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 cannot handle a bunch of packets and requests at once.** The logs show that: **There is a large number of TCP SYN requests coming from an unfamiliar address.** This event could be: **A 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. **A packet is sent from the host to destination to establish a connection** 2. **The destination accepts the packet and another packet is sent to the host to confirm. Information such as IP if collected** 3. **Host establishes the connection** Explain what happens when a malicious actor sends a large number of SYN packets all at once: **This would overwhelm the server as it would have to establish connections back and forth every time.** Explain what the logs indicate and how that affects the server: **The logs indicate that the webserver was overwhelmed and unable to process connections anymore, outputting timeout messages.**