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: That the server is not responding correctly The logs show that the server is receiving a large number of TCP SYN requests that are coming from an unfamiliar IP address and the server appears to be overwhelmed by the volume of this strange incoming traffic and is losing its ability to respond. This event could be generated by the server being under attack by a malicious actor, i suspect that a DoS attack have been taking place

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 (Synchronize)**: In the first step of the three-way handshake, the client (usually a web browser) sends a SYN packet to the server to initiate a connection. This packet contains a randomly generated sequence number to establish a starting point for data exchange. The purpose of this step is to request the server to synchronize and prepare for communication. 2. **SYN-ACK (Synchronize-Acknowledge)**: Upon receiving the SYN packet, the server acknowledges the request by sending a SYN-ACK packet back to the client. This packet also contains a randomly generated sequence number, and it acknowledges the client's SYN packet. At this point, the server is saying, "I'm ready to synchronize and communicate with you." 3. **ACK (Acknowledge)**: In the final step of the handshake, the client responds to the server's SYN-ACK packet by sending an ACK packet. This packet acknowledges the server's readiness to establish the connection. Now, both the client and server have exchanged synchronization information, and the connection is considered established. They can begin sending data to each other. When a malicious actor sends a large number of SYN packets all at once, it's known as a "SYN flood" attack. In this attack: - The malicious actor sends a barrage of SYN packets to the server, each with a spoofed source IP address, making it difficult to trace the attacker. - The server receives these SYN packets and allocates resources to prepare for

potential connections.

- However, because the attacker does not follow through with the final ACK step to complete the connection, the server's resources become exhausted as it awaits acknowledgment for each SYN packet.
- As a result, legitimate connection requests from other clients may be delayed or denied, as the server's resources are tied up dealing with the incomplete half-open connections from the attack.

In summary, a SYN flood attack overwhelms a server by initiating a large number of half-open connections that consume server resources, ultimately leading to the server's inability to respond to legitimate connection requests.

Luca Forma