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 server overload. The logs show that the web server stops responding after it is overloaded with SYN packet requests. This event could be a type of DoS attack called SYN flooding.

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.

SYN (Synchronize)

- Client initiates a connection by sending a SYN packet.

SYN-ACK (Synchronize-Acknowledgment)

- Server responds by sending SYN-ACK packet acknowledging the client’s request

ACK(Acknowledgment)

- Client replies by sending an ACK to confirm the connection between the client and server.

When a threat actor sends a large number of SYN packets to the server simultaneously, it consumes a significant amount of resources to respond to these incomplete connection requests. This can lead to resource exhaustion on the target server causing legitimate requests to be denied and delayed. This can cause the company both reputational and financial damages as customers are unable to get access to the website.

The logs show how the server was overwhelmed and being unable to respond to client SYN packets. To prevent attacks like this, I will work with the IT team to add WAF (Web Application Firewall) which can detect and block malicious traffic patterns preventing DoS attacks. We will also implement rate limiting to restrict the number of requests from a single source. In addition, we will be employing an IDPS (Intrusion Detection and Prevention Systems) that can detect patterns associated with SYN flood attacks. These systems can automatically trigger protective measures and alert network administrators.