NETWORK SCANNING CON NMAP

Nell'esercizio di oggi siamo andati a scansionare la macchina metasploitable con il tool nmap. Abbiamo eseguito diversi tipi di scan:

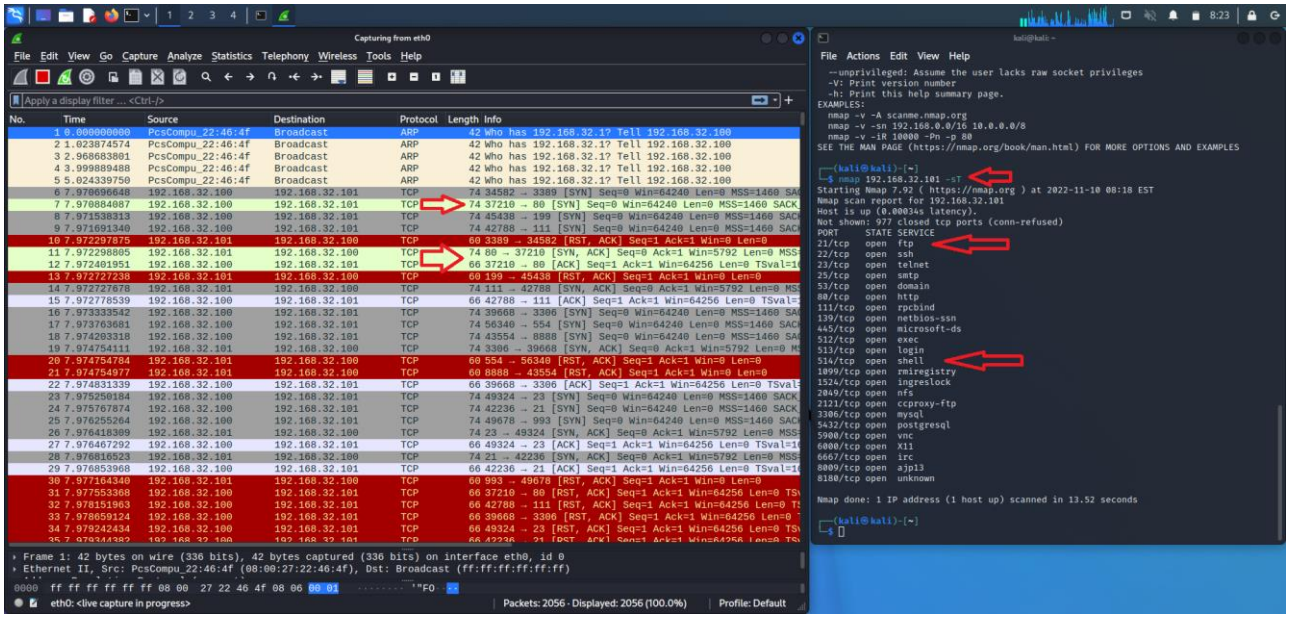
- Scansione TCP sulle porte well-known
- Scansione SYN sulle porte well known
- Scansione con switch "-A" sulle porte well-known

Abbiamo trovato le porte well-known aperte sul nostro terminale Kali, cioè tra quelle che vanno dalla porta 0 alla 1023:

