# 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 website is attacked with some suspicious big traffic that slow down the network bandwidth.  The logs show that: Multiple logs where the website was attacked.  This event could be:a DoS attack called 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.SYN  2. SYN-ACK  3.ACK  Explain what happens when a malicious actor sends a large number of SYN packets all at once: SYN flood attacks work by exploiting the handshake process of a [TCP](https://www.cloudflare.com/learning/ddos/glossary/tcp-ip/) connection.The attacker sends a high volume of SYN packets to the targeted server, often with [spoofed](https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/) IP addresses.  Explain what the logs indicate and how that affects the server: Approximately 47 messages were sent and received by the web server in the 3.1 seconds after starting the log. The network is down and the employees can’t access the sales page. The web server stops responding tolegitimate employee visitor traffic.. The visitors receive more error messages indicating that they cannot establish or maintain a connection to the web server. |