Cybersecurity Incident Report

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

One potential explanation for the website's connection timeout error message is a DOS attack. The web server is overwhelmed by the amount of TCP SYN requests coming from an unfamiliar IP address and it could not handle it. The logs show that the web server stopped responding to legitimate employee visitor traffic. This event could be as a result of the DOS SYN flooding 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. A SYN packet is sent from the source to the destination requesting a connection.
2. The destination will respond to the source with a SYN ACK packet to accept the connection requested. The destination will reserve resources for the source to connect.
3. A final ACK will be sent from the source to the destination acknowledging the permission to connect.

In the case of SYN flood attack, a malicious actor will send a large number of SYN packets all at once, which overwhelms the server's available resources to reserve for connection. When this happens, there are no server resources left to legitimate TCP connection requests.

The logs indicate that the web server has become overwhelmed and is unable to process the visitor's SYN requests. The server is unable to open a new connection to new visitors who receive a connection time out error.