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:

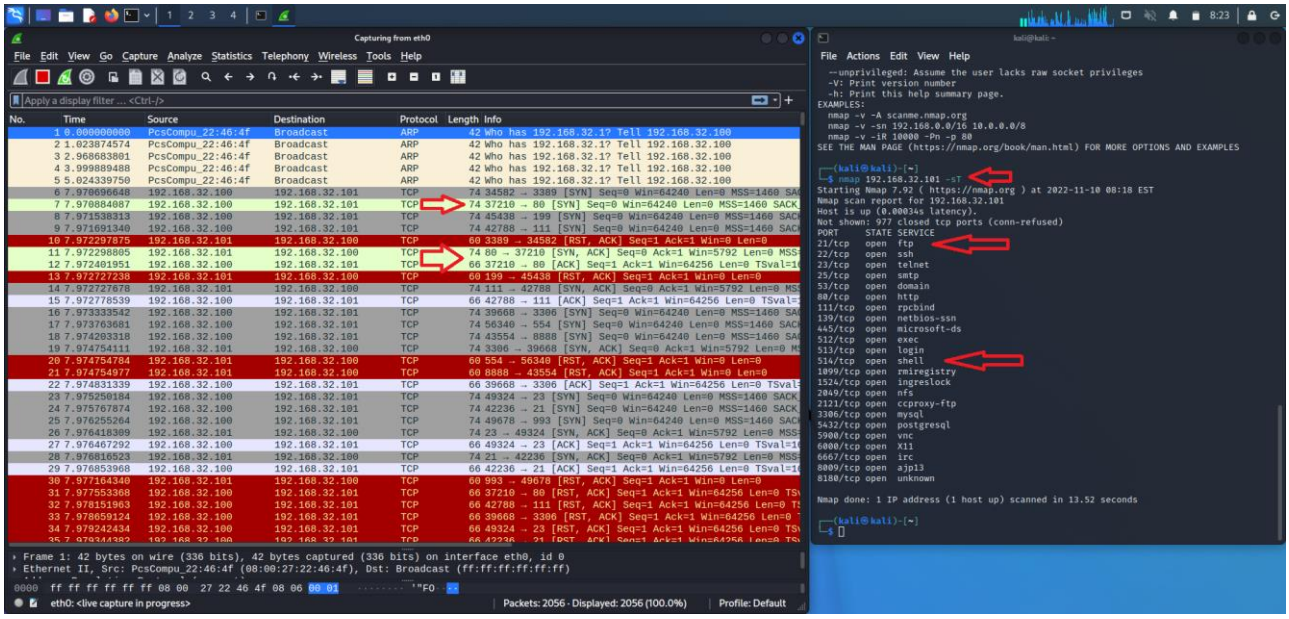
- Scansione TCP sulle porte well-known
- Scansione SYN sulle porte well known
- Scansione con switch "-A" sulle porte well-known

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

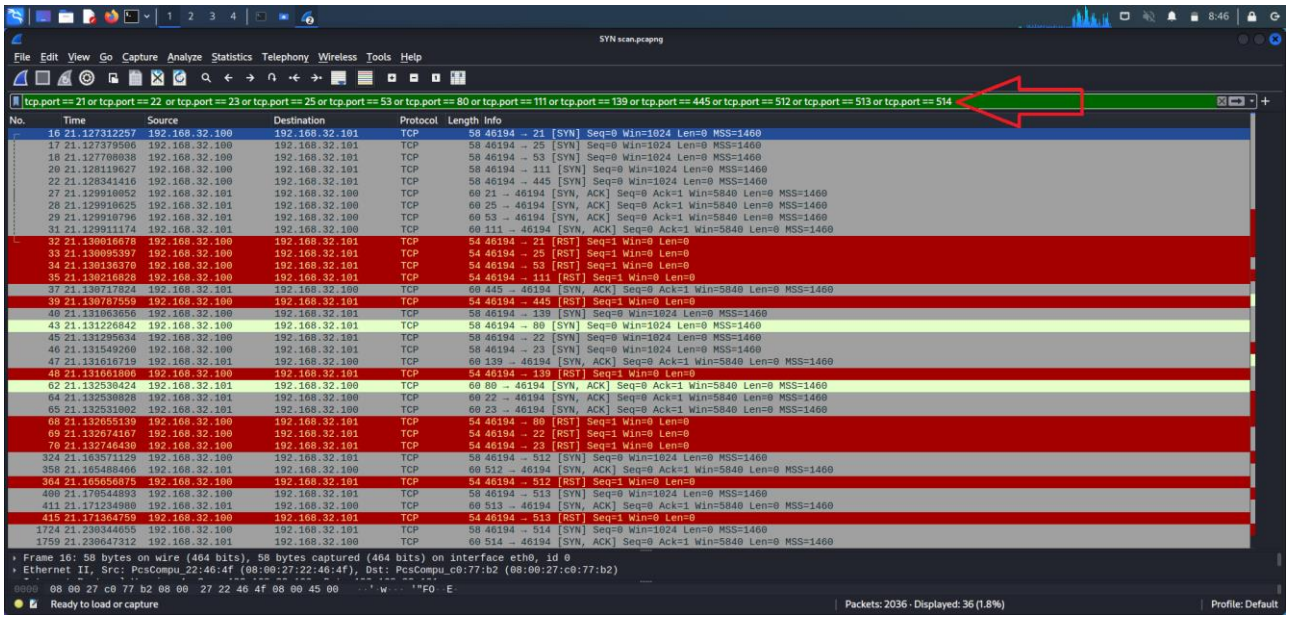
PORTE	STATE	SERVICE
21/tcp	Open	ftp
22/tcp	Open	ssh
23/tcp	Open	telnet
25/tcp	Open	smtp
53/tcp	Open	domain
80/tcp	Open	http
111/tcp	Open	rpcbind
139/tcp	Open	netbios-ssn
445/tcp	Open	microsoft-ds
512/tcp	Open	exec
513/tcp	Open	login
514/tcp	Open	shell

