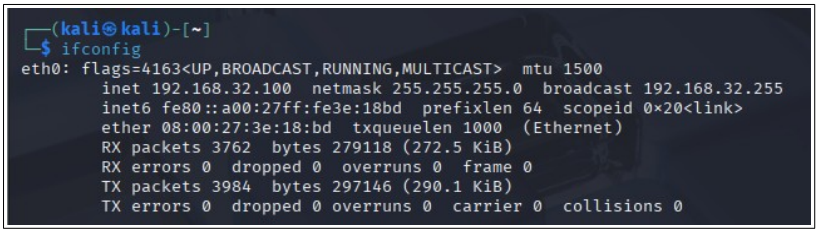
Report esercitazione con Nmap W9D1

In questo esercizio useremo lo strumento Nmap dalla macchina Kali per eseguire delle scansioni sulla macchina Metasploitable2.

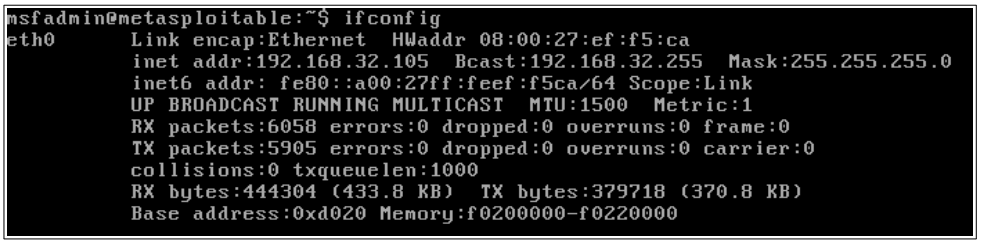
Prerequisiti:

Assicurarsi che le due macchine siano entrambe su rete interna e che possano comunicare tra di loro.

- Configurazione IP di Kali:

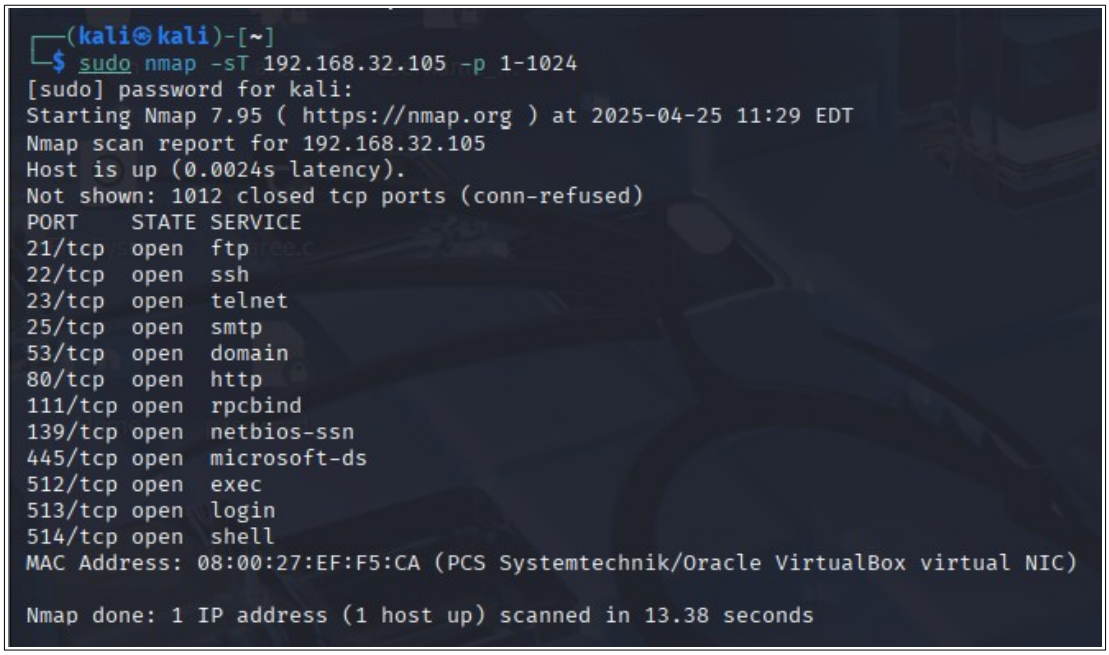


- Configurazione IP di Metasploitable2:



