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: an overflow of requests to the web server.

The logs show that: a large amount of SYN requests were sent to the web server from the IP address 203.0.113.0.

This event could be: a possible SYN flood attack on the organization’s web server from an unknown malicious actor.

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. SYN: The user makes a “synchronization” request to the webserver, indicating to the web server that someone is attempting to connect.

2. SYN, ACK: The web server sends back a “synchronization acknowledged” response to the user to indicate that the server has received their requests and has reserved resources preparing for connection.

2. ACK: The user sends the final part of the three-way handshake back to the web server, the “acknowledge” response to indicate that they are good to connect.

Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a malicious actor sends a large amount of SYN requests, the web server takes time to process and serve them all. This means the web-server will reserve space and resources to serve all of the separate request until the server has no more resources available for any more TCP connections. A type of DoS attack.

Explain what the logs indicate and how that affects the server: The logs show that a malicious actor from the source IP of 203.0.113.0 overloaded the webserver with a large amount of SYN requests to the point of locking out reputable users from accessing the organization’s website. Even though the IP was blocked through firewall configuration and web server reset, the malicious actor may spoof more IP’s to continue this attack and render the web server useless. Some ways to defend against this in the future could be implementing some form of NGFW (next generation firewall) which should within the service have the capability of detecting suspicious network traffic like this and prevent something like this from happening again.