SCANSIONE DI SERVIZI CON NMAP

L'esercitazione di oggi consiste nell'effetturare le seguenti scansioni sui target **Metaspoitable** e **Windows 7.**

Entrambe le macchine sono collegate alla stessa rete interna **192.168.50.X**

SCANSIONI Metaspoitable

- **OS Fingerprint**
- **Syn Scan**
- **TCP connect**
- **Version detection**

SCANSIONI WINDOWS 7

- **OS Fingerprint**

FASE 1

Nella prima fase abbiamo impostato le macchine in rete interna:
Metaspoitable – 192.168.50.103
Windows 7 – 192.168.50.101

FASE 2

Nella seconda fase abbiamo iniziato le scansioni richeste su entrambe le macchine.
Tramite il tool presente su Kali Linux **nmap** abbiamo iniziato a scansionare Metaspoitable

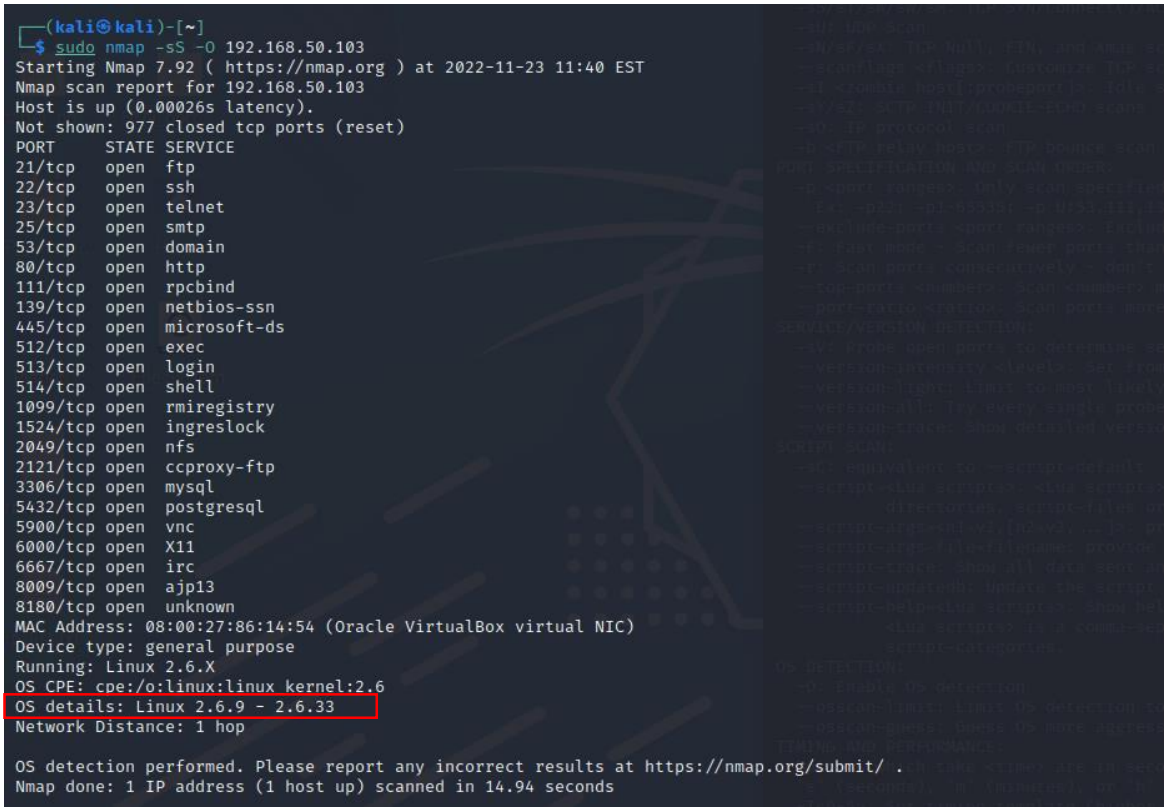
Con il comando "**nmap –sT –O 192.168.50.103**" abbiamo eseguito una scansione TCP (-sT) e la OS detection (-O) all'indirizzo IP target.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT -O 192.168.50.103
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 11:39 EST
Nmap scan report for 192.168.50.103
Host is up (0.00034s 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
MAC Address: 08:00:27:86:14:54 (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 14.87 seconds
```

Possiamo notare alla fine dei risultati anche la versione OS che è presente sulla macchina

La seconda scansione tramite il comando **“namp –sS –O 192.168.50.103”** abbiamo eseguito una scansione SYN (-sS) e la OS detection (-O) all’indirizzo IP target.



La differenza delle due scansioni anche se con risultati identici, consiste nel fatto che nella prima (TCP) la connsesisone viene stabilita e dopo rifiutata. Nella seconda (SYN) invece la connessione non viene del tutto stabilita ma viene resettata nel momento finale.

SYN

