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: a malicious attacker performing a DoS attack The logs show that an unrecognized IP address is repeatedly sending SYN requests to the web server This event could be a 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. Client sends a SYN packet to server 2. Server responds with a SYN/ACK packet 3. Client sends an ACK packet back and connection is established Explain what happens when a malicious actor sends a large number of SYN packets all at once: Explain what the logs indicate and how that affects the server:

One potential explanation for the website's connection timeout error message is a malicious attacker performing a denial-of-service attack on the web server. The log shows that an unrecognized IP address, 203.0.113.0, is repeatedly sending SYN requests to the web server. This event could be a SYN flood attack, where the attacker simulates a TCP connection and floods the server with SYN packets.

When website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. The client sends a SYN packet to the web server, indicating they want to establish a connection. The server responds with a SYN/ACK packet, acknowledging that the client wants to establish a connection. Finally, the client sends an ACK packet back to the server, and a connection is established. The client and server can now exchange data. When a malicious actor sends a large number of SYN packets all at once, the

server is unable to respond to all the requests and becomes overwhelmed. This can lead to a slowdown in the server's processes or even a complete shutdown. The logs indicate a SYN flood attack, which takes advantage of the three-way handshake by flooding the server with SYN packets. This led to the server being shut down and caused a slowdown in daily operations. The organization will be negatively affected by this because it costs them money and time.