Epicode
CS-0124
Pratica S9/L3

Francesco Ficetti

Traccia..... 3
Svolgimento..... 4

Traccia

Analizzare una cattura Wireshark e rispondere ai seguenti quesiti:

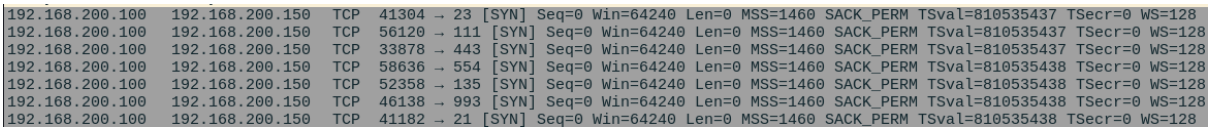
- Identificare gli IOC.
- In base agli IOC trovati, fare delle ipotesi sui potenziali vettori di attacco utilizzati.
- Consigliare un’azione per ridurre gli impatti dell’attacco.

Svolgimento

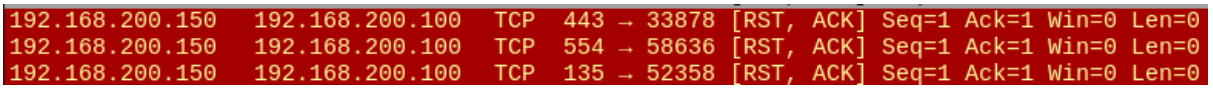
Analizzando questa cattura si nota subito che i soggetti della stessa sono due macchine:

1. 192.168.200.100 → la macchina che esegue le richieste;
2. 192.168.200.150 → la macchina che riceve le richieste.

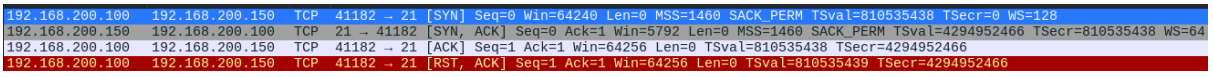
Si presume che la macchina 1 stia eseguendo una scansione *nmap* sulla macchina 2. Lo si può notare dal fatto che ci sono moltissime richieste di connessione tramite protocollo TCP, tutte su porte diverse.



Molte di queste richieste vengono rifiutate subito.



Alcune porte, invece, accettano la connessione in entrata. Essa però, viene interrotta subito dopo. Questo dimostra che non c'è un reale interesse ad effettuare una comunicazione, ma queste richieste vengono eseguite solo per verificare che le porte siano aperte.
Di seguito un esempio di quanto appena detto, filtro applicato sulla porta 21, tramite il comando *tcp.port == 21*.



Per ridurre gli impatti dell'attacco, si consiglia di bloccare, tramite un firewall, tutte le richieste provenienti dall'indirizzo IP della macchina 1.