Esercizio S2 L5 del 29/10/24 ***Daniele Paolone***

Scansione dei servizi con Nmap

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

- OS fingerprint.
- Syn Scan.
- TCP connect - trovare differenze tra i risultati della scansioni TCP connect e SYN
- Version detection.

E la seguente sul target Windows:

- OS fingerprint.

Tramite l' uso di Nmap si possono trovare varie informazioni sulla macchina metasploitable, sapendo il suo ip, che è il seguente: 192.168.1.90.

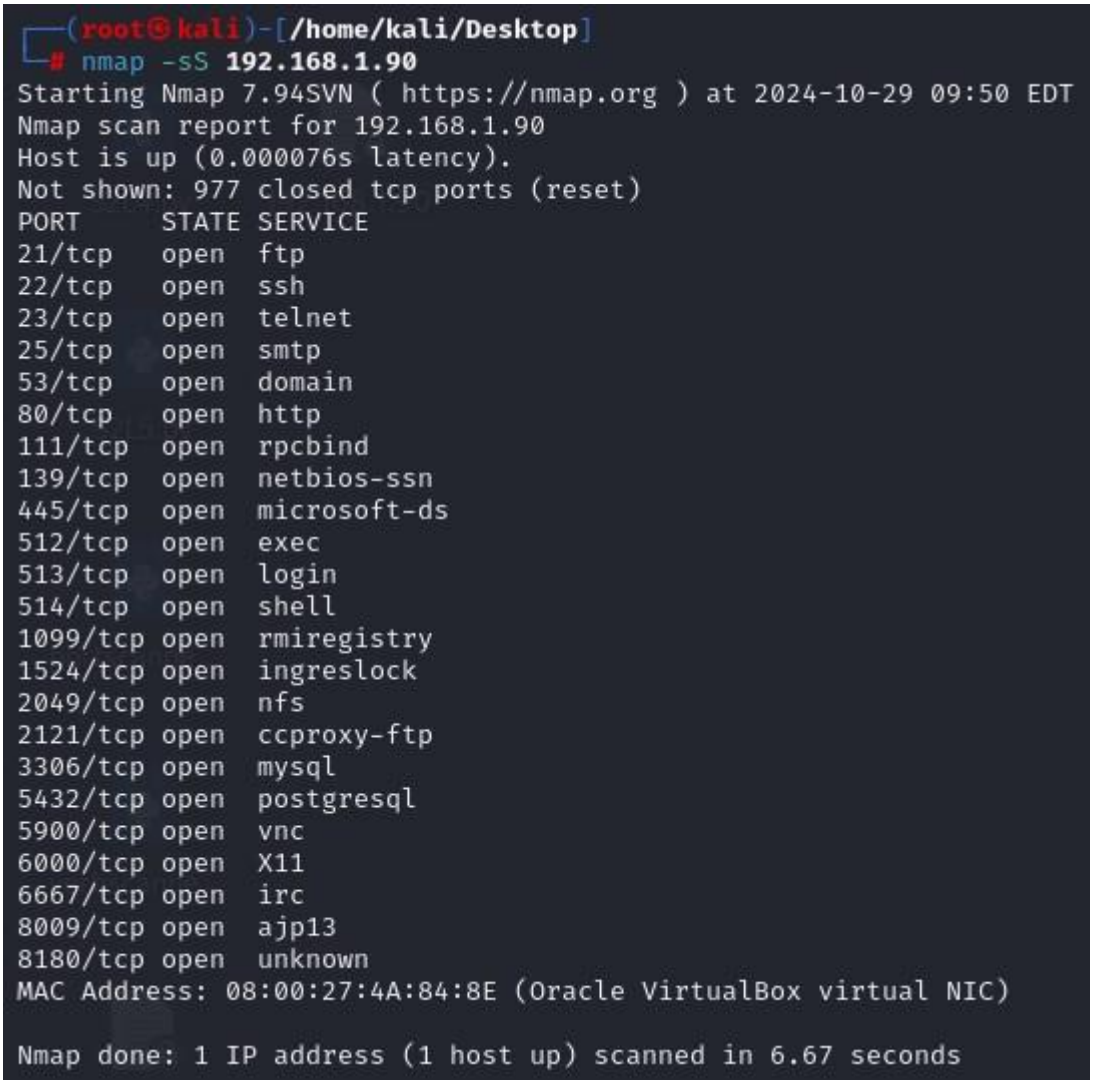
Comando *OS fingerprint*: *nmap –O 192.168.1.90*

