Report vari tipi di scansione da Kali a Metasploitable

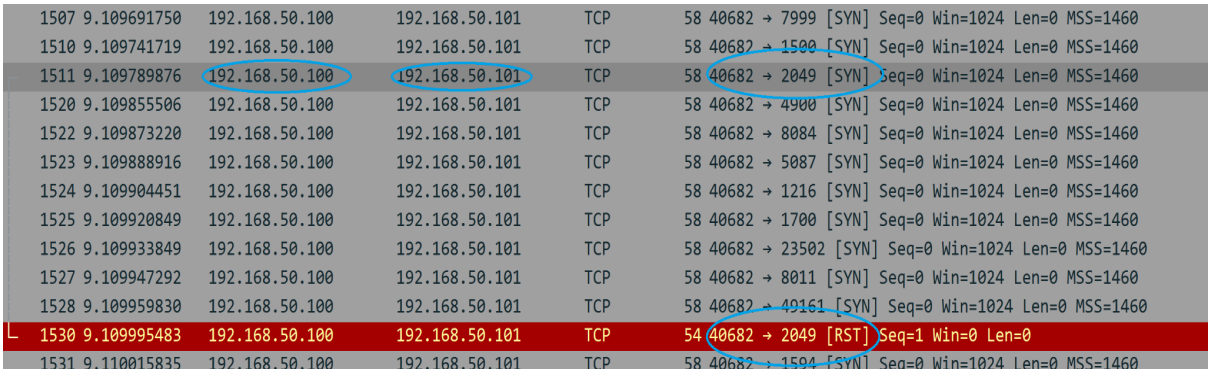
Dopo aver connesso le macchine a rete interna con indirizzi ip statici possiamo iniziare la scansione di Metasploitable da Kali utilizzando Nmap.

1) Scansione di tipo -sS

Eseguite da terminale root il comando:

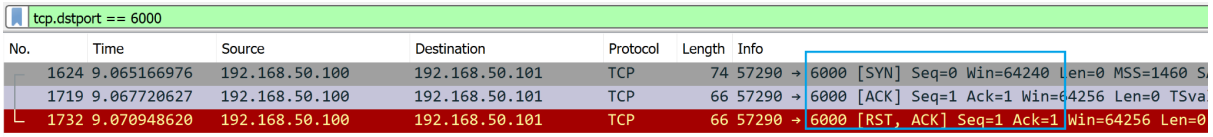
nmap -sS 192.168.50.101

Tale scansione viene detta di tipo meno invasivo (o SYN) poiché chiede informazioni sulle porte e servizi all'altra macchina senza stabilire una vera e propria connessione, infatti ottenute le informazioni desiderate resetta la connessione (RST). Possiamo notare tutto ciò dalla schermata di wireshark che catturava i pacchetti durante tale scansione.



2) Scansione di tipo -sT

A differenza della prima scansione questa utilizza una vera e propria connessione TCP completando il three-way-handshake. Viene considerata più "invasiva" in quanto è più facilmente identificabile.



In questo caso abbiamo preso come esempio la porta 6000. Possiamo notare la fase di SYN,ACK e RST (sincronizzazione, apprendimento e reset) l'ultima delle tre è utilizzata al posto del finale per non creare connessioni fatte e finite più facilmente identificabili.
Da tali scansioni otteniamo:

Tipo di scansione	Richiedente	Destinatario	Porte e servizi aperti
-sS	192.168.50.100(kali)	192.168.50.101(Metasploitable)	23
-sT	192.168.50.100(kali)	192.168.50.101(Metasploitable)	23