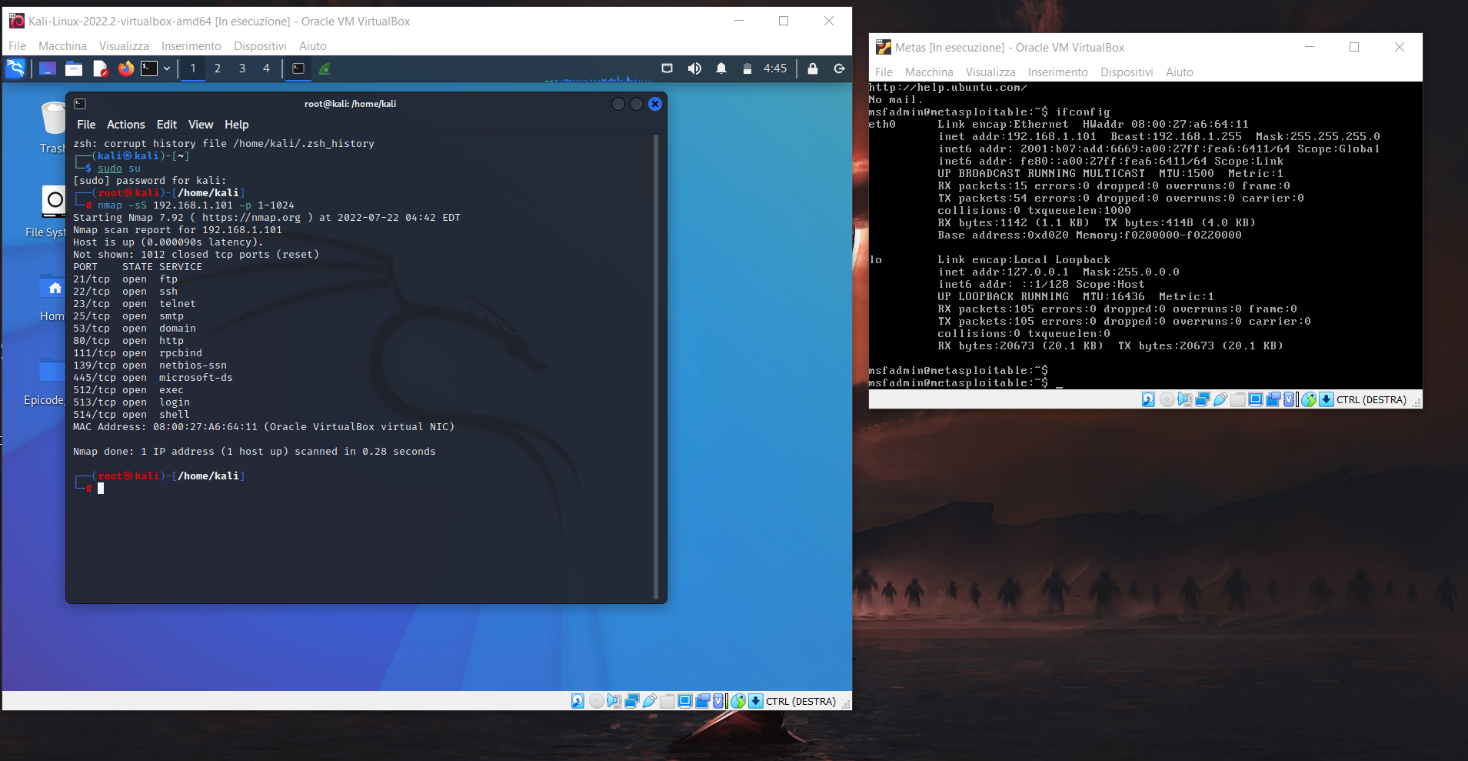
Scansioni con Nmap



Tramite la scansione col comando nmap -sS possiamo vedere lo stato delle porte con il relativo servizio, nella foto vediamo i vari servizi attivi:

Porta 21 ftp -> (file transfer protocol) è un protocollo usato per trasferire file tra computer su Internet. Si tratta di un protocollo basato sull'architettura client/server.

Porta 22 ssh -> (secure shell) è un protocollo che permette di stabilire una sessione remota con un altro host di una rete informatica.