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -O 192.168.1.90
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 09:46 EDT
Nmap scan report for 192.168.1.90
Host is up (0.00022s 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: 08:00:27:4A:84:8E (Oracle VirtualBox virtual NIC)
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 8.02 seconds
```

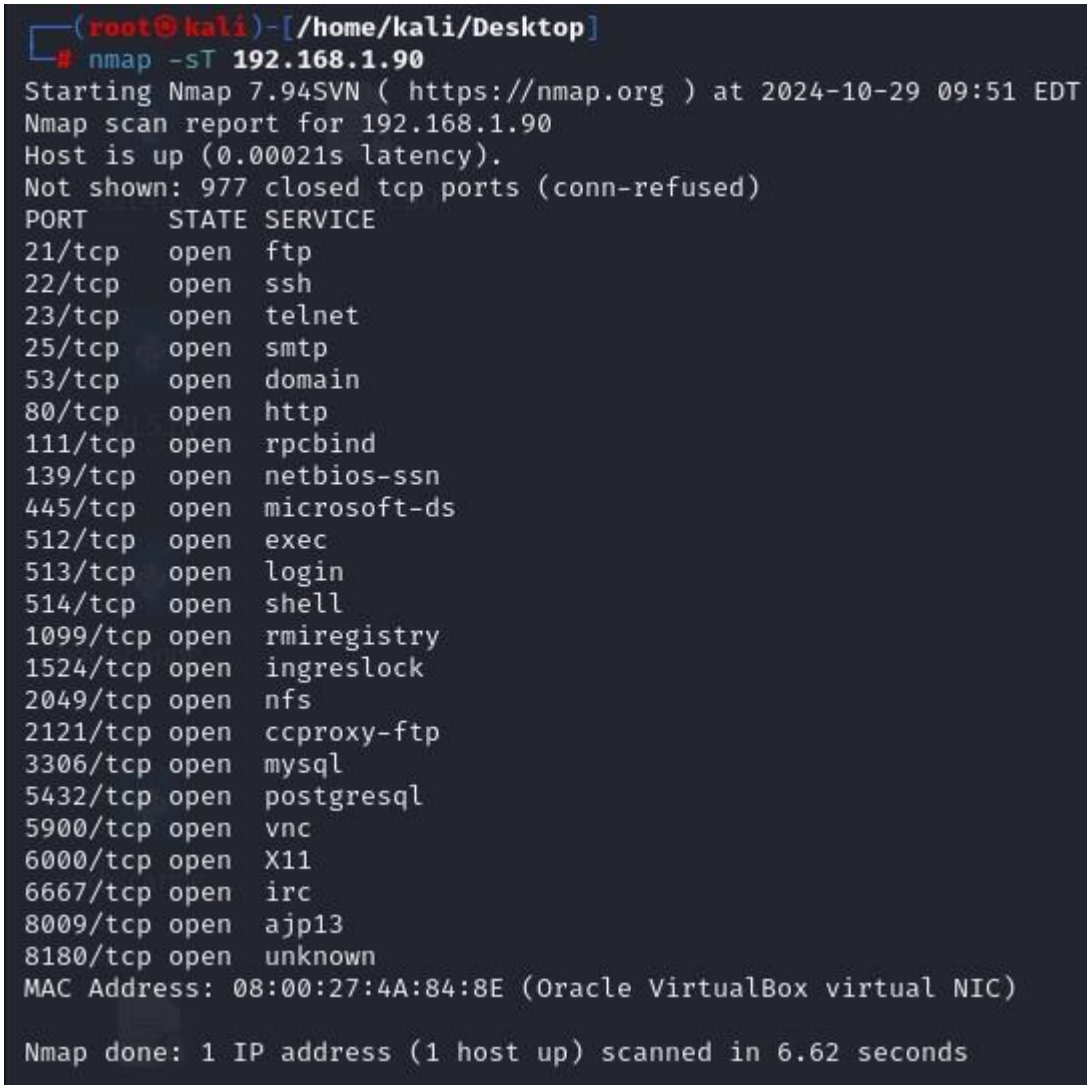
Con il comando eseguito nell' immagine soprastante possiamo capire quale OS è installato sulla macchina. Ma da questo comando ci rilascia anche informazioni per quanto riguarda le porte aperte sulla macchina, che possono essere sfruttare per effettuare un qualche tipo di attacco.

Comando *TCP Syn scan*: *nmap –sS 192.168.1.90*



Questo comando permette di vedere quali macchine sono aperte sulla macchina. Solamente non stabilisce una connessione completa attraverso il *three-way handshake.