S5/L3

Tecniche di scansione con Nmap

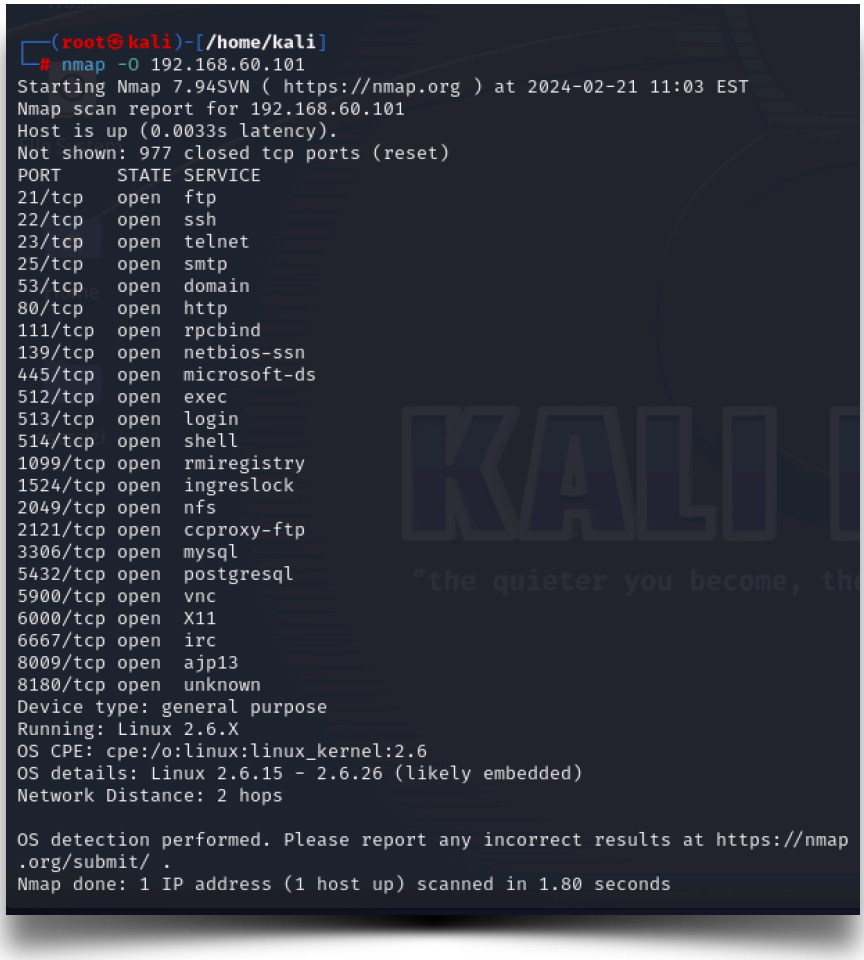
Nell'esercizio di oggi ci è stato richiesto di effettuare le seguenti scansioni con nmap sul target Metasploitable:

- 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

OS fingerprint



Abbiamo effettuato questa scansione con il comando:
nmap -O 192.168.60.101

Eseguendo questo comando, oltre a vedere le porte TCP aperte, ci fornisce anche il sistema operativo del target. (Linux 2.6.15 - 2.6.26).

Syn Scan

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.60.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 11:05 EST
Nmap scan report for 192.168.60.101
Host is up (0.0021s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

Abbiamo effettuato questa scansione con il comando:
nmap -sS 192.168.60.101

É un metodo meno invasivo in quanto una volta appurato che una porta è aperta chiude la comunicazione. Più difficile da individuare.

