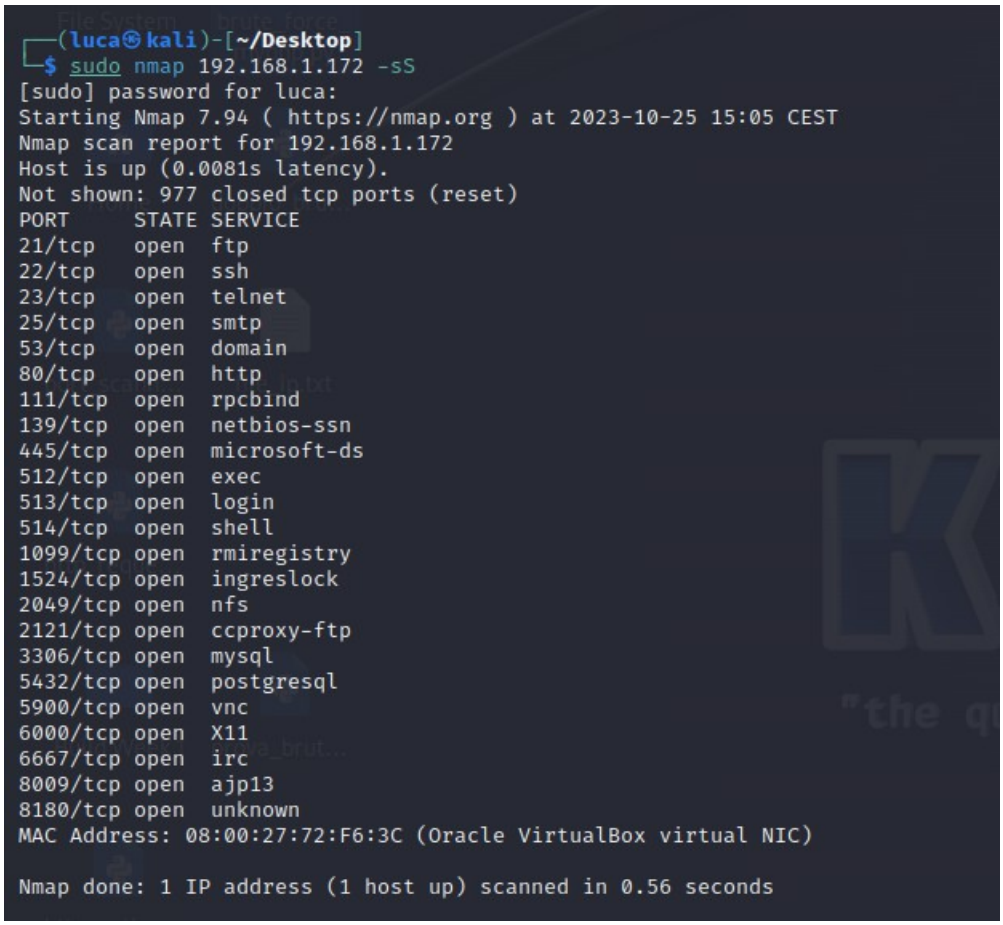
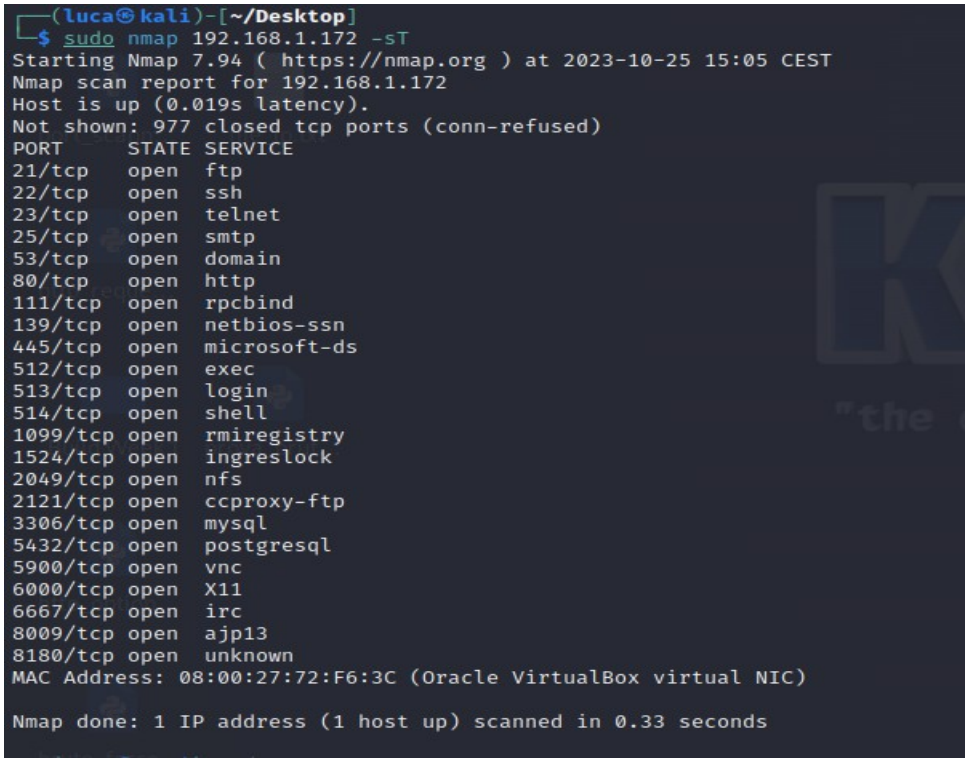
Pratica S5L3