Tab1

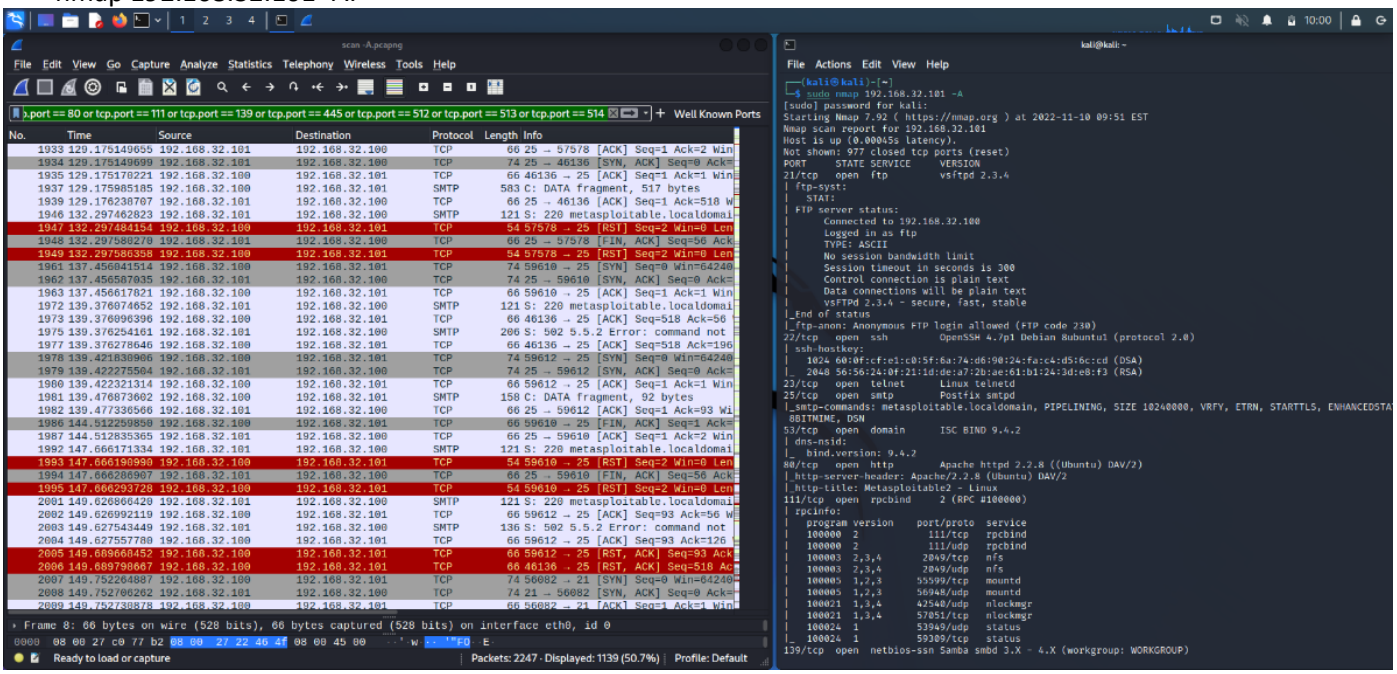
Durante la scansione abbiamo aperto Wireshark intercettando le richieste inviate dalla macchina sorgente.



