Cybersecurity Incident Report

STEP 1

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: it is likely possible that it is a DoS attack given the fact that it is coming from one IP address.

The logs show that: the web server stops once being overloading with SYN packet requests

This event could be: therefore known as SYN flooding (DoS attack)

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 packet sent from source to destination- requests to connect using the servers IP address
2. SYN-ACK. The server responds with a SYN-ACK(acknowledgment) message saying it accepts the connection.
3. ACK. The server sends a message confirming the connection and allowing it to communicate successfully.

Connection between server and users over a TCP network.

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

If a malicious actor sends a large number of SYN packets all at once it will overwhelm the servers resources to the connection causing the server to have no resources left over for TCP connection requests.

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

The logs indicate and who was the log entry attempt as well as the time the messages were sent and received from the web server.

We can see that the IP address 192.0.2.1 belongs to the company’s web server. The range of IP addresses from 198.51.100.0/24 belongs to employees' computers. The protocol indicates that the packets are being sent using the TCP protocol in this case—> HTTP at the application layer once it is established. We can see the attacker sending the SYN requests and where the server stops responding at No.125 in the logs where the server cannot open them.