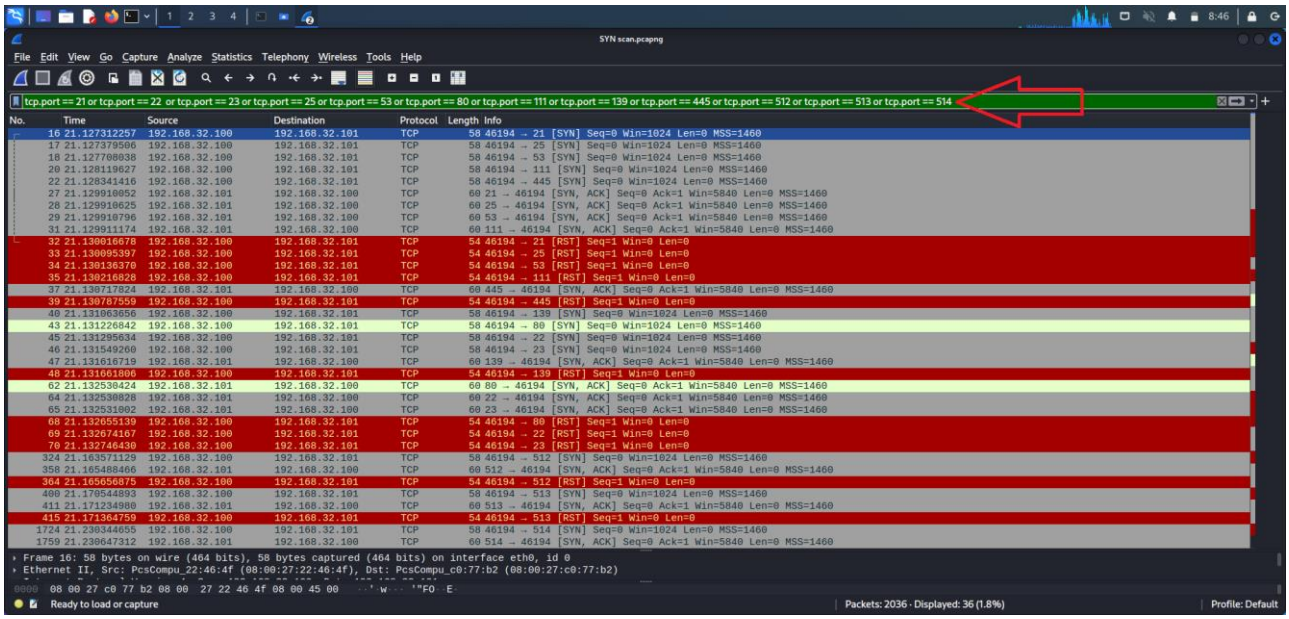
PORTE	STATE	SERVICE
21	Open	ftp
22	Open	ssh
23	Open	telnet
25	Open	smtp
53	Open	domain
80	Open	http
111	Open	rpcbind
139	Open	netbios-ssn
445	Open	microsoft-ds
512	Open	exec
513	Open	login
514	Open	shell