Andiamo ad effettuare le scansioni tramite nmap di tipo syn scan, tcp scan e Os fingerprint verso la macchina metasploitable con ip 192.168.1.172:

Syn Scan:

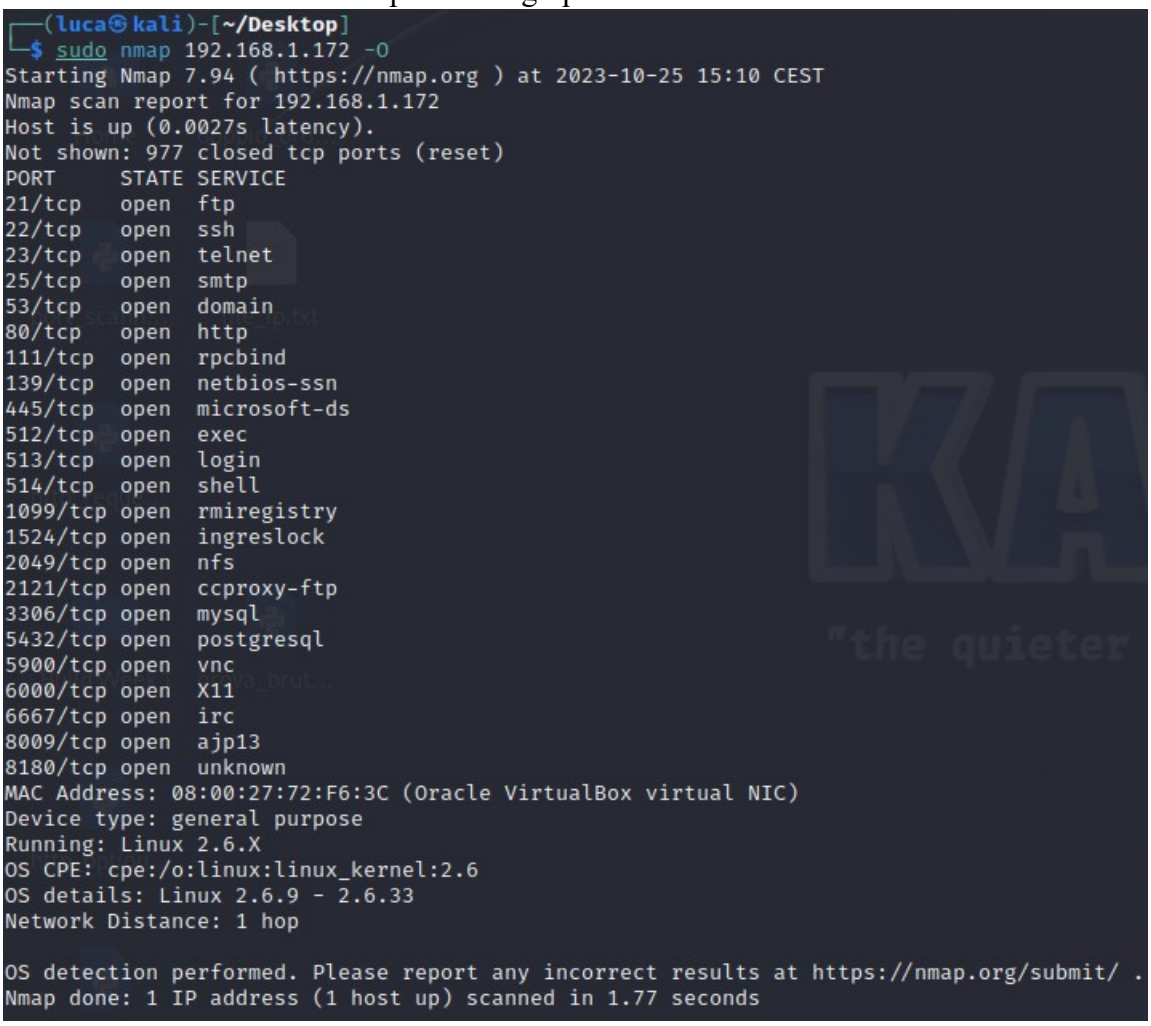


TCP Scan (qui viene effettuato il 3-way handshake completo):



A livello di output non notiamo nessuna differenza, ma sappiamo che la seconda scansione provocherà più rumore all'interno della rete.

