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 server is down or an issue with the firewall configuration. Alternatively, this could be a DoS attack. The logs show that multiple outside connection requests are being made by someone at IP address 203.0.113.0, showing an overload of SYN packet requests resulting in the server becoming non-responsive. Suspecting SYN flooding.

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 initial step is the connecting device sends a SYN packet requesting to connect. 2. That SYN is then acknowledged (ACK) by the server by sending a SYN/ACK packet to accept the request. 3. The SYN/ACK is then ACK'd by the initial device or source acknowledging the connection permission. Explain what happens when a malicious actor sends a large number of SYN packets all at once: This results in the server being unable to process the legitimate requests and the server being bogged down and possibly shut down. Explain what the logs indicate and how that affects the server: The logs indicate that a single IP address is initiating a high volume of requests resulting in the server being shut down. The knockdown effect that the server is unable to open new connections to users who will be receiving a timeout message.