Report: Analisi delle Scansioni Nmap su Metasploitable

Obiettivo: Effettuare una serie di scansioni di rete sul target Metasploitable per identificare il sistema operativo, le porte aperte, i servizi in ascolto e le loro versioni, secondo le richieste dell'esercizio. Il report finale documenta i risultati e le differenze tra i vari tipi di scansione.

---

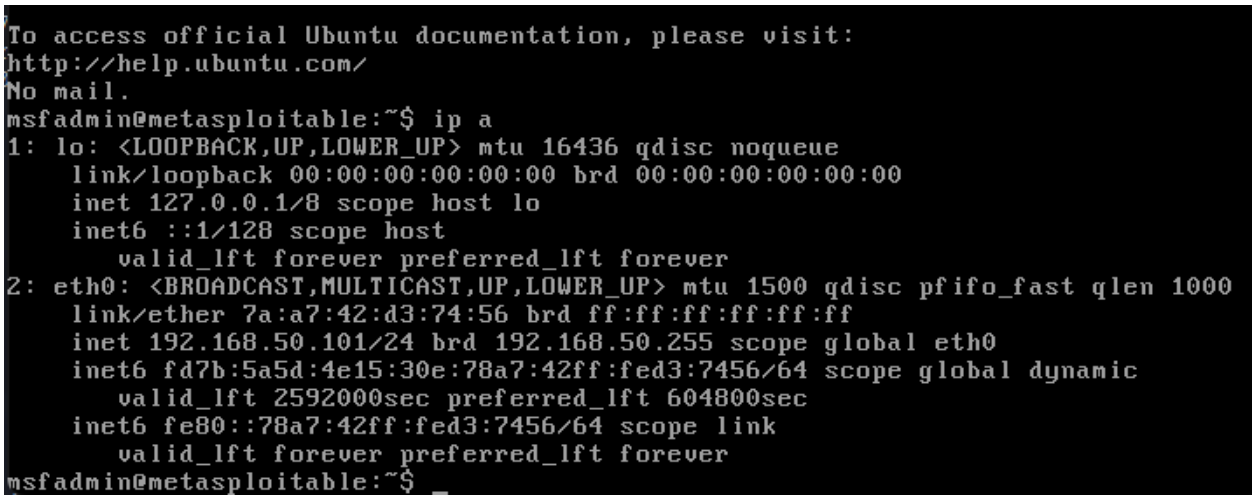
1. Configurazione del Laboratorio e Requisiti

Per l'analisi è stato utilizzato un ambiente di laboratorio composto da due macchine virtuali su una rete virtuale isolata:

- **Attaccante:** Kali Linux
- **Target:** Metasploitable

Entrambe le macchine virtuali sono state configurate in modalità **"Rete Condivisa" (NAT)**, permettendo loro di comunicare all'interno di una sottorete privata.

