TASK:

Eseguire le seguenti scansioni su Metasploitable:

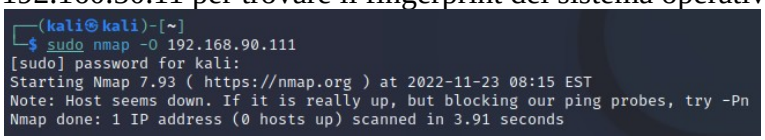
- OS fingerprint
- Syn Scan
- TCP connect
- Version detection

E le seguenti su Windows 7:

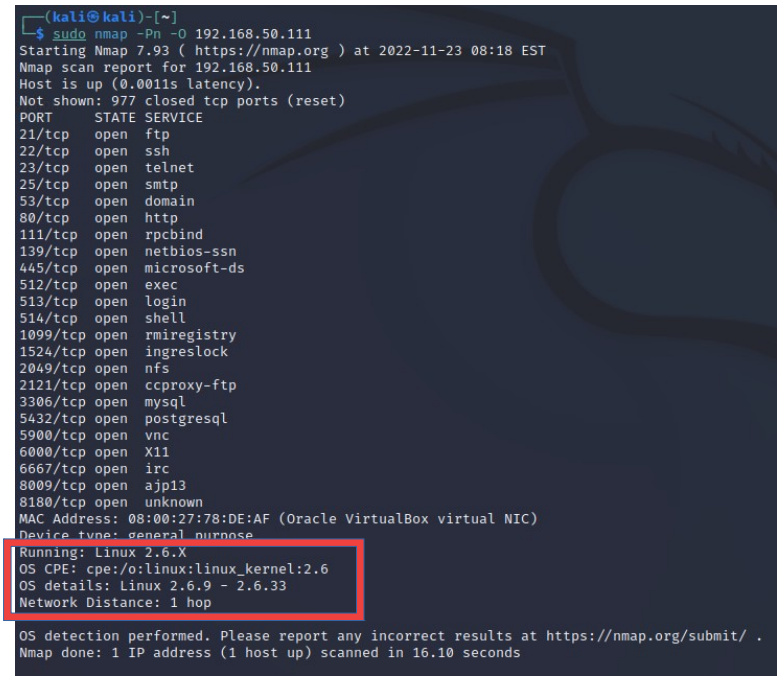
- OS fingerprint

Ho cominciato l'esercitazione lanciando da kali il comando fping -a -g 192.168.50.0/24 per trovare tutte le macchine attive sulla rete 192.168.50.*. Il risultato è stato il seguente:


Ho cominciato a scansionare l'IP 192.168.50.111. Ho lanciato per primo il comando sudo nmap -O 192.160.50.11 per trovare il fingerprint del sistema operativo associato a quell'indirizzo IP:

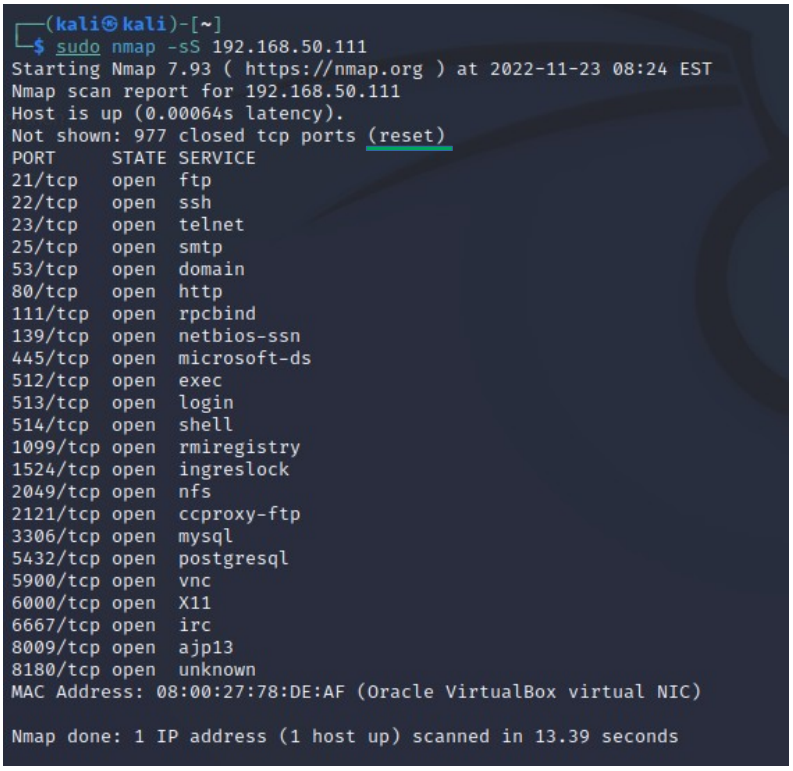



Non avendo avuto i risultati sperati ho lanciato lo stesso comando aggiungendo il -Pn:

