attivi come SSH, HTTP, NetBIOS e SMB.

3. TCP Connect

La scansione TCP Connect (`-sT`) è un’altra tecnica di scansione che, a differenza del Syn Scan, completa la connessione TCP. Viene eseguita con il comando:

nmap -sT <target\_IP>



Il TCP Connect meno stealth rispetto alla Syn Scan e solitamente più lento, ma comunque utile per identificare le porte aperte. I risultati della scansione hanno confermato le stesse porte aperte del Syn Scan, con alcune differenze:

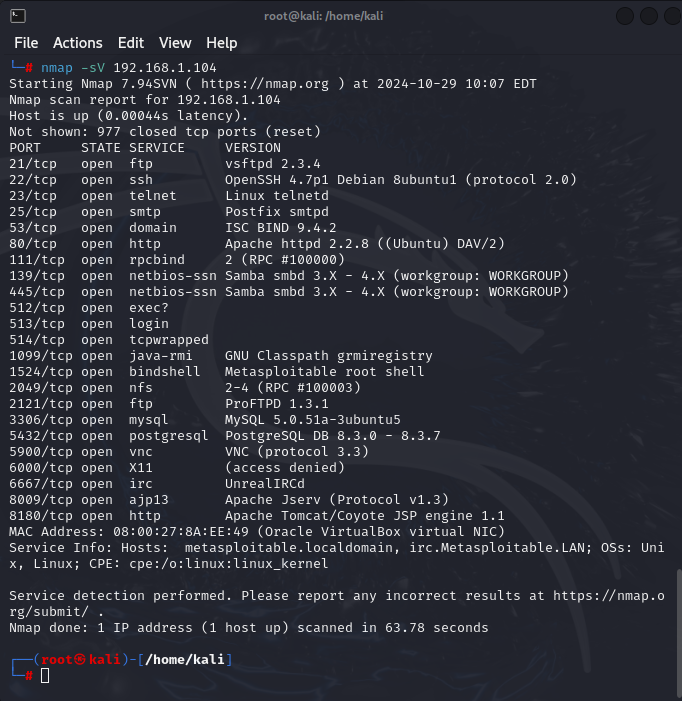
-Differenze tra Syn Scan e TCP Connect:

Syn Scan è generalmente più veloce e stealth, ideale per evitare sistemi di rilevamento intrusioni (IDS), poiché non completa la stretta di mano TCP. TCP Connect, invece, richiede il completamento della connessione, quindi è più probabile che venga rilevato da un IDS. In ambiente Metasploitable, i risultati di entrambi i metodi hanno confermato le porte aperte, ma la TCP Connect ha impiegato più tempo.

4. Version Detection

L’opzione Version Detection (`-sV`) permette di identificare le versioni specifiche dei servizi in esecuzione su ciascuna porta. Il comando è:

nmap -sV <target\_IP>



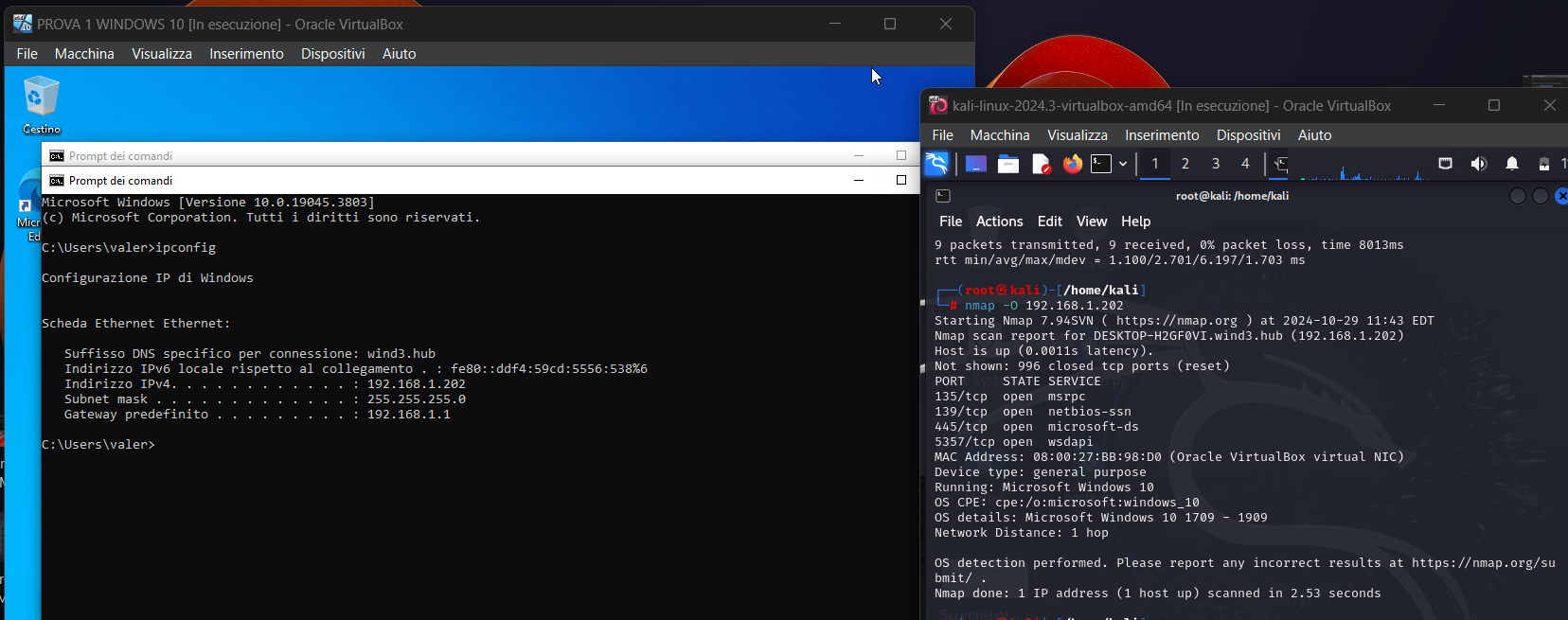
Questa scansione su Metasploitable ha restituito dettagli come la versione di “Apache” su porta 80, “vsftpd “su porta 21, e altri servizi vulnerabili. Questa tecnica è utile per identificare versioni obsolete e potenzialmente vulnerabili di software, facilitando l’analisi di sicurezza.

Scansione sul Target Windows

OS Fingerprint

L’OS Fingerprint sul target Windows è stato eseguito con il comando:

nmap -O <target\_IP>



In questo caso, Nmap ha correttamente identificato il sistema operativo come \*\*Windows\*\*, specificando la versione (Windows10) in base alle risposte ricevute.

Conclusioni

Le tecniche di scansione con Nmap sono strumenti essenziali per l’analisi della sicurezza di una rete. In particolare:

- OS Fingerprint 🡺 fornisce un’analisi dell’OS utile per capire l’ambiente operativo.

- Syn Scan 🡺 è più rapido e stealth rispetto a TCP Connect, e adatto a scansioni non invasive.

- TCP Connect 🡺 è efficace ma più facilmente rilevabile e meno stealth, con gli stessi risultati del Syn Scan per le porte aperte.

- Version Detection 🡺 consente di identificare versioni obsolete e vulnerabili, essenziale per individuare possibili vulnerabilità.

Queste tecniche offrono un panorama completo delle reti da analizzare, aiutando a valutare e migliorare la sicurezza dei sistemi analizzati.