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:

A Denial of Service (DoS) attack known as a **SYN flood attack**, where the attacker sends a large number of TCP SYN requests to the web server, causing the server to become overwhelmed and unable to respond to legitimate traffic.

The logs show that:

Numerous TCP SYN packets were captured originating from a single unfamiliar IP address. These packets were not followed by the expected ACK responses, meaning the three-way handshake was not completed. This pattern is typical of a SYN flood attack. The TCP flags in the Wireshark logs indicate repetitive SYN flags without corresponding ACKs, confirming the incomplete handshakes.

This event could be:

A **TCP SYN Flood Attack**, a type of Denial of Service (DoS) attack. This attack attempts to exhaust server resources and make the website unavailable to users. It can also be a precursor to a **Distributed Denial of Service (DDoS)** attack if conducted from multiple sources.

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. **SYN** – The client sends a TCP SYN (synchronize) packet to the server to request a connection.
2. **SYN-ACK** – The server responds with a SYN-ACK packet acknowledging the request.

3. **ACK** – The client responds with an ACK packet, completing the handshake and establishing the connection.

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

The server allocates resources for each SYN request and waits for the corresponding ACK to complete the handshake. If the ACK never arrives (as with a SYN flood), these resources remain tied up until the connection times out. When too many of these half-open connections accumulate, the server's capacity is exhausted, preventing it from processing legitimate connection attempts.

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

The logs show an abnormally high number of SYN requests without corresponding ACKs, suggesting incomplete TCP handshakes. This results in the server being overwhelmed and unable to handle legitimate traffic, leading to connection timeout errors for users. The performance degradation prevents employees from accessing the sales webpage, disrupting operations and customer service.

Optional: Recommendations:

- **Implement SYN cookies** on the server to protect against SYN flood attacks.
- **Use a firewall or intrusion prevention system (IPS)** that can detect and mitigate DoS/DDoS attacks.
- **Monitor network traffic** continuously using intrusion detection tools.
- **Rate-limit SYN requests** from single IPs to reduce risk.
- Consider a **Content Delivery Network (CDN)** or **DDoS mitigation service** to distribute traffic and absorb attacks.