Nmap scan su Meta e Windows 7

Metasploitable: (192.168.32.101)

Avendo una connessione tra Kali linux e metasploitable, ho lanciato diversi scan sul host Metasploitable, ecco la informazione raccolta:

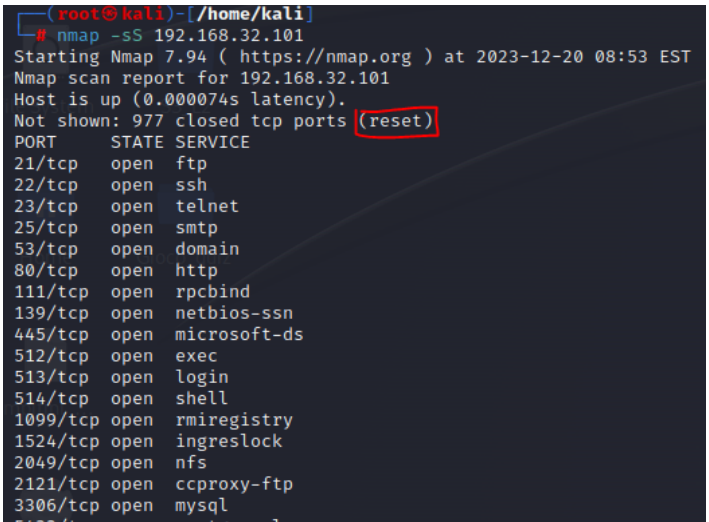
OS e MAC address e network distance:

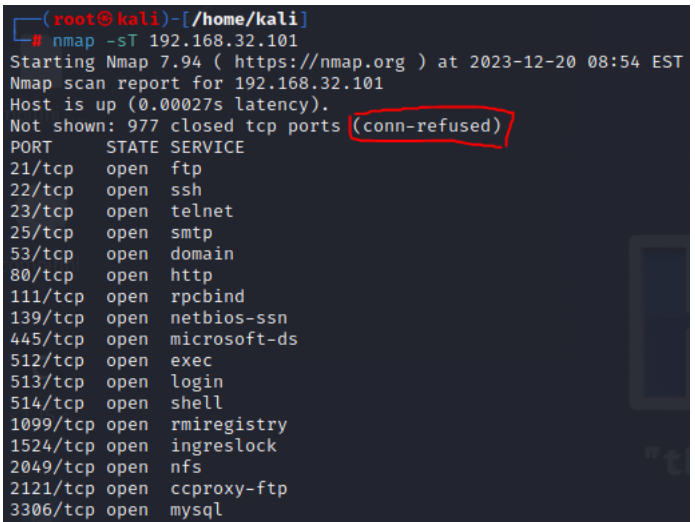
- MAC Address: 08:00:27:70:77:CA (Oracle VirtualBox virtual NIC)
- Device type: general purpose
- Running: Linux 2.6.X
- OS CPE: cpe:/o:linux:linux_kernel:2.6
- OS details: Linux 2.6.9 - 2.6.33
- Network Distance: 1 hop

Porte aperte:
21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8009, 8180

Syn scan and TCP connect:

