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 web server being unresponsive because of malicous behaviour which can cause the server to not respond to authorized requests. The logs show that an IP address “203.0.113.0” established a legitimate TCP connection with our web server, but shortly after a bunch of TCP “SYN” packets started to flood our web server from this same IP address. This event could be an Denial Of Service attack called “SYN Flood”. This attack consists of a layer 4 internet communication protocol that establishes a legitimate connection before the transmission of any data. During the connection process of the TCP protocol, it uses something called a “3 way handshake”. This Handshake consists of 3 flags/ packets being sent back and forth between the client device and the server to establish a connection, these packets are “SYN, SYN-ACK, SYN”. The “203.0.113.0” ip address flooded the server with “SYN” packets which caused the server to be unresponsive because of the overwhelming amount of traffic being sent.

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. A normal TCP connection begins with the client sending a SYN (synchronize) packet to the server it is trying to reach.
2. The server then responds with a “SYN-ACK” packet, which is acknowleging the client's “SYN” and proposing it’s own sequence number and the acknowledgement number.
3. The last “ACK” packet is sent by the client back to the server, acknowledging the server’s “SYN-ACK” packet and including the server’s sequence number.

Explain what happens when a malicious actor sends a large number of SYN packets all at once:

In a SYN flood attack, the attacker sends a flood of SYN packets to the server, often with spoofed IP addresses. The server responds to each SYN packet with a SYN-ACK, expecting the final ACK. However, the attacker never sends the ACK, causing the server to keep the connection open for a specific timeout period. As the server continues to receive SYN requests and keep the connections open, it exhausts its available resources, making it unable to handle legitimate traffic and causing the server to become unresponsive.

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

The logs indicate that 47 messages were sent and received by the web server in the 3.1 seconds after starting the log. IP address “203.0.113.0” initially had established a TCP connection with the web server because the server responded to the first couple “SYN” packets from this address. But the IP address kept sending the web server TCP “SYN” packets. As this is going on, a couple of employees were able to reach the web server successfully according to the logs. But eventually the overwhelming “SYN” packets from 203.0.113.0 caused the server to go down because of the amount of traffic it was getting flooded with from those TCP “SYN’ packets. This is a type of Denial of Service attack called “SYN Flood”.