Porta 23 telnet -> (terminal network) è un protocollo di rete, utilizzato tramite interfaccia a riga di comando per fornire all'utente sessioni di login remoto.

Porta 25 smtp -> (Simple Mail Transfer Protocol) è un protocollo standard per la trasmissione di email.

Porta 53 dns -> (domain name system) associa il nome di un dominio ad un indirizzo IP utilizzato dal computer.

Porta 80 http -> (Hypertext Transfer Protocol) è un protocollo a livello applicativo usato come sistema per la trasmissione d'informazioni sul web.

Porta 111 rcpbind -> converte i numeri RPC in indirizzi universali.

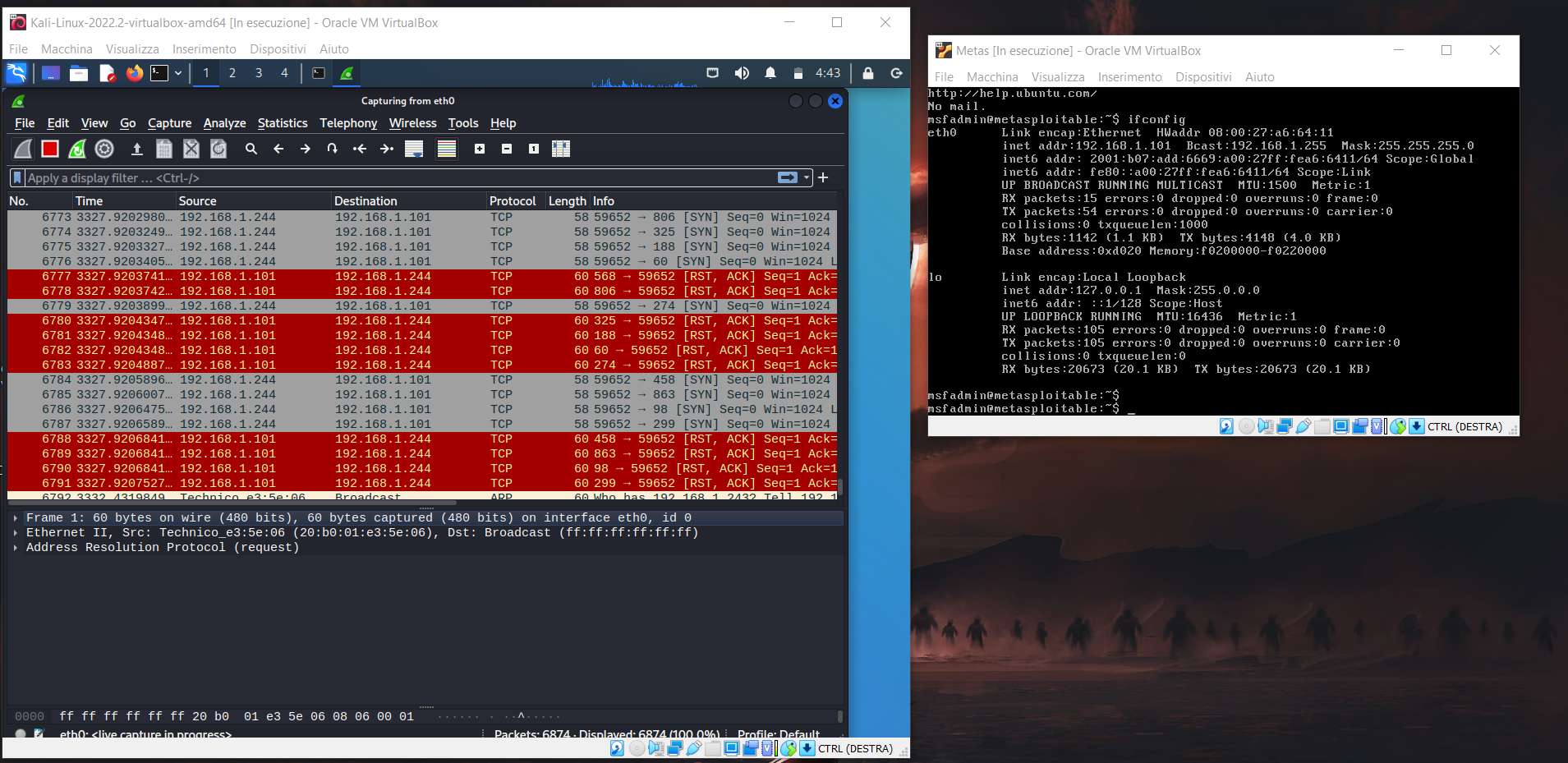
Porta 139 netbios-ssn -> (Network Basic Input/Output System), solitamente è riferito ad un'API per comunicazioni sulla rete locale.