```
Not shown: 977 closed tcp ports (reset)
```

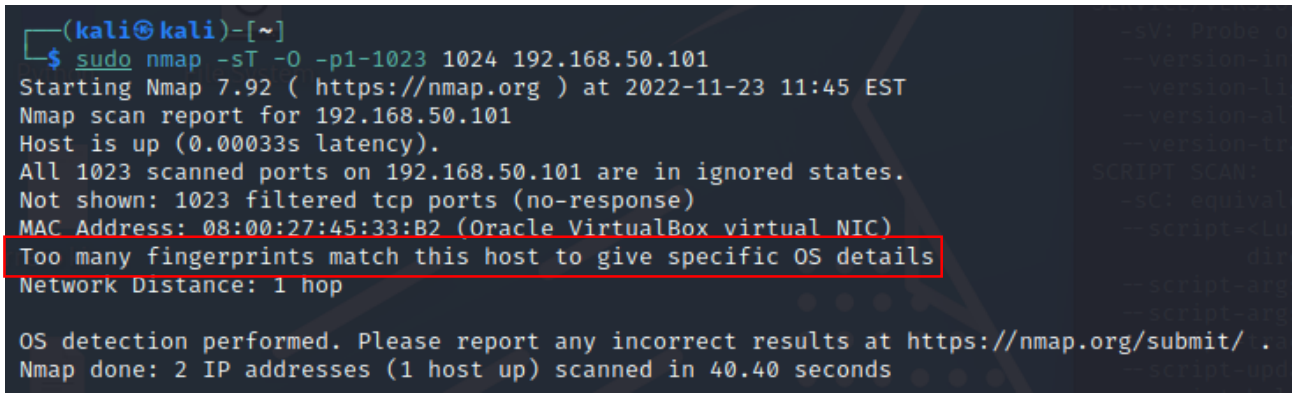
TCP

```
Not shown: 977 closed tcp ports (conn-refused)
```

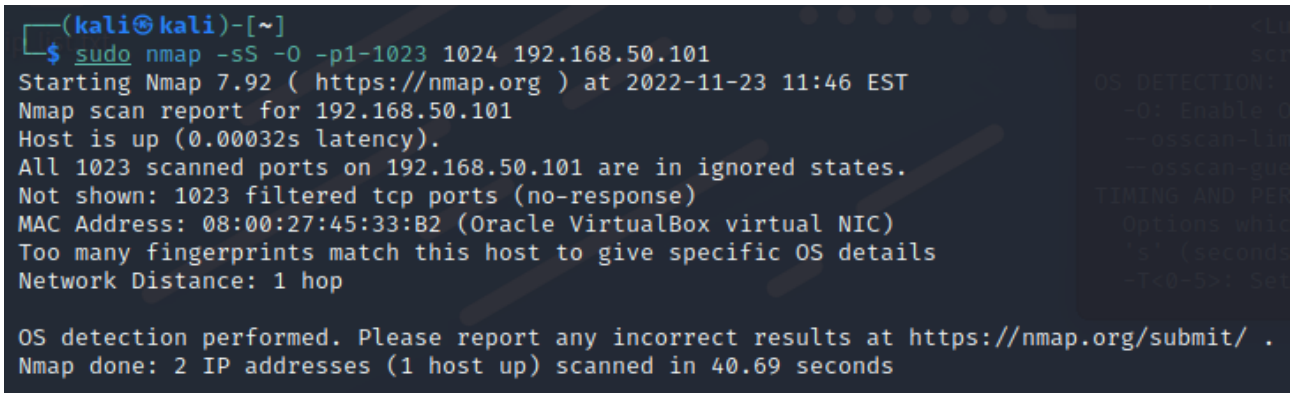
FASE 3

Nella terza fase abbiamo eseguito una scansione verso Windows 7

Utilizzando il comando “nmap –sT –O 192.168.50.101” abbiamo eseguito una scansione TCP (-sT) e la OS detection (-O) all’indirizzo IP target.



La seconda scansione tramite il comando **“namp –sS –O 192.168.50.101”** abbiamo eseguito una scansione SYN (-sS) e la OS detection (-O) all’indirizzo IP target.



Purtroppo in entrambi i casi non siamo riusciti a visualizzare OS e le porte presenti sulla macchina. La differenza tra i due dispositivi scansionati è la presenza di un **Firewall** che limita le connessioni in ingresso in ambiente Windows.

Abbiamo provato ad aggirare questo ostacolo.
Utilizzando il comando "**-sS –O –T2 –mtu 8 –f –vv –p80 192.168.50.101**" abbiamo eseguito una scansione SYN (-sS) e la OS detection (-O) all'indirizzo IP target. Aggiungendo –T2 abbiamo rallentato il numero di richieste fatte verso Windows 7. Com --mtu 8 – f abbiamo frammentato i pacchetti per essere meno "riconoscibili" dal firewall (--mtu 8 associato a –f come specificato nel help di nmap).
-vv invece ci è servito per ricevere piu informazioni in output da nmap (come la porta 80 che risulta chiusa e non piu solo filtrata).
-p80 è servito per scansionare la porta 80 che di solito rimane aperta, anche con il firewall attivo per i protocolli HTML

```
-f; --mtu <val>: fragment packets (optionally w/given MTU)
-v: Increase verbosity level (use -vv or more for greater effect)
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -O -T2 --mtu 8 -f -vv -p80 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 11:57 EST
Initiating ARP Ping Scan at 11:57
Scanning 192.168.50.101 [1 port]
Completed ARP Ping Scan at 11:57, 0.41s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:57
Completed Parallel DNS resolution of 1 host. at 11:57, 13.00s elapsed
Initiating SYN Stealth Scan at 11:57
Scanning 192.168.50.101 [1 port]
Completed SYN Stealth Scan at 11:57, 0.40s elapsed (1 total ports)
Initiating OS detection (try #1) against 192.168.50.101
Retrying OS detection (try #2) against 192.168.50.101
Nmap scan report for 192.168.50.101
Host is up, received arp-response (0.00033s latency).
Scanned at 2022-11-23 11:57:40 EST for 6s

PORT   STATE  SERVICE REASON
80/tcp closed http    reset ttl 128
MAC Address: 08:00:27:45:33:B2 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=7.92%E=4%D=11/23%OT=%CT=80%CU=33772%PV=Y%DS=1%DC=D%G=N%M=080027%TM=637E510A%P=x86_64-pc-linux-gnu)
SEQ(CI=I%II=I)
T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)
T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 1 hop

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.80 seconds
           Raw packets sent: 14 (1.740KB) | Rcvd: 14 (1.672KB)
```