* Si limita ad inviare pacchetti SYN e ad attendere una risposta SYN/ACK (indicando una porta aperta) o RST (indicando una porta chiusa). Se riceve un SYN/ACK, invia un pacchetto RST per terminare la connessione, senza completare il *three-way handshake* TCP.

Comando *TCP Connect Scan: nmap –sT 192.168.1.90*



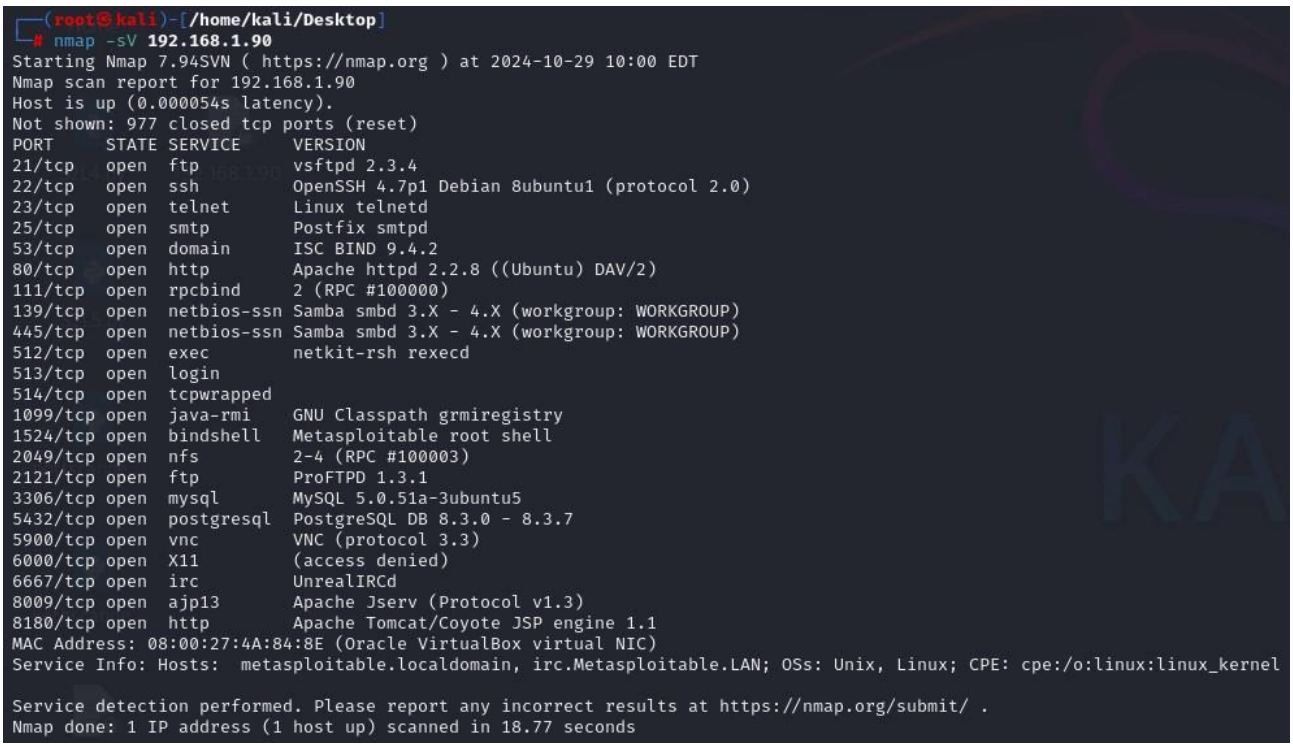
Come si può notare nell' immagine, il risultato è lo stesso del comando *TCP Syn scan*, ma in questo caso stabilisce una connessione completa attraverso il *three-way handshake*. Le diffenze tra i due comandi sta nello stabilire tipi di connessioni diverse: completa e incompleta. In base a questi due parametri differenti, questi comandi possono essere utilizzati in diverse situazioni:

- Il TCP connect scan è meno furtivo e può essere rilevato
- Il TCP Syn scan è più furtivo e può eludere i sistemi anti-intrusione