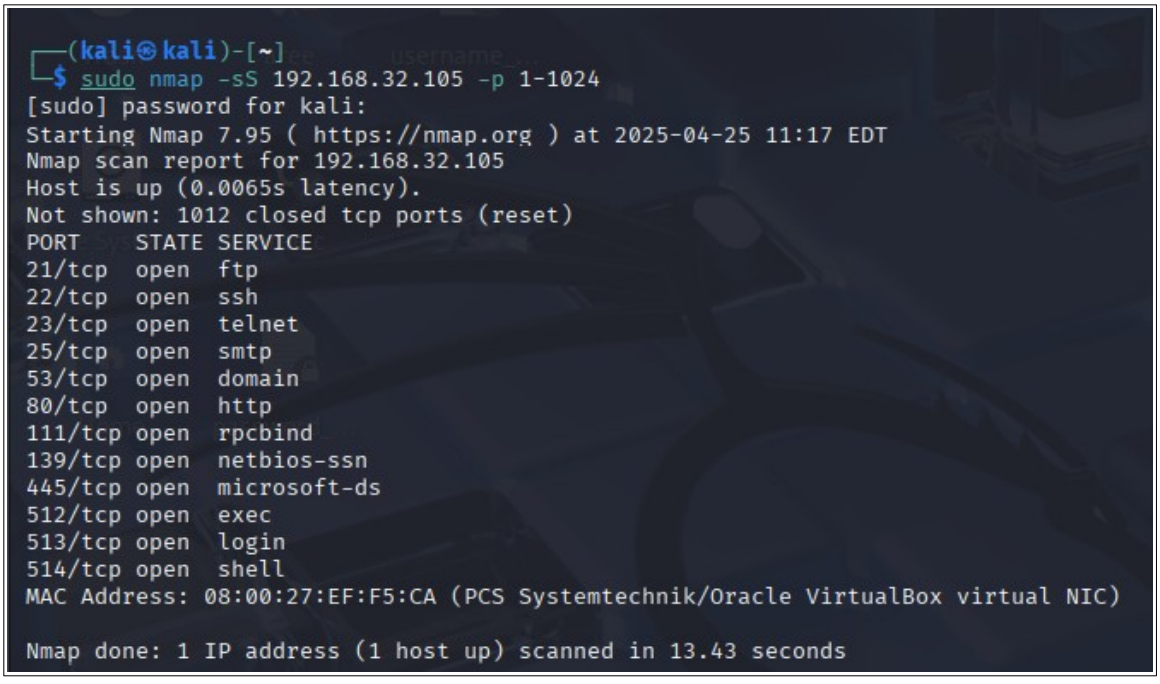
Scansione TCP

La scansione TCP tramite Nmap si effetua tramite il comando *sudo nmap -sT <IP target> -p <range di porte>*, è una scansione invasiva perché stabilisce una connessione completa con il target, completando la three-way-handshake (syn, syn-ack, ack).