Porta 512 exec -> (Remote Execution Protocol) si usa per eseguire un programma da remoto.

Porta 513 login -> utilizzato per l’amministrazione da remoto.

Porta 514 shell -> utilizzato per la manipolazione degli indirizzi IP.

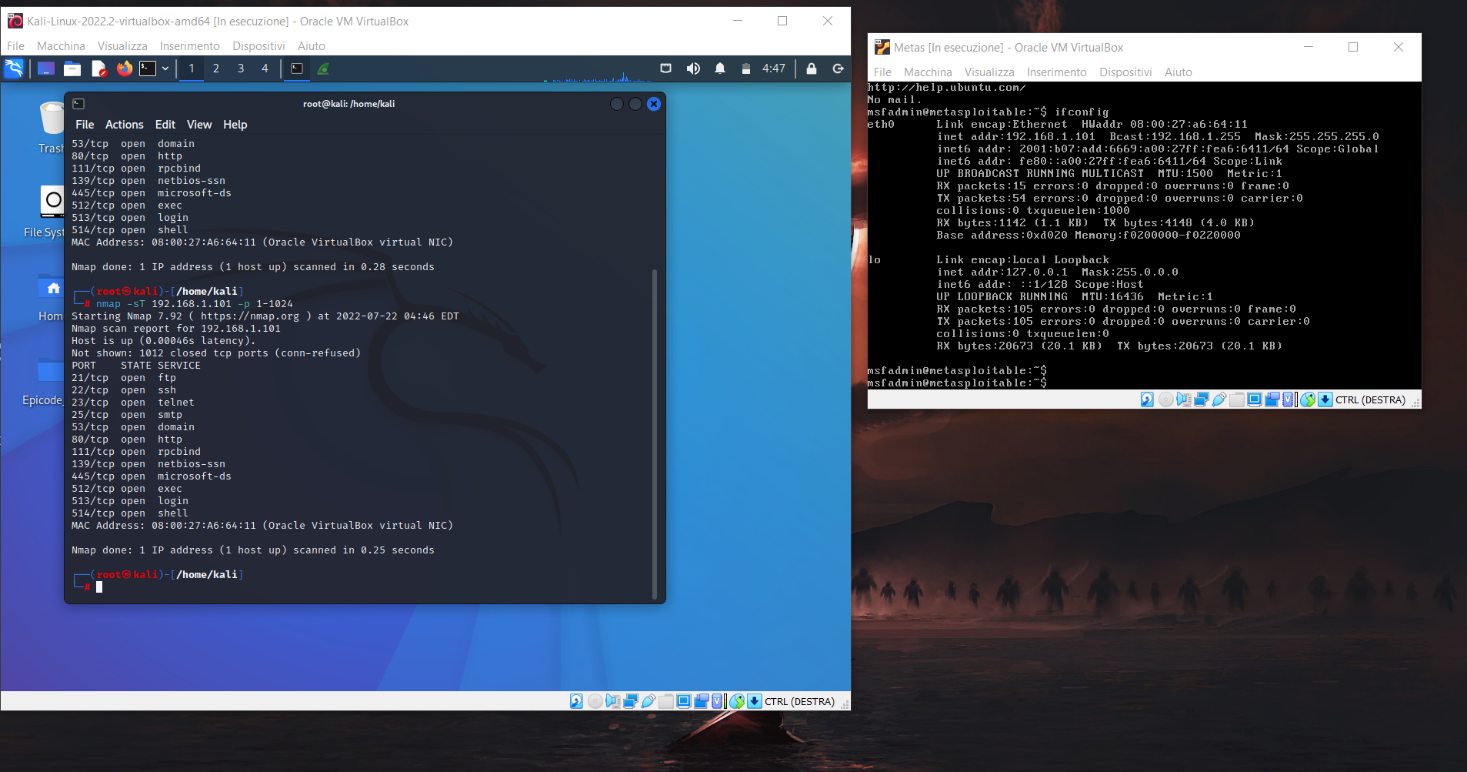
Possiamo notare anche l’indirizzo mac della macchina che stiamo ascoltando.



