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 immense number of data packets the website is receiving in a short timeframe. It might have been too overwhelmed and stopped responding. The logs show that the attacker tries to establish connection handshakes at first by IP spoofing. After that, the attacker continues to overload the servers with data packets over the span of a few milliseconds. The website does try to respond to a few of the requests, but fails due to being overwhelmed by the attacker. This event could be an SYN flooding, which simulates a TCP connection before flooding the server with data packets.

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 handshake consists of three steps:

1. Synchronization is the first step, this is the part when the employee or visitor’s IP address is trying to establish a connection with the site.

2. The next step is the synchronized acknowledge step, this is when the web server agrees to the connection from the first step.

3. The final step is the acknowledge, which allows the connection handshake to be established and allows data packets to transfer.

The webpage’s servers become too overloaded. The network bandwidth becomes too slow from all the processing and the server ends up crashing.

The logs indicate that the IP address “203.0.113.0” is flooding the server with tons of data packets. This causes the site to malfunction, and the immense traffic that is occurring is causing the TCP connections to fail from other addresses.