ESERCIZIO

Traccia: Tecniche di scansione con Nmap

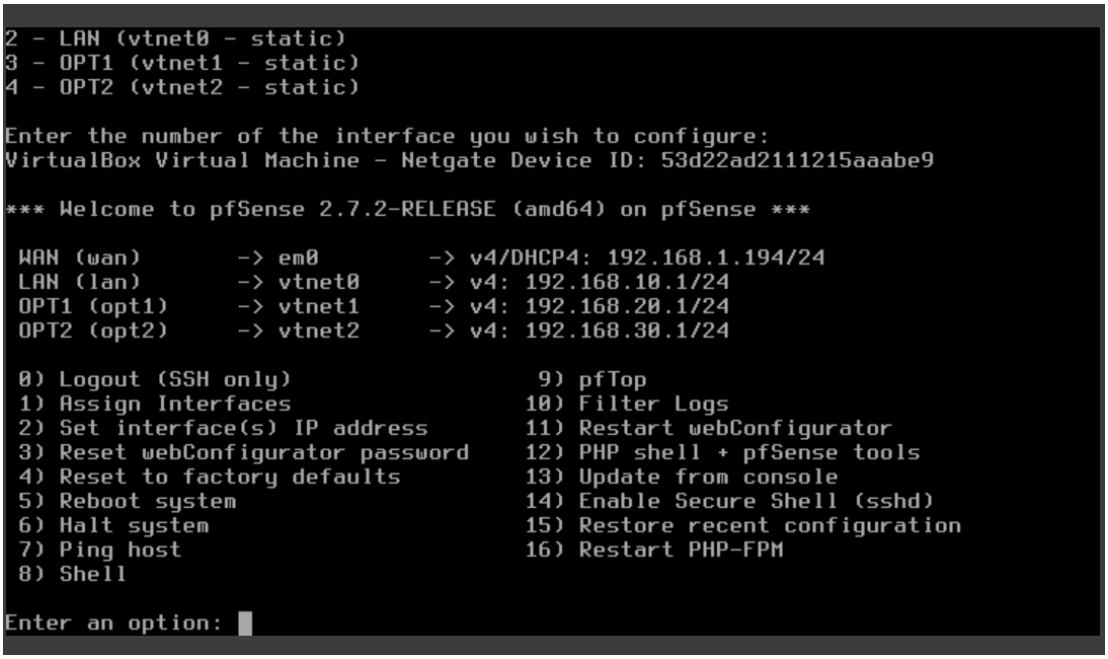
Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

- OS fingerprint;
- Syn Scan;
- TCP connect (trovate le differenze tra TCP connect e Syn Scan);
- Version detection

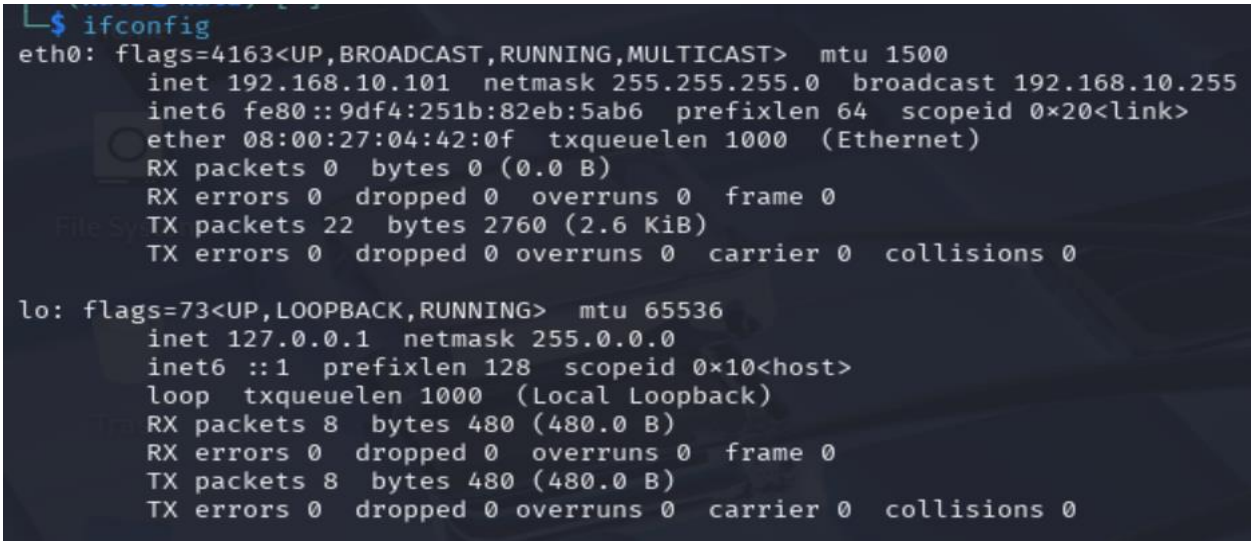
E la seguente sul target Windows:

