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 server has been timed out due to a malicious actor

The logs show that: the server has been flooded by TCP SYN packets from an unidentified IP address, causing it to shut down

This event could be: a malicious DOS 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. The source first sends a SYN packet

2. The receiving network acknowledges the SYN and sends one back

3. The initial sender receives the opposing SYN and establishes a connection

Explain what happens when a malicious actor sends a large number of SYN packets all at once: The receiving IP gets overloaded and shuts down

Explain what the logs indicate and how that affects the server: Logs indicate there is a large number of SYn packets being sent by an unknown IP address, causing the server to time out and become unreachable as well as vulnerable to further attacks