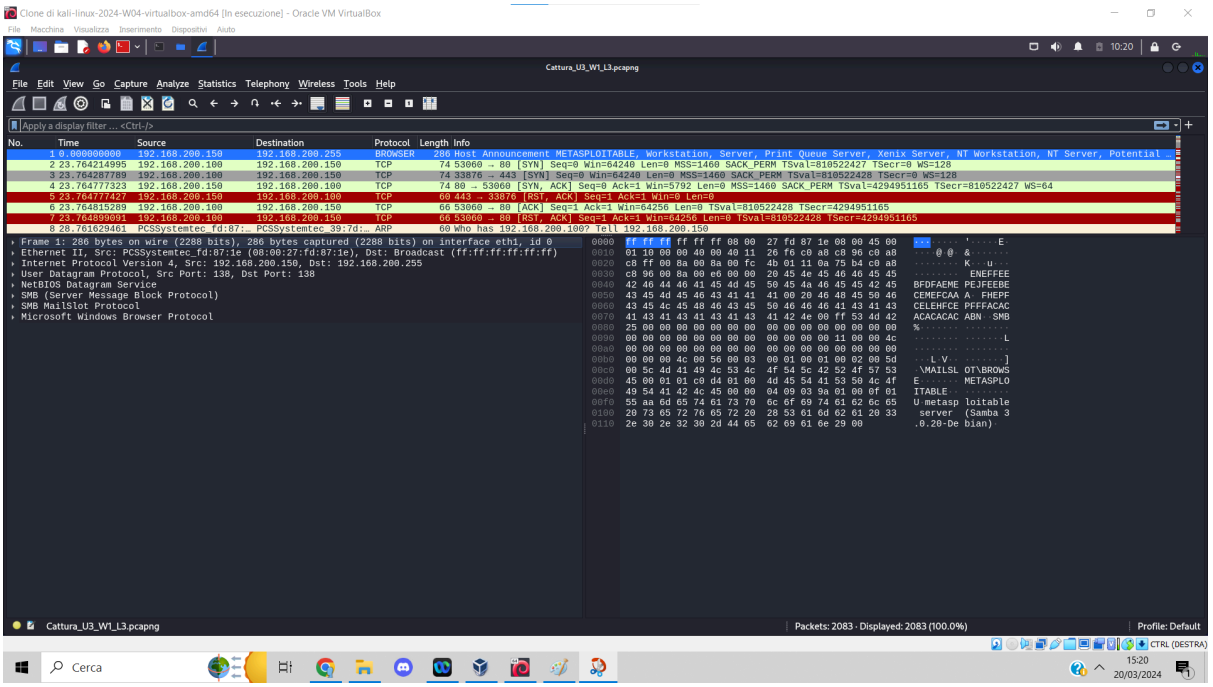
una volta aperto il file dentro kali tramite la cartella condivisa
ci si aprirà wireshark :



Immediatamente notiamo un'elevata quantità di pacchetti TCP SYN provenienti da due indirizzi IP sconosciuti, suggerendo possibili attività malintenzionate. Questo flusso massiccio di richieste potrebbe indicare un tentativo di scansione delle porte dell'host di destinazione, finalizzato a individuare vulnerabilità (conosciuto come scansione malevola delle porte), oppure, più preoccupante, potrebbe essere un attacco mirato a sovraccaricare l'host di destinazione, rendendolo inaccessibile (DDoS).

In aggiunta, osservando un notevole traffico di richieste ARP, il che potrebbe indicare un'ulteriore tattica dell'attaccante. In particolare, potrebbe essere coinvolto l'ARP spoofing, un metodo attraverso il quale un malintenzionato può dirottare il traffico di rete verso un dispositivo compromesso.

Basandomi su questi Indicatori di Compromissione (IOC), è plausibile supporre che sia stato attuato un attacco di ARP spoofing per dirottare il traffico verso due host compromessi. Il ARP spoofing è una tecnica che consente a un aggressore di fingere di essere un altro host sulla rete. In questo scenario, gli host compromessi inviano una serie di pacchetti TCP SYN al target designato, saturandolo e rendendolo inaccessibile.

Per difendersi efficacemente da attacchi di ARP spoofing, è necessario adottare diverse misure di protezione:

- Mantenere aggiornati i software di sistema e del sistema stesso al fine di correggere eventuali vulnerabilità sfruttabili dagli attacchi ARP spoofing.
- Configurare il firewall per bloccare specificamente i pacchetti ARP spoofing.
- Implementare un sistema SIEM per rilevare e rispondere agli attacchi ARP spoofing in tempo reale.
- Educare gli utenti sulle pratiche di sicurezza informatica al fine di prevenire con successo gli attacchi di ARP spoofing