- OS fingerprint.

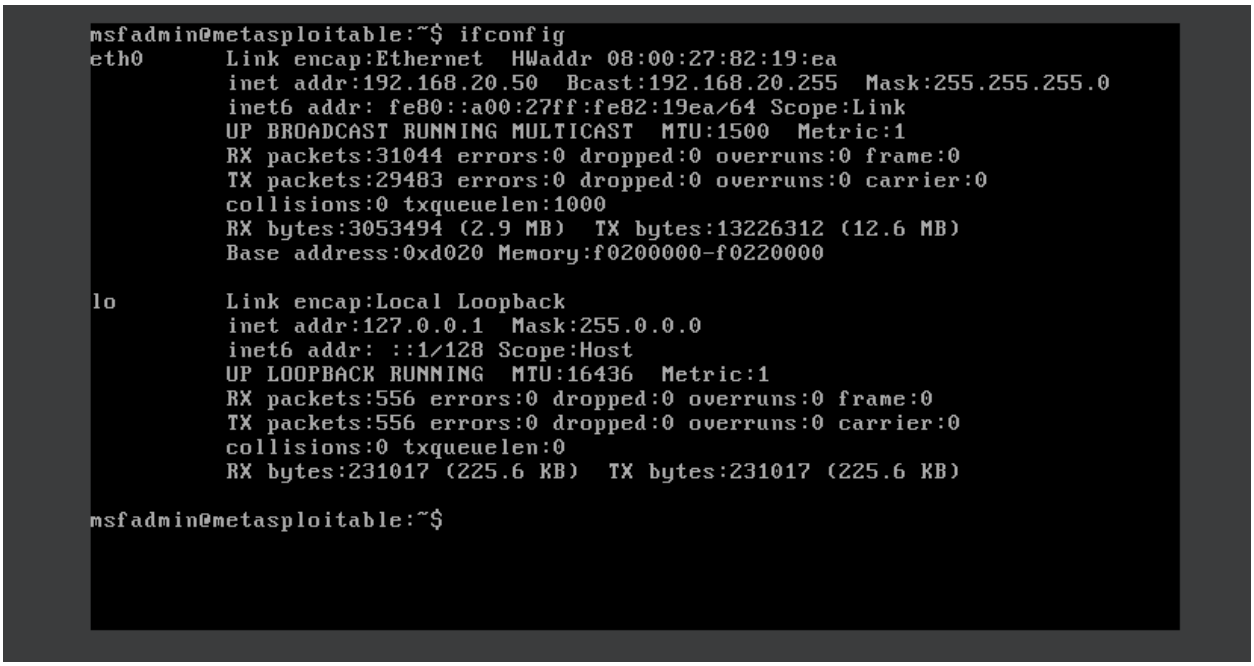
Prima di cominciare l'esercizio dovremo assicurarci che il nostro laboratorio sia configurato correttamente. Avremo bisogno delle VM Kali, Metasploitable2 e Windows7 su delle reti interne. Per far questo utilizzeremo Pfsense (che ha funzioni sia router che firewall) e con il quale simuleremo schede di rete aggiuntive.