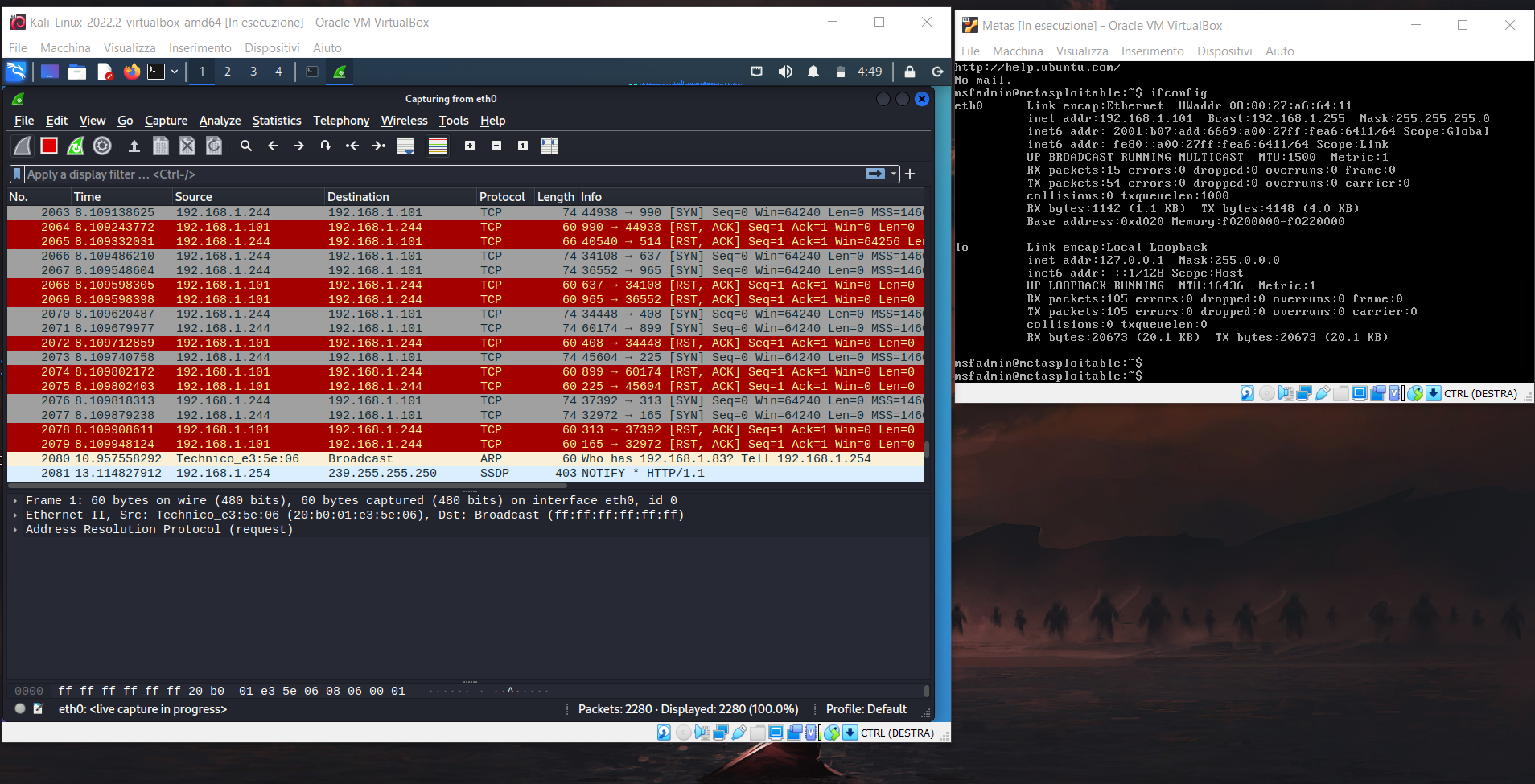
Tramite wireshark possiamo notare che la scansione -sS ovvero Syn scan,

una volta ricevuto il pacchetto dalla macchina che stiamo ascoltando, non conclude la stretta a 3 vie, ma sapendo che la porta è aperta chiude la comunicazione per evitare di fare rumore.

