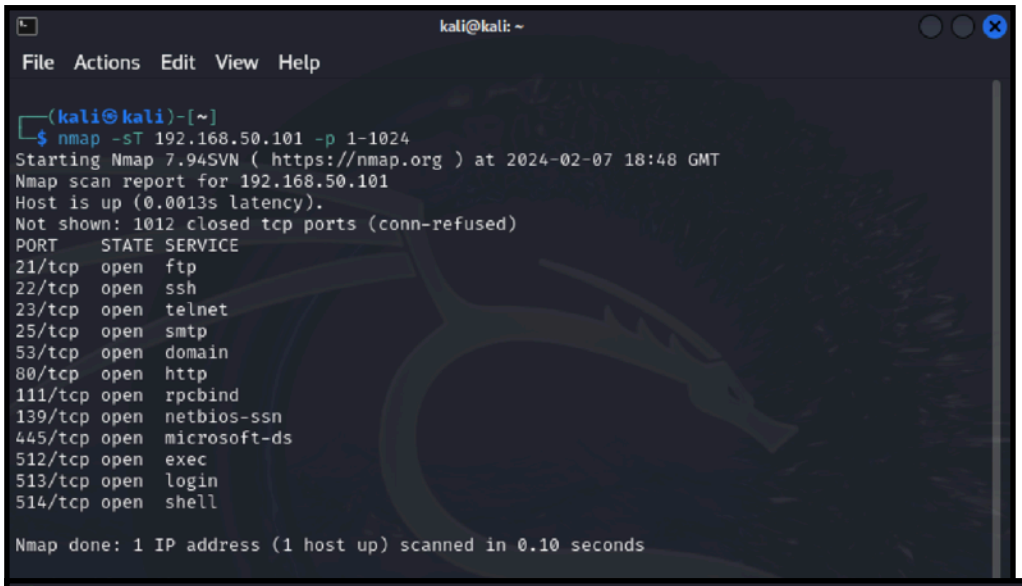
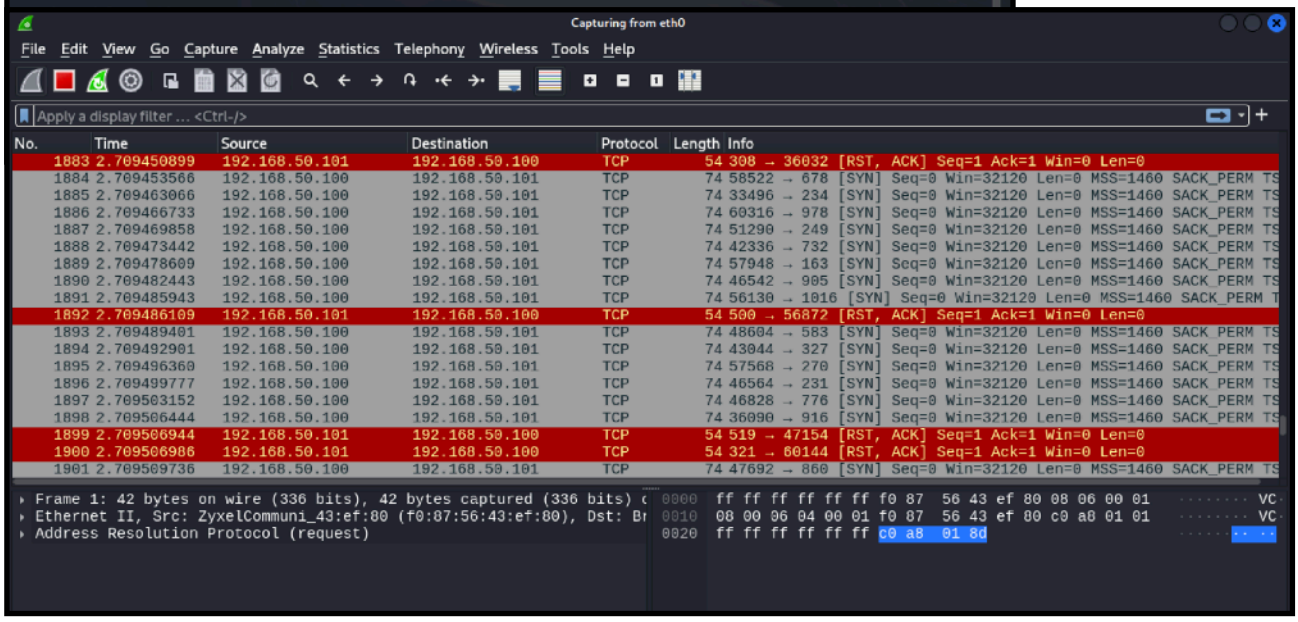
M3_W9D3

Scansione dei Servizi di Rete attivi tramite il tool Nmap di Kali Linux su macchina Metasploitable (192.168.50.101).

