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: a flood of SYN packets The logs show that: The attacker is sending several SYN request every second, a time out error message, a RST,ACK This event could be: A SYN flood 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. The first step in the synchozize; those who want access asking for access 2. SYN,ACk is the synchonize acknowledgement; where the receiving end of the handshake is acknowledging that someone wnts access to the information they have 3. ACK is the receiving end acknowledging the ok for giving access to the requested information Explain what happens when a malicious actor sends a large number of SYN packets all at once: This floods the system making it unable to process incoming requests Explain what the logs indicate and how that affects the server: The logs indicate a flood of SYN requests from a threat actor using the empployee's identity to send these requests