- Il TCP connect scan non richiede privilegi elevati
- Il TCP Syn scan richiede privilegi elevati

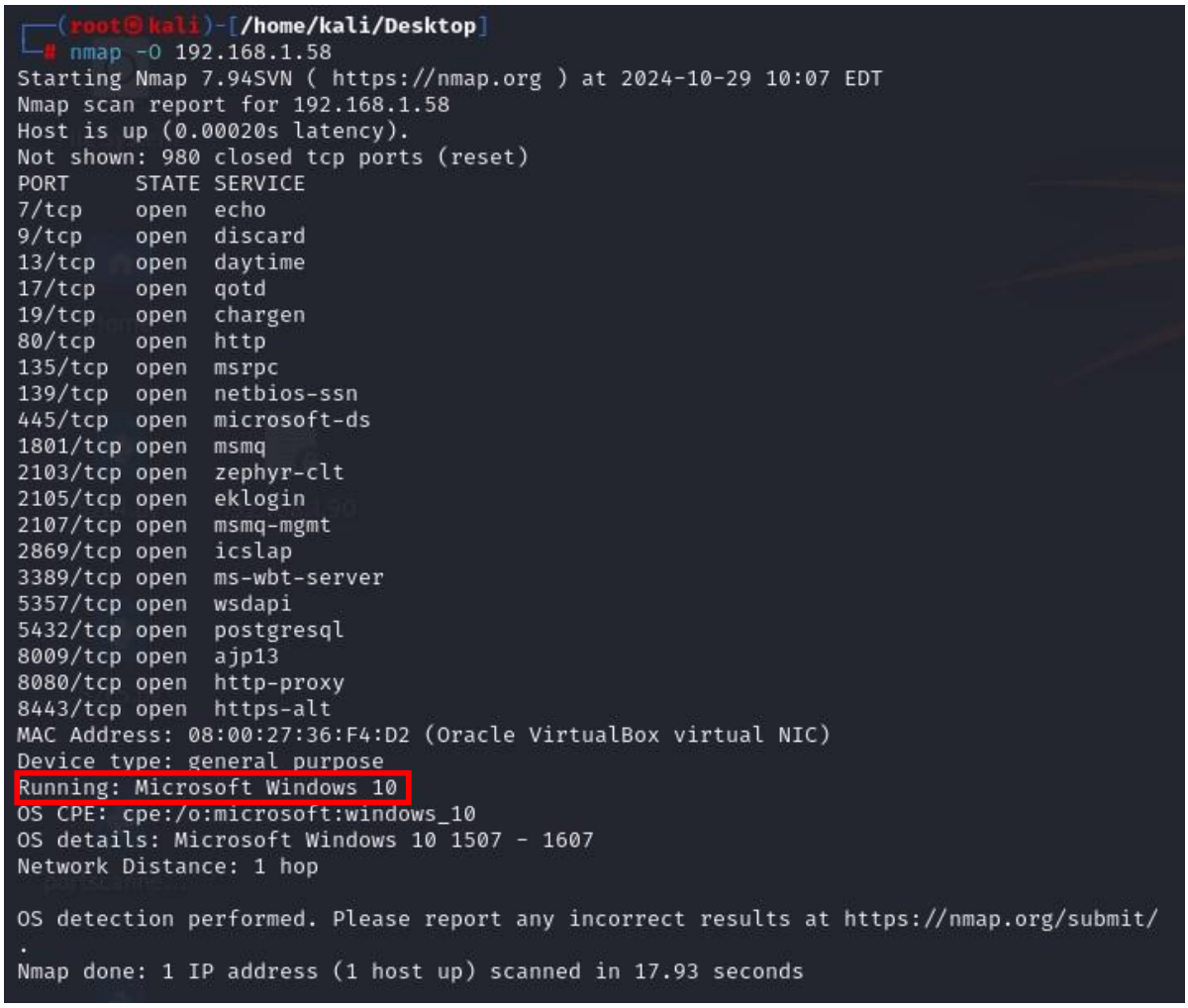
- Il TCP connect scan esegue scansioni più complete ed affidabili
- Il TCP Syn scan esegue scansioni più veloci

Comando *Banner Grabbing*: *nmap –sV 192.168.1.90*



Il comando rileva la versione dei servizi in esecuzione sulle porte aperte. Inoltre può includere dettagli come il nome del servizio, il sistema operativo, e altre informazioni utili per identificare le vulnerabilità.

Un ulteriore test è stato eseguito su un' altra macchina. Attraverso il suo indirizzo ip (192.168.1.58), con l' utilizzo di nmap, più specificatamente con il comando *OS fingerprint*, si è riuscito a capire quale sistema operativo monta.



In questo caso, come possiamo notare nell' immagine, il sistema operativo utilizzato è windows, nella versione 10.