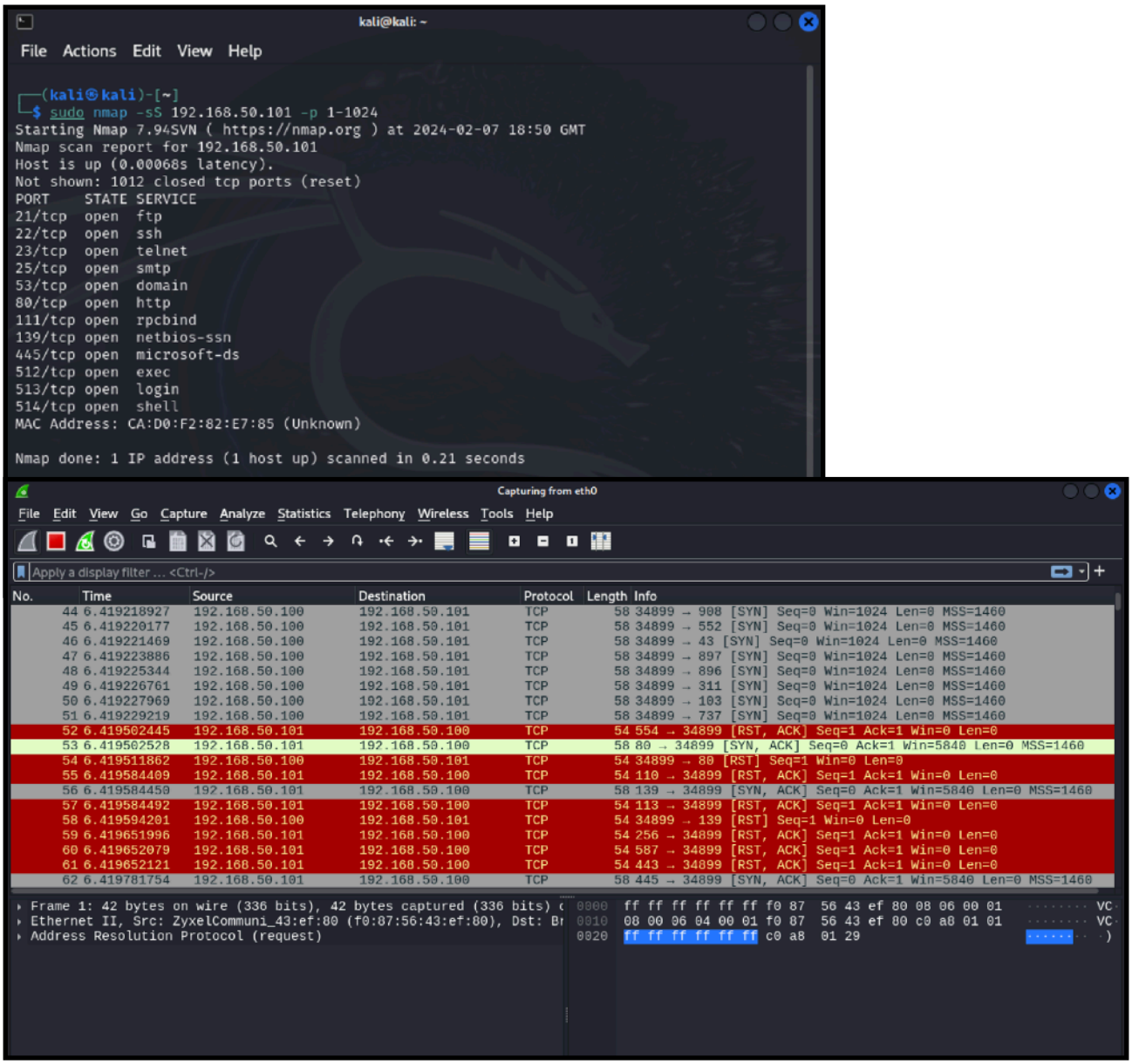
Prima scansione completa delle porte incluse nel range 1-1024 con la flag -sT.