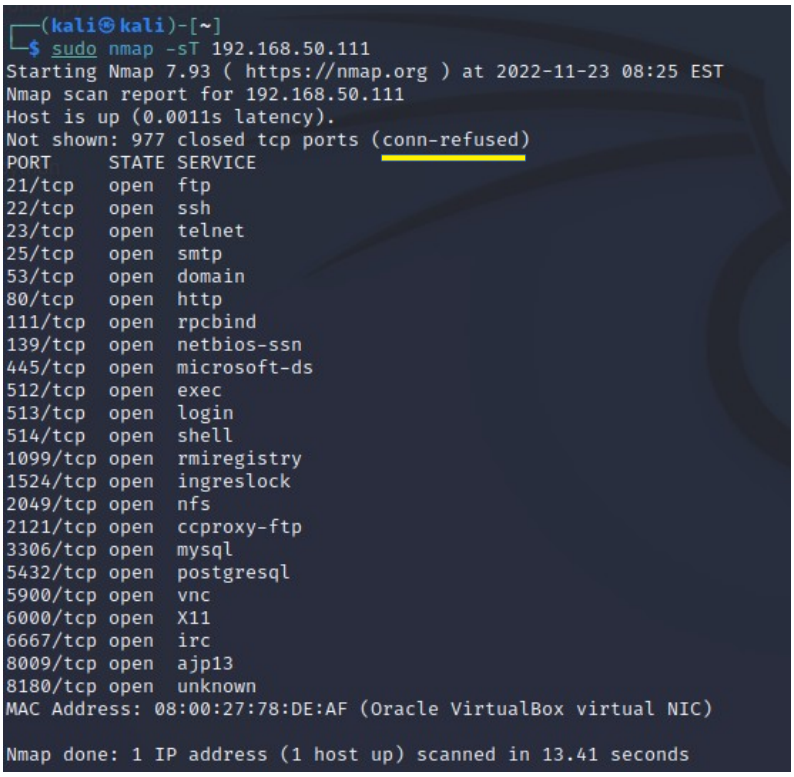



Possiamo vedere nel riquadro rosso della foto qui a sinistra il sistema operativo della macchina associata all'IP che siamo andati a scansionare e quali sono le porte attive.

Sono quindi passato a fare il SYN scan, il cui risultato può vedersi nell'immagine qui sotto:

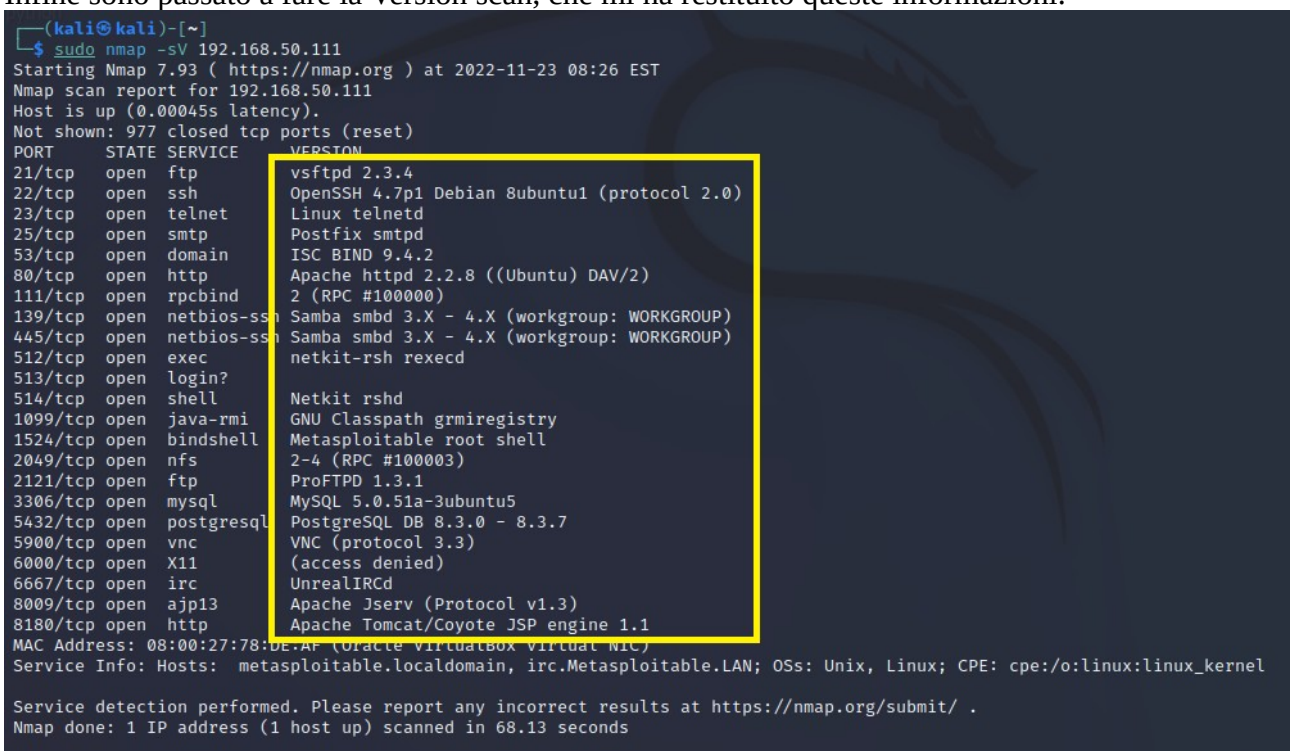



Successivamente sono quindi andato a fare il TCP scan che mi ha restituito queste informazioni:



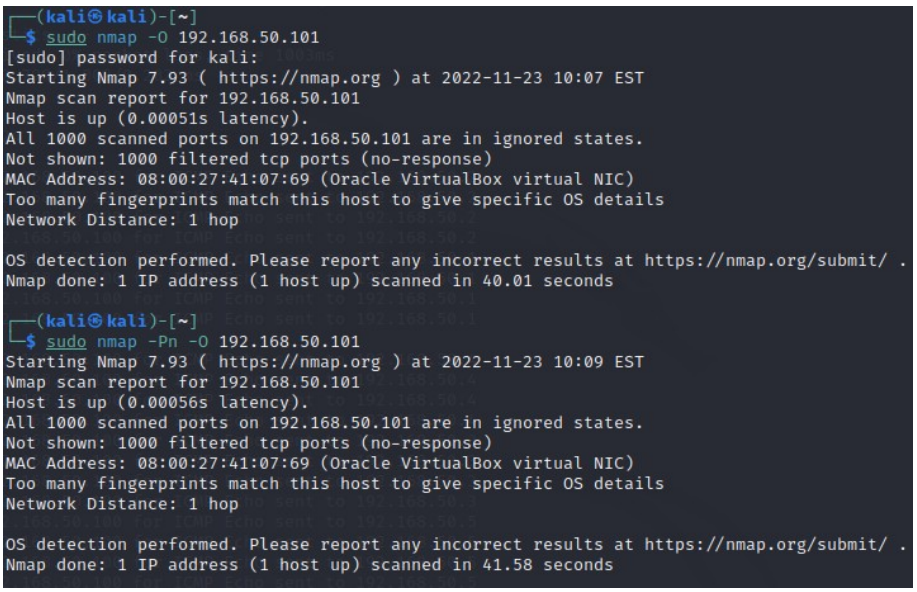

La differenza che ho notato è che mentre nel SYN scan per le porte chiuse dice che ha concluso la comunicazione con il reset (sottolineato in verde), nella scansione TCP la connessione alle porte chiuse è stata rifiutata (sottolineato in giallo)

Infine sono passato a fare la Version scan, che mi ha restituito queste informazioni:




Possiamo vedere nel riquadro giallo le versioni dei servizi attivi su Metasploitable.

A questo punto ho cominciato la scansione dell'altra macchina con OS Windows 7. Sono andato per prima cosa a controllare le policy del firewall non permettendo alcuna comunicazione in entrata. Ho provato prima il comando "sudo nmap -O 192.168.50.101" e successivamente il comando "sudo nmap -Pn -O 192.168.50.101" ottenendo i risultati visibili nell'immagine qui sotto:




cioè non sono riuscito a scoprire il sistema operavito della macchina con indirizzo IP 192.168.50.101.

Ho quindi provato a lanciare lo script suggerito nelle slide: sudo nmap 192.168.50.101 --script smb-os-discovery per vedere se fosse possibile scoprire l'OS tramite uno degli script di nmap ma come si può vedere dall'immagine neanche così ho avuto successo:

