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: is a Denial of Service (DoS) attack, specifically a **SYN Flooding** attack. The logs reveal that the web server stopped responding after being overwhelmed by a high volume of SYN packet requests. In a SYN Flooding attack, an attacker sends numerous SYN packets to the server without completing the TCP handshake, causing the server to exhaust its resources managing these half-open connections.Consequently, the server's inability to handle genuine connection attempts results in disrupted service and accessibility issues for legitimate users. This event could be:SYN flood Atack

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." e 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: 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.

Explain what the logs indicate and how that affects the server:The logs indicate that the web server has become overwhelmed and is unable to process incoming SYN requests. The server's inability to handle the high volume of SYN packets, as represented in red in the logs, exhausts its resources and prevents it from establishing connections with legitimate visitors. Consequently, these visitors receive connection timeout messages, as the server is unable to open new connections and process their requests. This overload results from the malicious actor's excessive SYN requests, which prevent the server from responding to genuine user traffic.