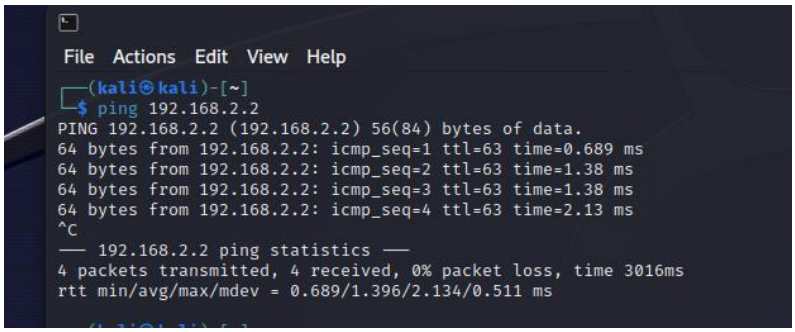
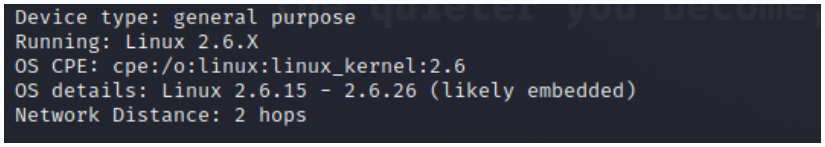
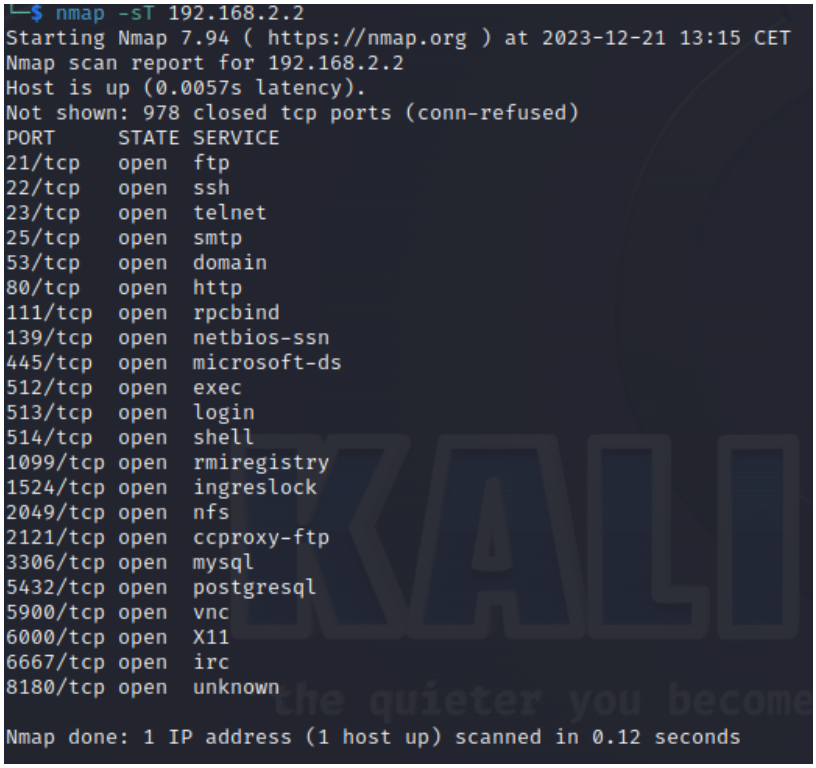
Inizio dal target meta e verifico prima se l'host è raggiungibile con il ping.



Procedo con l'OS fingerprint e così ottengo le informazioni sul sistema operativo



Successivamente con la scansione TCP connect verifico le porte aperte e relativi servizi. Questo tipo di scansione stabilisce una connessione con il target completando il three-way-handshake, lasciando tracce nel suo log.



Una SYN scan mi dà gli stessi risultati, ma è più furtiva perché il nostro sistema non conclude in three-way-handshake, dato che chiude la connessione una volta appurato se la porta è chiusa o aperta.

```
└─$ sudo nmap -sS 192.168.2.2
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-21 13:16 CET
Nmap scan report for 192.168.2.2
Host is up (0.0017s latency).
Not shown: 978 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
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

Infine la version detection che è una tcp connect, ma che in aggiunta mi dà informazioni più dettagliate sulle versioni dei servizi offerti

```
└─$ nmap -sV 192.168.2.2
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-21 13:21 CET
Nmap scan report for 192.168.2.2
Host is up (0.0010s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          vsftpd 2.3.4
22/tcp   open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet?
25/tcp   open  smtp?
53/tcp   open  domain       ISC BIND 9.4.2
80/tcp   open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind      2 (RPC #100000)
139/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell?
1099/tcp open  java-rmi     GNU Classpath grmiregistry
1524/tcp open  bindshell    Metasploitable root shell
2049/tcp open  nfs          2-4 (RPC #100003)
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql?
5432/tcp open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc          VNC (protocol 3.3)
6000/tcp open  X11          (access denied)
6667/tcp open  irc          UnrealIRCd
8180/tcp open  unknown
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 196.35 seconds
```

Ora tocca al target Windows. Inizio con un ping.

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.3.2
PING 192.168.3.2 (192.168.3.2) 56(84) bytes of data.
64 bytes from 192.168.3.2: icmp_seq=1 ttl=127 time=1.17 ms
64 bytes from 192.168.3.2: icmp_seq=2 ttl=127 time=1.81 ms
64 bytes from 192.168.3.2: icmp_seq=3 ttl=127 time=0.680 ms
64 bytes from 192.168.3.2: icmp_seq=4 ttl=127 time=2.16 ms
^C
── 192.168.3.2 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 0.680/1.454/2.156/0.570 ms
```

L'OS fingerpint non mi dà informazioni precise sull'OS del target ma ne stima diversi

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.3.2
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-21 13:42 CET
Nmap scan report for 192.168.3.2
Host is up (0.0010s latency).
All 1000 scanned ports on 192.168.3.2 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.21 seconds
```

Neppure con altri metodi di os fingerprint o script riesco ad ottenere informazioni precise.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --osscan-limit 192.168.3.2
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-21 13:49 CET
Nmap scan report for 192.168.3.2
Host is up (0.00078s latency).
All 1000 scanned ports on 192.168.3.2 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 21.36 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap --osscan-guess 192.168.3.2
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-21 13:50 CET
Nmap scan report for 192.168.3.2
Host is up (0.00079s latency).
All 1000 scanned ports on 192.168.3.2 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 21.37 seconds

┌──(kali㉿kali)-[~]
└─$ nmap 192.168.3.2 --script smb-os-discovery
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-21 13:53 CET
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.15 seconds
```

Le scansioni tcp connect e sys non riescono perché nmap rileva l'host in down. Credo sia il firewall di windows che blocca questo tipo di connessioni in entrata.