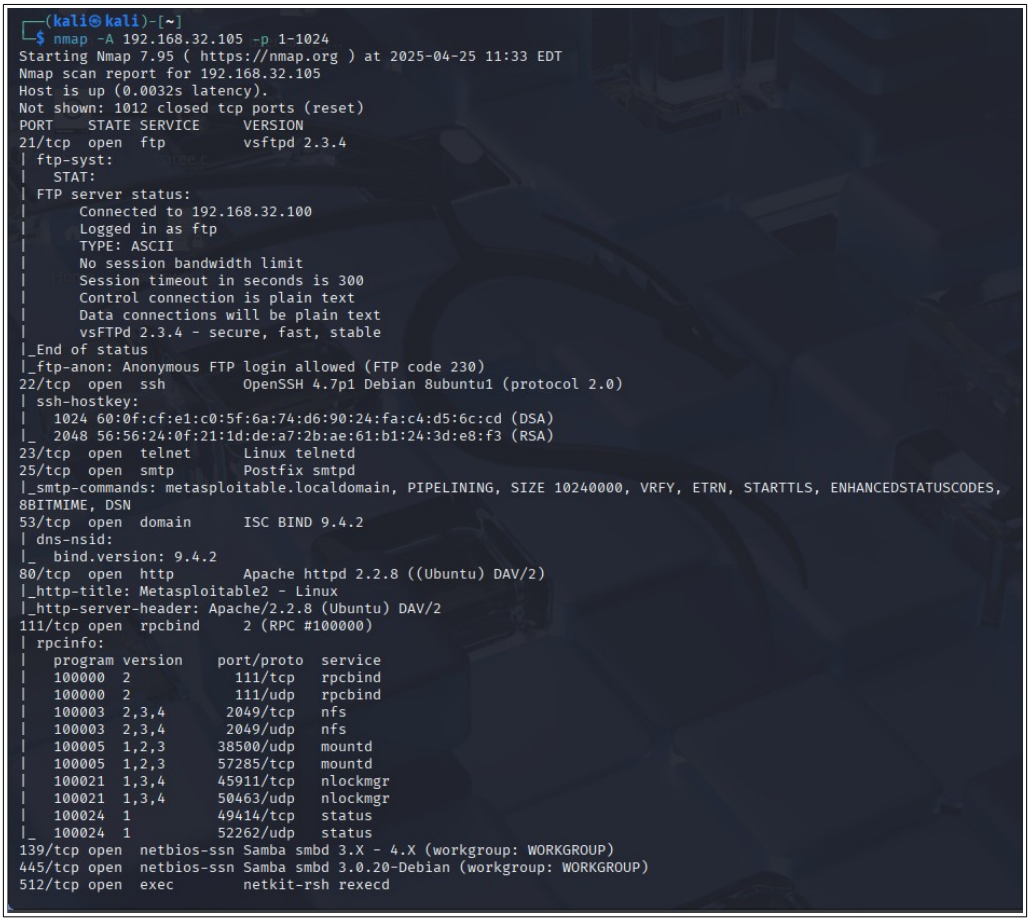
Scansione SYN

La scansione SYN è meno invasiva rispetto alla TCP in quanto è utilizzata per scoprire quali porte sono aperte sulla macchina target senza completare la three-way-handshake. Il comando per iniziare la scansione è sudo nmap -sS <IP target> -p <range di porte>.



Scansione con switch -A

È una delle scansioni più invasive, in quanto invia molte richieste, ma ci permette di recuperare molte informazioni sulla macchina target, come ad esempio la versione del sistema operativo, le porte aperte ed i servizi attivi su di esse.