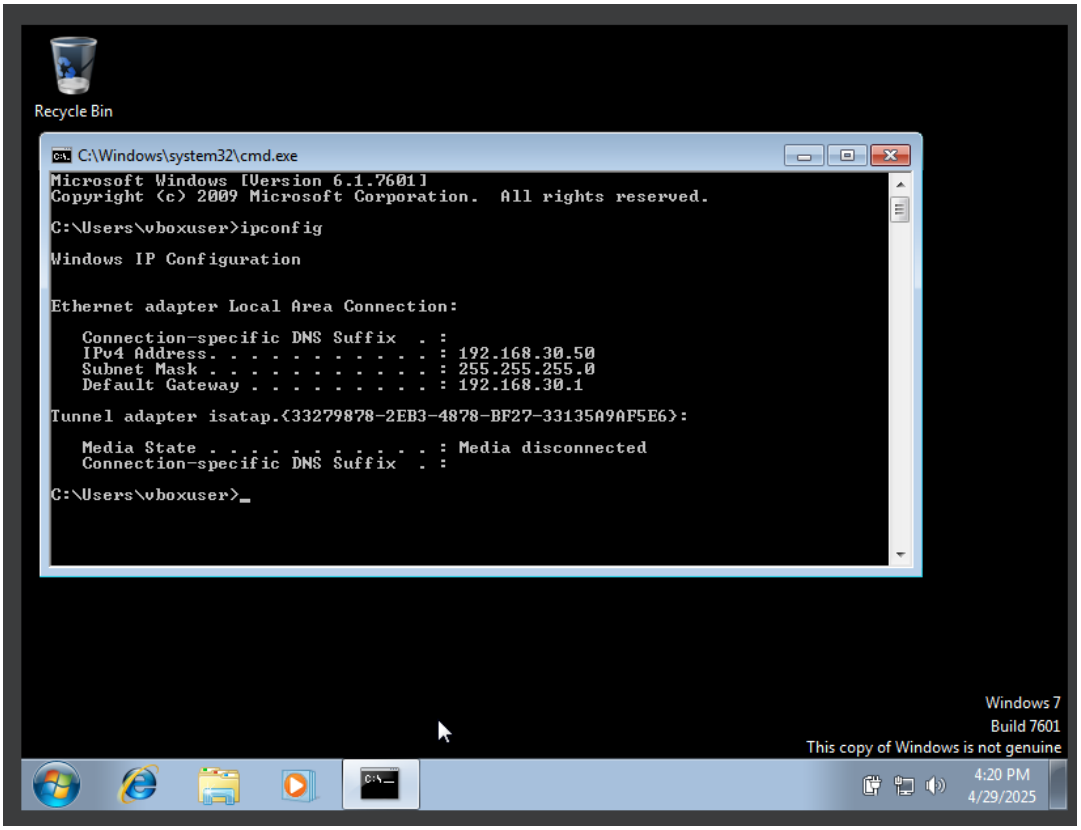
Come possiamo vedere dall'immagine, abbiamo creato 3 Vlan, che andremo ad assegnare rispettivamente alla Kali, a Metaspoitable 2 e Windows 7. Utilizzeremo degli indirizzi IP statici.



Nell'immagine sopra vediamo l'IP assegnato alla Kali.



Nell’immagine sopra vediamo l’IP assegnato alla Metaspoitable2.

