CYBER SECURITY INCIDENT RESPONSE

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:
network traffic analysis reveals a spike in connection requests, a single source ip, **203.0.113.5**, initiated a high volume of tcp/syn packets around 150 requests within a 4-second duration. These requests were directed at the web server https port 443. Unlike legitimate traffic seen earlier in the log, these requests remained incomplete, suggesting a deliberate attempt to overwhelm the server resources not allowing for business continuity.

This event could be: A focused denial of service attack or dos, by flooding the server with handshake requests that are never finalized, the attacker prevents the server from processing legitimate user traffic leading to the service timeout reported by employees.

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. A device sends a Syn (synchronized) request to the server to establish connection

2. The server acknowledges the request and reserves resources for the connection ,an opened port in this case 443.

3.ack the client is expected to send a final acknowledgement to establish the session. the server then leaves a port open for the device in order to establish a connection, waiting for the device to connect.

Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a malicious actor floods a server with a syn packet the attacker sends the initial syn but never responds to the servers syn/ack. This leaves the connection in a half opened state. Because the server must keep a memory buffer open for each of these pending connections, the tcp backlog quickly becomes overloaded.

Explain what the logs indicate and how that affects the server:
 The Wireshark logs confirm that prior to the alert legitimate users such as 198.51.100.14 were able to successfully connect and receive http 200 ok responses. However once the flood from 203.0.113.5 began, the server’s response time slowed until it eventually stopped responding to new syn requests entirely and the connection timeout errors experienced by the staff. This interruption affects business continuity and a risk to the agency's reputation and potential sales revenue.