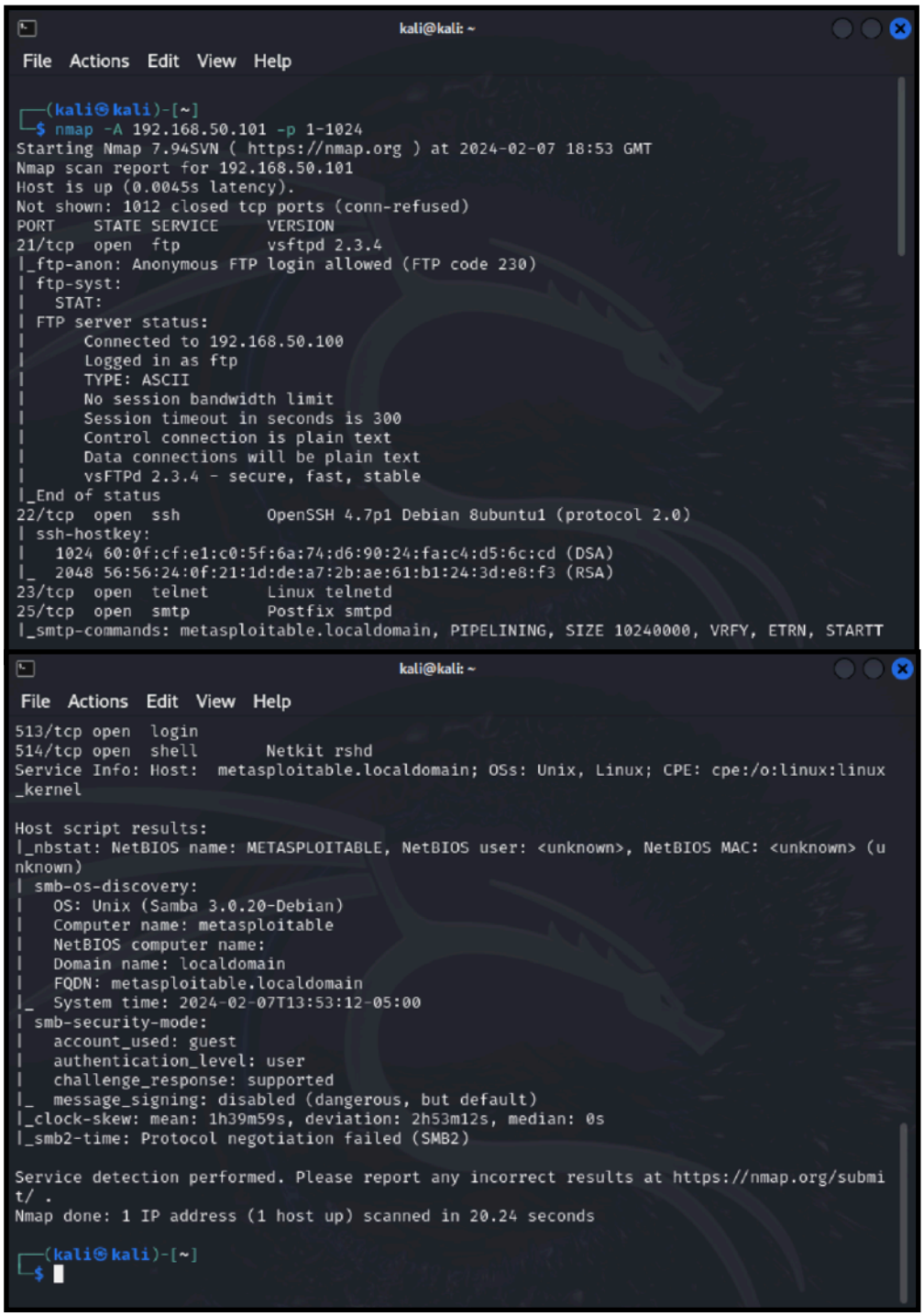
La scansione -sT è una delle opzioni disponibili in Nmap,
La flag -sT indica a Nmap di eseguire una scansione TCP connect.
Quando si esegue una scansione TCP connect (-sT), Nmap tenta di stabilire una connessione TCP completando.
Tuttavia, è importante notare che l'utilizzo di una scansione TCP connect può essere più rumorosa e meno furtiva rispetto ad altre tecniche di scansione offerte da Nmap, come -sS (scansione SYN).

