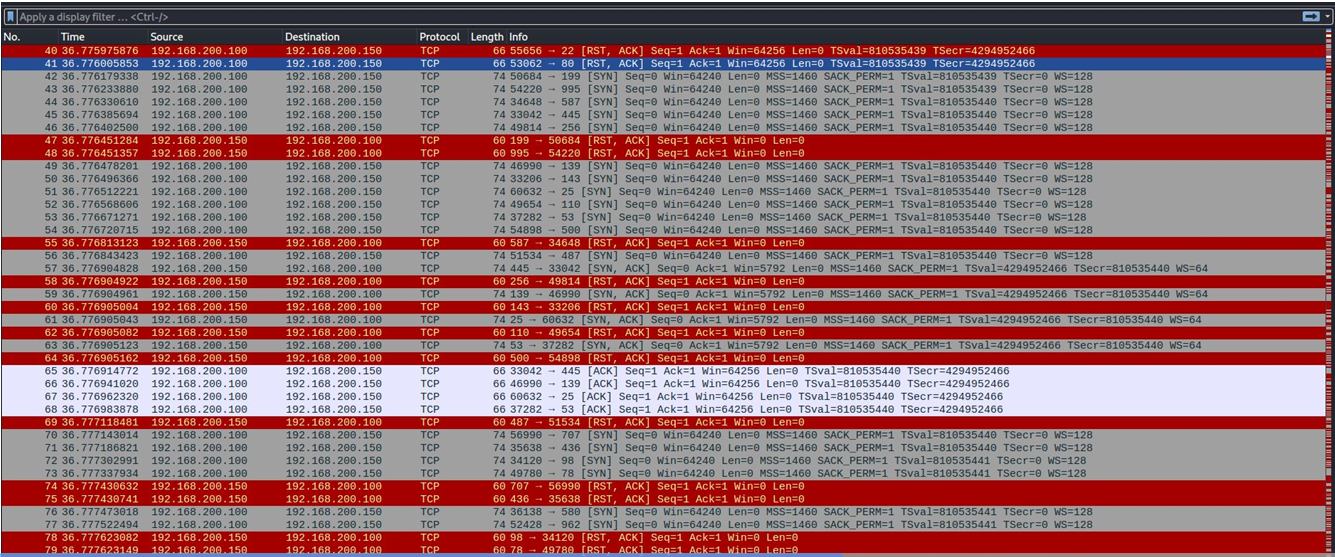
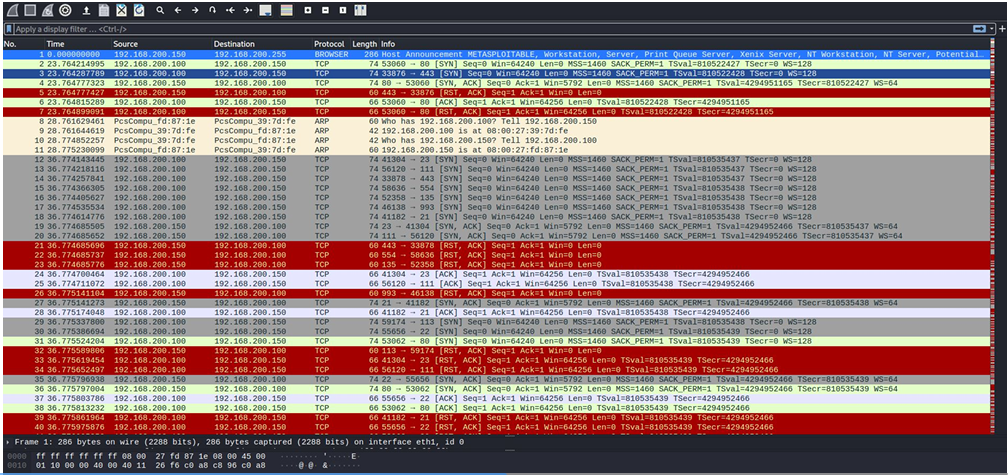
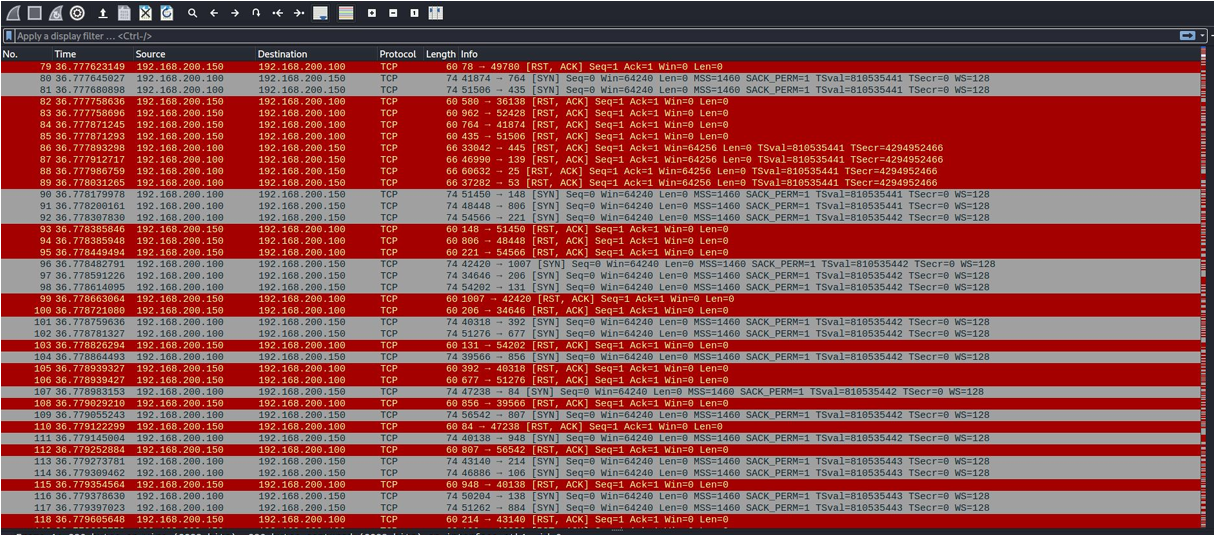
**S9/L5**

