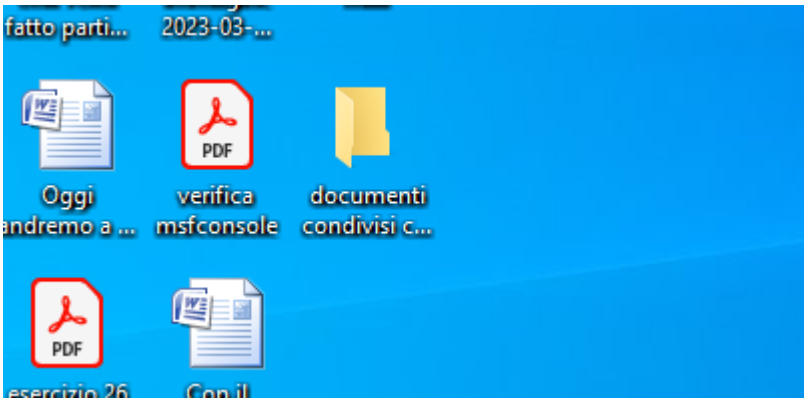
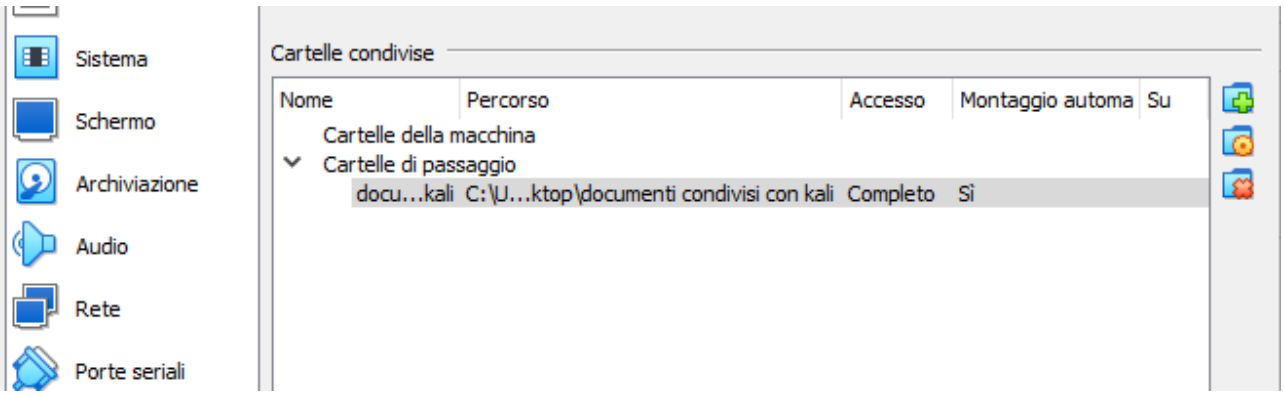
Oggi andremo ad analizzare un una cattura con whyreshark alla ricerca di un IOC, quindi di una prova di un attacco in corso.

Per prima cosa creiamo la cartella condivisa sull mio windows 10 che chiameremo “documenti condivisi con kali”:



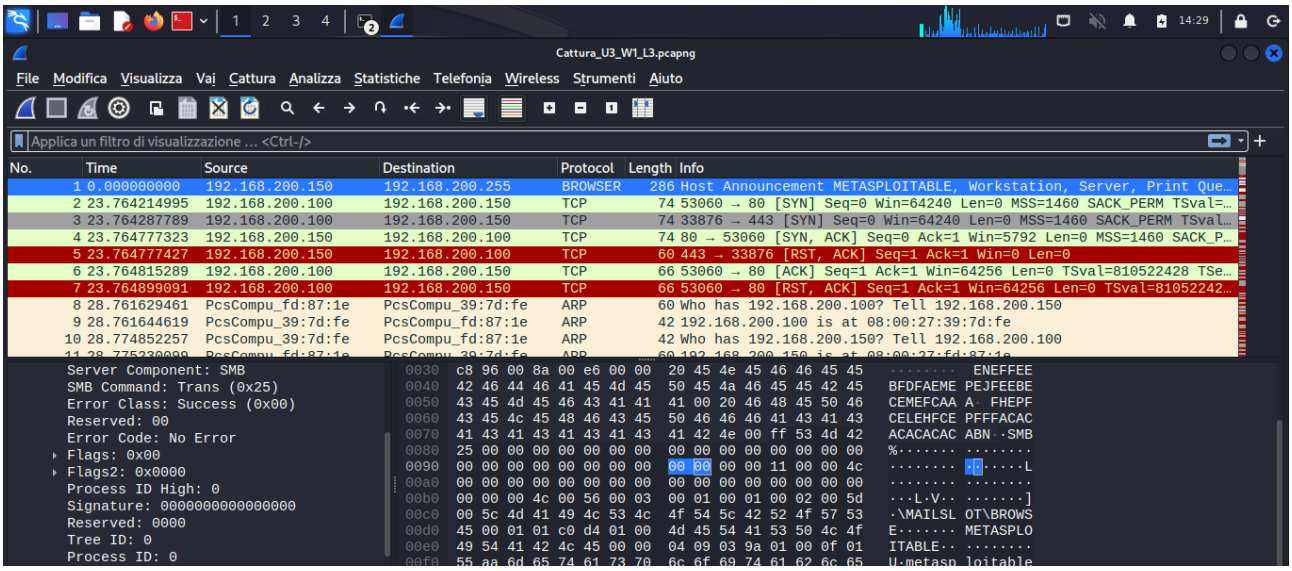
Una volta creata la cartella, creiamo il collegamento con la macchina virtuale:



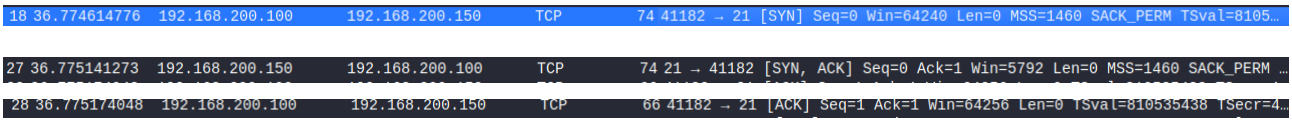
Ed una volta che abbiamo creato il collegamento e caricato il file in questione nella cartella condivisa, lo apriamo da terminale linux:

```
File  Azioni  Modifica  Visualizza  Aiuto
┌──(root㉿kali)-[~]
└─# cd /media

┌──(root㉿kali)-[/media]
└─# pwd
/media

┌──(root㉿kali)-[/media]
└─# ls
cdrom  cdrom0  sf_documenti_condivisi_con_kali

┌──(root㉿kali)-[/media]
└─# cd sf_documenti_condivisi_con_kali

┌──(root㉿kali)-[/media/sf_documenti_condivisi_con_kali]
└─# ls
Cattura_U3_W1_L3.pcapng

┌──(root㉿kali)-[/media/sf_documenti_condivisi_con_kali]
└─#
```

Ora che abbiamo il documento sulla nostra macchina virtuale, lo carichiamo su whyreshark e siamo pronti allo spoofing:



La prima cosa che mi balza all'occhio e che sia in corso una scansione delle porte(che sappiamo serve proprio per vedere quali porte aperte ha la macchina attaccata ed in caso vedere se sono presenti servizi vulnerabili su quest ultime). Si puo evincere dal fatto che vengono richieste connessioni velocemente e con tante porte diverse. Si puo notare anche che l'ip attaccante (192.168.200.100)stia cercando di connettersi con l'ip della macchina attaccata (192.168.200.150) con un approccio invasivo, tentando di chiudere il 3wayhandshake, come si puo evincere dal fatto che sono presenti i parametri syn ed ack nel tentativo di connessione. Infatti possiamo notare come la macchina attaccante, quando trova una porta perta possa chiudere il 3 way hand shake :



Come possiamo notare, la machina attaccante ha trovato una porta aperta (la 21) finendo il 3 way hand shake.

Nello specifico, possiamo notare come l'ip attaccante (192.168.200.100) mandi un pacchetto (SYN9 dalla porta 41182 alla porta 21 della macchina attaccata (192.168.200.150) e come la macchina attaccata accetti il pacchetto e ne rimandi uno indietro (SYN ACK) ed infine la macchina attaccante chiuda il 3 way hand shake rimandando un pacchetto (ACK) alla macchina attaccata scoprendo che, effettivamente, la porta e aperta.

La soluzione che io impronterei subito per far fronte alla situazione e creare una policy nel firewall che vieti alla macchina attaccata di scambiare pacchetti con fonti esterne, oppure fare (molto piu lungo pero) un P.T. sulla macchina attaccata, scoprire quali sono i servizi vulnerabili e di conseguenza chiuderli, lasciando aperte e visionabili solo le porte che offrono servizi sicuramente non attaccabili.