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: that there was a DoS Service attack and they were using a SYN packet to overload the network traffic.

The logs show that: there is unknown server that is intercepting the IP addresses from an external drive and is slowing down the connection and has interrupted the work station

This event could be: a 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.The visitor contacts the source and the source sends an SYN to the visitors side

2. SYN,ACK is the customers server confirming the transport from port 443 to the external server

3.ACK is the source confirming by sending customers response back to source which is the website

Explain what happens when a malicious actor sends a large number of SYN packets all at once: When the malicious actor sends a large number of SYN Packets all at once it slows down the TCP connection.
Explain what the logs indicate and how that affects the server: T server starts to slow down and eventually crashes. There is no more connection between the customer and the website