S5L2

EPICODE

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.

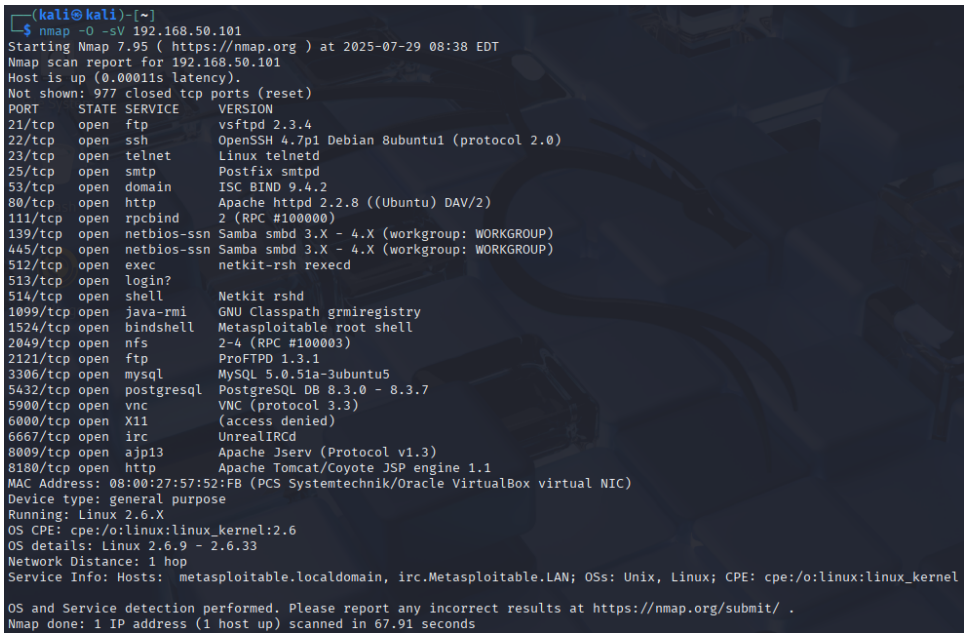
Per completare l'esercizio, ho impostato gli indirizzi IP delle macchine in modo da averli in una rete locale, in questo modo: Windows = 192.168.50.104 e Metaspoitable2 = 192.168.50.101.

Fatto questo possiamo passare alla parte delle scansioni su Metaspoitable.

Windows: Ho utilizzato il programma nmap con **-O** per l'OS fingerprint e **-sV** per identificare i programmi che girano dentro l'host e la loro versione. (Sono consapevole che sV non fa parte della richiesta, ma per comodità di digitazione, ho ricopiato la sintassi utilizzata per Metaspoitable2.