Tab1

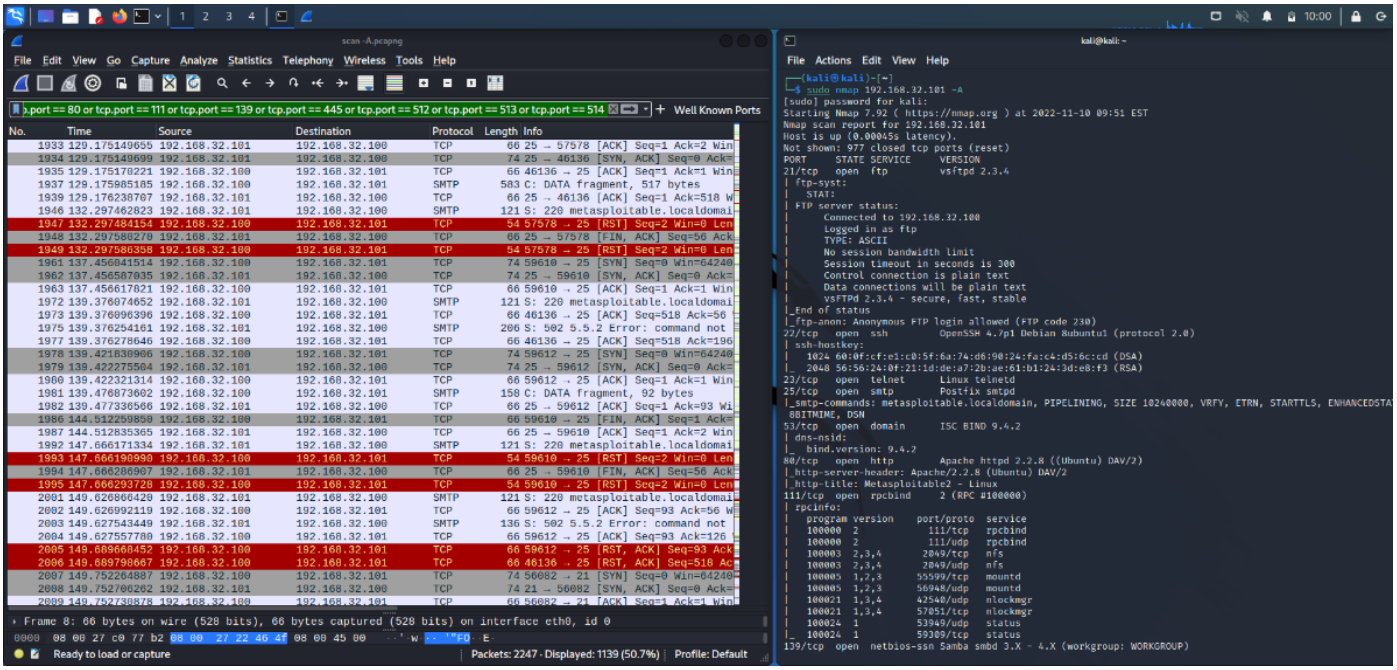
Durante la scansione abbiamo aperto Wireshark intercettando le richieste inviate dalla macchina sorgente.



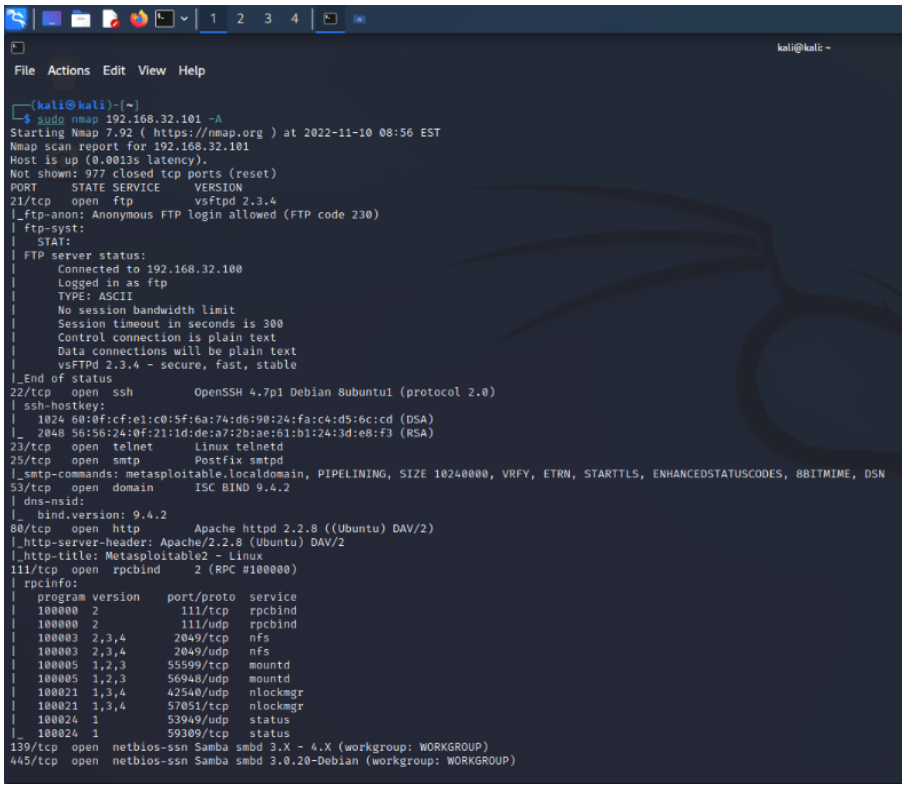
Abbiamo filtrato per vedere solo le porte interessate (Tab1):



