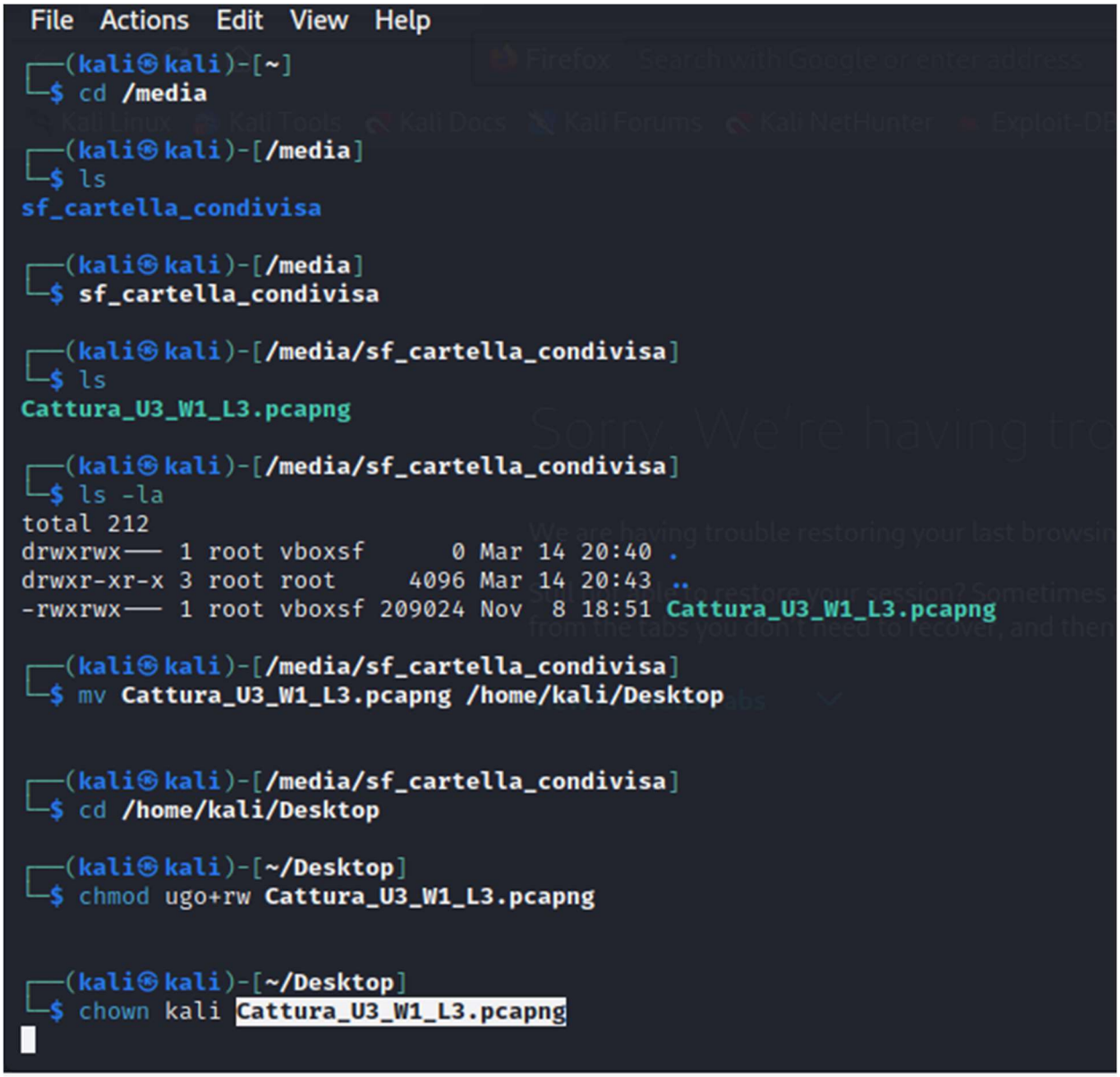
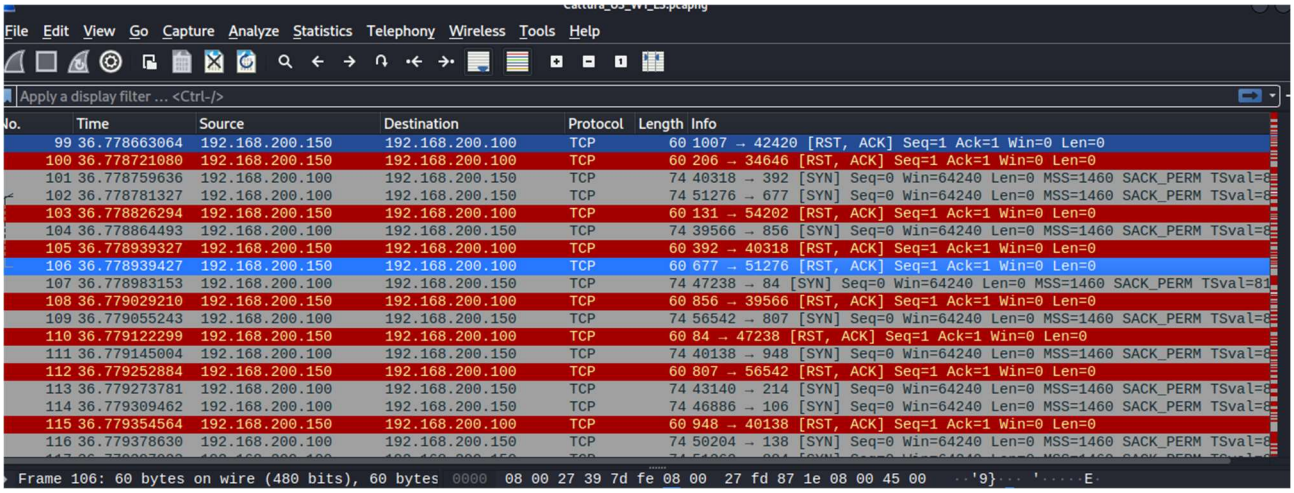
Traccia:

