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: this seems to be a DOS attack from a threat actor

The logs show that: logs 47, 48, and 49 show that this is a DOS attack

This event could be: from a single threat actor

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 SYN packet is sent to a source destination, requesting to connect.

2. The destination replies to the source with the SYN-ACK packet to accept the request. In which the destination will reserve resources to connect.

3. After this is accomplished, the final ACK packet is sent to the source to the destination to connect the two.

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

Answer: When a malicious actor sends large numbers of SYN packets all at once, it becomes difficult for the server to establish the SYN/ACK due to the flooding of SYN packets, which causes the website to not work properly.

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

Answer: The logs indicate that the threat actor is on one device, causing a DOS attack to the server. Flooding it with SYN packets.