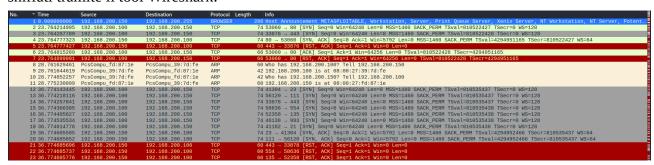
TASK:

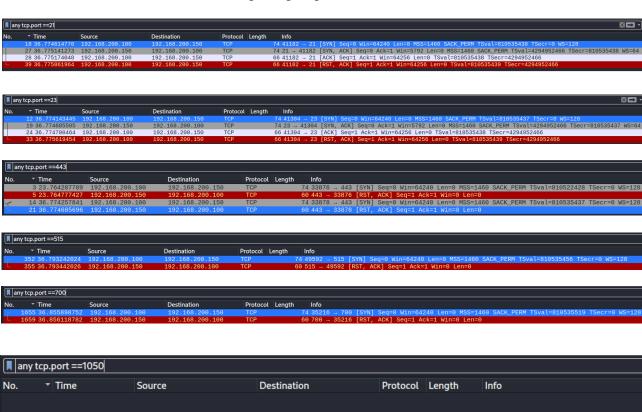
Per l'esercizio pratico di oggi, analizzare la cattura attentamente e rispondere ai seguenti quesiti:

- Identificare eventuali IoC
- Fare delle ipotesi sui vettori d'attacco utilizzati
- Consigliare un'azione per ridurre gli impatti dell'attacco

Dalle analisi del file che ci è stato fornito si può notare come ci sia una serie di connessioni che partono da una macchina avente indirizzo IP 192.168.200.100 verso un'altra macchina avente indirizzo IP 192.168.200.150. Nella foto qua sotto possiamo vedere i primi pacchetti che sono stati sniffati tramite il tool Wireshark:



Nella prima riga possiamo vedere l'host announcement, messaggio che viene inviato dal server quando il suo servizio viene avviato, per annunciarsi. Nelle righe successive possiamo vedere come l'IP 192.168.200.100 faccia una serie di connessioni usando il protocollo TCP. Nelle immagini successive ho selezionato alcune tra le principali porte well known:



La mia ipotesi è che quanto intercettato da Wireshark sia una scansione con Nmap, o comunque un altro tool di scansione, per andare a vedere quali siano le porte aperte e i relativi servizi della macchina con indirizzo IP 192.168.200.150. Possiamo notare la differenza tra le porte aperte e quelle chiuse dal fatto che il nelle prime viene completato il three way handshake (es porta 21, 23, 443). Per le porte chiuse non viene completato il three way handshake (es porta 515, 700). invece notiamo come andando oltre la porta 1024 non vi è alcun tentativo di connessione (es porta 1050). Questo rientra tra gli indicatori di compromissione, poiché multiple richieste TCP su ampi intervalli di porte indicano una scansione in corso.

Il mio consiglio per andare a ridurre l'impatto d'attacco è quello di configurare il firewall in modo tale che solo indirizzi IP scelti possano andare a comunicare con la nostra macchina, andando ad impedire così che una macchina estranea possa andare ad eseguire delle scansioni per scoprire le porte aperte e i relativi servizi per cercare una vulnerabilità da sfruttare e causare danni alla nostra macchina.