DoS Incident Report

Section 1: Identify the type of attack that may have caused this network interruption

After observing the analysis logs, it is clear that the cause for the website's connection timeout error messages is a DoS attack, more specifically, a SYN Flood Attack. This is a DoS attack rather than a DDoS attack because only one Device (IP) is being used to flood the server with SYN packets. The logs show an IP address (203.0.113.0) sending multiple SYN requests to the server every second. This event then overloaded the server, causing any "legitimate requests" to time out, thus resulting in error messages.

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. The three-way handshake works as follows:

- (SYN) A user sends a SYN request in an attempt to make a connection with the web server.
- (SYN, ACK) The web server acknowledges the user's attempt to connect and sends back an acknowledgment.
- (ACK) The user's computer finalizes and establishes the connection to the web server with a final acknowledgment.

When a malicious threat actor sends a large number of SYN packets all at once, the server is overloaded and eventually stops responding. The server takes time to receive the [SYN] request and send back a [SYN, ACK] packet. So, when a threat actor sends multiple [SYN] packets a second, the server is unable to respond to all the requests causing it to overload and stop responding to all requests (legitimate and illegitimate). This whole process can be seen in the logs provided as the server is able to send [SYN, ACK] packets back to the malicious actor while still processing and allowing a connection to be formed with a legitimate user. However, as the rate of [SYN] packets being flooded increased, the server was unable to respond, resulting in the timeout of all requests and the eventual freezing of the server.
This would then result in the inability of any user to establish a connection with the server until the server is reset and all the piled-up SYN packets are gone. One potential method to secure the network quickly is to blacklist the IP address that is flooding the server. This would be a temporary fix to get the servers back up while more in-depth measures are implemented. Such measures might include the upgrade of the firewall that performs an analysis of packets incoming to the server, protecting it from SYN flood attacks.