Cybersecurity Incident Report

Cybersecurity Incident Report

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

One potential explanation for the website's connection timeout error message is that the web server is experiencing a Denial of Service (DoS) attack, specifically a TCP SYN flood attack.

The logs show that the web server is receiving an unusually large number of TCP SYN requests from an unfamiliar IP address within a short period of time. These requests are not being completed with the final acknowledgment required to establish a connection.

This event could be a TCP SYN flood DoS attack, which targets the availability of the server by overwhelming it with incomplete connection requests until it can no longer respond to legitimate users.

Section 2: Explaination 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:

1. The client sends a SYN (synchronize) packet to request a connection.
2. The server responds with a SYN-ACK (synchronize-acknowledge) packet.
3. The client completes the process by sending an ACK (acknowledge) packet, establishing the connection.

When a malicious actor sends a large number of SYN packets all at once, the server responds to each request with a SYN-ACK and waits for the final ACK that never arrives. These incomplete connections remain open and consume server memory and processing resources.

The logs indicate a high volume of half-open TCP connections, which causes the server to exhaust its available resources. As a result, the server becomes overwhelmed and is unable to respond to legitimate connection requests, leading to connection timeout errors for employees and customers accessing the website.