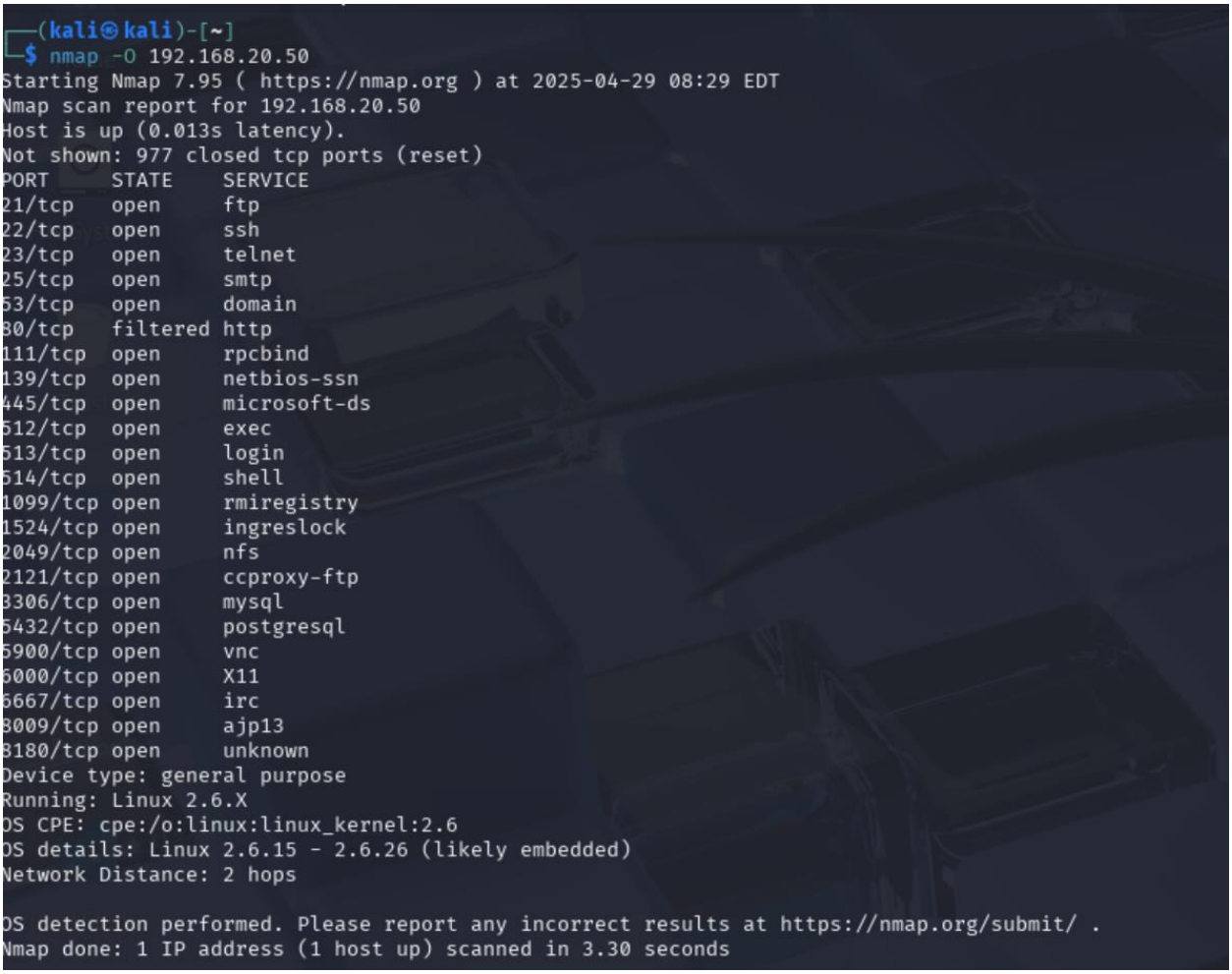


Nell’immagine sopra vediamo l’IP assegnato a Windows 7.

