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 that the network was experiencing a malicious attack. The logs show that there are an influx of SYN requests coming from IP address 203.0.113.0 causing the server to stop responding after an overload of SYN packet requests. This event could be a denial of service (DoS) SYN Flood 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 a device/source to the destination, this a request to connect. 2. The server/destination will then reply and send a SYN-ACK to acknowledge the connection and accept the request. 3. A final ACK packet is sent from the source to the destination acknowledging the permission to connect. **Explain what happens when a malicious actor sends a large number of SYN packets all at once:** When a malicious actor sends a large number of SYN packets all at once, it overwhelms the server's resources to reserve for connection. When this happens, there are no server resources left for actual TCP connections. **Explain what the logs indicate and how that affects the server:** The logs indicate that the attack first started at log item 52, was continuously sending SYN requests, then finally at log item 80, it began to be overwhelmed only allowing a couple of connections until log item 98 and on, the server was unable to open new connections. This affects the server because when the server is flooded with SYN requests, the server has no reserve for new connections, therefore new visitors receive a connection timeout message.