Ora vedremo le differenze con l’altro tipo di scansione.

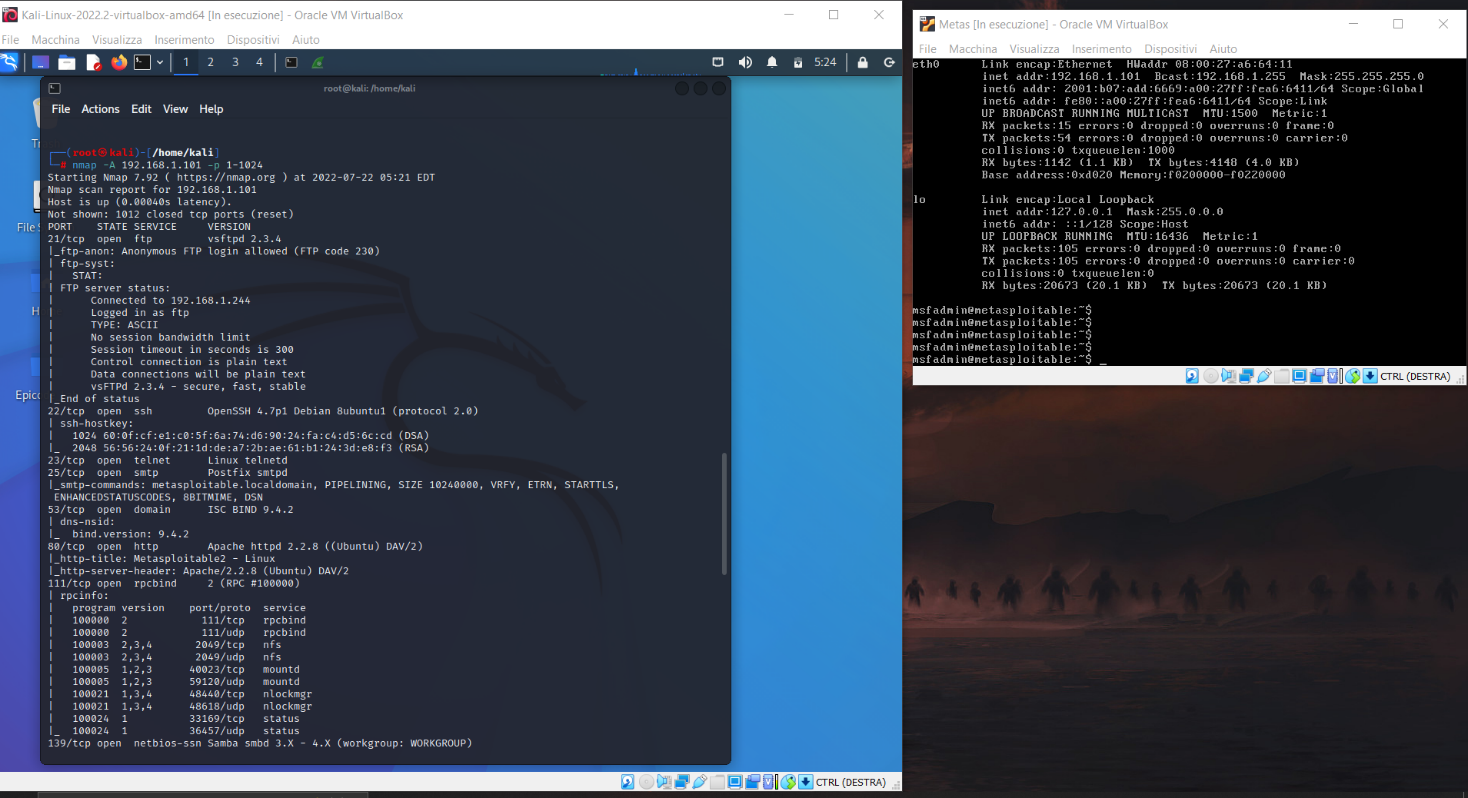
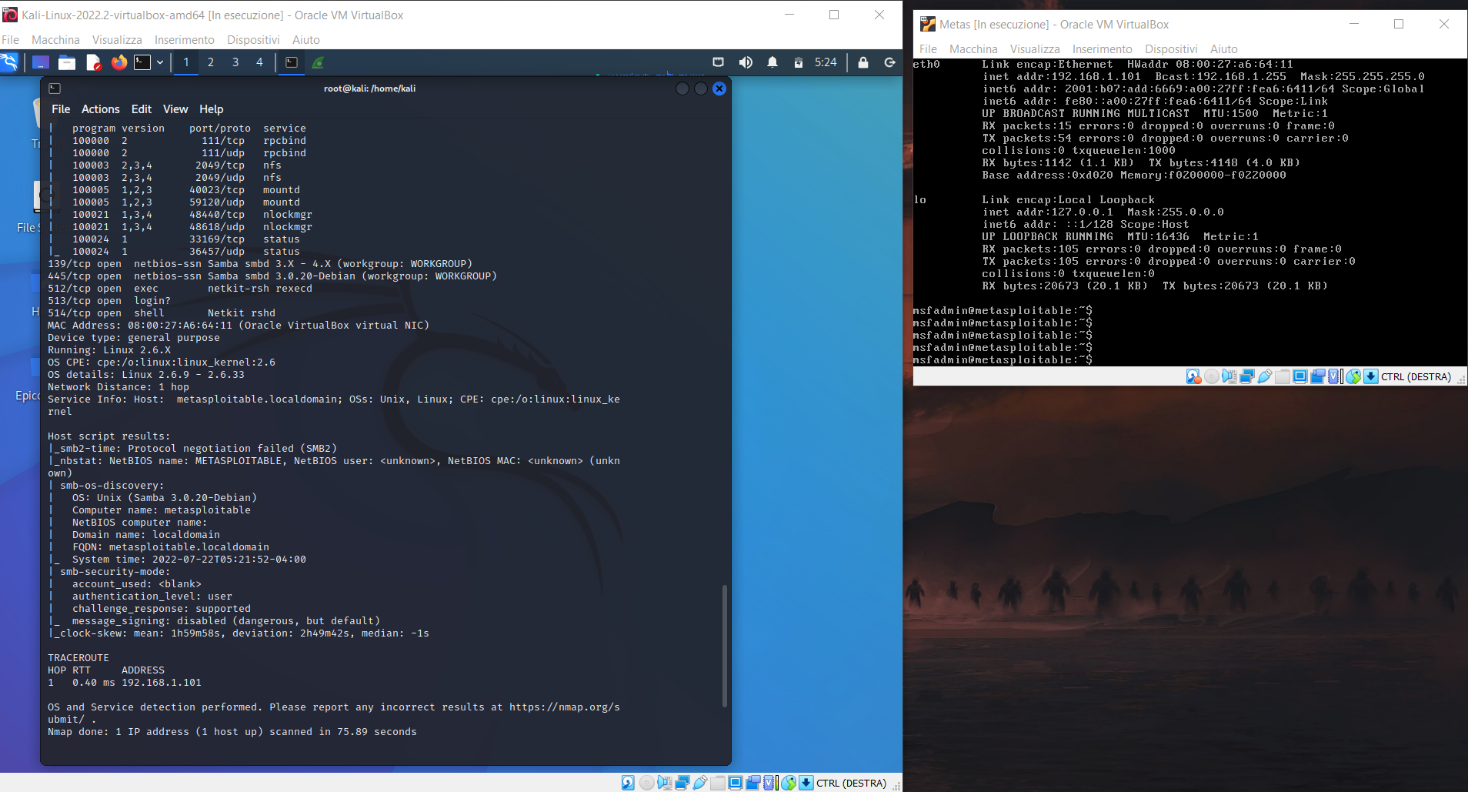


