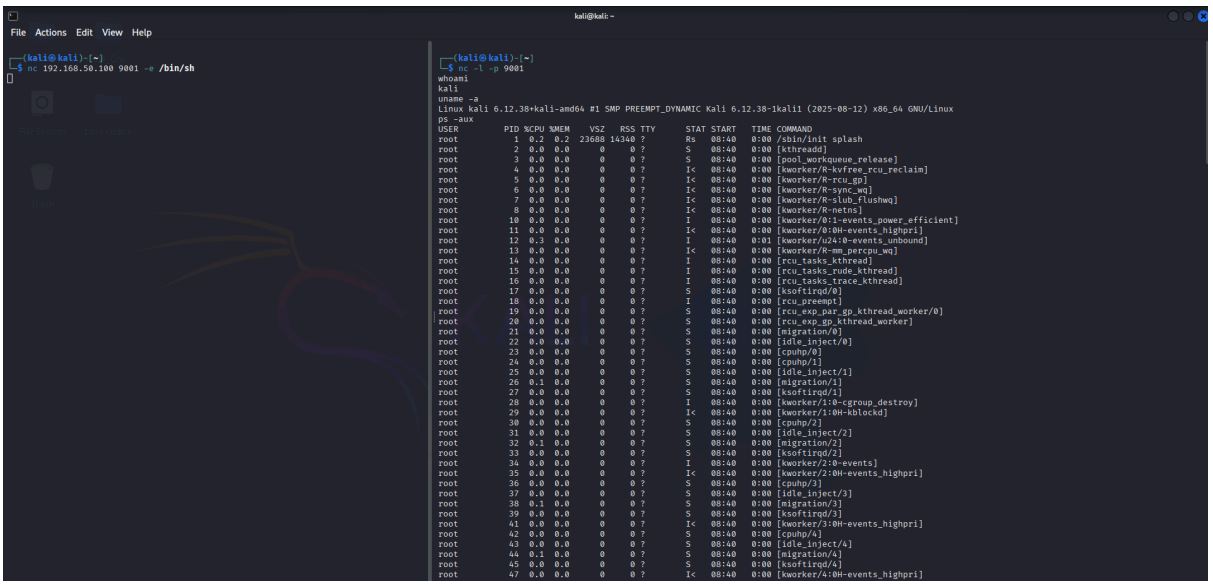
NETCAT E NMAP SCAN

- **Netcat**

Utilizziamo Netcat per aprire un listener per connessioni in entrata nella console di destra, Connettiamo invece la console di sinistra all'indirizzo della nostra macchina nella porta assegnata, creando una shell per poter eseguire comandi dal terminale.

Ora utilizziamo dei comandi dalla shell che siamo riusciti a creare, usiamo il comando "whoami" per sapere il nome utente corrente, successivamente usiamo il comando "uname -a" per avere informazioni sul sistema nel quale abbiamo la shell ed infine usiamo il comando "ps-aux" per vedere tutti i processi in esecuzione sulla macchina alla quale siamo connessi.