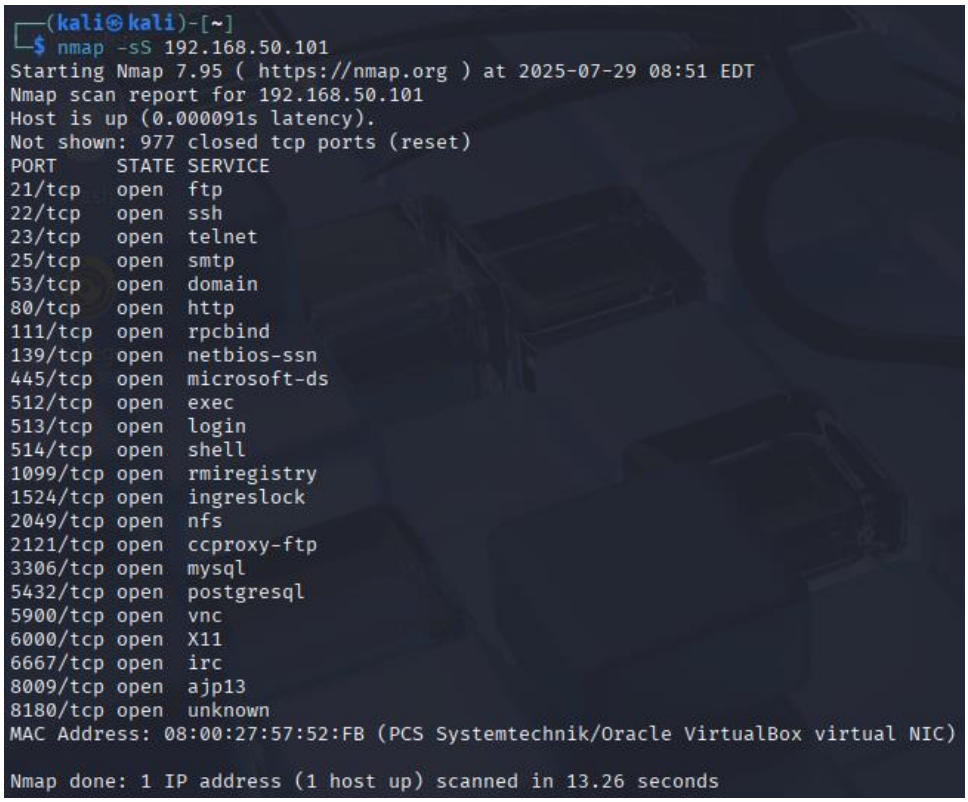
```
┌──(kali㉿kali)-[~]
└─$ nmap -O -sV 192.168.50.104
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 08:32 EDT
Nmap scan report for 192.168.50.104
Host is up (0.00013s latency).
Not shown: 982 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
7/tcp    open  echo
9/tcp    open  discard?
13/tcp   open  daytime       Microsoft Windows International daytime
17/tcp   open  qotd          Windows qotd (English)
19/tcp   open  chargen
80/tcp   open  http          Microsoft IIS httpd 10.0
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
1801/tcp open  msmq?
2103/tcp open  msrpc         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5432/tcp open  postgresql?
8009/tcp open  ajp13         Apache Jserv (Protocol v1.3)
8080/tcp open  http          Apache Tomcat/Coyote JSP engine 1.1
8443/tcp open  ssl/https-alt
MAC Address: 08:00:27:88:CE:24 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
Network Distance: 1 hop
Service Info: Host: DESKTOP-9K1O4BT; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 173.92 seconds
```

Metaspoitable: Anche qui chiaramente ho utilizzato nmap con **-O** per l'OS fingerprint e **-sV** per identificare i programmi che girano dentro l'host e la loro versione. Ho utilizzato due comandi in un'unica richiesta per comodità. Nello screen troveremo le porte aperte, il tipo di OS e la versione dei programmi che girano al suo interno.

