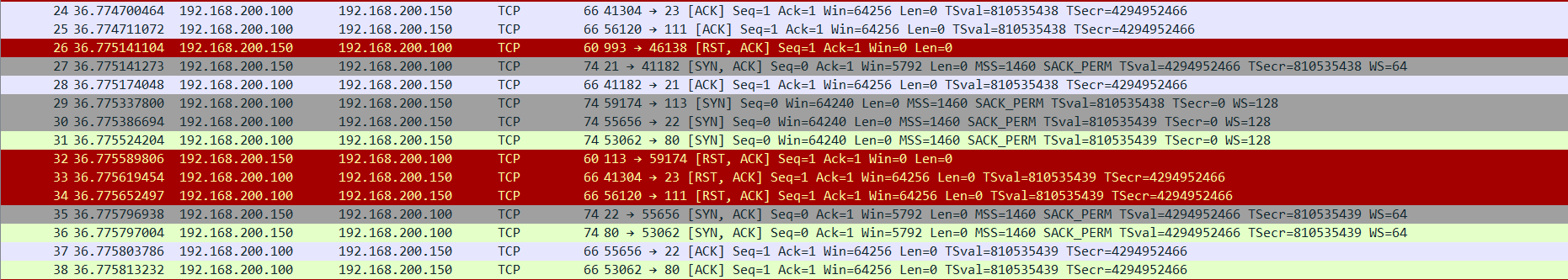
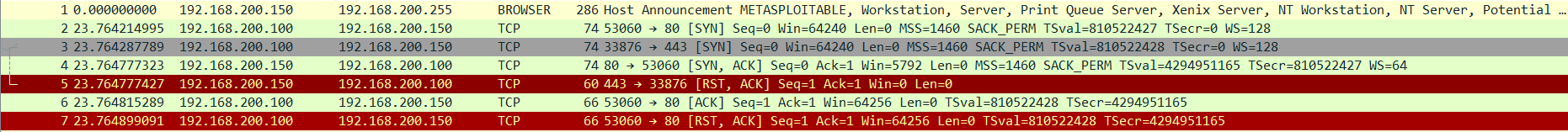
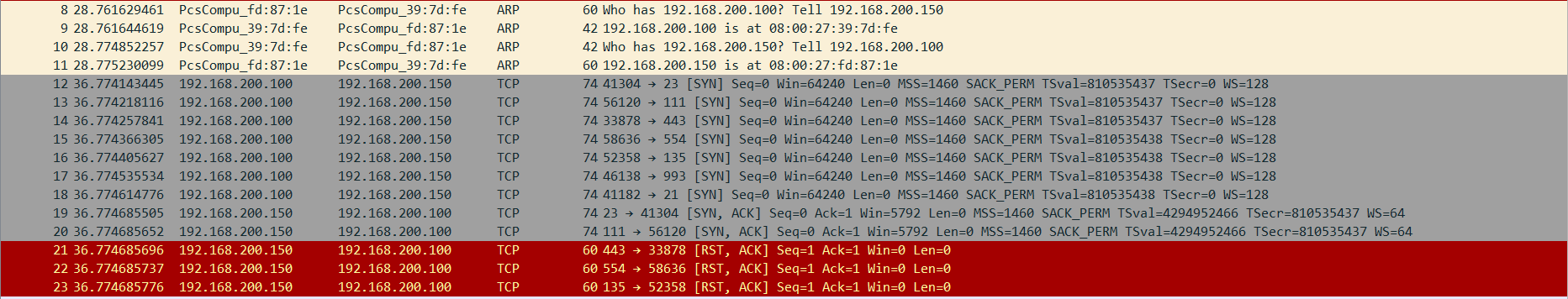
**THREAT INTELLIGENCE & IOC**

**CENNI TEORICI**

Threat Intelligence: è una forma di information gathering di segnali, dati ed evidenze in modo da costruire un modello o una strategia per prevenire e difendersi da minacce e attacchi.

Indicatori di compromissione (IOC): sono dei segnali (o evidenze) degli attacchi subiti in modo da ricostruire uno storico per capire cosa è accaduto durante un attacco.  
  
**ESERCIZIO**

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.



1) INDIVIDUARE LE EVIDENZE DI ATTACCHI IN CORSO  
  
Come possiamo notare, sono presenti alcuni pacchetti che riportano il tag “RST”.  
Questo tag sta a significare che, in una connessione TCP, durante il 3WHandshake, la connessione viene bruscamente interrotta. Possiamo vedere come siano presenti molti pacchetti col tag RST, questo perché il client invia un’enorme quantità di richieste SYN su diverse porte a cui il server prova a rispondere.

2) IPOTESI SUI POTENZIALI VETTORI DI ATTACCO UTILIZZATI  
  
Il flag RST è utilizzato dal protocollo TCP per indicare che una connessione deve essere chiusa immediatamente. Questo può essere causato da diversi fattori, tra cui:  
- Un errore di rete  
- Un attacco informatico  
- Un problema con il software o l'hardware di uno dei due dispositivi

Quando il flag RST è presente, il computer mittente indica al computer destinatario che la connessione deve essere chiusa immediatamente.   
Il computer destinatario è quindi obbligato a chiudere la connessione.

Un attacco informatico in cui viene interrotto frequentemente il protocollo TCP con l'invio di pacchetti RST ACK può essere descritto come un attacco di "TCP Reset Attack".   
In questo tipo di attacco, un aggressore invia intenzionalmente pacchetti RST ACK per terminare in modo improprio le connessioni TCP tra i due dispositivi.   
Questo può portare a interruzioni nella comunicazione e compromettere l'integrità della connessione oltre che creare latenza, interrompere servizi, creare confusione nella rete e compromettere la disponibilità dei servizi online.

Questo tipo di attacco può essere utilizzato per causare:  
- DOS (Denial Of Service).  
- MITM (Man In The Middle).

Possiamo inoltre notare come l’attaccante si trovi sulla stessa network del target.

3) CONSIGLI PER RIDURRE GLI IMPATTI DELL’ATTACCO  
  
- Aggiornare e antivirus software del computer: I bug nel software possono essere utilizzati dagli attaccanti per sfruttare le vulnerabilità, mentre gli antivirus possono rilevare e rimuovere possibili malware.  
- Essere cauti quando si clicca sui link: Gli attaccanti potrebbero utilizzare link o file infetti per infettare il computer con dei malware.  
- Implementare tecniche di sicurezza fisiche: Nel caso in cui l’attacco avvenisse dalla stessa rete, è probabile che ci sia stato un accesso non autorizzato nell’azienda o sia presente una talpa. Conviene quindi implementare dei sistemi di accesso nell’azienda (es. badge) e monitorare giornalmente (se non costantemente) i file di log per capire da quale dispositivo è stato avviato l’attacco.