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 logs show that: coming from one IP address Direct DoS SYN Flood Attack  This event could be: Direct syn DoS 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.SYN  2. SYN/ACK  3.ACK  Explain what happens when a malicious actor sends a large number of SYN packets all at once:  It floods the server with requests, and the server gets overwhelmed trying to respond eventually essentially crashing the website,  Explain what the logs indicate and how that affects the server: The logs indicate that at first some employee requests were going through and the DoS attacks were not until the server was flooded with continuous SYN packet requests. This caused the system to fail.  Server had to be shut down to stop the attack but will continue shortly after. A fix needs to be completed to block the SYN attack. There is only one IP address attacking the website so we can safely assume this is a Direct DoS SYN flood attack. |