TCP connect

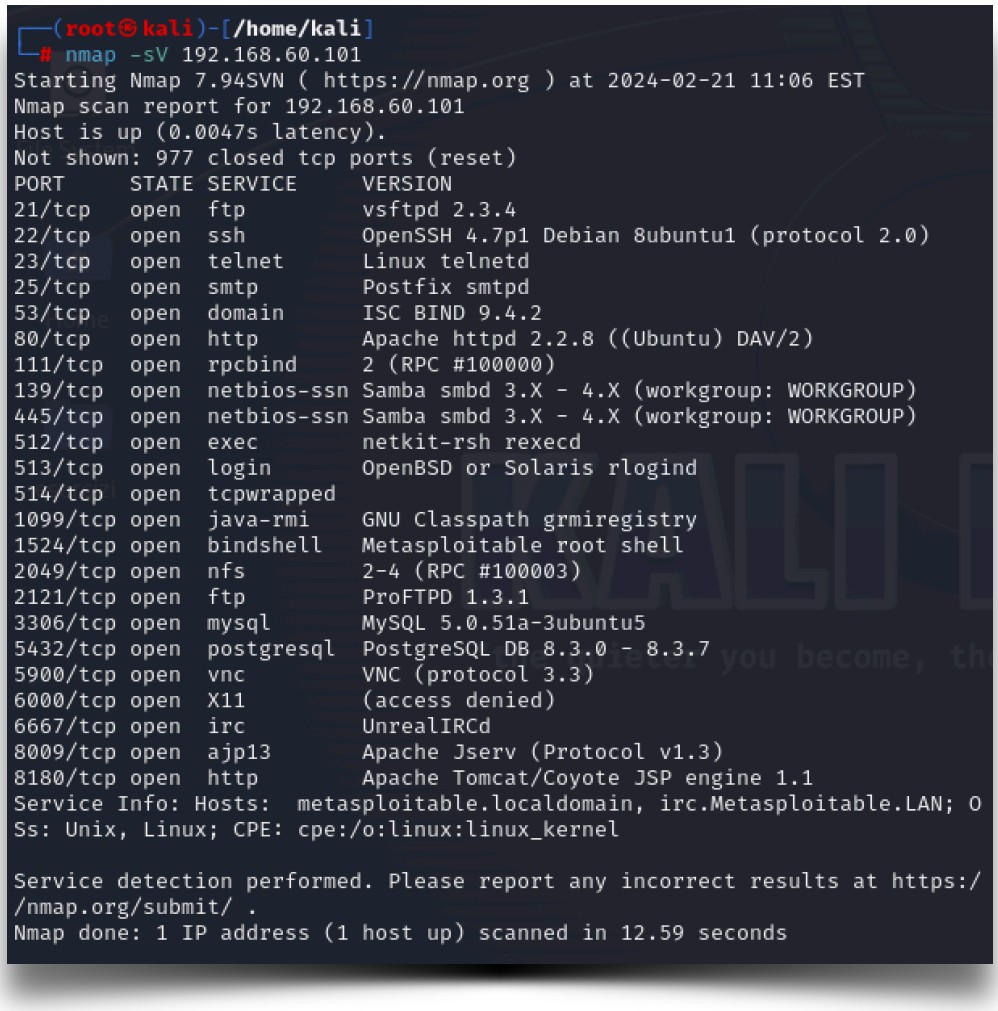
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.60.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 11:06 EST
Nmap scan report for 192.168.60.101
Host is up (0.0055s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

Abbiamo effettuato questa scansione con il comando:
nmap -sT 192.168.60.101

A differenza del Syn Scan, il TCP Connect è un metodo molto invasivo oltre a controllare se una porta è aperta crea un canale e per questo è facilmente individuabile.

Come possiamo notate non ci sono differenze tra il Syn Scan e il TCP Connect.

Version detection

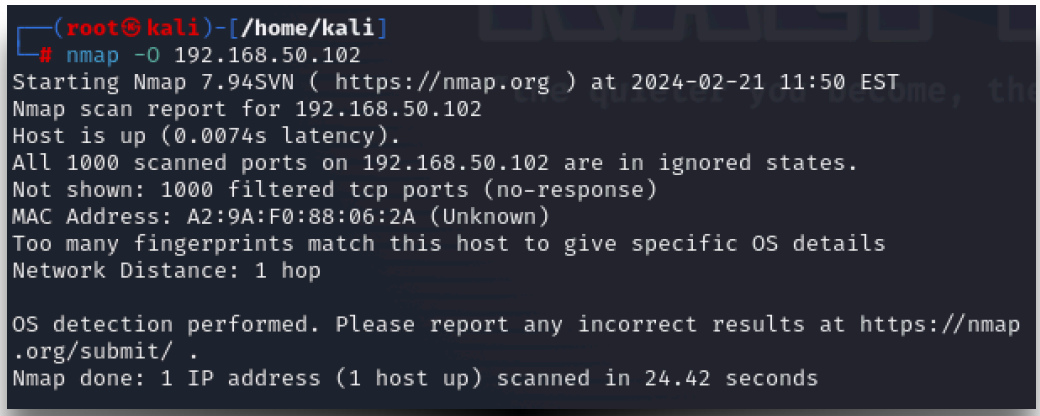


Abbiamo effettuato questa scansione con il comando:
<< nmap -sV 192.168.60.101>>

Con questa scansione possiamo identificare i servizi attivi sulle specifiche porte e le versioni.
Possiamo anche notare che rispetto alle altre scansioni i tempi aumentano notevolmente.

OS fingerprint su Windows7

Nel primo tentativo, il firewall era attivo, e non siamo riusciti ad ottenere nessuna informazione.



Mentre nel secondo tentativo, abbiamo disattivato il firewall, e come possiamo notare la scansione è avvenuta in modo corretto restituendoci le informazioni disponibili tra cui il sistema operativo Windows7.
Da notare i tempi molto più lunghi nel primo tentativo.