Vediamo ora la scansione di tipo OS Fingerprint:

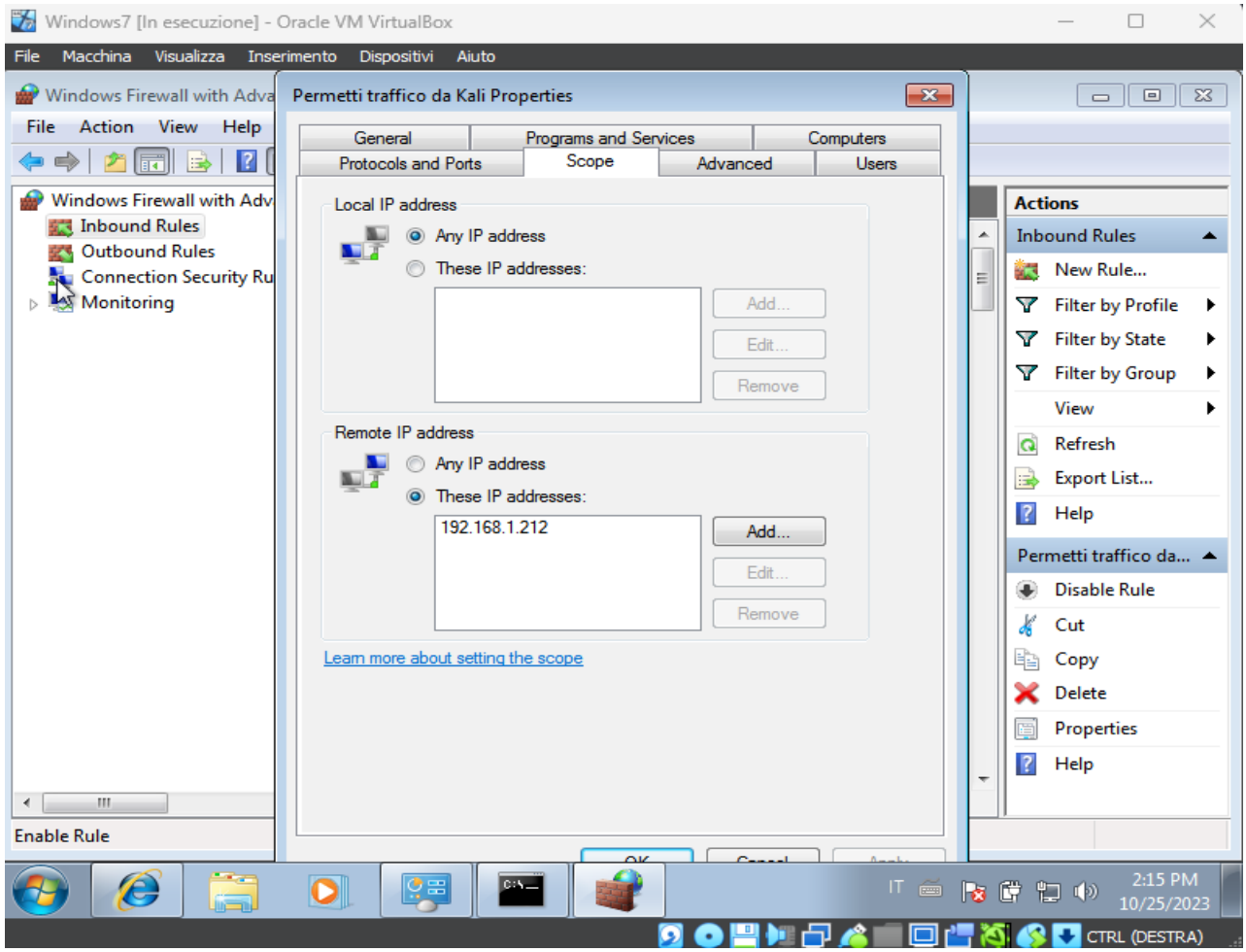


Oltre alla informazioni precedenti nmap ci dice che il sistema operativo target è di tipo Linux, e la sua versione dovrebbe risiedere nell'intervallo 2.6.9 – 2.6.33

