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: Overwhelmed Server  The logs show that: There is a large number of TCP/SYN requests coming from an unfamiliar IP address  This event could be: Smurf Attack or 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 device sends a SYN request to a server  2.The server responds with a SYNACK  3. Once the server receives the final ACK packet from the device, a TCP connection is established.  Explain what happens when a malicious actor sends a large number of SYN packets all at once: It is considered a SYN flood attack where a large amount of SYN requests get sent to the server overwhelming it and causing connectivity problems  Explain what the logs indicate and how that affects the server: The logs indicate that there are an overwhelming amount of TCP SYN requests coming from an unfamiliar address causing the server to hold connection and even worse possible threat attacks to the company website and customer data. |