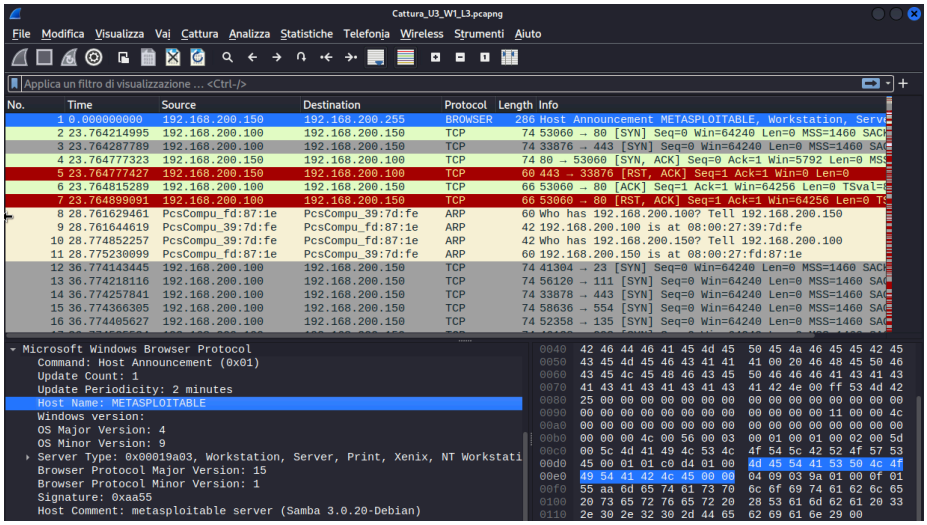
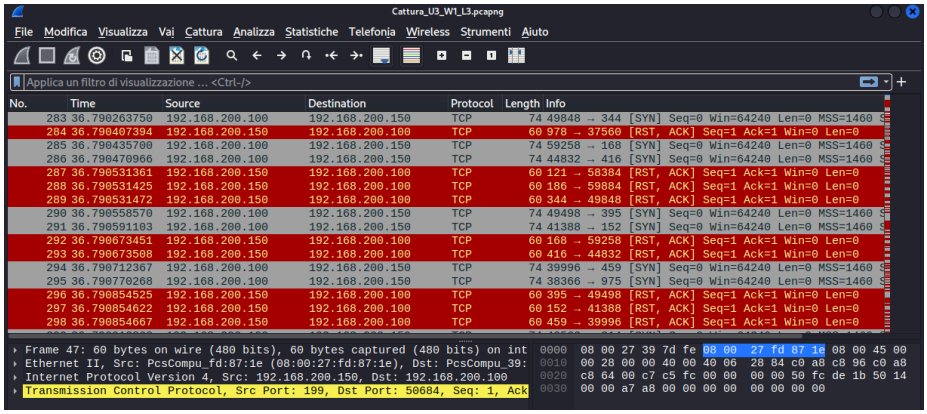
3. Monitorare gli eventi con i SIEM

Cattura di rete effettuata con Wireshark.

Analizzando la parte iniziale, capiamo che l'host è Metasploitable.





Andiamo ora ad analizzare i pacchetti catturati.

Identificare eventuali IOC, ovvero evidenze di attacchi in corso.
Possiamo osservare come ci siano molteplici richieste TCP su ampi intervalli di porte, che ci permette di identificare un compromissione.

In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati.
Possiamo ipotizzare che ci sia una scansione in corso da parte di un attaccante, che probabilmente utilizza nmap.
Dalla cattura osserviamo come non ci sia un 3-way-handshake per questo ipotizziamo avvenga un TCP Syn Scan.

Consigliate un'azione per ridurre gli impatti dell'attacco.
Probabilmente non c'è la presenza di un firewall che impedisca la scansione nmap, per questo il consiglio sarebbe quello di configurare un firewall, in modo da non ricevere delle scansioni che possano dare vantaggi agli attaccanti.