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 received multiple SYN requests from the attacker causing it to be flooded by the volume of requests at once so the gateway server returns an RST error message and the web server crashes and stops responding.

The logs show that: The logs show that there is anormal traffic and several requests at the same time from unknown IP addresses trying to infiltrate the network and therefore causing a DDOS attack with multiple visits.

This event could be:

according to the log the attacker could detect before launching a request the open ports which facilitates the infiltration in the network very likely that he used a malware.

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 an employee 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:

malicious actors can take advantage of the TCP protocol by flooding a server with SYN packet requests for the first part of the handshake. However, if the number of SYN requests is greater than the server resources available to handle the requests, then the server will become overwhelmed and unable to respond to the requests. This is a network level denial of service (DoS) attack, called a SYN flood attack, that targets network bandwidth to slow traffic. A SYN flood attack simulates a TCP connection and floods the server with SYN packets. 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.

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

The logs indicate two types of errors :

- An HTTP/1.1 504 Gateway Time-out (text/html) error message. This message is generated by a gateway server that was waiting for a response from the web server. If the web server takes too long to respond, the gateway server will send a timeout error message to the requesting browser.
- An [RST, ACK] packet, which would be sent to the requesting visitor if the [SYN, ACK] packet is not received by the web server. RST stands for reset, acknowledge. The visitor will receive a timeout error message in their browser and the connection attempt is dropped. The visitor can refresh their browser to attempt to send a new SYN request.