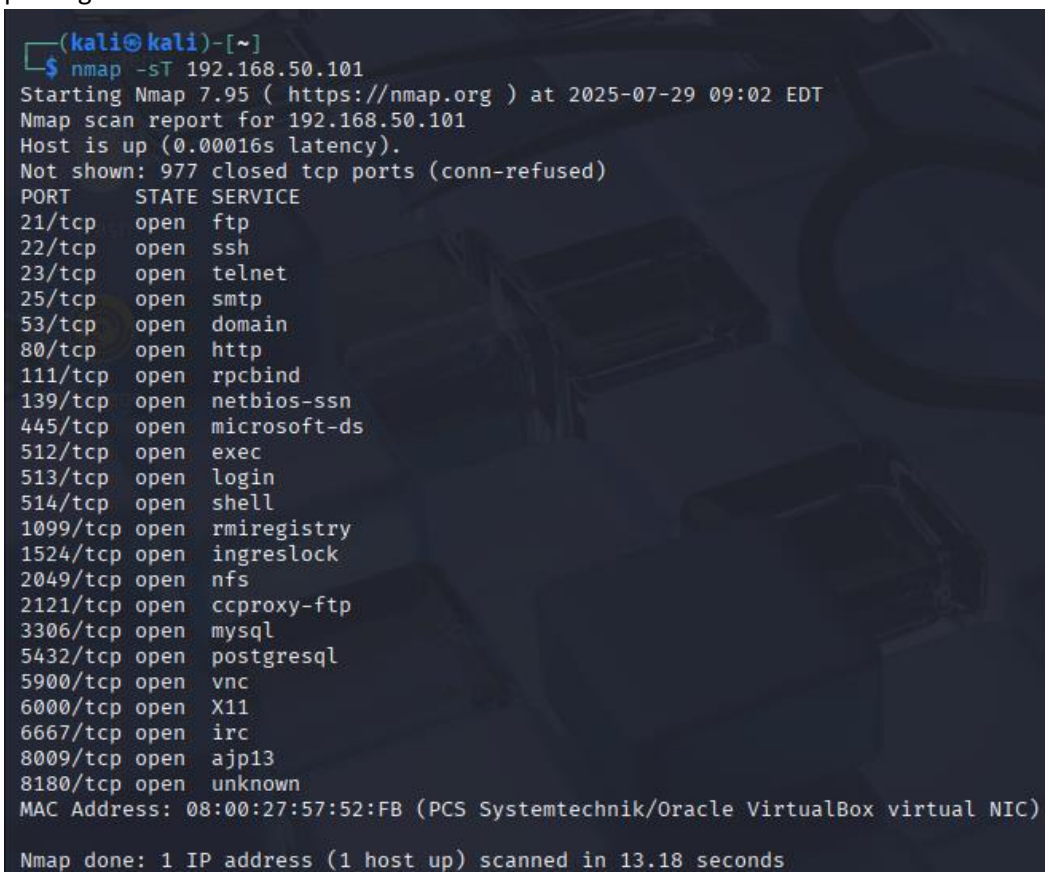


Nmap -Ss: (Metaspoitable2): Questo comando serve per la TCP SYN Scan. Questo comando è una scansione che "bussa" alla porta ma non entra. Da qui deriva il termine "Scansione stealth".

Questo comando non completa il 3-way-handshake e richiede privilegi da amministratore.



Nmap -sT (Metaspoitable2): Questo comando serve per la TCP connect scan. Questo comando è una scansione che al contrario di -sS non si limita a bussare, ma completa il 3-way-handshake e non richiede privilegi da amministratore.



Ricapitolando nel corso di questa esercitazione i comandi impiegati sono stati:

OS Fingerprinting: Utilizzando il comando nmap -O, ho ottenuto informazioni dettagliate sui sistemi operativi in esecuzione su entrambe le macchine. Questo ha permesso di confermare le versioni dei sistemi operativi e di identificare potenziali vulnerabilità associate a ciascun sistema.

TCP Connect Scan: Con il comando nmap -sT, ho eseguito una scansione delle porte, scoprendo quali porte erano aperte e quali servizi stavano girando sulla macchina in questione. Questo tipo di scansione è utile per rilevare eventuali servizi non protetti o vulnerabili.

Syn Scan: Con l'uso del comando nmap -sS, ho effettuato una scansione stealth, che permette di raccogliere informazioni senza completare il 3-way handshake, riducendo così la possibilità di essere rilevati.

Version detection: Utilizzando il comando -sV, ho ottenuto la versione dei programmi che girano nel dispositivo e il rispettivo sistema operativo. Tramite questo comando si possono ottenere informazioni dettagliate sul dispositivo.

In generale, l'esercizio mi ha permesso di mettere in pratica diverse tecniche di scansione e raccolta informazioni cruciali per questa fase in un attacco informatico.

L'accuratezza delle informazioni che ho ottenuto da Nmap dimostra l'efficacia degli strumenti di penetration testing nel determinare le caratteristiche di una rete e dei sistemi in essa contenuti, fornendo un punto di partenza fondamentale per l'analisi di sicurezza***.***