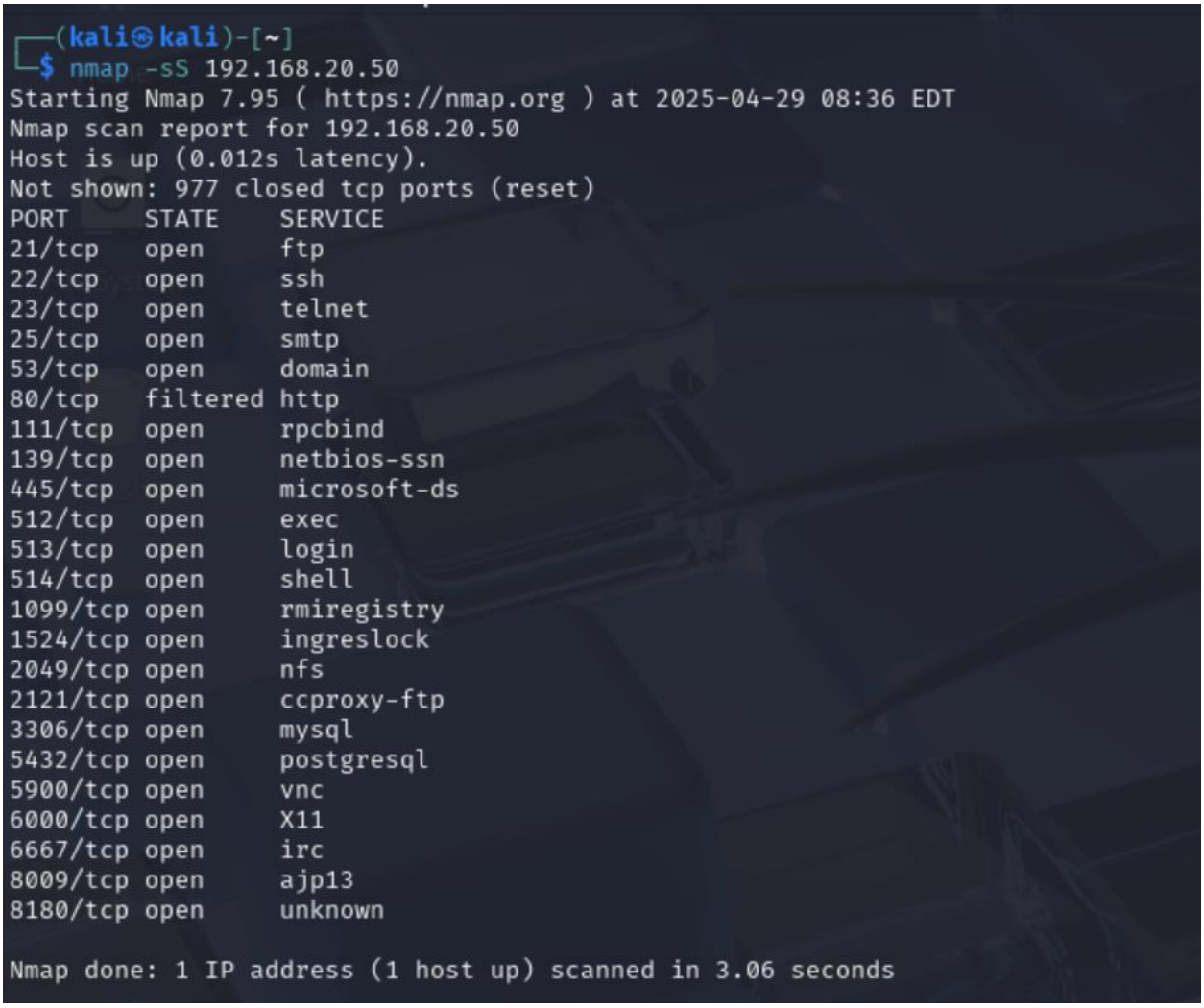
Una volta impostato il nostro laboratorio correttamente possiamo verificare che sia funzionante mandando dei ping dalla Kali a Metasploitable 2 e Windows 7.

Se riceveremo risposta ai ping vorrà dire che la configurazione è stata effettuata correttamente.