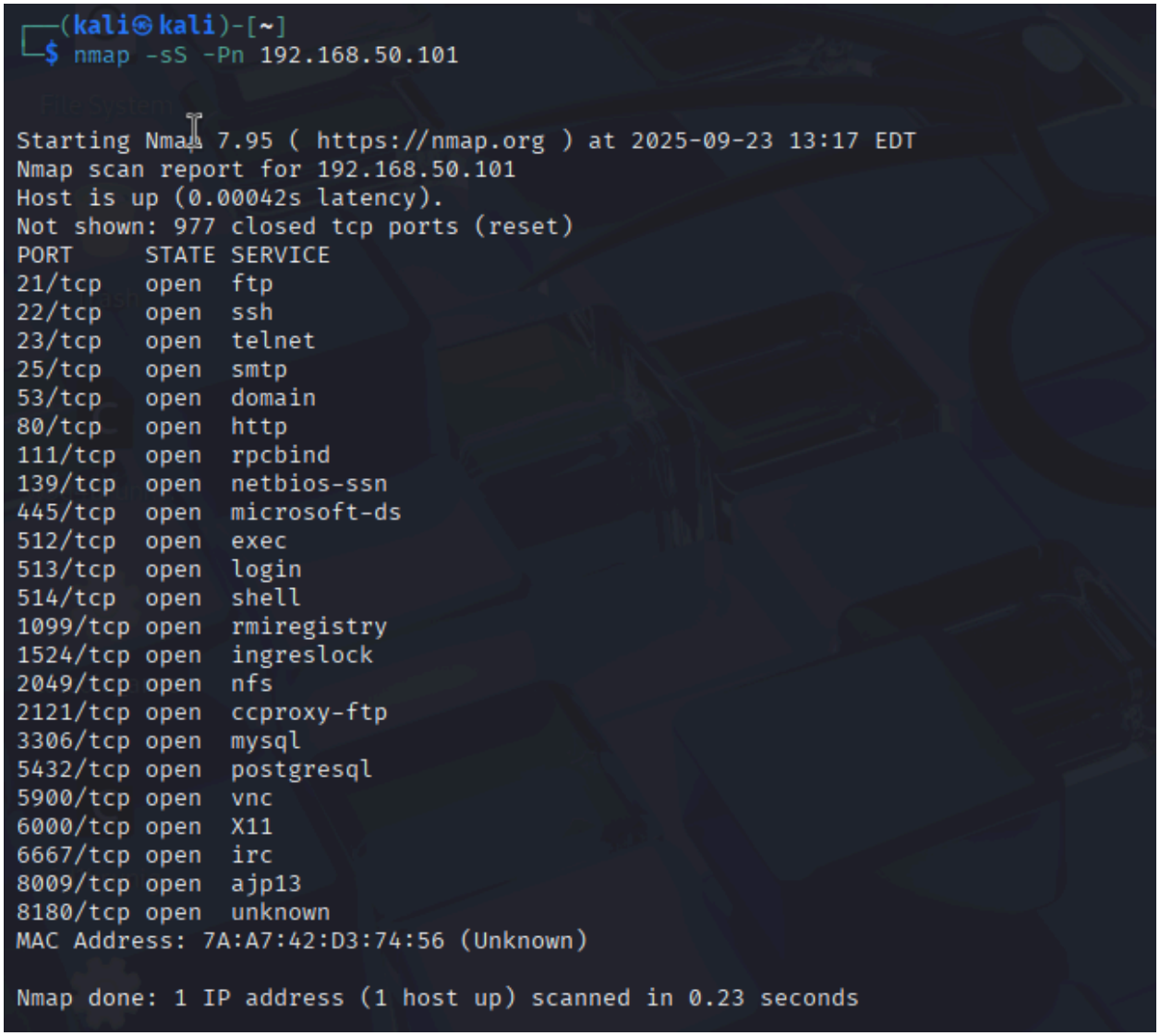
L'indirizzo IP del target, rilevato tramite il comando ip a su Metasploitable, è **192.168.50.101**.



2. Esecuzione delle Scansioni

Sono state eseguite le seguenti scansioni Nmap per raccogliere le informazioni richieste. Inizialmente, il target non rispondeva al ping, pertanto è stata utilizzata l'opzione -Pn per forzare la scansione delle porte.