Fatte le ricerche per nmap “IP” -sT e per nmap “IP” -sS abbiamo fatto una scansione -A:



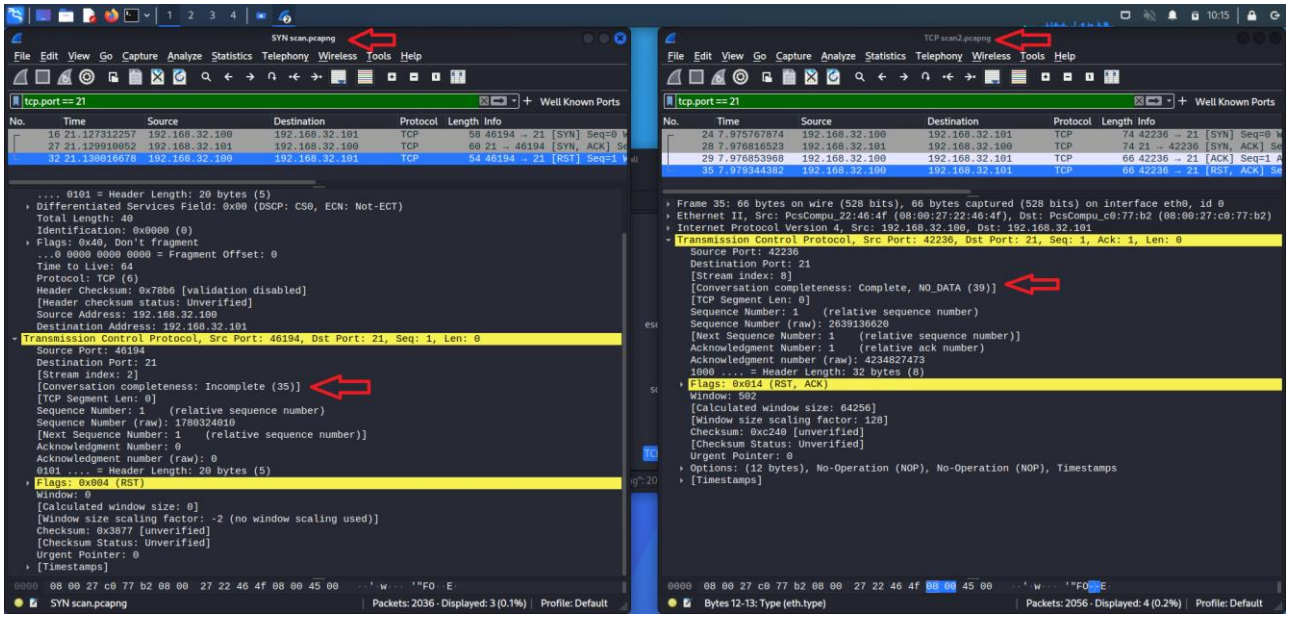
Come possiamo vedere la scansione -A fa una scansione molto più approfondita (img sopra e sotto).



Abbiamo poi evidenziato le porte well-known filtrando le scansioni di Wireshark per notare le differenze:

Qui vediamo un esempio di scansione della stessa porta (porta 21) dove possiamo vedere come la scansione -sT, essendo più invasiva rispetto alla -sS, completa la connessione 3-way-handshake.

Infatti, la scansione TCP darà la connessione completa, mentre, la scansione SYN darà connessione incompleta, dato che verrà chiusa dopo il SYN/ACK.



FONTE SCAN	TARGET SCAN	TIPO DI SCAN	RISULTATO OTTENUTO
192.168.32.100	192.168.32.101	nmap -sT	23 servizi aperte di cui 12 di porte well-known

192.168.32.100	192.168.32.101	nmap -sS	23 servizi aperte di cui 12 di porte well-known