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: A large number of TCP SYN requests are originating from a single unfamiliar IP address (203.0.113.0) targeting the company's web server (192.0.2.1) on port 443. The server is becoming overwhelmed and eventually stops responding to legitimate traffic, instead sending [RST, ACK] packets or timing out. This event could be: a Direct Denial of Service (DoS) 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. SYN (Synchronize): The client initiates a connection by sending a SYN packet to the server. This packet requests to synchronize sequence numbers. 2.SYN-ACK (Synchronize-Acknowledgment): The server responds to the client's SYN packet with a SYN-ACK packet. This acknowledges the client's SYN and sends its own synchronization request to the client. The server also reserves resources for this half-open connection. 3. ACK (Acknowledgement): The client sends a final ACK packet back to the server, acknowledging the server's SYN-ACK. This completes the three-way handshake, and a full TCP connection is established, allowing data transfer to begin. Explain what happens when a malicious actor sends a large number of SYN packets all at once: 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 without completing the handshake (i.e., not sending the final ACK packet), it's known as a SYN flood. The server, for each SYN packet received, attempts to establish a connection by sending a SYN-ACK and dedicating a portion of its resources to that half-open connection.

By flooding the server with these uncompleted SYN requests, the attacker quickly exhausts the server's connection queue and memory resources allocated for pending connections. This prevents the server from accepting new, legitimate connections.

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

The logs indicate a continuous stream of [SYN] packets from the attacker's IP (203.0.113.0) to the web server (192.0.2.1). While the server initially attempts to respond with [SYN, ACK] packets (e.g., log item 53), the attacker does not send the final ACK. As the attack progresses, the server becomes overwhelmed. The logs show this by:

The server sends [RST, ACK] packets to legitimate employee connection attempts (e.g., log item 73, 80, 121), indicating it's actively resetting connection attempts due to resource strain.

The server generates HTTP/1.1 504 Gateway Time-out errors (e.g., log item 77), meaning it's too busy to process HTTP requests.

From log item number 125 onwards, the log shows only the attacker's [SYN] packets, with no successful legitimate connections or even server responses to legitimate users. This signifies that the server is completely overwhelmed and has lost its ability to respond to any new, valid connection requests, effectively bringing the website down and causing a Denial of Service.