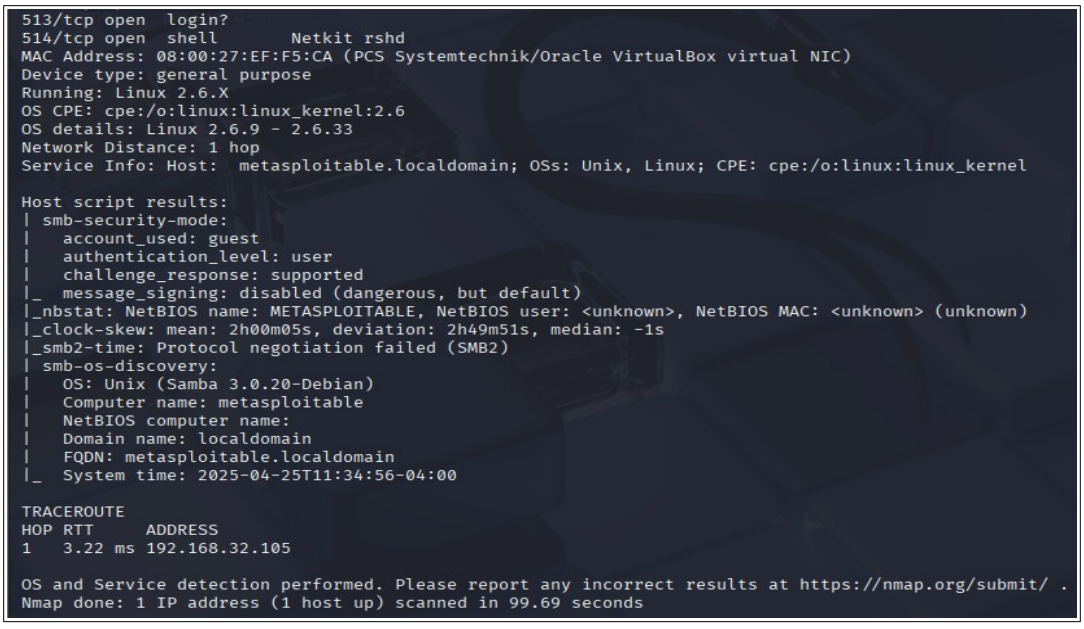


Tabella riassuntiva delle scansioni

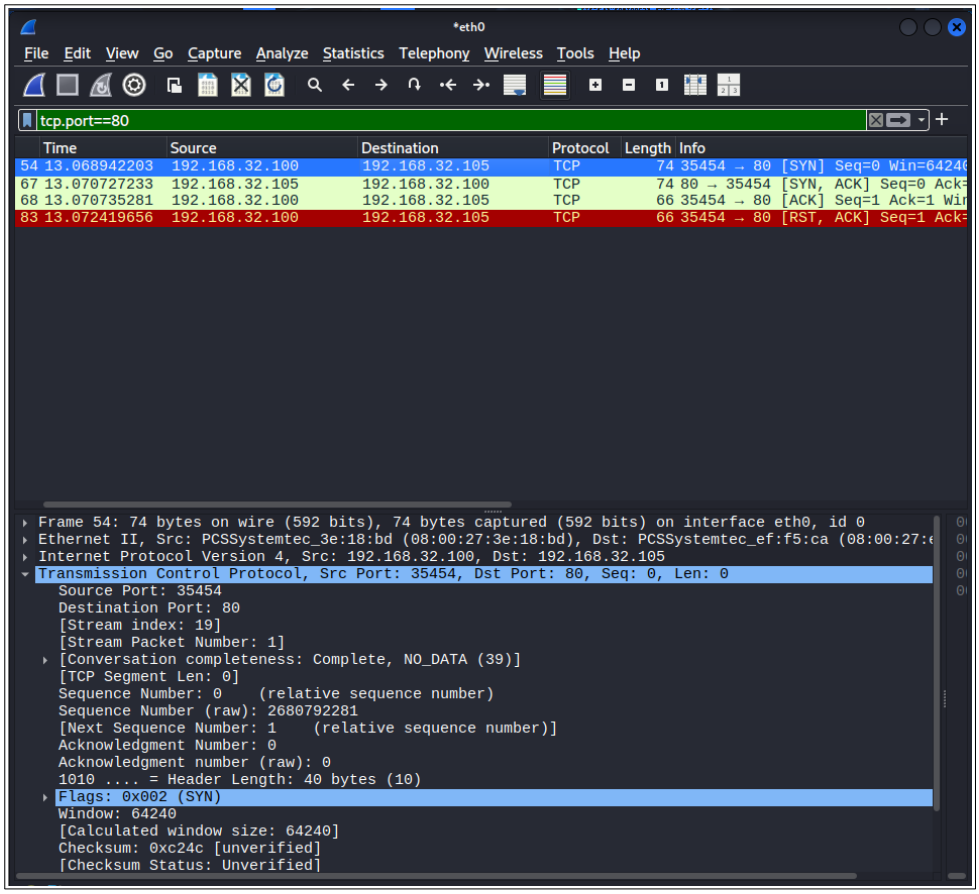
Tipo scansione	IP sorgente	IP target	Risultati scansione
TCP	192.168.32.100	192.168.32.105	12 porte aperte
SYN	192.168.32.100	192.168.32.105	12 porte aperte
Switch -A	192.168.32.100	192.168.32.105	12 porte aperte, servizi e versioni associati alle porte, info sul sistema operativo, traceroute