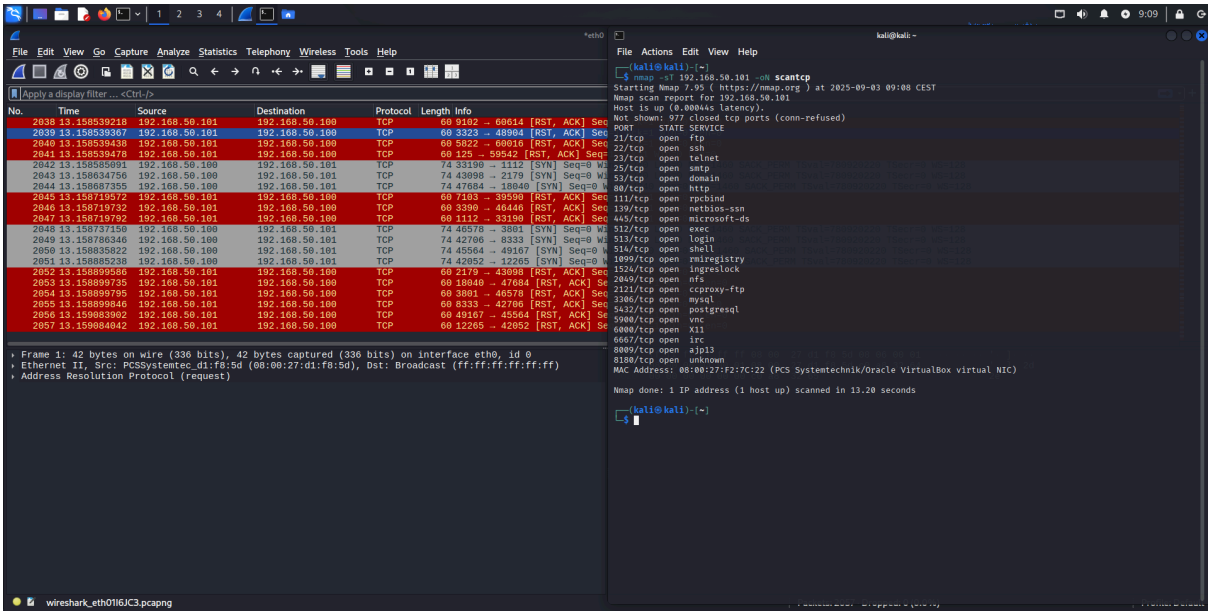


- **Nmap + Facoltativo**

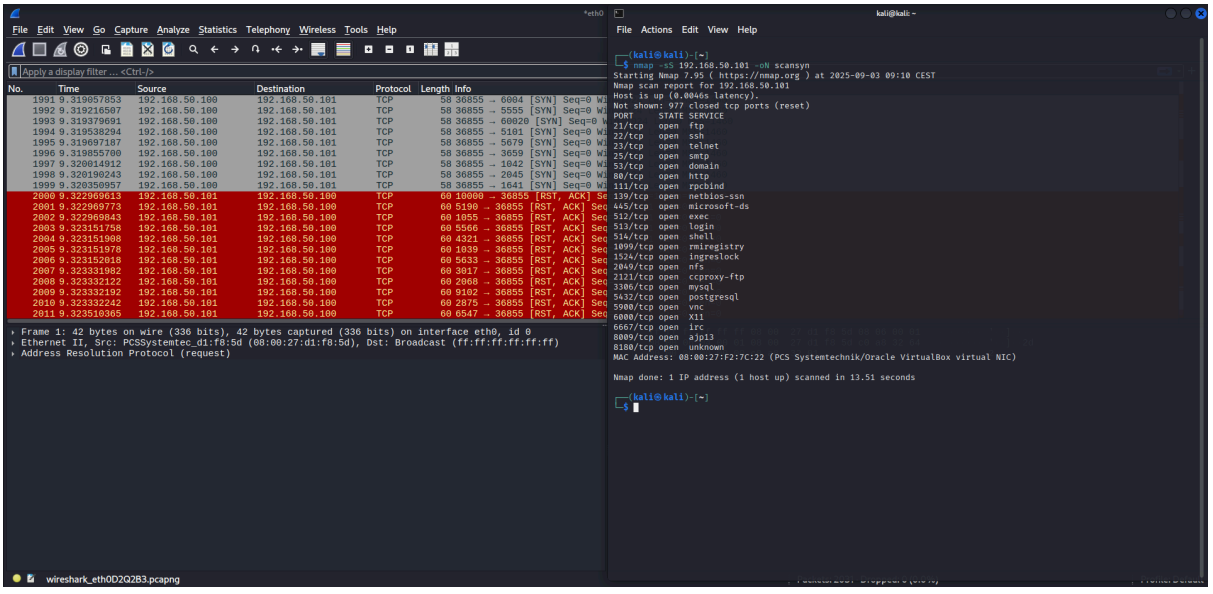
Valutiamo di fare una scansione delle porte aperte sulla nostra metasploitable

Fonte	Macchina Target	Tipo di scan	Numero porte attive
192.168.50.100	192.168.50.101	Tcp “-sT”	23 porte attive
192.168.50.100	192.168.50.101	SYN “-sS”	23 porte attive
192.168.50.100	192.168.50.101	“-A”	12 porte attive

Eseguiamo una scansione delle porte TCP catturando con wireshark le richieste fatte dalla nostra macchina attaccante e le risposte date dalla macchina target, possiamo vedere come la macchina attaccante cerchi di creare una connessione 3-way-handshake per scansionare le porte della macchina target.



Eseguiamo ora una scansione di tipo SYN catturando con wireshark le richieste fatte dalla nostra macchina attaccante e le risposte date dalla nostra macchina target, possiamo notare come la macchina attaccante chiuda la connessione tcp prima di dare una risposta alla macchina target chiudendo la connessione con un RST.



Eseguiamo ora una scansione piu' accurata utilizzando il flag “-A” catturando con wireshark le richieste fatte dalla nostra macchina attaccante e le risposte date dalla nostra macchina target, possiamo notare come il flag “-A” ci dia informazioni in piu' riguardanti le porte ed i servizi che trova aperte