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: That the website is being flooded with data packets in an attempted DoS attack. This would overwhelm the servers bandwidth and prevent is it from responding to valid requests.

The logs show that:
Using the Wireshark logs, the server began receiving numerous TCP SYN request packets from the unfamiliar IP address 203.0.113.0 in addition to regular traffic from IP addresses associated with the company's devices. This traffic started out as mized with regular requests before overwhelming the server and preventing regular requests from being executed

This event could be:
This event is likely a SYN flood attack. This is a type of Denial of Service attack where the attacker floods the server with SYN packets. These SYN packets are one step of the normal TCP protocol for establishing connections with devices, however, the attacker is sending such a high volume that is clear there is malicious intent not just a normal connection.

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 first step is that the visitor's device sends a SYN packet to the server as a request to establish a connection.
2. The request is then reviewed by the server and if it is determined as a valid request the server will send back a SYN-ACK packet as an acknowledgement and perform the necessary steps for the visitor's device to connect.
3. The visitor's device then sends an ACK packet to the server and is then able to make the desired request, in this case an HTTP request for a webpage.

Explain what happens when a malicious actor sends a large number of SYN packets all at once:
The attacker is simulating a normal TCP handshake, but rather than intending to actually establish a connection they just send a high volume of packets in an attempt to overwhelm a server and prevent it from establishing connections with the valid requests.

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

The Wireshark logs indicate that several valid TCP requests were failing due to the high volume of SYN packets. Eventually, the server stopped receiving those valid requests entirely indicating the success of the attack. As an immediate defese, the malicious IP address should be blocked using the firewall and the firewall settings should be configured to recognize repeated SYN requests and block the IPs sending them. This can help prevent later SYN flood attacks from different IP addresses.