Facoltativo

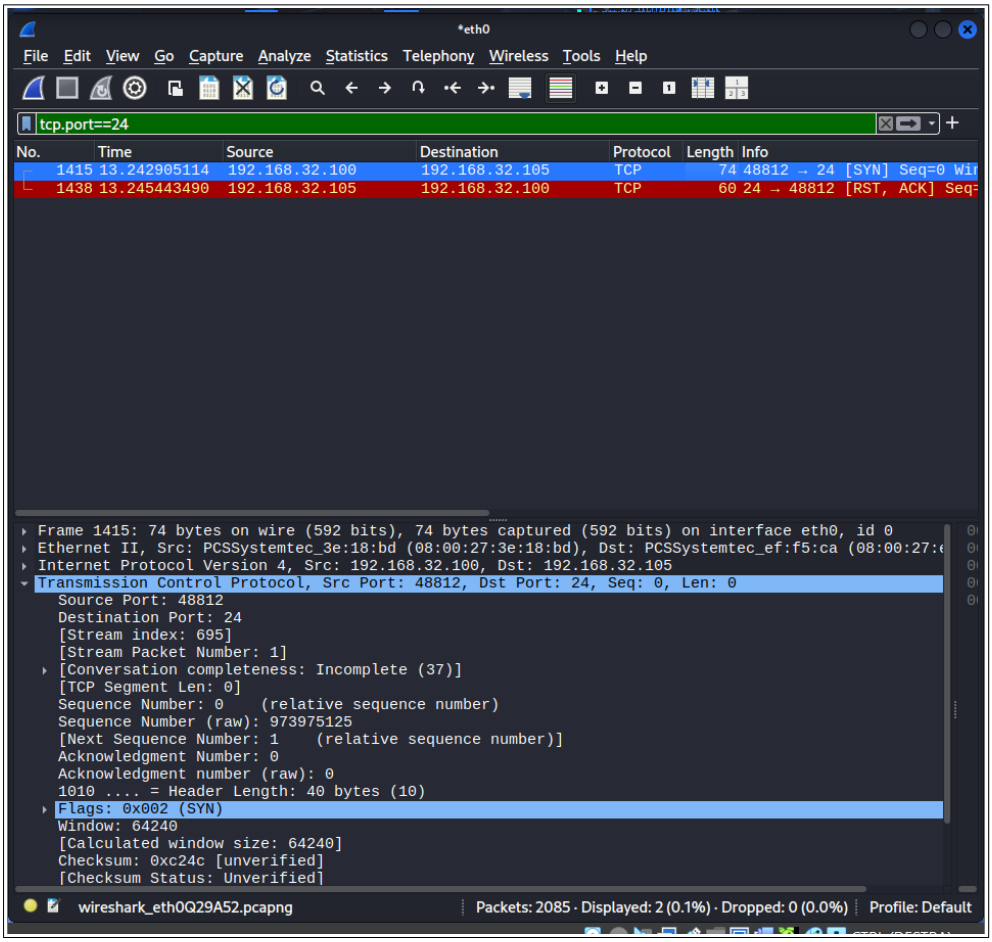
Evidenziare le differenze tra scansione TCP e SYN tramite cattura di Wireshark.

Scansione TCP

Tramite la cattura con Wireshark dei pacchetti possiamo notare come la connessione restituisca la sequenza della three-way-handshake [SYN, SYN-ACK, ACK], nelle porte che risultano aperte. Se la porta è chiusa restituisce la dicitura [RST, ACK].
Di seguito viene mostrata la scansione sulla porta 80 (servizio HTTP) e come si presenta la cattura in caso Nmap trovi una porta aperta.

