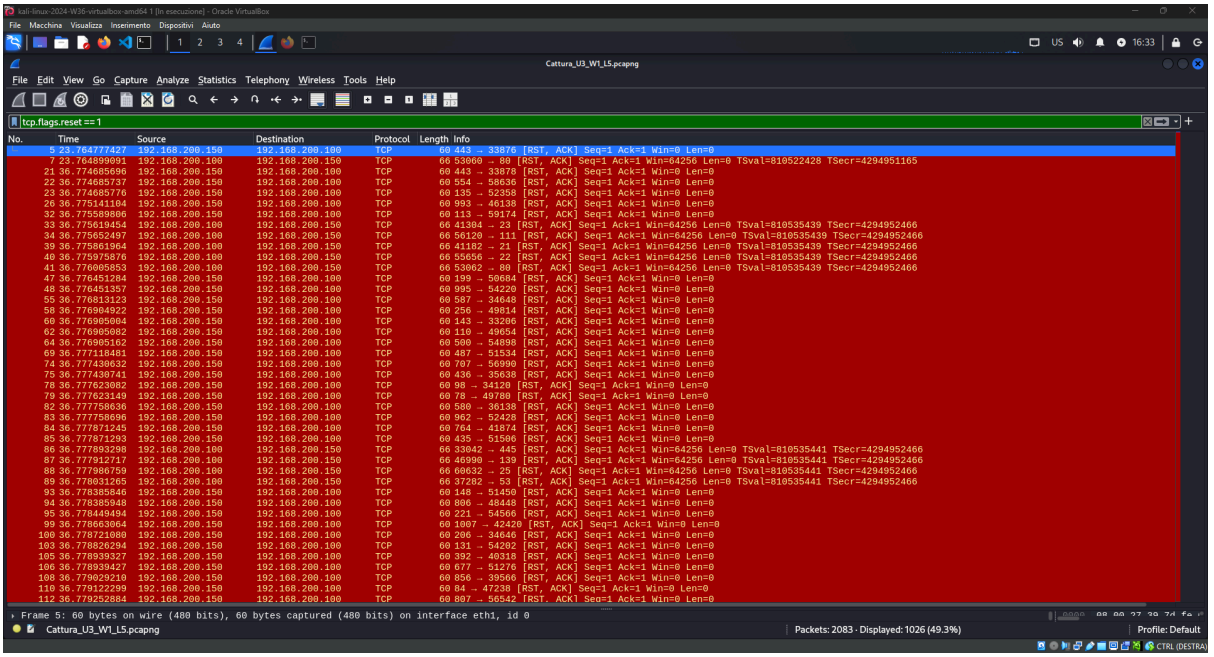
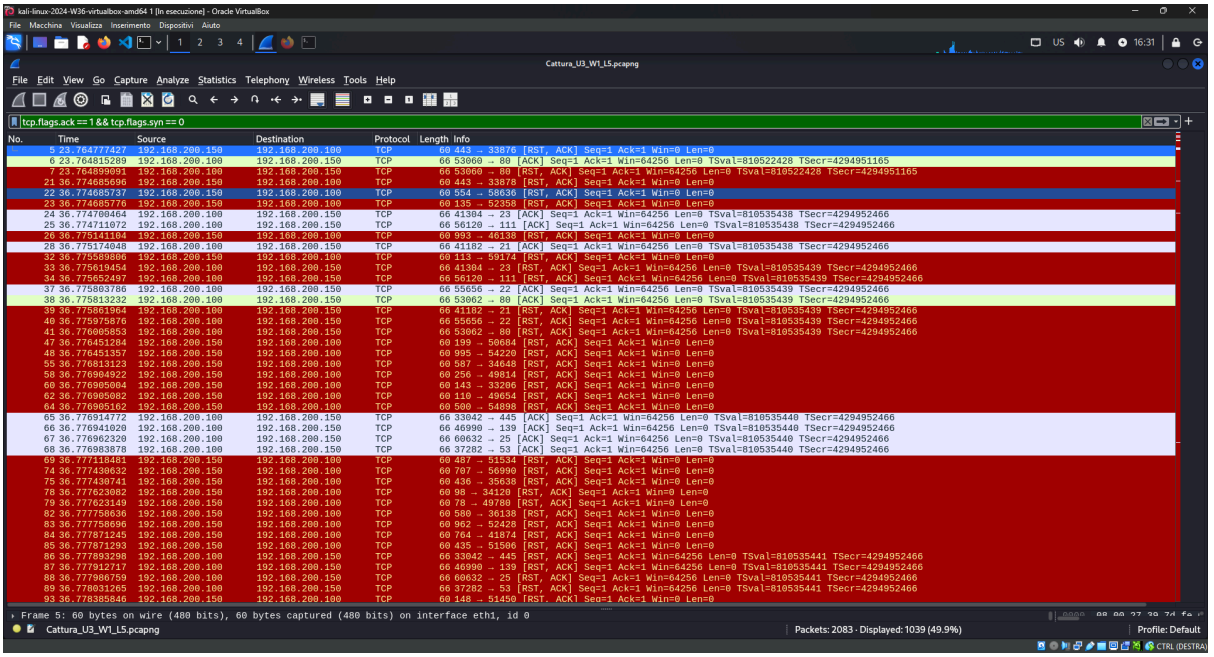
Threat Intelligence & IOC

In base all’analisi di Wireshark si possono notare due tipi di attacco principale:

- Reset con ACK che tenta di interrompere le connessioni esistenti con le porte chiuse(1026 pacchetti) senza connessioni SYN

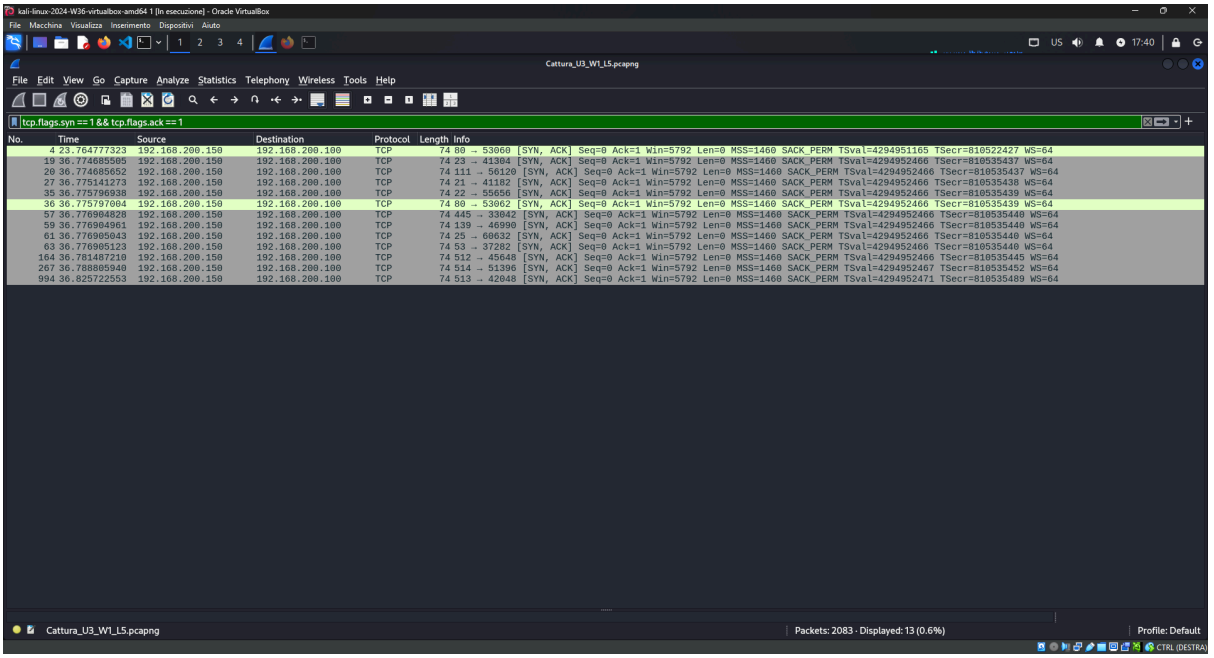


- SYN Flood con spoofing delle porte si capisce perché ci sono molteplici pacchetti TCP con il flag SYN senza avere una risposta ACK(1039 pacchetti) ,



- Indirizzi ip: 192.168.200.100(source) 192.168.200.150(destination)
- porte scansionate: tutte le porte

- pacchetti SYN ACK andati a buona fine



Da qui si evince che molto sicuramente è un attacco di brute force, probabilmente l'attacco è partito con l'utilizzo da un nmap utilizzando una scansione molto aggressiva come -sV. Ipotizzo questa soluzione perché utilizzano un RST accompagnato da ACK che rifiuta tutte le connessione con le porte chiuse mentre quelle aperte le accetta.

Azioni per mitigare l'attacco attuale:

- Abilitare il Rate Limiting: configurando il Firewall o router per limitare il numero di richieste SYN e RST da una singola attività
- Filtraggio dei Pacchetti Anomali: inserendo delle regole nel Firewall per rifiutare pacchetti SYN e RST non richiesti o che provengono da indirizzi IP sconosciuti
- Attivare il SYN Cookie: per ridurre l'impatto degli attacchi SYN flood
- Utilizzare un Sistema di Prevenzione delle Intrusioni (IPS): per monitorare e bloccare traffico sospetto, compresi gli attacchi SYN e RST flood.
- Contattare il Fornitore di Servizi Internet (ISP): potrebbero essere in grado di bloccare il traffico malevolo prima che raggiunga la tua rete.

Azioni per prevenire attacchi futuri:

- Chiudi le porte non necessarie: Mantieni aperte solo le porte essenziali per il funzionamento dei servizi richiesti. Questo riduce le possibilità per gli attaccanti di scoprire servizi vulnerabili.
- Usa porte non standard: Sposta i servizi su porte non standard per ridurre la probabilità che vengano scansionate da strumenti automatici come Nmap.
- Blocco degli IP sospetti: Blocca l'accesso agli IP che mostrano comportamenti sospetti, come scansioni ripetitive.
- Rate limiting: Imposta dei limiti sul numero di connessioni che un singolo IP può stabilire in un determinato periodo.
- Geoblocking: Se appropriato, limita l'accesso da regioni geografiche non rilevanti per il tuo business.
- Configura un IDS o IPS come Snort, Suricata, o Zeek per rilevare e prevenire scansioni di rete e attività sospette.
- Imposta regole specifiche per rilevare le firme delle scansioni di Nmap e bloccare automaticamente il traffico proveniente da queste sorgenti.
- Imposta honeypots o honeynets che simulano servizi vulnerabili per attirare e monitorare attività di scansione. Questo ti permette di raccogliere dati sugli attaccanti senza esporre sistemi reali.