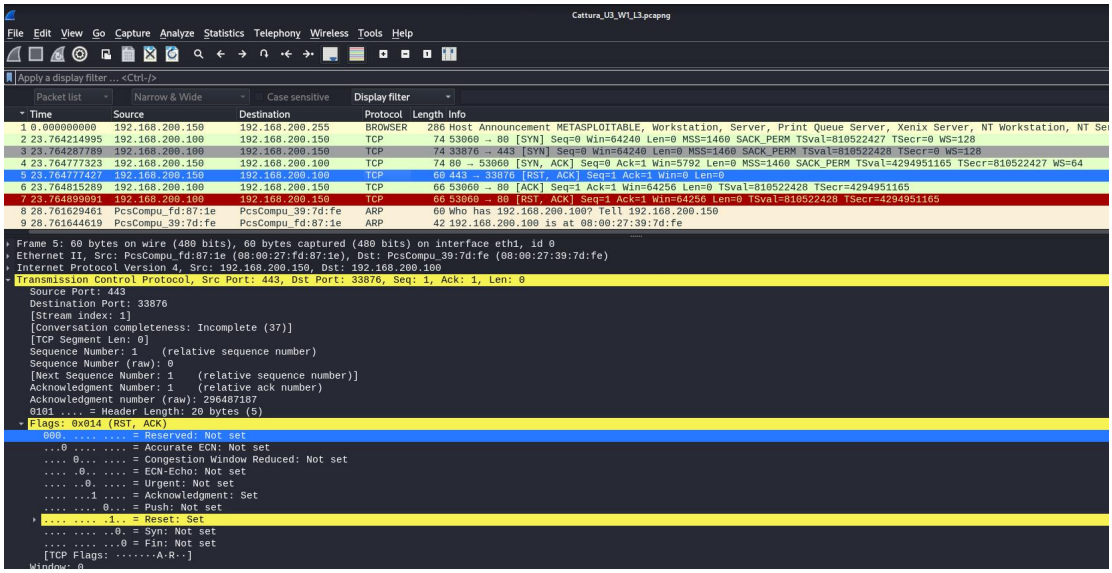
ESERCIZIO



In questo esercizio abbiamo analizzato uno screensave da parte di wireshark e abbiamo scoperto che è stato effettuato un NMAP, non ancora un effettivo attacco ma un analisi di porte attive e vulnerabili attraverso le quali essere attaccati.

SUGGERIMENTO

- Usare un firewall è per cominciare un ottimo modo per far si che non vengano effettuate con molta facilita analisi di questo tipo, dato che il firewall permette filtrare e bloccare ip indesiderati, questo mezzo di sicurezza fa si che non mostri il nostro contenuto.
- utilizzo di un SIEM, questo strumento analizza multeplici attivita e ci avvisa di tali, con la possibilità di ricevere in ingresso i log diversi da diverse sorgenti, correlazione dei dati tra diverse fonti, monitoraggio real time e definire preventivamente degli alert configurabili.
- usare il SOAP, fa da gestore delle vulnerabilita e delle minacce, delle risposte agli incidenti e da gestore dell'autonomazione delle security operations