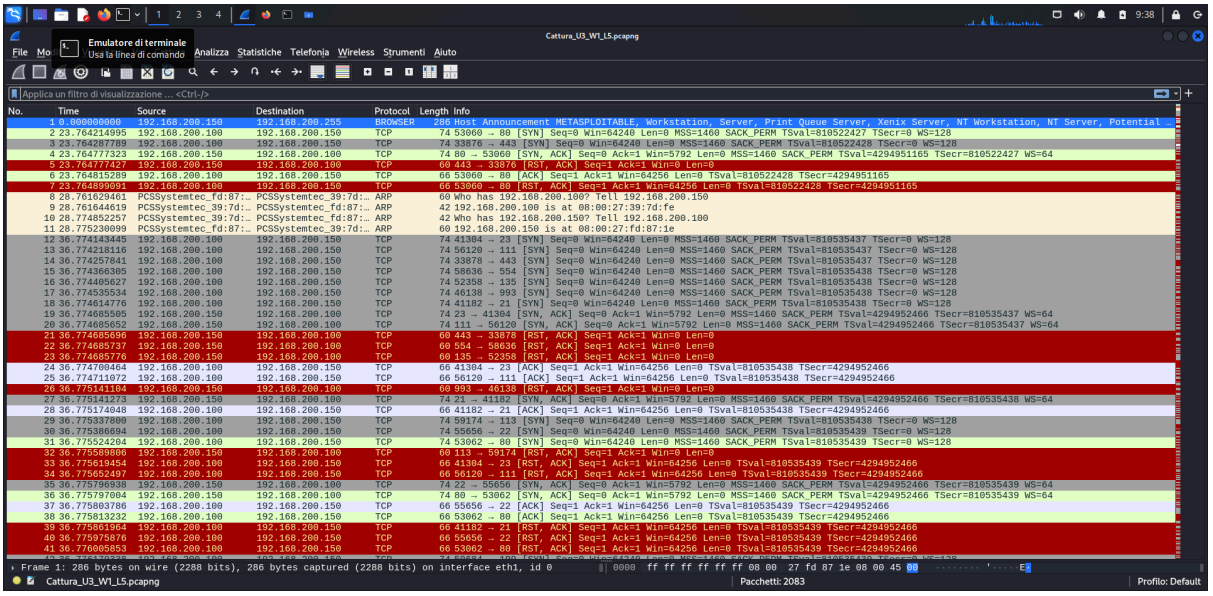
Threat Intelligence e Indicatori di Compromissione

In questo esercizio ho analizzato un file con estensione **.pcapng** utilizzando il programma **Wireshark**, con l'obiettivo di individuare eventuali **attività sospette nella rete** che possano indicare un attacco informatico in corso o già avvenuto. L'attività prevedeva i seguenti passaggi:

- **identificare gli Indicatori di Compromissione (IOC)**,
- ipotizzare il tipo di attacco
- proporre possibili soluzioni per proteggere la rete in futuro.



Indicatori di Compromissione (IOC)

Dall'analisi del traffico di rete ho notato un comportamento anomalo da parte dell'indirizzo IP **192.168.200.100**, che tenta di stabilire connessioni con l'host target **192.168.200.150**. Le connessioni avvengono su numerose porte diverse, tra cui per esempio:

- **22 (SSH)**
- **80 (HTTP)**
- **443 (HTTPS)**
- **445 (SMB)**

La maggior parte di queste connessioni viene **rifiutata**, come si può osservare dalla presenza di pacchetti TCP con flag **RST, ACK**, che indicano una chiusura forzata della comunicazione. Questo comportamento mi fa pensare ad una **scansione delle porte**.

Un altro elemento che ho notato si trova all'inizio della cattura, dove appare un pacchetto **BROWSER** contenente il termine **"Metasploitable"**. In questo caso, però, penso si tratti

semplicemente di un **messaggio di annuncio sulla rete** del protocollo NETBIOS, che serve per comunicare la presenza di un host.

Ipotesi sul tipo di attacco

Le informazioni raccolte indicano che l'indirizzo IP **192.168.200.100** sta probabilmente effettuando una **ricognizione della rete**, cioè uno **scanning**, che corrisponde alla fase iniziale di molti attacchi informatici, durante la quale l'attaccante cerca di identificare i dispositivi attivi e i servizi in ascolto, per poi sfruttare eventuali vulnerabilità.

È possibile che sia stato utilizzato **Nmap**, oppure il framework **Metasploit**.

Qualora l'attaccante riesca a sfruttare una vulnerabilità presente su una delle porte aperte, è possibile che tenti di **ottenere accesso remoto alla macchina** attraverso una **shell** (ad esempio una reverse shell). Successivamente, potrebbe anche **installare una backdoor** per garantirsi un accesso stabile e continuativo nel tempo.

Come difendersi e ridurre il rischio

Per prevenire o bloccare attacchi di questo tipo è importante adottare le seguenti misure:

- **Bloccare l'indirizzo IP sospetto** (192.168.200.100) tramite le regole del firewall.
- **Segnalare l'attività sospetta** agli amministratori di sistema o al team responsabile della sicurezza informatica.
- **Isolare il dispositivo** per evitare la diffusione dell'attacco.
- **Chiudere tutte le porte non necessarie** nei dispositivi della rete, riducendo i punti di accesso.
- **Segmentare la rete**, creando zone separate (ad esempio con VLAN).
- **Aggiornare regolarmente i software e i sistemi operativi**, così da correggere eventuali vulnerabilità note.
- **Utilizzare sistemi IDS/IPS (Intrusion Detection/Prevention Systems)**, in grado di riconoscere automaticamente comportamenti sospetti e intervenire in tempo reale.