Seconda scansione completa delle porte incluse nel range 1-1024 con la flag -sS.



Quando si esegue una scansione SYN stealth (-sS), Nmap invia pacchetti SYN al target su porte specifiche e analizza le risposte per determinare lo stato dei porti sul sistema di destinazione.
La scansione SYN stealth è considerata una delle tecniche di scansione più furtive, poiché non completa la connessione TCP come la scansione TCP connect (-sT). Invece, Nmap invia solo il pacchetto di SYN e analizza le risposte senza completare la connessione TCP.L'utilizzo della scansione SYN stealth è spesso preferito per eseguire scansioni di rete in modo discreto, in particolare quando si vuole evitare il rilevamento da parte dei sistemi di difesa della rete.

Terza scansione completa delle porte nel range 1-1024 con la flag -A.



La scansione con la flag -A in Nmap è una delle opzioni avanzate che fornisce un insieme completo di informazioni sull'host e sulle porte scansionate. Questa flag combina diverse tecniche di scansione e l'analisi dei dati raccolti per fornire una visione dettagliata delle caratteristiche del sistema target.
L'utilizzo della flag -A è consigliato quando si desidera ottenere informazioni complete e dettagliate sull'host di destinazione, inclusi dettagli sulla versione del servizio e sul sistema operativo. Tuttavia, è importante notare che l'utilizzo della flag -A può richiedere più tempo e risorse rispetto alle scansioni standard.

REPORT						
TCP SCAN (-sT)						
FONTE		TARGET	SCAN TYPE	SERVIZI ATTIVI		
Indirizzo IP	Range di Porte	Indirizzo IP	TCP	PORT	STATO	SERVIZIO
192.168.50.100	1-1024	192.168.50.101	TCP	21	OPEN	ftp
192.168.50.100	1-1024	192.168.50.101	TCP	22	OPEN	ssh
192.168.50.100	1-1024	192.168.50.101	TCP	23	OPEN	telnet
192.168.50.100	1-1024	192.168.50.101	TCP	25	OPEN	smtp
192.168.50.100	1-1024	192.168.50.101	TCP	53	OPEN	domain
192.168.50.100	1-1024	192.168.50.101	TCP	80	OPEN	http
192.168.50.100	1-1024	192.168.50.101	TCP	111	OPEN	rpcbind
192.168.50.100	1-1024	192.168.50.101	TCP	139	OPEN	netbios-ssn
192.168.50.100	1-1024	192.168.50.101	TCP	445	OPEN	microsoft-ds
192.168.50.100	1-1024	192.168.50.101	TCP	512	OPEN	exec
192.168.50.100	1-1024	192.168.50.101	TCP	513	OPEN	login
192.168.50.100	1-1024	192.168.50.101	TCP	514	OPEN	shell
SYN SCAN (-sS)						
192.168.50.100	1-1024	192.168.50.101	TCP	21	OPEN	ftp
192.168.50.100	1-1024	192.168.50.101	TCP	22	OPEN	ssh
192.168.50.100	1-1024	192.168.50.101	TCP	23	OPEN	telnet
192.168.50.100	1-1024	192.168.50.101	TCP	25	OPEN	smtp
192.168.50.100	1-1024	192.168.50.101	TCP	53	OPEN	domain
192.168.50.100	1-1024	192.168.50.101	TCP	80	OPEN	http
192.168.50.100	1-1024	192.168.50.101	TCP	111	OPEN	rpcbind
192.168.50.100	1-1024	192.168.50.101	TCP	139	OPEN	netbios-ssn
192.168.50.100	1-1024	192.168.50.101	TCP	445	OPEN	microsoft-ds
192.168.50.100	1-1024	192.168.50.101	TCP	512	OPEN	exec
192.168.50.100	1-1024	192.168.50.101	TCP	513	OPEN	login
192.168.50.100	1-1024	192.168.50.101	TCP	514	OPEN	shell