**Threat Intelligence & IOC**

L’obiettivo di oggi è quello di analizzare e comprendere un flusso di traffico rete monitorato dall’applicazione **Wireshark** tra due indirizzi IP facenti parte della stessa rete.   
  
Gli host in questione sono due: **192.168.200.150** e **192.168.200.100**  
  
Analizzando il traffico catturato con Wireshark, si nota un flusso che punta a una scansione delle porte TCP, effettuata con un tool automatizzato come Nmap. Il dialogo si sviluppa tra due indirizzi IP: 192.168.200.150, che funge da mittente, e 192.168.200.100, che riceve i pacchetti. La natura della comunicazione suggerisce una scansione volta a verificare lo stato delle porte sull’host di destinazione, senza mai completare una vera connessione.

I pacchetti SYN inviati dall’host sorgente mirano a sondare diverse porte, con risposte che variano tra SYN/ACK (porte aperte), RST (porte chiuse) e, in alcuni casi, l’assenza di risposta, che potrebbe indicare l’intervento di un sistema di filtraggio o firewall.

Quello che colpisce è la ripetitività del traffico e l’assenza di contenuti applicativi: non c’è alcun tentativo di stabilire comunicazioni autentiche con i servizi eventualmente attivi, ma solo l’obiettivo di mappare il sistema. Dettagli tecnici, come il supporto per SACK o i valori temporali TSval e TSecr, suggeriscono che il processo sia altamente strutturato e guidato da uno strumento sofisticato, non da un’azione manuale.

Ci sono alcune porte che rispondono positivamente con un SYN/ACK, lasciando intendere la presenza di servizi in ascolto. Questi dettagli rappresentano per un attaccante una base preziosa per individuare potenziali vulnerabilità e pianificare eventuali exploit. Allo stesso tempo, la quantità di pacchetti RST conferma che gran parte delle porte sull’host sono chiuse, il che riduce le possibilità di attacco immediato, ma non elimina i rischi.

Per concludere si può confermare che ci troviamo di fronte a un’operazione di controllo, probabilmente tramite una scansione SYN eseguita con Nmap. In un ambiente controllato, come un laboratorio di sicurezza, questo comportamento sarebbe del tutto normale, parte di un esercizio di analisi delle vulnerabilità. In un contesto reale, invece, rappresenterebbe un chiaro segnale di allarme, sintomatico di un tentativo di raccolta informazioni da parte di un soggetto esterno.