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 logs show that: The destination IP address 192.0.2.1 is receiving an excessive number of SYN and SYN ACK requests on HTTPS port 443. These requests are left open or incomplete, and starting with the 80th request, they begin generating reset acknowledgments. From that point on, subsequent requests originate from the same IP address: 203.0.113.0, port 54770. This event could be:The large number of "open" requests suggests a malicious SYN flood attack with IP spoofing.

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. Visitor asks SYN 2. The destination answers a SYN-ACK 3. Visitor send ACK to complete the handshake Explain what happens when a malicious actor sends a large number of SYN packets all at once: The server's memory becomes saturated and it stops functioning correctly. Explain what the logs indicate and how that affects the server: This type of malicious attack aims to prevent the server from responding to legitimate requests and cause websites, entire networks, or even entire servers to malfunction, resulting in serious financial losses if not addressed promptly. Upon receiving too many requests, the HTTPS server begins responding with HTTP/1.1 504 Gateway Timeout (text/html) and 443->42584 [RST, ACK] Seq=1 Win-5792 Len=120... The attacker reveals their IP spoofing, and numerous requests continue to arrive, now from the same IP address as a source (203.0.113.0). This is known as a SYN flood attack. Our next step should be to review the firewall settings to block access from the attacking IP address and reduce the number of allowed open requests, in order to resume service as soon as possible.