Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption

We have identified that the error message timeout was caused by an influx of messages that caused the port to crash. This is due to the fact that a particular IP address(203.0.113.0) was sending abnormal amount of SYN requests to the server. The logs show that the first attempt was launched on log entry number 52, three seconds and .390692 milliseconds after the logging tool started recording. It commenced many other entries afterwards which caused the server to stop responding because of the overload. This event could be a SYN flooding attack which is a type of 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. A SYN packet source sends a request to the server destination requesting to connect.

2. The destination replies with an SYN-ACK for the source to acknowledge the connection request and it will provide the necessary resources it needs to connect.

3. Then the final ACK is sent to the destination, allowing that it may connect.

The malicious actor will send an influx number of SYN packet requests to the destination requesting to connect. The large amounts of requests being sent cause the server to overload and it is not able to reserve any resource for the overwhelming requests trying to connect. This is an example of a SYN flood attack.

The logs show that the server got overwhelmed with the large number of requests. The server was unable to respond due to no resources available for the requests to be accommodated and caused the server to go down.