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:

This event could be:

This afternoon, the monitoring system indicated a problem with the web server, causing connections to timeout with an error message. Using a packet sniffer revealed numerous TCP SYN requests from a single IP address, overwhelming the server. The findings likely indicate a SYN flood attack by a malicious threat actor intending to cause a denial of services.

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. The host/client sends a SYN packet to the server after establishing a connection to access their webpages.

2. The server will send an acknowledgement in the form of a SYN-ACK response, acknowledging this request.

3. Once the host/client receives the response, an automatic acknowledgement ACK is sent to finalize the process. This establishes a connection where data can be sent reliably and with stability.

Explain what happens when a malicious actor sends a large number of SYN packets all at once:

With a single IP address (probably spoofed), a malicious actor can cause a denial of services on a company website through SYN flooding. This is accomplished by sending numerous SYN requests to the server, with the goal of eliminating available port space for legitimate traffic to access the site. Once the server receives these SYN requests, it will respond with SYN-ACK packets, which the malicious IP will not respond to, leaving these ports occupied and unusable for legitimate SYN requests.

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

The logs will show that numerous SYN requests were received from this malicious IP, but when a SYN-ACK is sent back, it will yield no response from the client. The logs will indicate the server sending multiple SYN-ACK packets attempting to complete the TCP handshake, with no success. Ultimately, the server's available ports will all be overwhelmed leaving nothing for legitimate users to access.