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 server is under attack by a malicious actor. Possible DOS attack The logs show that: MULTIPLE LOGS FROM SAME IP ADDRESS WHICH COMPRIMISING THE SYSTEM This event could be: DOS ATTACK,server is under attack by a malicious actor. One afternoon, an automated alert was received from the monitoring system indicating a problem with the web server. You attempt to visit the company's website, but you receive a connection timeout error message in your browser. Packet sniffer used to capture data packets in transit to and from the web server. A large number of TCP SYN requests coming from an unfamiliar IP address. The web server appears to be overwhelmed by the volume of incoming traffic and is losing its ability to respond to the abnormally large number of SYN requests. The server is under attack by a malicious actor. Possible DOS attack called SYN flooding

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 large number of TCP SYN requests coming from an unfamiliar IP address. 2. web server appears to be overwhelmed by the volume of incoming traffic 3.MULTIPLE LOGS FROM SAME IP ADDRESS WHICH COMPROMISING THE SYSTEM

Explain what happens when a malicious actor sends a large number of SYN packets all at once:losing its ability to respond to the abnormally large number of SYN requests.

Explain what the logs indicate and how that affects the server: TCP/HTTP LOGS

MULTIPLE LOGS FROM SAME IP ADDRESS WHICH COMPROMISING THE SYSTEM with a large number of TCP SYN requests coming from an unfamiliar IP address.The web server appears to be overwhelmed by the volume of incoming traffic losing its ability to respond to the abnormally large number of SYN requests.The server is under attack by a malicious actor. Possible DOS attack.