Cybersecurity Incident Report

Review of an attack which occurred leading to network interruption

Section 1: Type of attack that may have caused this network interruption

One potential explanation for the website's connection timeout error message is there exists an increase in the amount of requests being made to initiate the TCP handshake.

The logs show that there is an IP address which is not part of the employee’s network sending SYN packets to the web server of the company repeatedly, leading to a decrease in time for the TCP handshake to be established.

This event could be a DoS attack, particularly being a SYN flood attack, with the increased number of SYN packets being sent to the website’s server.

Section 2: 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 is the first step, where the original request is sent to the server, requesting synchronization via the sending of a “synchronize” packet.

2. SYN/ACK is the second step, where the destination server sends back a ”synchronize” “acknowledge” packet back to the requesting device, to establish a connection between the server and the device on the network.

3.ACK is the last step, where the requesting device sends an “acknowledge” packet to the server, completing the three steps of the TCP protocol, and giving rise to an active connection between the requesting device and the server. The protocol now at work will be HTTP.

Explain what happens when a malicious actor sends a large number of SYN packets all at once: The increased number of SYN packets leads to the network being flooded with requests to establish a TCP connection between the server and the malicious actor’s device. This decreases the time it would take for a working connection to be established between the requesting device’s on the network and the server, and in due time leads to the server being unable to process the abnormal amount of requests, and causing the server to be unreachable or shut down.

Explain what the logs indicate and how that affects the server: The logs indicate there is a malicious actor sending through SYN packets to the server.The malicious actor is sending SYN packets from an unrecognized IP address which is not a part of the network. The stated IP address is 203.0.113.0. The abnormal amount of requests has affected the server and the suspected conclusion is that this is a DoS attack.