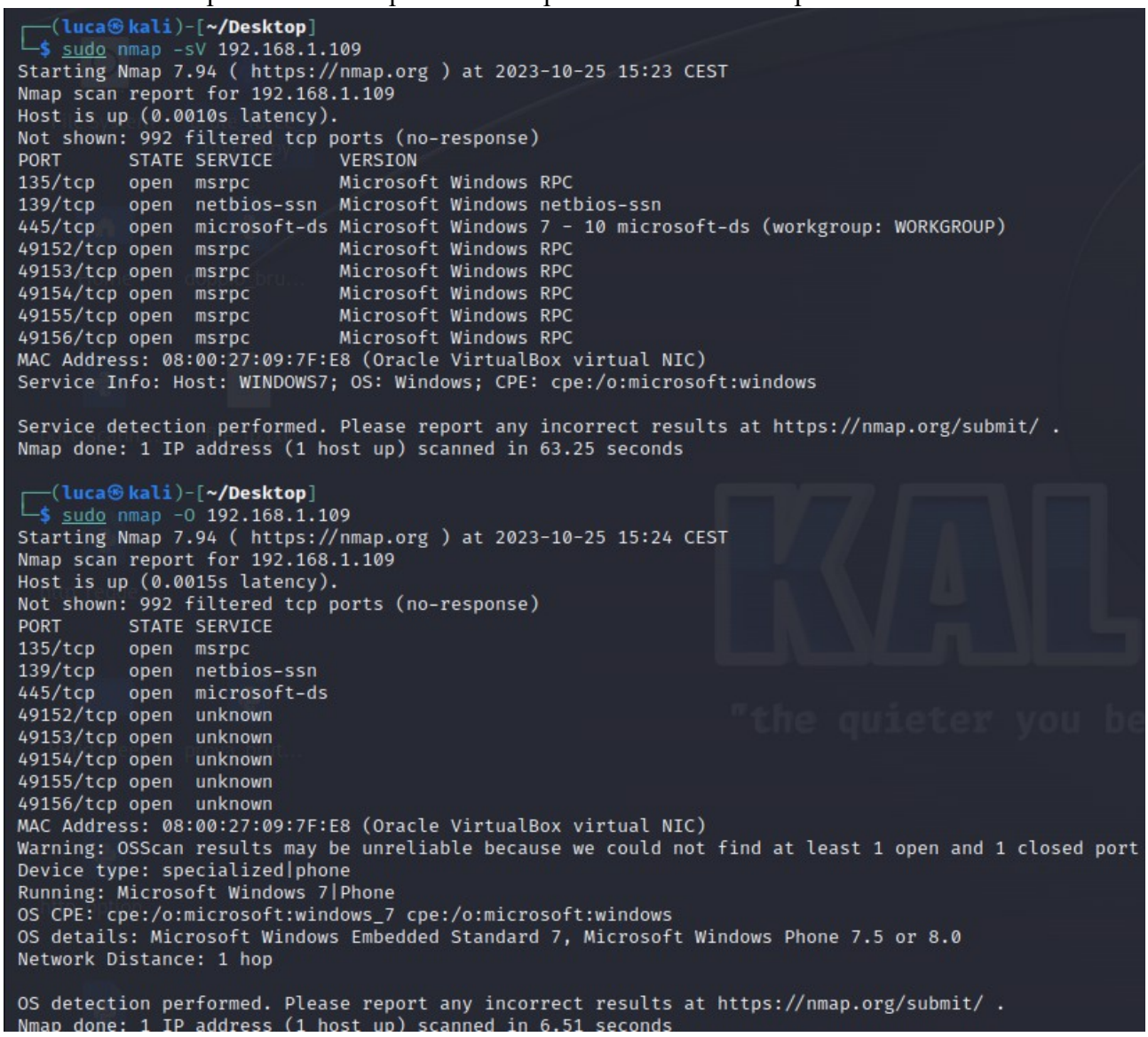
Andiamo ora a provare le scansioni verso la macchina Windows 7, con ip 192.168.1.109:

```
┌──(luca㉿kali)-[~/Desktop]
└─$ sudo nmap -sS 192.168.1.109
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:14 CEST
Nmap scan report for 192.168.1.109
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.1.109 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:09:7F:E8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 21.49 seconds

┌──(luca㉿kali)-[~/Desktop]
└─$ sudo nmap -O 192.168.1.109
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:15 CEST
Nmap scan report for 192.168.1.109
Host is up (0.00084s latency).
All 1000 scanned ports on 192.168.1.109 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:09:7F:E8 (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/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.04 seconds
```

