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 logs show that: Connections of the Attacker and the Legitimate user and how the server has failed to respond to the legitimate website visitor due to the attacker sending too much traffic to the Web Server at the same time.

This event could be: A Syn Flood DOS Attack where the atttacker send several SYN Packets from one device or loaction to this target Web 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. First of all they is a Synchronization request from the person that wants to access the server facilities.

2. Then the Server Responds with a SYN ACK where the server acknowledges the response from the Web page visitor.

3. Here is the ACK once this is established TCP connection begins meaning that the connection is secure the webserver can give the visitor the resources he or she asks for.

Explain what happens when a malicious actor sends a large number of SYN packets all at once:What happens when a Malicious Actor s end too much SYN Packets its that it floods the server Intially the is only supposed to be SYN,SYN ACK, ACK but the attacker asks for SYN Connection more than once this goes on until the server goes out of resources maybe like shutting out legitimate users so as to accumulate enough facilities and if he cannot do it the Server Crashes down.

Explain what the logs indicate and how that affects the server: The logs indicate that the server is overwhelmed with the SYN packets coming from the attacker IP Address which is 203.0.113.0