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap 192.168.50.101 --script smb-os-discovery
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 10:13 EST
Nmap scan report for 192.168.50.101
Host is up (0.00039s latency).
All 1000 scanned ports on 192.168.50.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:41:07:69 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 39.37 seconds
```

Ho quindi provato a fare lo l'OS fingerprint a T1 senza ottenere le informazioni che stavamo cercando come dimostra l'immagini qui sotto:

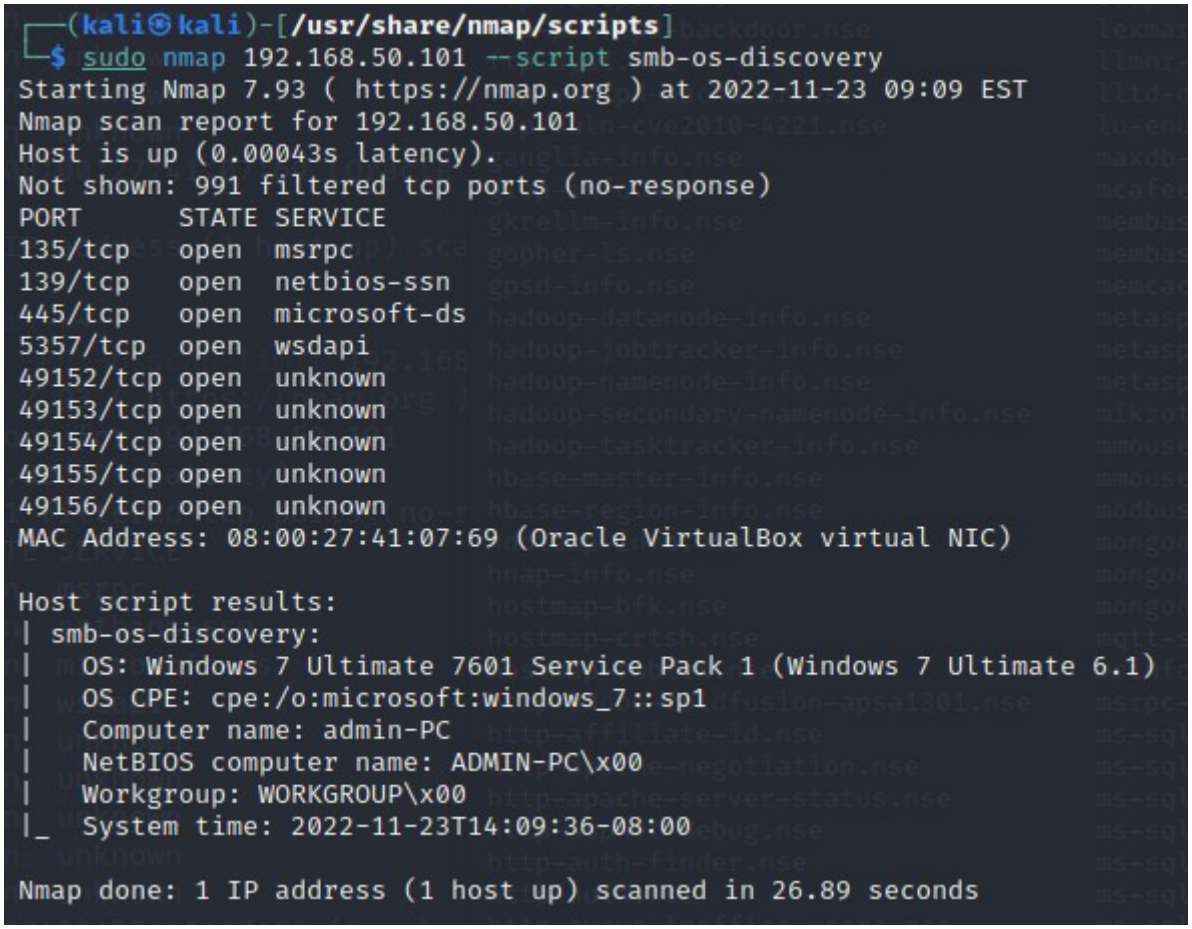
```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -O -T1 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 11:48 EST
Nmap scan report for 192.168.50.101
Host is up (0.00042s latency).
All 1000 scanned ports on 192.168.50.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:41:07:69 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
```

Andando invece a modificare le policy firewall di Windows 7 invece possiamo vedere come le scansioni restituiscono tutti i risultati che la traccia richiede. Inizialmente la scansione di tutti gli OS della rete ha restituito queste informazioni da cui non si ha la certezza della versione del sistema operativo Windows:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 09:02 EST
Nmap scan report for 192.168.50.101
Host is up (0.00094s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 08:00:27:41:07:69 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft
::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Phone 7.5
 Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop
```

Provando invece a lanciare lo script di nmap che ho utilizzato precedentemente invece abbiamo ottenuto l'informazione che cercavamo:




L'unico modo che ho trovato per cui da kali si possano fare le scansioni di windows 7 è abbassare totalmente il firewall o comunque implementare delle policy che permettano la communicazione tra le 2 macchine.