Tecniche di scansione con Nmap

Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

Vincenzo Colletta

L’OS Fingerprint

L'OS fingerprinting (rilevamento del sistema operativo) con Nmap è una tecnica che Nmap utilizza per cercare di determinare il sistema operativo in esecuzione su un host target. Può essere utile per identificare il sistema operativo di un server remoto durante il processo di scansione. Questo Comando lo si esegue con:

Sudo nmap -O <Ip_target>

```
┌──(fox㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.16
[sudo] password for fox:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 13:39 BST
Nmap scan report for kali.station (192.168.1.16)
Host is up (0.0010s 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
MAC Address: 22:86:43:0D:3F:C6 (Unknown)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.50 seconds
```

```
┌──(fox㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.15
[sudo] password for fox:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:48 BST
Nmap scan report for MBP-di-Tiziana.station (192.168.1.15)
Host is up (0.0024s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 3A:CC:F3:86:AA:E7 (Unknown)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_200
windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.54 seconds
```

Syn scan

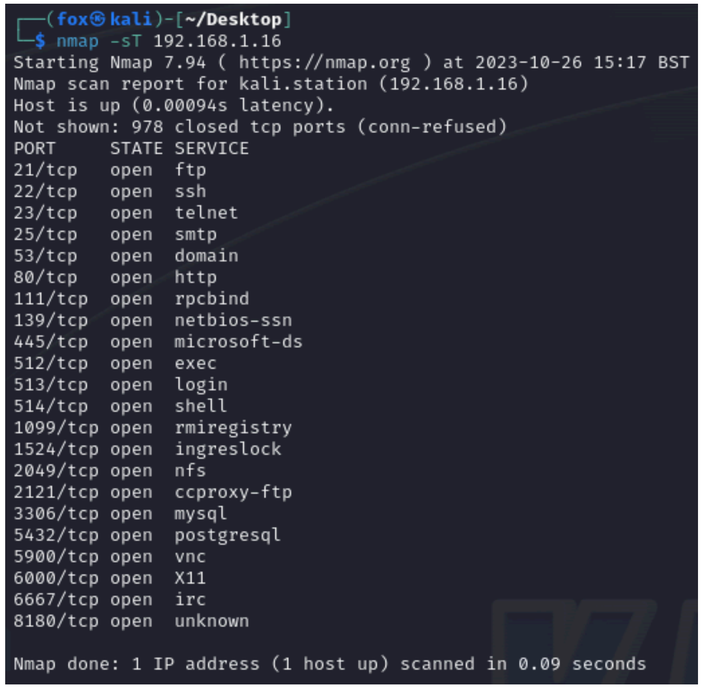
Lo scan SYN (abbreviazione di "synchronize") in Nmap è una delle tecniche di scansione più comuni e utilizzate per scoprire informazioni su una rete o su un host remoto. Questa tecnica di scansione è spesso chiamata "SYN scan" o "half-open scan". La sua funzione principale è quella di determinare quali porte di un host remoto sono aperte e disponibili per la comunicazione.

```
┌──(fox㉿kali)-[~]
└─$ sudo nmap -sS 192.168.1.15
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:56 B
Nmap scan report for MBP-di-Tiziana.station (192.168.1.15)
Host is up (0.0010s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 3A:CC:F3:86:AA:E7 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.44 seconds
