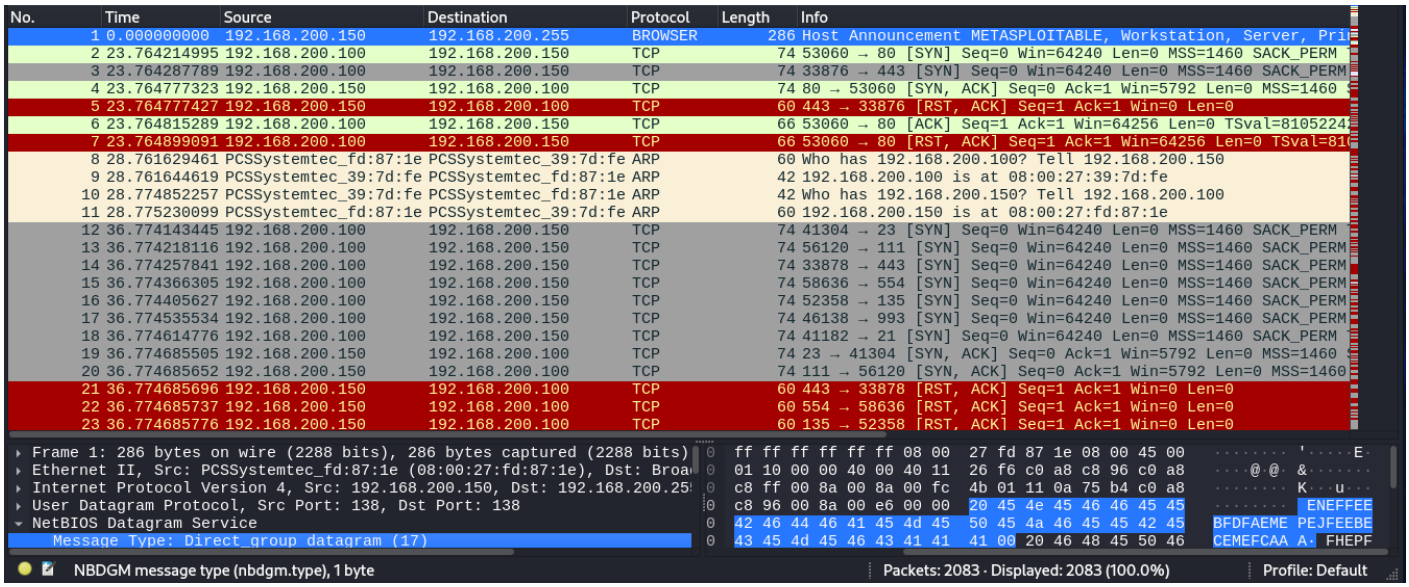
REPORT CS0124

S9L3

Traccia: Durante la lezione teorica, abbiamo visto la Threat Intelligence e gli indicatori di compromissione. Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto. Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark. Analizzate la cattura attentamente e rispondere ai seguenti quesiti: Identificare eventuali IOC, ovvero evidenze di attacchi in corso In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati Consigliate un'azione per ridurre gli impatti dell'attacco



Come possiamo vedere dallo screenshot eseguito su kali si evince che ci sono ripetute richieste TCP dalle macchine source alla macchina destination, fanendo intendere che l'attaccante sta eseguendo una scansione dei servizi e delle porte aperte.

CONCLUSIONI

Per sventare una possibile scansione delle porte e servizi vulnerabili e contrastare un possibile attacco possiamo utilizzare diversi metodi a nostra disposizione.

Uno di questi e' attivare un firewall sulla macchina target in modo tale da bloccare o droppare qualsiasi richiesta da parte di indirizzi ip attaccanti.

Un altro metodo potrebbe essere quello di andare a risolvere le singole vulnerabilita' all'interno della macchina o server target cosi da eliminare o ridurre il rischio di attacchi interni \\\\\\\\\\\\\\\