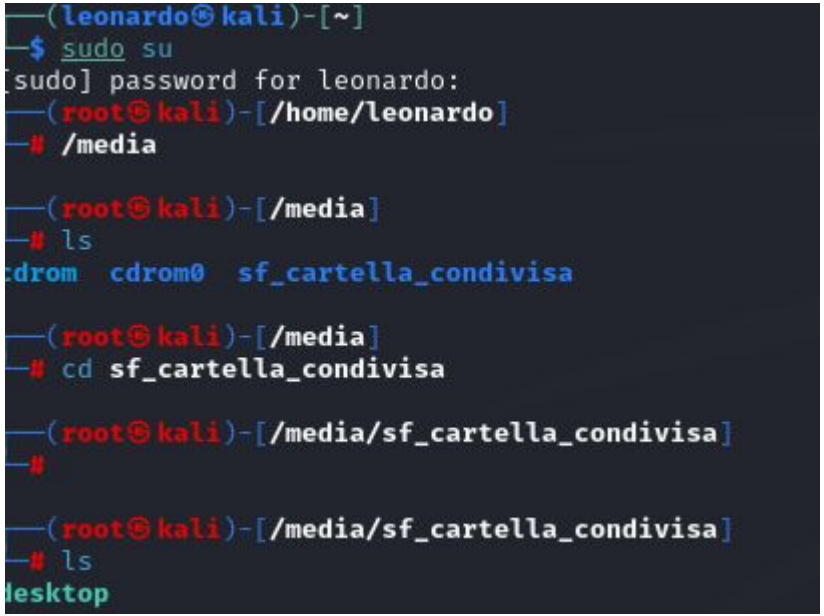
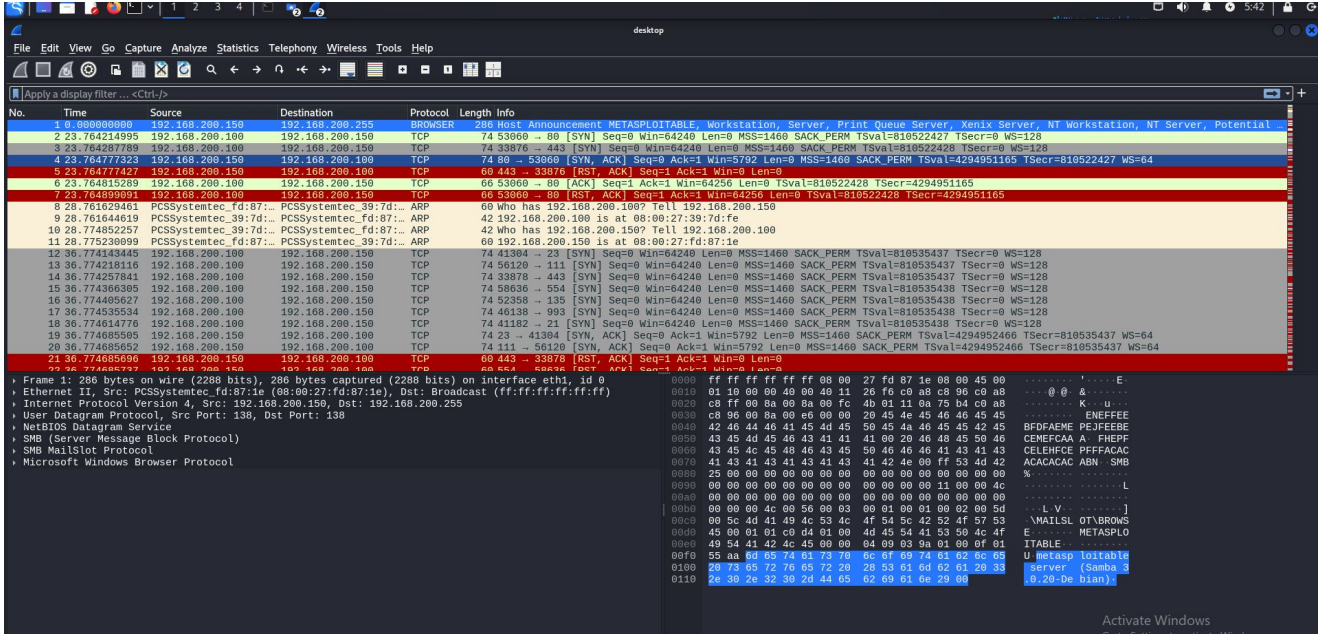



con questa prima immagine si puo notarer che tramite i comandi stiamo andando a navigare tra le directory per arrivare a quella denominata cartella condivisa dove abbiamo il file chiamato cattura_u3_w1_l3 che deve da noi essere analizzato




in questa immagine possiamo vedere il file aperto
e una volta analizzato ci rendiamo conto che si  tratta di attacco

## 1. ARP Spoofing/Poisoning

**Descrizione:** ARP Spoofing o ARP Poisoning è un tipo di attacco in cui l'attaccante invia messaggi ARP (Address Resolution Protocol) falsificati sulla rete locale. L'obiettivo è collegare l'indirizzo MAC dell'attaccante con l'indirizzo IP di un altro dispositivo, di solito il gateway di rete o un altro dispositivo di destinazione. **Effetto:** L'attaccante può intercettare, modificare o interrompere il traffico tra i dispositivi della rete. **Mitigazione:**

- Utilizzare tecnologie di sicurezza come DHCP Snooping e Dynamic ARP Inspection (DAI).
- Abilitare il port security sui dispositivi di rete per limitare gli indirizzi MAC che possono accedere alla rete.

## 2. SYN Flood

**Descrizione:** Un SYN Flood è un tipo di attacco Denial-of-Service (DoS) che sfrutta il processo di handshake TCP, inondando il server di pacchetti SYN (synchronize) senza completare il handshake. **Effetto:** Il server può diventare incapace di rispondere alle richieste legittime, esaurendo le risorse disponibili per nuove connessioni. **Mitigazione:**

- Abilitare SYN Cookies per gestire in modo efficiente le richieste SYN.
- Configurare il firewall per limitare le richieste SYN e proteggere il server.
- Implementare rate limiting per controllare il numero di connessioni in un determinato periodo.

**3. TCP Reset Attack**

**Descrizione:** In un TCP Reset Attack, l'attaccante invia pacchetti TCP con il flag RST (reset) impostato per interrompere le connessioni esistenti tra due dispositivi. **Effetto:** L'interruzione delle connessioni può causare interruzioni nei servizi e nella comunicazione tra i dispositivi della rete. **Mitigazione:**

- Utilizzare firewall e IDS/IPS per monitorare e bloccare pacchetti RST sospetti.
- Configurare il tempo di inattività del timeout TCP per ridurre la finestra di opportunità per gli attacchi.

**4. Enumerazione SMB**

**Descrizione:** L'enumerazione SMB coinvolge la raccolta di informazioni sui dispositivi e servizi disponibili su una rete utilizzando il protocollo SMB (Server Message Block). **Effetto:** L'attaccante può ottenere informazio

ni sui dispositivi della rete, come nomi di computer, condivisioni di rete e utenti, che possono essere utilizzate per ulteriori attacchi.
**Mitigazione:**

- Disabilitare l'SMBv1 e utilizzare versioni più sicure del protocollo SMB (SMBv2 o SMBv3).
- Configurare il firewall per limitare l'accesso ai servizi SMB.
- Implementare politiche di sicurezza rigide per le condivisioni di rete e gli ute