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: A Denial of Service(DoS) attack- an attack that targets a network or server and floods it with network traffics

The logs show that: The web server stops responding after it is overloaded with SYN packets requests from an attacker with the IP address of 203.0.113.0.

This event could be: A type of DoS attack called SYN (synchronize) flood attack- a type of DoS attack that simulates a TCP connection and floods a server with SYN 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. Explain the three steps of the handshake:

1. The [SYN] packet is the initial request from a website visitor trying to connect to a web page hosted on the web server. SYN stands for “synchronize.”
2. .The [SYN, ACK] packet is the web server’s response to the visitor’s request agreeing to the connection. The server will reserve system resources for the final step of the handshake. SYN, ACK stands for “synchronize acknowledge.”
3. The [ACK] packet is the visitor’s machine acknowledging the permission to connect. This is the final step required to make a successful TCP connection. ACK stands for “acknowledge.”

Explain what happens when a malicious actor sends a large number of SYN packets all at once: In the case of a SYN flood attack, a malicious actor will send a large number of SYN packets all at once, which overwhelms the server’s available resources to handle the requests. The server will become overwhelmed and unable to respond to both the attacks and legitimate TCP connection requests. A DoS direct attack originates from a single source. A distributed denial of service (DDoS) attack comes from multiple sources, often in different locations, making it more difficult to identify the attacker or attackers. In this case, since attacks only occur from one IP address, it is a DoS attack instead of DDoS attacks.

Explain what the logs indicate and how that affects the server: The logs indicate the web server has become overwhelmed with SYN packets from an IP address (attacker) of 203.0.113.0 and is unable to process other legitimate visitors’ SYN requests from IP address such as 198.51.100.22. Moreover, as the log goes on, the web server stops responding to legitimate employee visitor traffic. From log item number 125 on, the web server stops responding. The only items logged at that point are from the attack. As there is only one IP address attacking the web server. The server then is unable to open a new connection to new visitors who only receive a connection timeout message.