Come possiamo notare non ci sono differenze in termini di servizi o porte attive tra i due comandi.



Il comando -sT al contrario per vedere se una porta è aperta conclude tutti i passaggi della stretta a 3 vie rispondendo con un Ack, stabilendo una connessione.

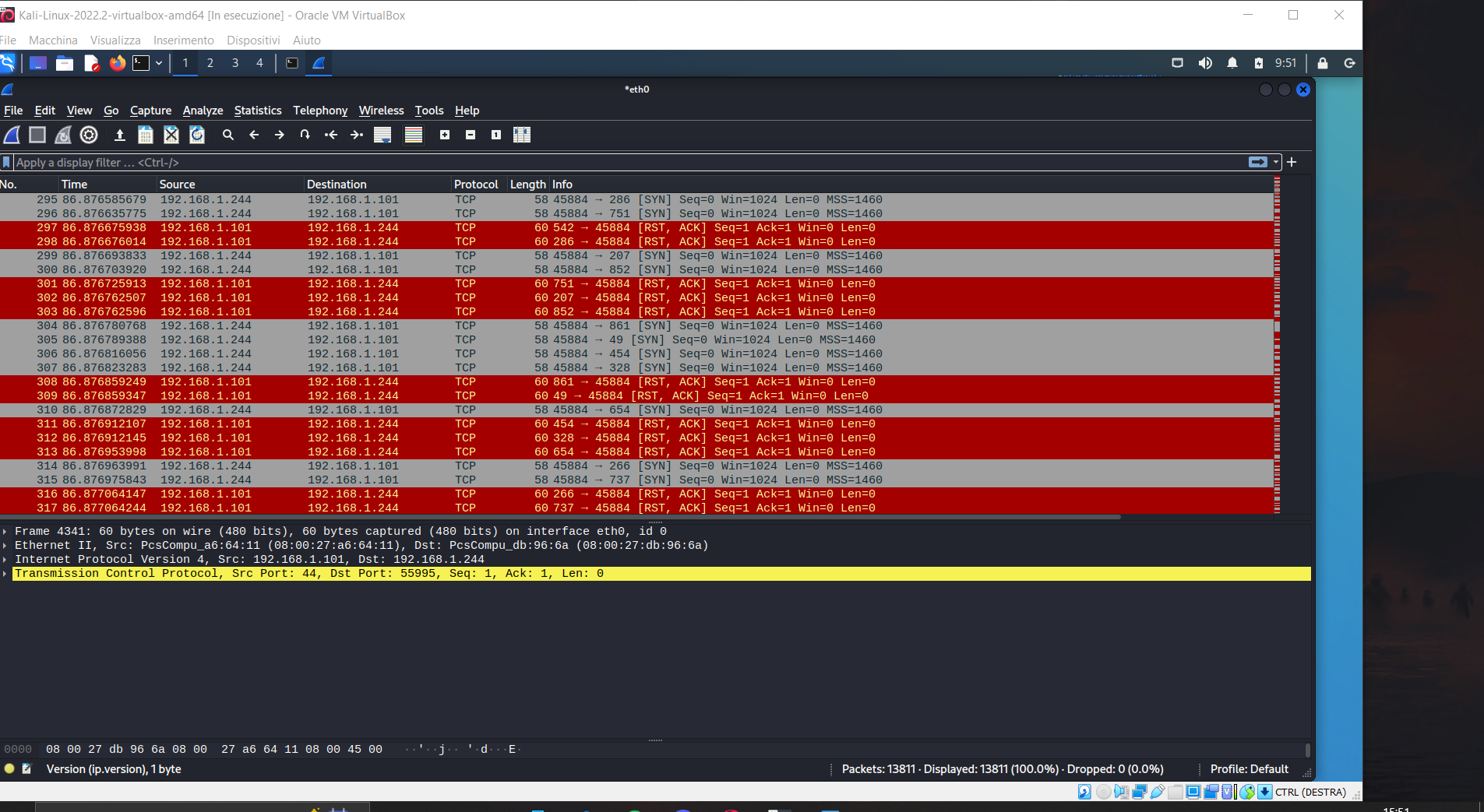
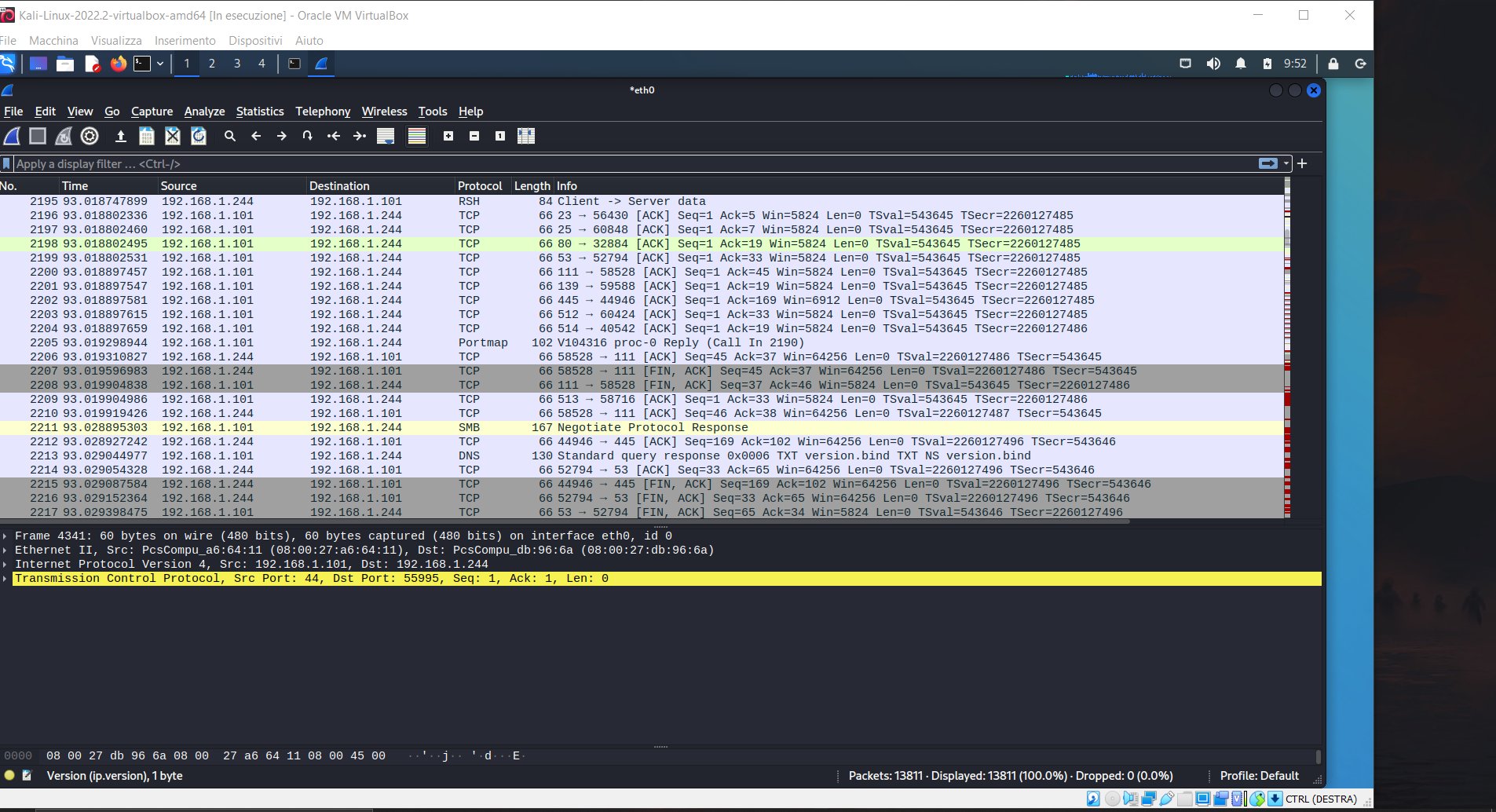
Le principali differenze dunque sono che con -sS non mandiamo l’ACK di risposta e chiudiamo la comunicazione, però riusciamo a recuperare informazioni relativo lo stato delle porte senza creare <rumore>.

Con -sT creiamo un canale completando la stretta di mano per recuperare le informazioni sulle porte però con questo metodo creiamo più rumore a livello di rete

Possiamo vedere che c’è un altro tipo di scansione ancora più approfondita e più rumorosa che si esegue con il comando -A.

Oltre ai vari alle cose già viste con questa scansione troviamo anche il tipo di Sistema Operativo e della versione, lo script scanning e il traceroute.

Trova anche dei servizi che con gli altri comandi non trova.

Anche con wireshark possiamo notare il maggior numero di pacchetti trovati oltre ai protocolli e ip sorgente e destinatario.

Per riassumere :

-Fonte scan ip Kali

-Target scan ip Metaspoitable