Durante la lezione teorica, abbiamo visto la Threat Intelligence e gli indicatori di compromissione. Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto. Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark. Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

- Identificare eventuali IOC, ovvero evidenze di attacchi in corso
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliate un'azione per ridurre gli impatti dell'attacco





- Multiple richieste TCP su ampi intervalli di porte, generalmente evidenzia una scansione in corso.
- Quando si osservano molteplici richieste TCP su ampi intervalli di porte, ci sono diverse ipotesi sui potenziali vettori di attacco che potrebbero essere utilizzati da parte degli aggressori:

1. Scansione delle porte per individuare vulnerabilità: Gli aggressori potrebbero effettuare una scansione delle porte per individuare servizi o protocolli aperti su un sistema. Questo potrebbe essere un precursore per individuare eventuali vulnerabilità note o configurazioni non sicure sui servizi in esecuzione.

2. Preparazione per un attacco mirato: Una scansione delle porte può essere utilizzata come fase preliminare per preparare un attacco mirato. Gli aggressori potrebbero cercare di individuare servizi specifici o applicazioni vulnerabili che possono essere sfruttate in seguito per compromettere il sistema o la rete.

3. Ricerca di punti di ingresso: Gli aggressori potrebbero essere alla ricerca di possibili punti di ingresso nella rete, come porte aperte o servizi non protetti, che possono essere utilizzati per ottenere accesso non autorizzato ai sistemi o per diffondere malware all'interno dell'ambiente aziendale.

4. Raccolta di informazioni per futuri attacchi: La scansione delle porte può essere utilizzata per raccogliere informazioni sulle infrastrutture di rete e sulle configurazioni dei sistemi. Queste informazioni possono essere utilizzate per pianificare attacchi più mirati e sofisticati in futuro.

- Quando si rileva un alto numero di richieste TCP su ampi intervalli di porte, ciò potrebbe indicare un comportamento tipico di scansione di rete da parte di un attaccante. Per ridurre gli impatti di tale attacco, è consigliabile adottare diverse azioni:

1. Monitoraggio del traffico di rete: Implementare un sistema di monitoraggio del traffico di rete per rilevare e analizzare le attività di scansione. Questo può aiutare a identificare rapidamente gli indirizzi IP sospetti o le serie di porte coinvolte nell'attività di scansione.

2. Blocco degli indirizzi IP sospetti: Utilizzare firewall o sistemi di rilevamento delle intrusioni per bloccare gli indirizzi IP che sono coinvolti nell'attività di scansione. Questo può limitare l'accesso dell'attaccante alla rete e ridurre l'impatto degli attacchi.

3. Limitazione dei tentativi di connessione: Impostare politiche per limitare il numero di tentativi di connessione per unità di tempo da parte di singoli indirizzi IP. Questo può aiutare a prevenire attacchi di scansione che tentano di individuare servizi aperti o vulnerabilità di sicurezza.

4. Implementazione di sistemi di autenticazione e accesso sicuri: Utilizzare sistemi di autenticazione robusti e meccanismi di accesso sicuri come VPN (Virtual Private Network) per proteggere l'accesso alla rete e ai servizi interni. Ciò può ridurre la possibilità che gli attaccanti utilizzino le scansioni di rete per individuare punti deboli nell'infrastruttura di sicurezza.