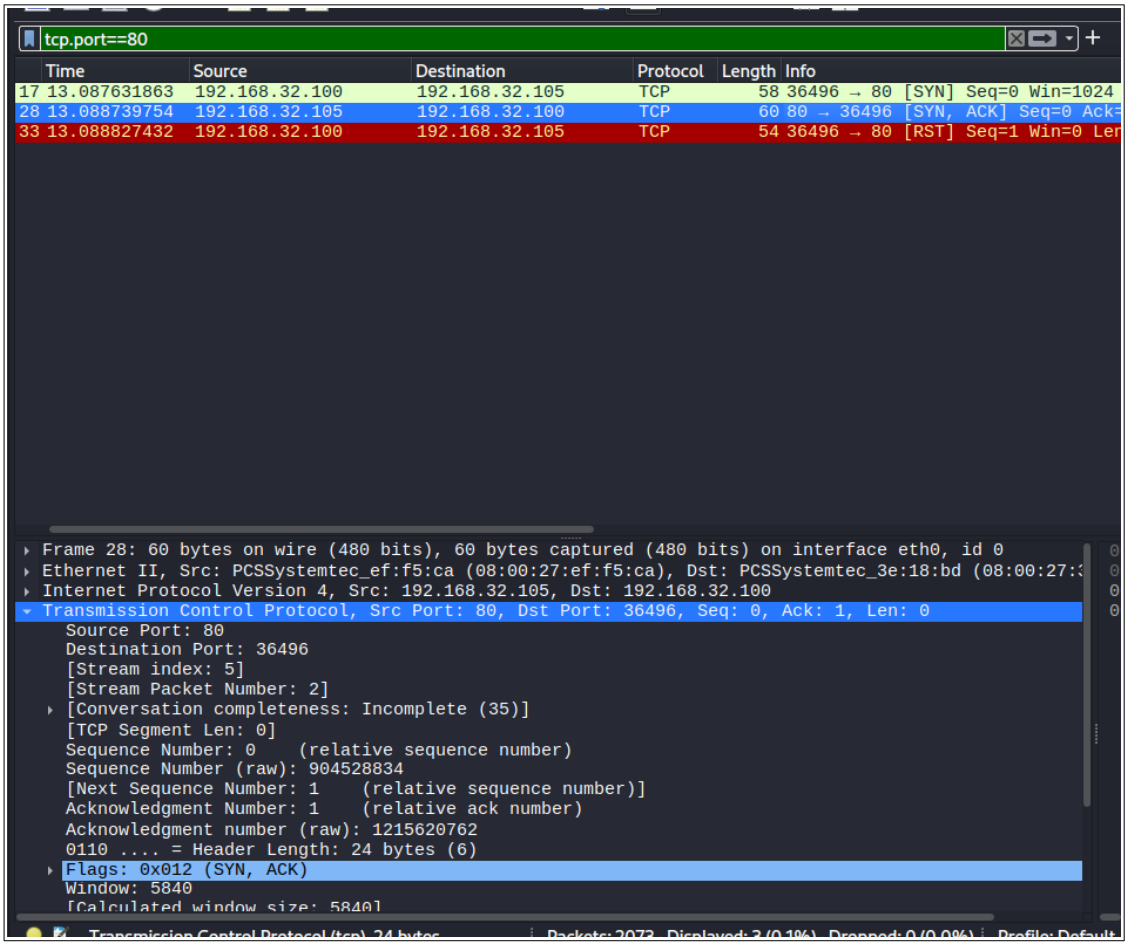


Qui sotto viene mostrata la scansione sulla porta 24 e che sappiamo essere chiusa, infatti non viene completata la three-way-handshake e subito dopo il tag [SYN], viene inviato il segnale [RST, ACK].



Scansione SYN

Mediante la cattura con Wireshark possiamo notare come, una volta trovata una porta aperta, non venga completata la three-way-handshake, in quanto subito dopo aver ricevuto il flag [SYN, ACK] la connessione viene interrotta e viene emesso il messaggio [RST].



Quando la scansione di Nmap trova una porta chiusa, come per TCP, invia il flag [RST,ACK]