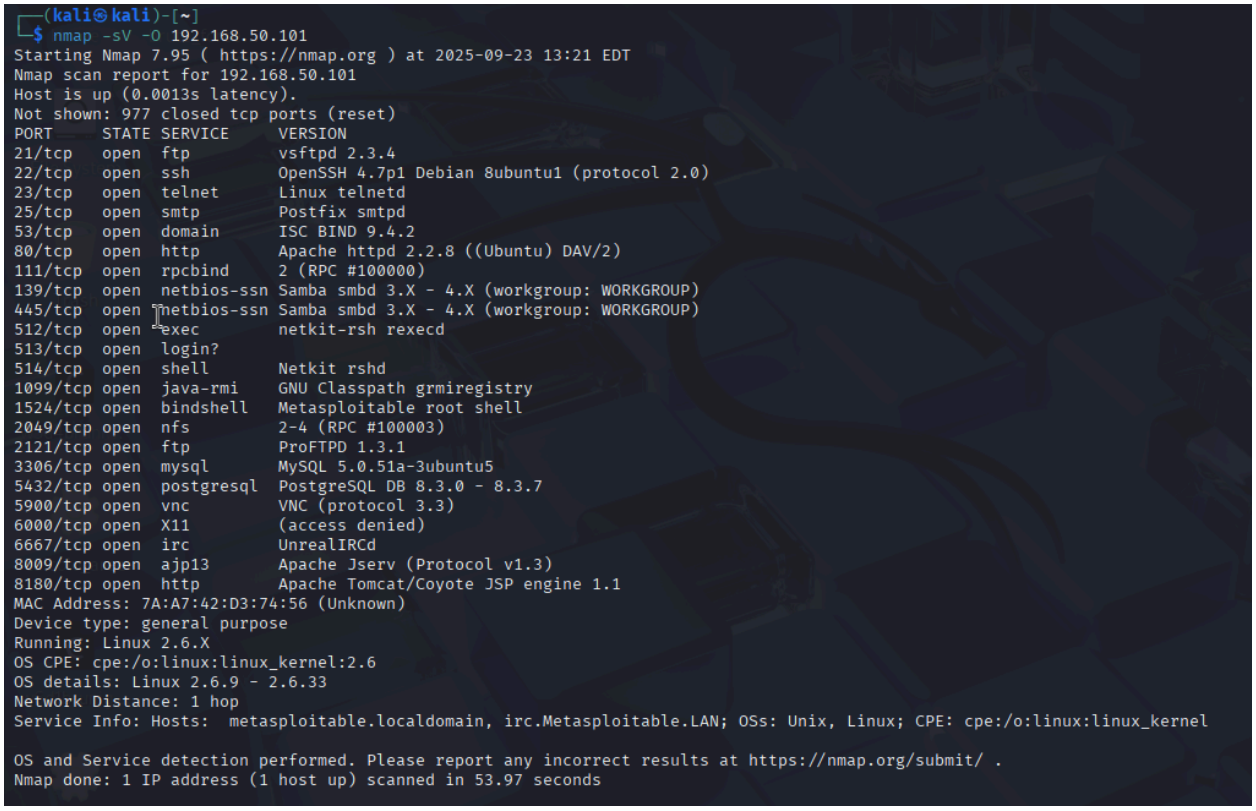
A. Scansione SYN (-sS)



Comando: nmap -sS -Pn 192.168.50.101

Risultati: La scansione SYN ha avuto successo, rilevando una vasta gamma di porte aperte e i relativi servizi. Questo tipo di scansione, noto come "half-open", è stata efficace nel mappare le porte attive del target senza completare il three-way handshake di TCP.

B. Rilevamento della Versione dei Servizi e del Sistema Operativo (-sV, -O)



Comando: nmap -sV -O 192.168.50.101

Risultati: Questa scansione ha fornito informazioni dettagliate sui servizi in esecuzione, inclusi i numeri di versione. Nmap è riuscito anche a identificare con successo il sistema operativo del target.

3. Analisi dei Risultati e Conclusioni

Differenze tra Scansione TCP Connect e SYN:

Sebbene l'esercizio richieda una scansione TCP Connect, il risultato non cambierebbe significativamente in termini di porte aperte in questo specifico ambiente. La differenza cruciale risiede nella metodologia: la **scansione SYN** è più veloce e discreta (non completa la connessione TCP), mentre la **scansione TCP Connect** è più lenta e facilmente rilevabile da un sistema di protezione, poiché crea una connessione completa per ogni porta scansionata.

Descrizione dei Servizi:

- **FTP (Porta 21):** Utilizzato per il trasferimento di file. La versione vsftpd 2.3.4 è nota per

la sua vulnerabilità ad un backdoor.
- SSH (Porta 22): Consente l'accesso remoto sicuro. La versione OpenSSH 4.7p1 può avere vulnerabilità note.
- **HTTP (Porta 80):** Server web Apache che ospita il sito predefinito di Metasploitable.
- **MySQL (Porta 3306):** Database che gestisce i dati per diverse applicazioni web.
- **Samba (Porte 139 e 445):** Permette la condivisione di file e stampanti tra sistemi Windows e Linux. Le versioni obsolete di Samba sono spesso vulnerabili a exploit noti.

Conclusioni:

L'analisi Nmap ha fornito una mappa chiara delle vulnerabilità e dei servizi esposti sul target Metasploitable. I risultati evidenziano che l'host ha numerose porte aperte e servizi con versioni obsolete, confermando che è una macchina vulnerabile e un bersaglio ideale per ulteriori test di penetrazione.