Cybersecurity Incident Report

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

This type of activity indicates it's an SYN Flood attack as the same IP address keeps on requesting SYN request Handshake and it's a direct Denial of Service Attack. Which is connection timeout error. Wireshark TCP log indicates the is an overwhelming request for the SYN request protocol for the TCP Handshake made by IP address 203.0.113.0 to company web server IP address 192.0.2.1. The log indicates that at No. 52 a request was made by that IP address and eventually the ACK (Handshake confirmation) from our web server acknowledge it at No.54. And normal operations are present as legitimate employee's address where able to access the web server. But then the suspicious IP address made another request No. 57, which then started to raise concern and now the request kept on coming until the web server handling of the SYN request started to overwhelm the server and couldn't complete the three-way handshake.

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 to connect to the destination.
2. The destination then replies to the source with SYN-ACK packet to accept the connection request. The destination will reserve resources for the source to connect.

3. A final ACK packet is sent from the source to the destination acknowledging the permission to connect.

In the case of a SYN flooding attack the threat actor sends large amounts of SYN packets all at the same time, this then overwhelms the server's available resources to reserve for the connection. Then this leaves no room for legitimate TCP connection requests for the verification from the server

The logs indicate that the web server has become overwhelmed and is unable to process the visitors SYN requests. The server is unable to open a new connection to new visitors who receive connection timeout message.