S9L3

Consegna:

L’esercizio di oggi consiste nell’ottenimento delle informazioni elencate di sotto basandosi su delle immagini che ci sono state fornite

- Identificare eventuali Indicatori di Compromissione (IoC)

- Ipotizzare che tipo di attacco stanno veicolando

- Proporre un modo per potersi difendere da questo attacco

Esecuzione:

Le immagini fornite sono delle schermate di wireshark che mostrano un ingente quantità di pacchetti inviati da un host (192.168.200.100) verso la macchina vittima (192.168.200.150). Se si controlla meglio sono tutti dei protocolli TCP, per via della quantità dei pacchetti inviati si potrebbe pensare ad un attacco DoS, tuttavia le richieste TCP in questione sono state inviate a porte diverse si potrebbe dunque pensare ad una scansione effettuata da un attaccante (in questo caso 192.168.200.100). A supporto di questa tesi è possibile vedere come ci sono delle richieste accettate che riportano la sigla [SYN] (segnate in grigio) e altre rifiutate che riportano la sigla [RST, ACK] (segnate in rosso)

Glossario:

Wireshark: è un tool per l’analisi del traffico di rete (o packet sniffer) che analizza e sviluppare protocolli di software

Protocollo TCP (Trasmission Control Protocol): è un protocollo che si occupa del controllo della trasmissione e a rendere affidabile la comunicazione di dati all’interno di una rete

Attacco DoS (Denial of Service): è una tipologia di attacco che ha come obiettivo la negazione di un servizio tramite la saturazione della CPU della vittima.