Consegna S5-L3

Nmap su metasploitable

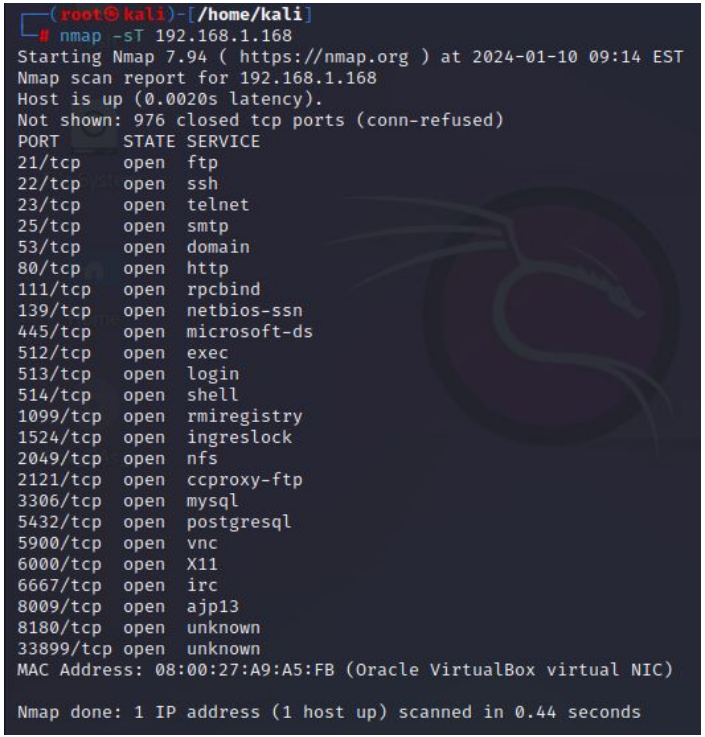
Con il comando nmap -O riusciamo a vedere che tipo di OS abbiamo nel dispositivo ispezionando i pacchetti di risposta ricevuti.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.1.168
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-10 09:07 EST
Nmap scan report for 192.168.1.168
Host is up (0.0025s latency).
Not shown: 976 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
33899/tcp open  unknown
MAC Address: 08:00:27:A9:A5:FB (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 1.97 seconds
```

Nmap su metasploitable

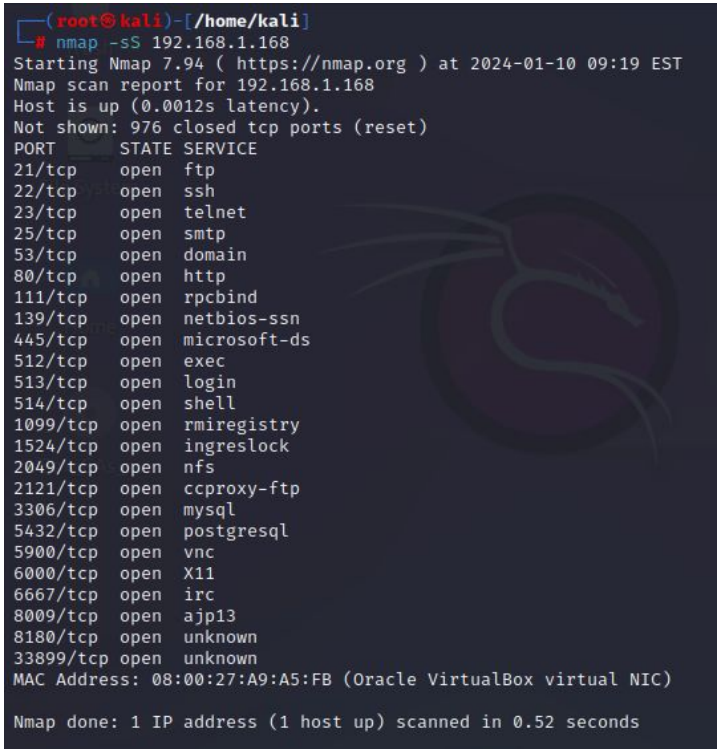
Con il comando nmap -sT si effettua uno scan invasivo. Nmap completa il 3-way-handshake, creando così il canale. Recupera info sullo stato della porta, ma crea più «rumore a livello network» ed è quindi più identificabile.



Nmap su metasploitable

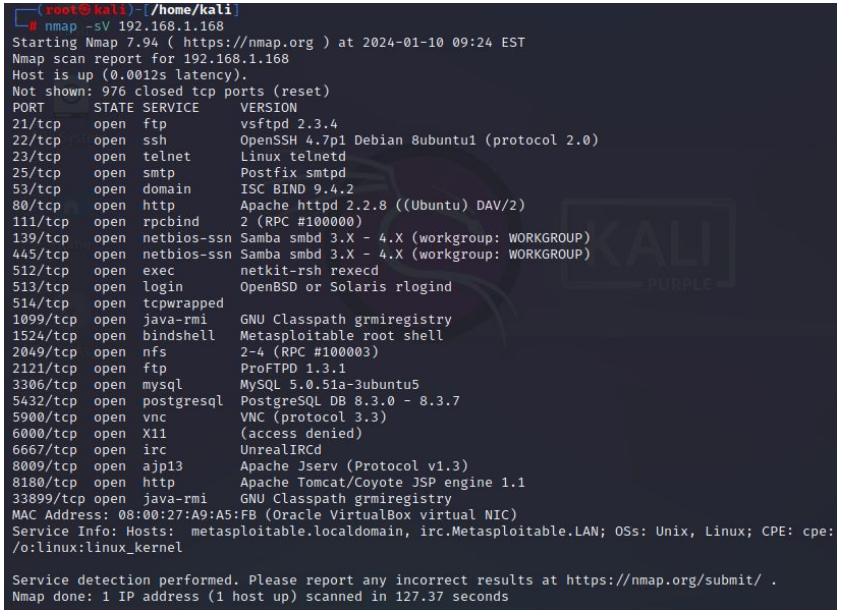
Con il comando nmap -sS Nmap non completa il 3-way-handshake, ma chiude la comunicazione inviando un pacchetto RST (reset). Tuttavia, riesce a recuperare informazioni sullo stato della porta e crea meno «rumore» a livello di rete.

Come si può notare nel mio caso, tra questa slide e la precedente non ci sono differenze.



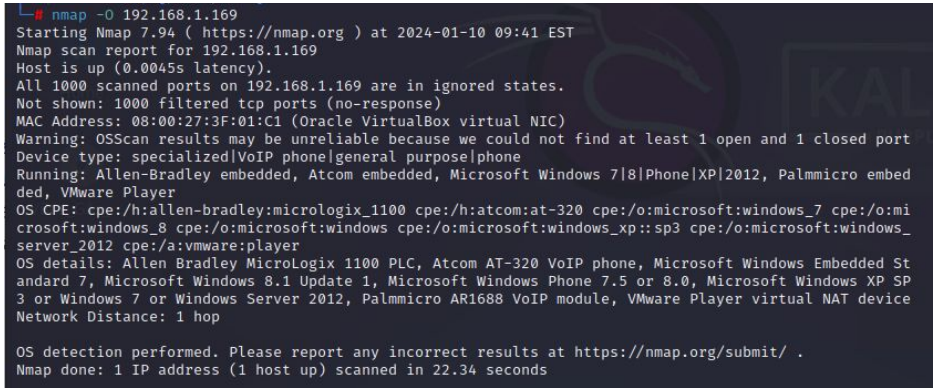
Nmap su metasploitable

Con il comando nmap -sV è il banner grabbing dove consiste nel recupero delle informazioni esposte da un determinato software o servizio, come la versione e il nome nome del software / servizio stesso.



Nmap su windows 7

Su windows 7 ci sono dei problemi con il firewall e quindi bene aggiungere come eccezione la vostra macchina kali. Faccio vedere entrambe le situazioni.



```
└─# nmap -O 192.168.1.169
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-10 09:41 EST
Nmap scan report for 192.168.1.169
Host is up (0.0045s latency).
All 1000 scanned ports on 192.168.1.169 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:3F:01:C1 (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: specialized|VoIP phone|general purpose|phone
Running: Allen-Bradley embedded, Atcom embedded, Microsoft Windows 7|8|Phone|XP|2012, Palmmicro embedded, VMware Player
OS CPE: cpe:/h:allen-bradley:micrologix_1100 cpe:/h:atcom:at-320 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player
OS details: Allen Bradley MicroLogix 1100 PLC, Atcom AT-320 VoIP phone, Microsoft Windows Embedded Standard 7, Microsoft Windows 8.1 Update 1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, Palmmicro AR1688 VoIP module, VMware Player virtual NAT device
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 22.34 seconds
```

Nmap su windows 7