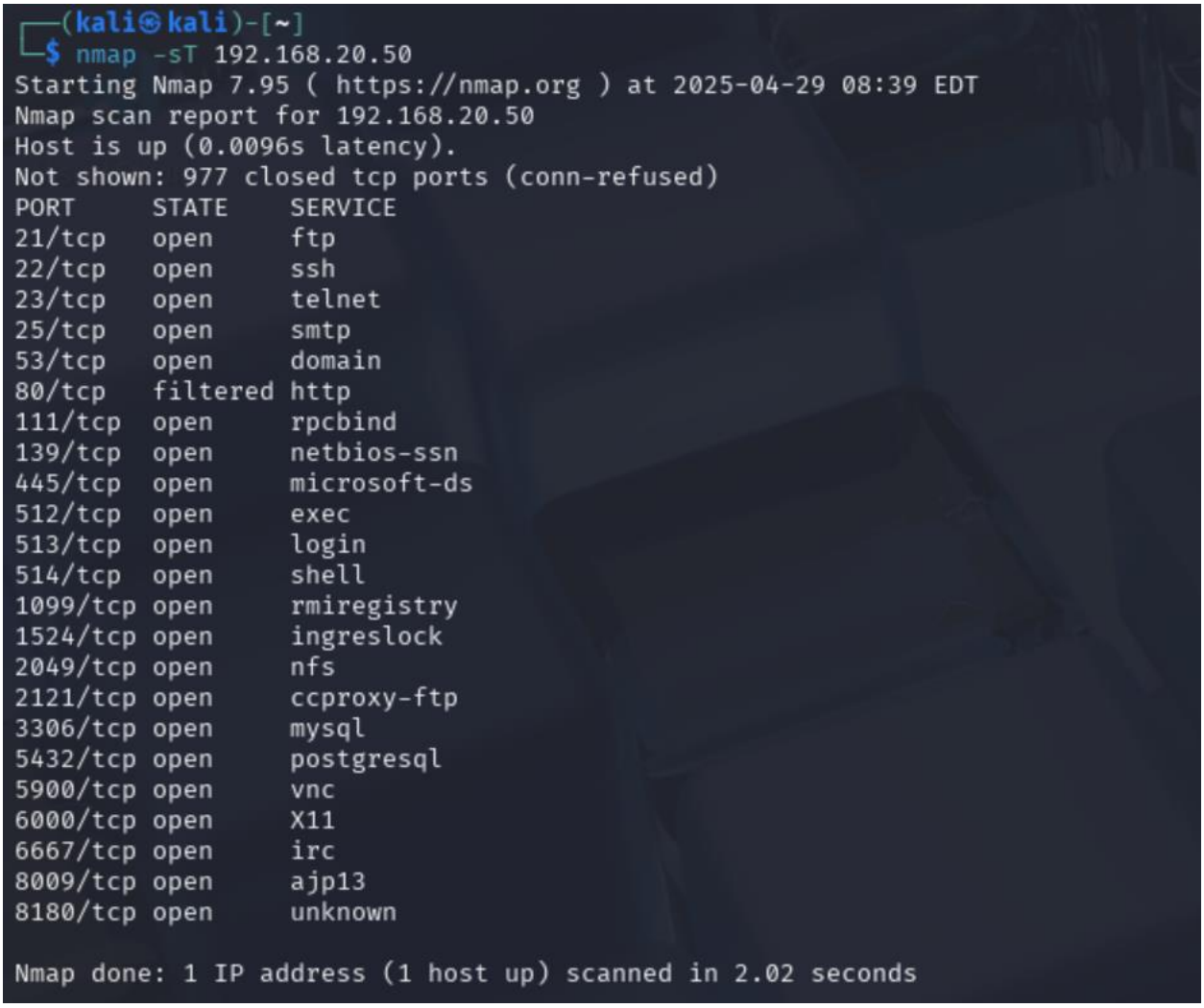
A questo punto possiamo procedere a fare le scansioni con nmap richieste dalla traccia.



nmap –O 192.168.20.50 --> oltre le porte aperte, ci restituisce il SO utilizzato dalla Metasploitable 2.



nmap –sS 192.168.20.50 --> ci permette di vedere i servizi in esecuzione sull'host.