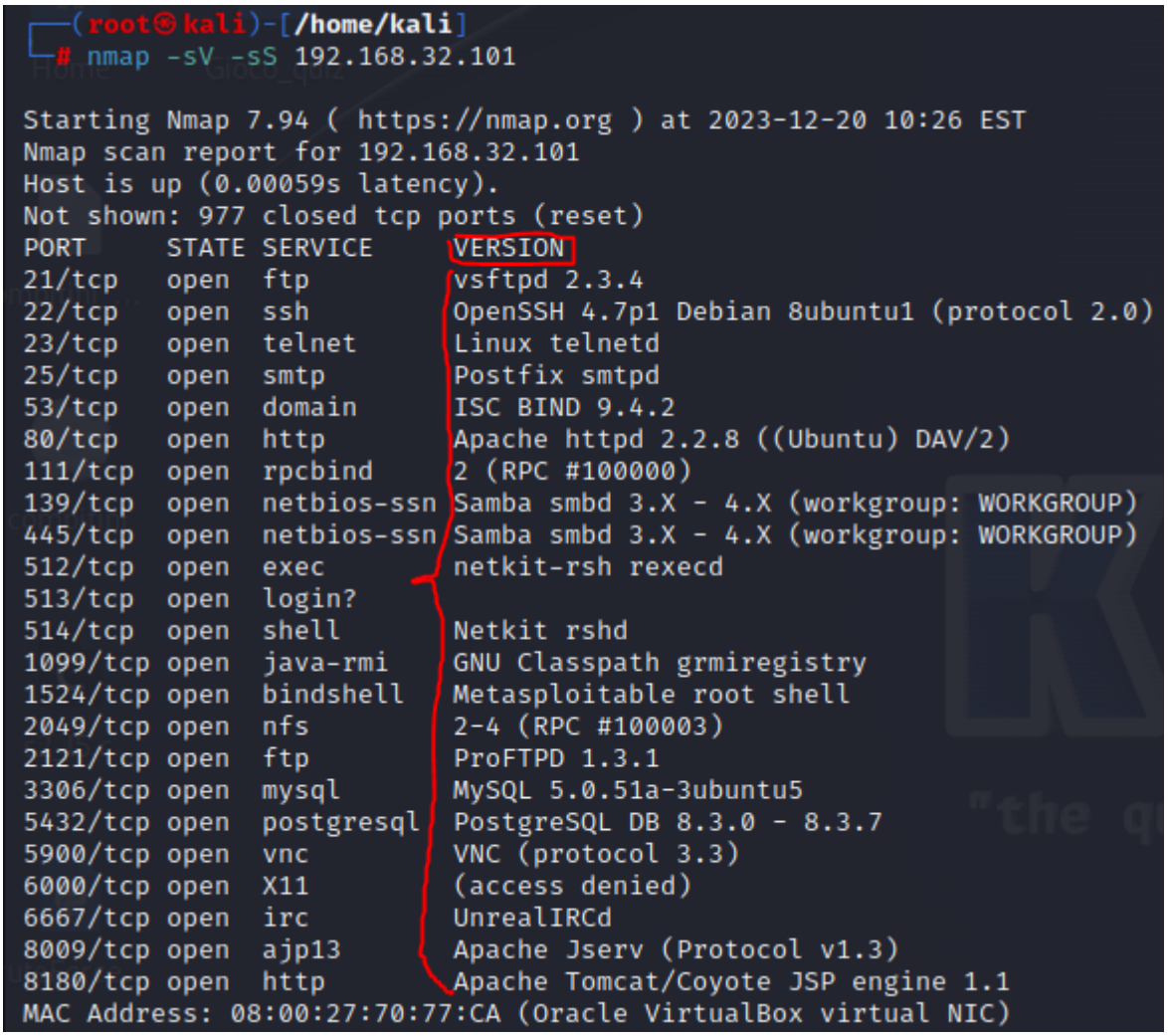
Questi due scan ci indicano in forma di lista le stesse che porte sono aperte, e quali servizi offre ogni una. La differenza é che il Syn scan (-sS) non completa un *three way handshake*, mentre che il TCP scan (-sT) lo fa.





Version detection:

Utilizzare lo switch -sV ci da la informazione che ci danno i primi 2 tipi di scan, ma anche ci indica la versione di ogni servizio fornito:



Windows 7: (192.168.32.102)

Probando a fare OS fingerprinting alla ip 192.168.32.102 solo con lo switch **-O** ci da un problema, non ci da una risposta conclusiva su quale versione esatta di windows si sta usando. Questo ci lo dice perché non si è trovato né un porto aperto né uno chiuso, lavoro del firewall sicuramente.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O -Pn 192.168.32.102

Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 10:38 EST
Nmap scan report for 192.168.32.102
Host is up (0.00067s latency).
All 1000 scanned ports on 192.168.32.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:E4:A1:4E (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, VM
ware 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 cp
e:/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 36.85 seconds
```

Per risolvere questo problema si può: Disattivare il firewall di Windows 7 per quanto riguarda i protocolli TCP e UDP, oppure utilizzare un timing -T1, che teoricamente dovrebbe bypassare il firewall.