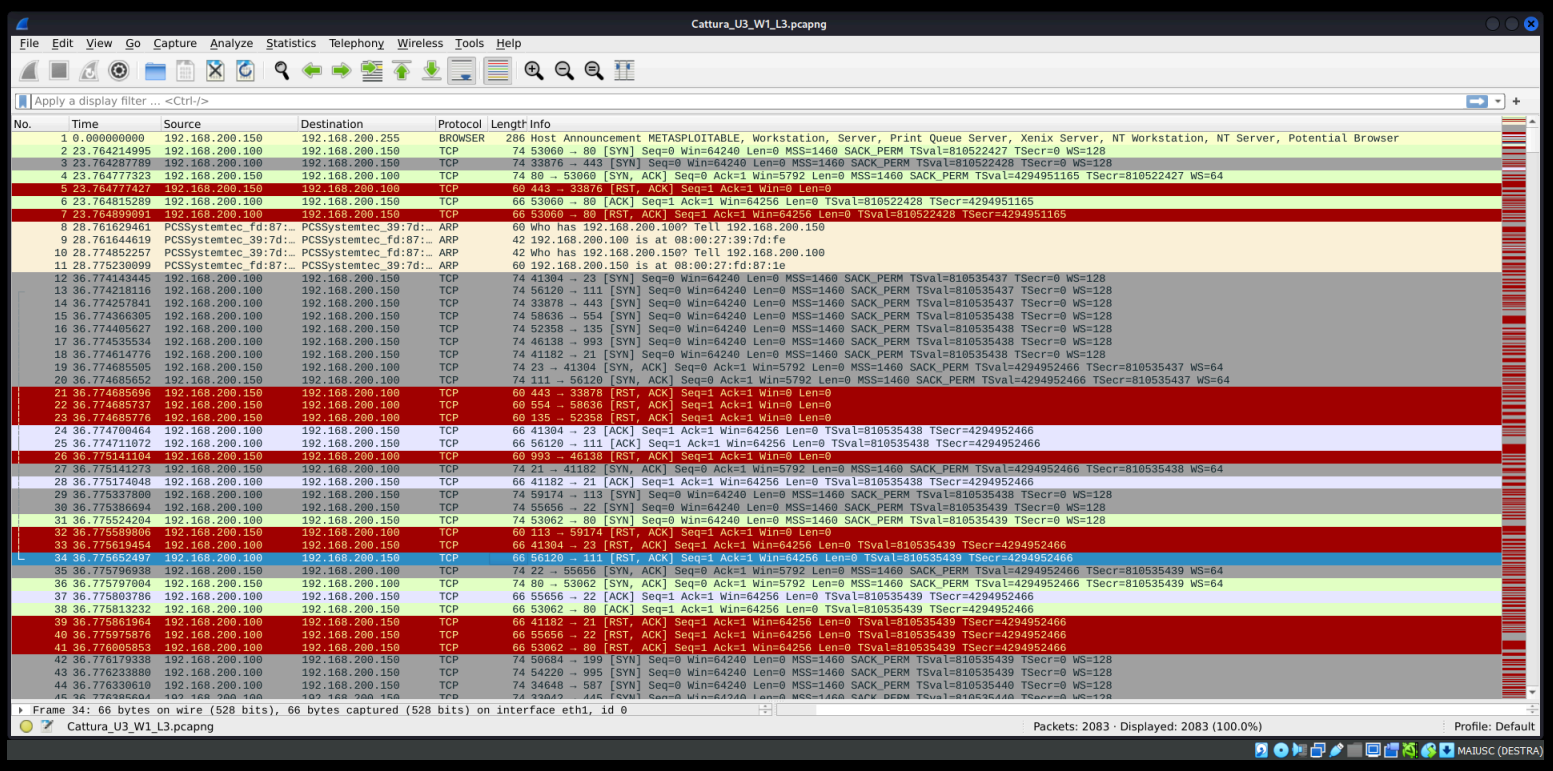
IOC e Threat Intelligence

Richiesta: Sulla base del file riportante una cattura del traffico di rete con Wireshark, analizzate attentamente e:
1.Identificare eventuali IOC, ovvero evidenze di attacchi in corso
2.In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
3.Consigliate un'azione per ridurre gli impatti dell'attacco

Cattura Wireshark



Identificazione degli IOC:

Sulla base di questa cattura possiamo notare:

Attività Sospetta: Vi è una sequenza di pacchetti che indicano un tentativo di scanning delle porte da parte dell'indirizzo IP 192.168.200.100 verso il target 192.168.200.150.

Pattern di Scansione: La scansione è eseguita porta per porta, come indicato dalla sequenza incrementale delle porte di destinazione e dai numerosi pacchetti TCP con flag SYN.

Ipotesi sui potenziali vettori di attacco:

Scanning del sistema: Sulla base delle considerazioni precedenti (IOC), si intuisce che l'attaccante stia attuando un port scanning per identificare possibili porte aperte.

Preparazione per Altri Attacchi: La scansione può precedere tentativi di exploit verso servizi vulnerabili trovati, attacchi di brute force, o l'installazione di backdoor se vengono scoperte porte aperte.

Azioni consigliate per ridurre gli impatti dell'attacco:

Firewall: Configurare il firewall per bloccare connessioni in ingresso non necessarie e per permettere solo traffico legittimo verso e dalla rete. Si potrebbero configurare delle regole che bloccano l'IP sospetto.

IPS/IDS: Utilizzare sistemi di prevenzione e rilevamento delle intrusioni per rilevare e potenzialmente bloccare gli scan delle porte. Questi sistemi possono essere configurati per riconoscere e bloccare comportamenti sospetti come un numero elevato di tentativi di connessione su diverse porte.

Rate Limiting e Blocking: Molti firewall e router hanno la capacità di limitare la velocità delle connessioni o bloccare indirizzi IP che eseguono troppe richieste in un breve lasso di tempo.