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:

The logs show that: there was a lot of SYN packets sent to our server from a certain IP address which overwhelmed the server causing it to shutdown

This event could be: an IP spoofing event that is bringing it a high number of DoS caused by a smurfing attack, where our server was receiving a numerous number of packets at once IP spoofing sending a lot of SYN packets..

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. The HPTTs or the device sends a SYN message request which is known as synchronize request

2. The server respond's with an ACK response to the IP address that requested information or data to acknowledge that it's request was received

3. There is our third process known as the SYN-ACK handshake established which means that the device that sent the SYN request is now receiving data from the server the network has established.

Explain what happens when a malicious actor sends a large number of SYN packets all at once: The server will shutdown and this can affect the daily productivity of an organization.

Explain what the logs indicate and how that affects the server: The logs indicates that there has been numerous of SYN packets sent to our server, somebody might have managed to get their hands to one of our IP by using the IP spoofing method attack in this case smurf attack and they sent numerous SYN packets which caused our server to shutdown.