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 potential explanation for the website's connection timeout error message is a threat actor trying to conduct a DNS attack to the company's servers by overwhelming them with TCP SYN requests. Which is a SYN flooding attack** The logs show that: **In the logs they show that everything is going fine from message 47 to 70 where the server was able to handle the SYN requests, but at message 60 the IP address for an employee is 198.51.100.5 made a GET /sales.html HTTP/1.1 request. After that we witness the Source IP address 203.0.113.0 starts spamming SYN requests that the server can barely handle. Therefore, it results in the server to be shut down.** This event could be: **Like said before, this is happening because an attacker is issuing a SYN flooding attack, where it overwhelms the server with SYN requests**

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. **First the website has to receive the SYN request from the user which is the Source IP address to the Destination IP address** 2. **Second the Destination IP address accepts the request with a SYN-ACK and then the Destination IP address leaves resources for the source IP address** 3. A final ACK packet is sent from the source IP address to the destination IP address acknowledging the permission to connect Explain what happens when a malicious actor sends a large number of SYN packets all at once: **If malicious actors sends a large number of SYN packets all at once causes the server to not have enough time to acknowledge the SYN requests and there won't be enough resources for the large amount of**

SYN requests. Therefore, there won't be any resources left for legitimate TCP SYN requests

Explain what the logs indicate and how that affects the server:

The logs indicate that the web server has become overwhelmed and is unable to process the visitors' SYN requests. The server is unable to open a new connection to new visitors who receive a connection timeout message.