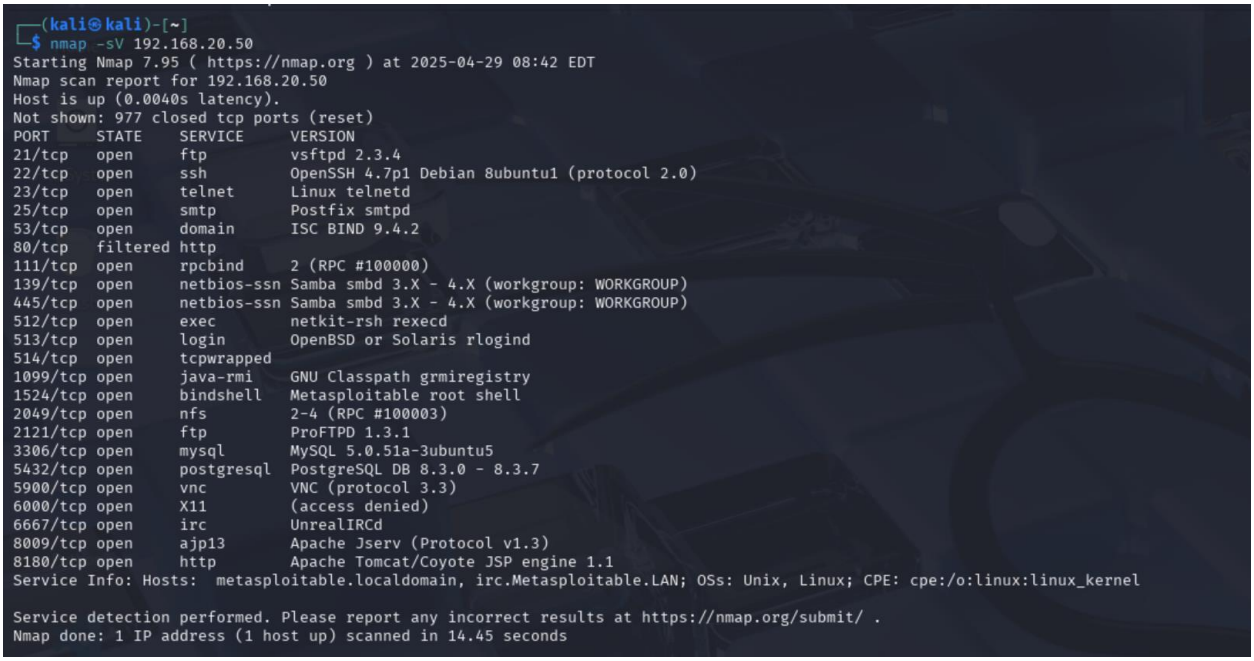


nmap –sT 192.168.20.50 --> ci restituisce lo stesso risultato visto in precedenza.

La differenza tra nmap –sS e –sT non è nel risultato che otteniamo. La differenza consiste nella modalità in cui vengono effettuate le due scansioni.

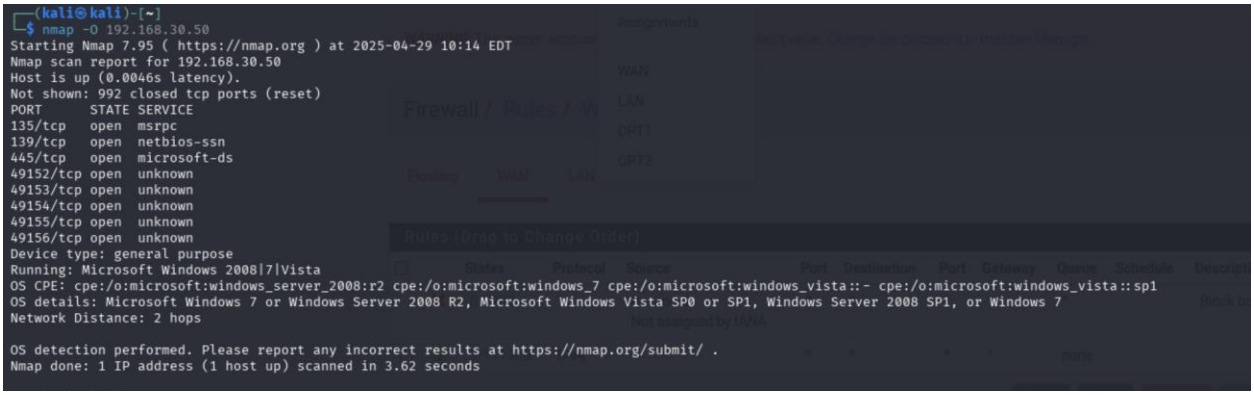
sT: è il metodo di scansione più invasivo, in quanto per controllare se una porta è aperta o meno e recuperare informazioni sul servizio in ascolto, nmap completa tutti i passaggi del 3 way handshake, stabilendo di fatto un canale.

sS: è un metodo meno invasivo, in quanto nmap, una volta ricevuto il pacchetto SYN/ACK dalla macchina target, non conclude il 3 way handshake, ma appurato che la porta è aperta chiude la comunicazione, evitando overload dato dalla creazione del canale.



nmap –sV 192.168.20.50 --> identifica i servizi in esecuzione e le loro versioni.

Infine, per quanto riguarda Windows7:



nmap –O 192.168.30.50 --> oltre le porte aperte, ci restituisce il SO in uso, in questo caso Windows 7.