Come vediamo nmap non riceve risposta ai tentativi di SYN nel primo caso, mentre nel secondo ci informa anche che ha rilevato troppe fingerprint diverse per poter stabilire il sistema operativo target. Ricordiamo però che la macchina W7 ha un firewall abilitato di default, quindi andiamo a creare una regola che permetterà il traffico dalla macchina Kali verso quella W7 e riproviamo con le scansioni:

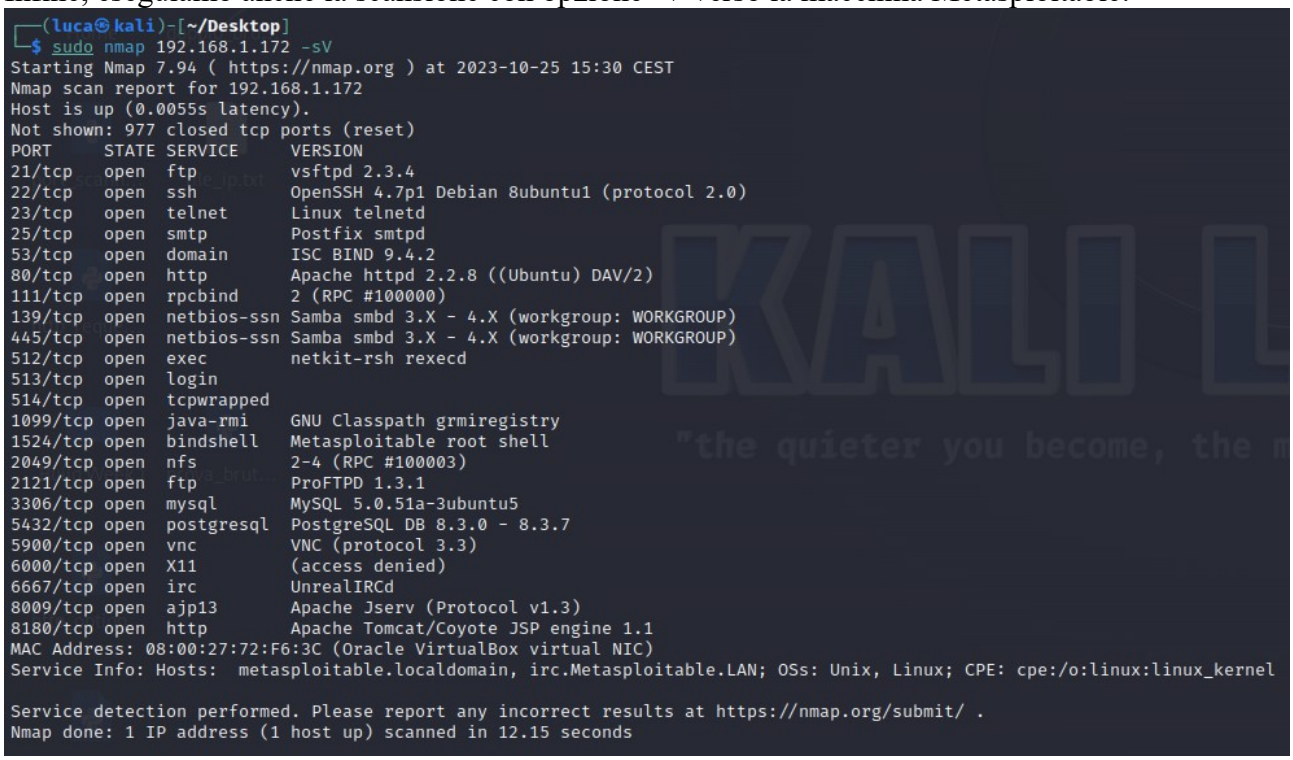


Riproviamo a scansionare, aggiungendo l'opzione -V per andare a recuperare informazioni anche sulla versione dei protocolli corrispondenti alle porte eventualmente aperte:



Notiamo come ora vengano restituite anche diverse informazioni nella colonna “version” nel primo caso, e anche sulla versione del sistema operativo che viene rilevato essere W7. Nel secondo caso, con l'opzione -O, nel campo **OS Details** vengono restituite più possibilità in quanto le fingerprint probabilmente sono comuni anche ai sistemi Windows Phone 7.5 e 8.0

Infine, eseguiamo anche la scansione con opzione -V verso la macchina Metasploitable:



Anche in questo caso nella colonna version possiamo recuperare più informazioni, spesso anche la versione supportata dal protocollo (es. ftp 2.3.4).