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: This is Showing signs of a SYN Flood Attack which it simulated a TCP packet and proceed to flood server with SYN Packets This error message sent by a gateway server that was waiting for a response from web server, since the web server took too long to respond it started sending out more frequent timeout error messages to requesting browsers The logs show that: At 3.390692 the attacker with IP of 203.0.113.0 first connection attempt was received to the server 192.0.2.1 on port 443 which was responded to normally by web server but that was promptly followed by Attacker sending repeated SYN packets which shows the servers trying to deny request but the large amount as long with real user requests that quickly caused deterioration of servers and showed how the more the systems overloaded the less actual users were able to connect which eventually led to a halt to server connections and no one requests were being received while the Attacker kept sending SYN packets and overwhelming the server . This event could be: SYN Flood Attack which is a type of Denial of Service 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. Synchronize the client sends SYN packet to server to start a connection which along with SYN includes a random sequence number 2. Synchronize-Acknowledge Server acknowledges clients SYN and random sequence number and creates a SYN-ACK with its own Random sequence number from the clients sequence number 3. Acknowledge Client sends acknowledge packet to server and acknowledges servers syn-ack including its random sequence number and includes a number one higher to sequence number which completes the handshake

Explain what happens when a malicious actor sends a large number of SYN packets all at once:
It causes the server to flood with half open connections that take server resources and queries and makes it increasingly difficult for the server to keep up and proceeds to slow down or completely crash the servers making it so no more connections can be made and make its services / websites useless.

Explain what the logs indicate and how that affects the server:
The logs show a SYN flood coming from 203.0.113.0 which proceeded to cause an impact on legitimate clients and our services. Causes resource exhaustion, connection rejections, and service disruption making the website inaccessible because of the attack.

To Prevent this from happening we can implement SYN cookies which makes it so only connections with handshakes with proper acknowledgment are allowed which prevents the servers connection queue from being exhausted or create a rate limiter for connections which could potentially also cause problems for legitimate users so SYN cookies would be better.