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: The fact that the source IP address of the attacker (203.0.113.0) is sending a ridiculous amount of requests to the server, which is causing the server to malfunction due to the request overload.

The logs show that: At log 52, which is where the request of the attacker started, and on log 77 we can see that the server is no longer responding to any requests normally due to the overloading.

This event could be: SYN Attack, mainly because the attacker (203.0.113.0) repeatedly sends TCP SYN packets to initiate connections but never completes the three-way handshake. This leaves many half-open connections which exhausts the server.

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. The Ip source sends a SYN packet to the server to request a connection

2. The server responds with a SYN-ACK packet, which acknowledges and offers to establish a connection between both Ip's.

3. Finally, the Ip source sends an ACK back to the server to confirm the connection is established.

Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a malicious actor sends a large number of SYN packets, the server beggins the TCP, which consumes resources within the server, so when a lot of SYN packets are send and not completed, the half-completed connection overloads the server, making it to malfunction.

Explain what the logs indicate and how that affects the server: Each log indicates the time at which the event (log) occurred (since the SIEM tool started to monitor), also shows the Ip source from where the request of a connection is coming, and the Ip destination, which is the Website, service or system to which the Ip source want to make a connection. It also shows the protocol (TCP, HTTPS, etc…). Finally at the end shows a small piece of information with the ports that are interacting, which stage of the three handshake the current log is, etc.