Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption

The website's connection timeout error message is a result of a flooding of packets in the network. The logs show that from log no. 47-51 The network established was performing as usual, as the three-way handshake was used to establish a connection in the TCP protocol: SYN > SYN ACK > ACK. However, from log no. 125-214 It can be seen that there is an increase in requests for SYN packets. Therefore, we can conclude that this is a DoS attack dealing with a TCP SYN flood attack.

Section 2: Explain how the attack is causing the website to malfunction

When website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. Explain the three steps of the handshake:

1. Synchronize (SYN) client sends a SYN packet to the server to request a connection.
2. Synchronize Acknowledgement (SYN, ACK) Server responds with SYN ACK to acknowledge the request.
3. Acknowledgement (ACK) The client sends an ACK to confirm that connection and communication can begin.

Explain what happens when a malicious actor sends a large number of SYN packets all at once:

A larger number of SYN packets all at once causes excess network traffic and depletion of resources, leading to a crash in the server/error.

Explain what the logs indicate and how that affects the server:

The logs show the events leading up to the SYN flood attack; in essence, it shows the network traffic leading up to the crash of the server.