Esercizio S9L3

Traccia:

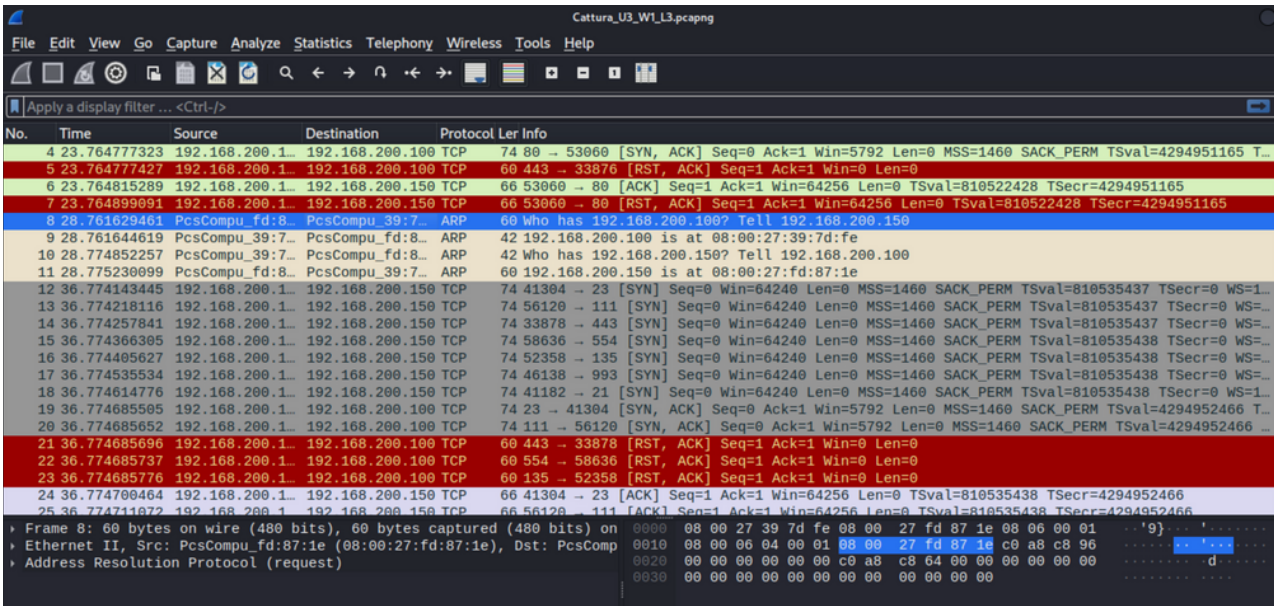
Durante la lezione teorica, abbiamo visto la Threat Intelligence e gli indicatori di compromissione. Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto.

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

Cattura_U3_W1_L3.pcapng

Da quello che possiamo dedurre dalla cattura che abbiamo effettuato con Wireshark (analisi passiva) che è in corso una scansione sul target 192.168.200.150 dall'attaccante 192.168.200.100 vista dalla quantità di richieste TCP ripetute quindi potremmo configurare delle policy del firewall per bloccare l'accesso a tutte le porte da parte dell'attaccante, in modo tale da evitare che le informazioni vengano rubate dall'attaccante.



Richiesta SYN da parte dello scanner

Risposte negative da parte dell'host. La porta è chiusa