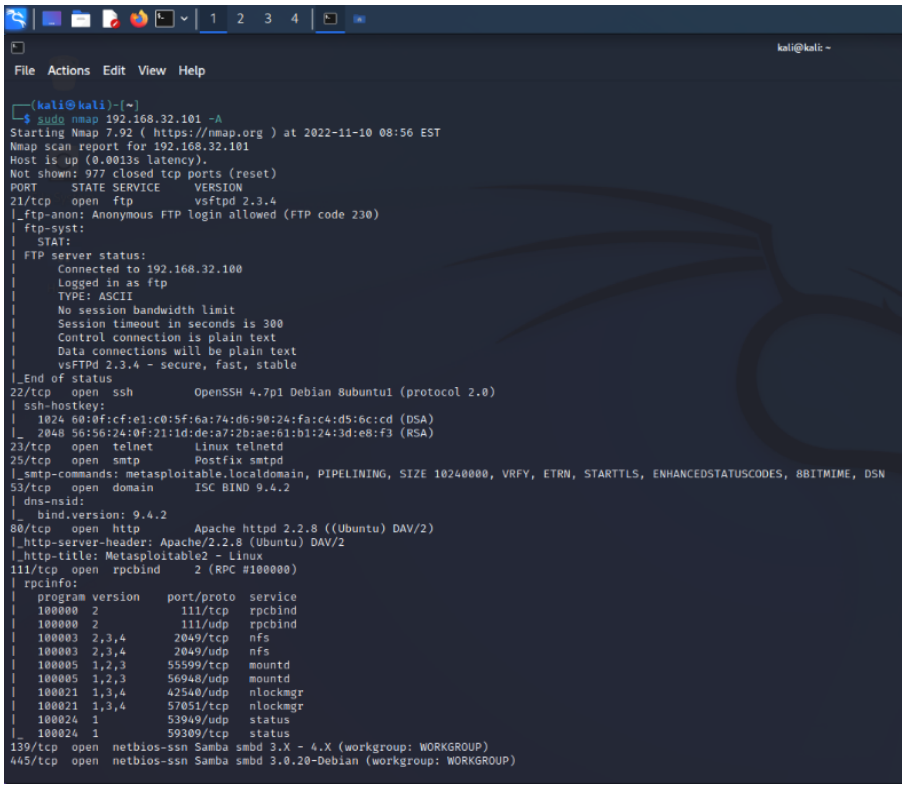
Abbiamo filtrato per vedere solo le porte interessate (Tab1):



Fatte le ricerche per nmap 192.168.32.101 -sT e per nmap 192.168.32.101 -sS abbiamo fatto una scansione nmap 192.168.32.101 -A:



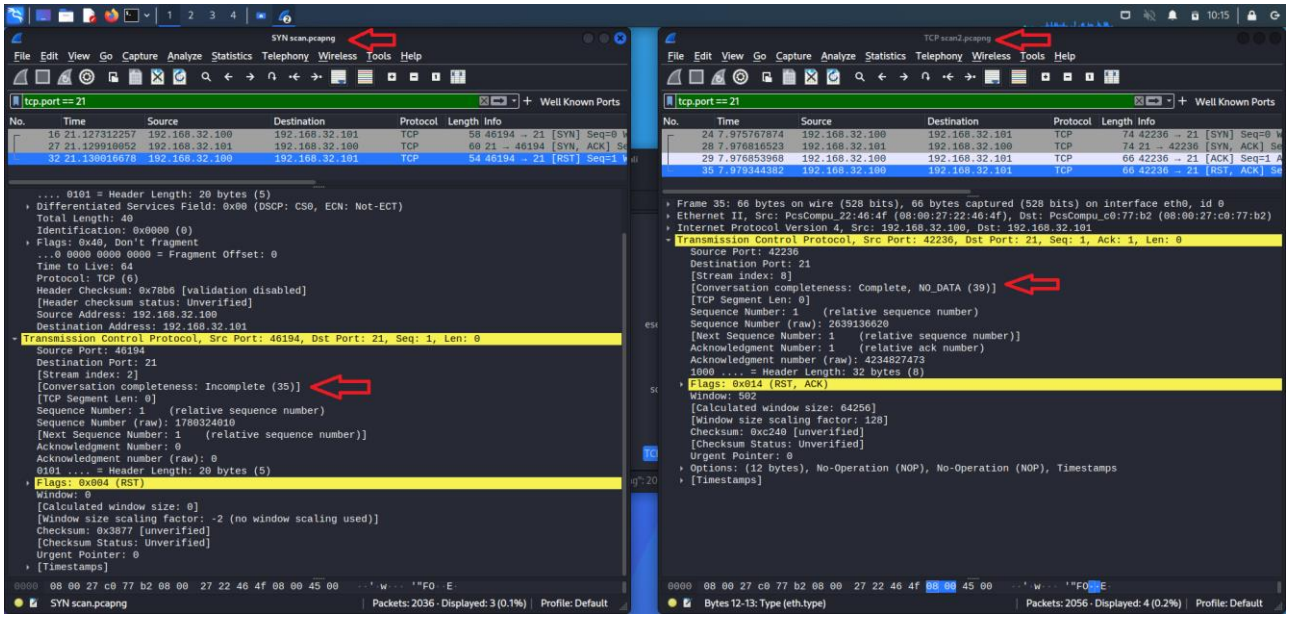
Come possiamo vedere la scansione nmap 192.168.32.101 -A fa una scansione molto più approfondita e aggressiva rispetto alle altre viste prima (img sopra e sotto).



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 192.168.32.101 -sT	23 servizi aperte di cui 12 di porte well-known

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