```

```
┌──(fox㉿kali)-[~]
└─$ sudo nmap -sS 192.168.1.16
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:55 BST
Nmap scan report for kali.station (192.168.1.16)
Host is up (0.00069s 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
MAC Address: 22:86:43:0D:3F:C6 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

- Nmap invia un pacchetto TCP con il flag SYN impostato al server di destinazione su una specifica porta. Questo pacchetto inizia una richiesta di connessione.
- Se la porta è aperta e il server è in ascolto su quella porta, risponderà con un pacchetto TCP con il flag SYN/ACK, indicando che è pronto ad accettare la connessione.
- Nmap non completa mai la connessione, ma invia invece un pacchetto RST (reset) per interrompere la connessione. Questo è il motivo per cui il SYN scan è spesso chiamato "half-open scan". Non si stabilisce mai una connessione completa, ma si verifica solo se la porta è aperta o chiusa.

TCP connect

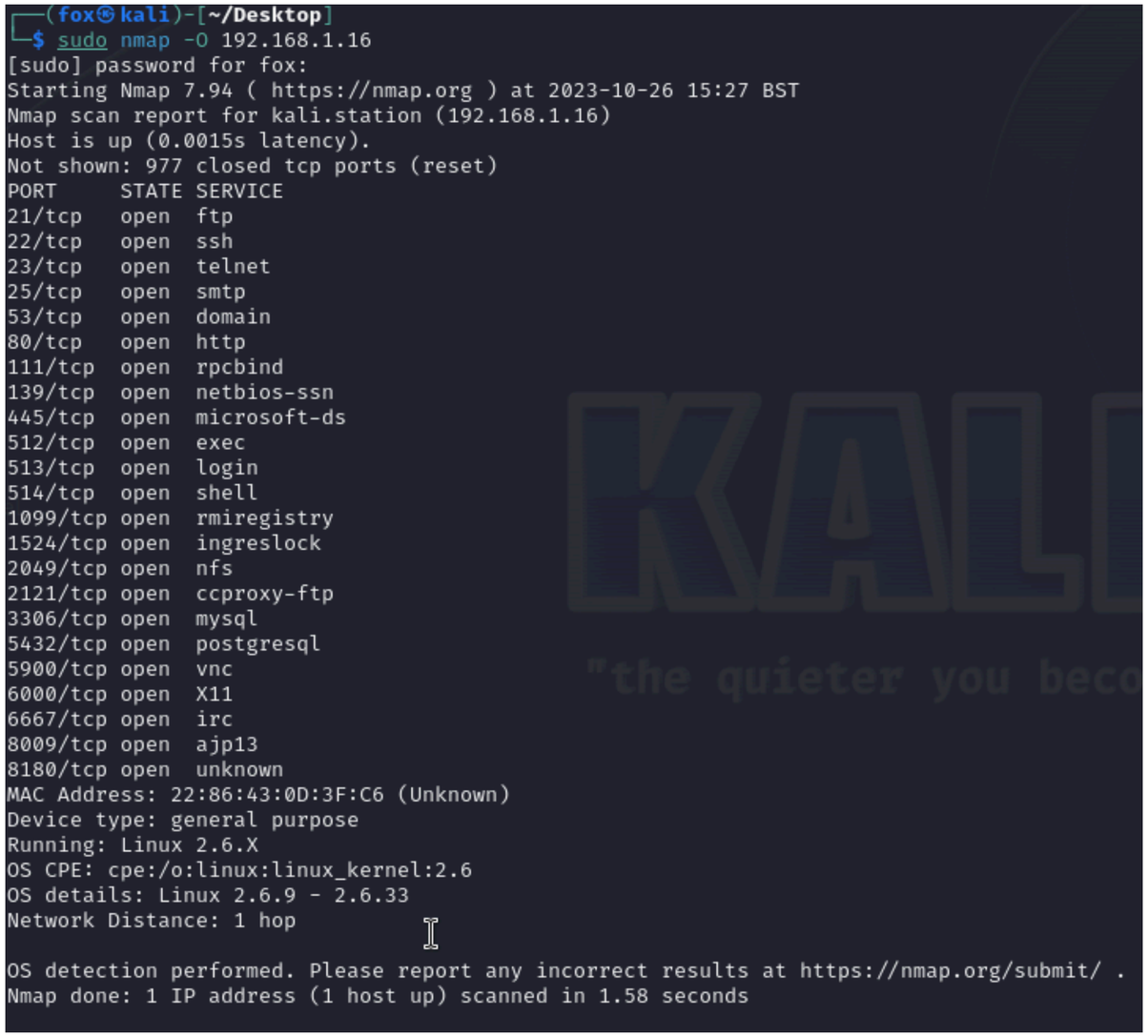


Quando si utilizza Nmap per eseguire una scansione TCP, è possibile farlo in diversi modi. Si può eseguire una scansione TCP con Nmap utilizzando il comando “*nmap -sT <IP_Target>*”
Nmap cercherà di stabilire una connessione TCP con le porte aperte su questo dispositivo e fornirà un rapporto sullo stato delle porte.

Differenze tra SYN e TCP

In sintesi, la principale differenza tra le due modalità di scansione è il grado di intrusività. La scansione TCP stabilisce effettivamente connessioni, mentre la scansione SYN invia solo pacchetti SYN e riceve risposte per determinare lo stato delle porte. La scansione SYN è spesso preferita per le scansioni di sicurezza, ma potrebbe non rilevare tutte le porte aperte in alcune configurazioni di rete o firewall.

Version Detection



Per eseguire una scansione del sistema operativo su una rete o su un host specifico utilizzando Nmap, si utilizza il comando “*nmap -O <Ip_target>*”. Questa opzione invierà pacchetti al sistema di destinazione e cercherà di determinare il sistema operativo in esecuzione.