# 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: the IP address 200.0.113.0 is attacking the web server by flooding it with multiple syn requests thus overwhelming it.  This event could be: A direct DoS 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: The [SYN] packet is the initial request from an employee visitor trying to connect to a web page hosted on the web server. SYN means synchronize.  2.Syn, Ack: The [SYN, ACK] packet is the web server’s response to the visitor’s request agreeing to the connection. The server will reserve system resources for the final step of the handshake. SYN, ACK stands for “synchronize acknowledge.  3.ACK: The [ACK] packet is the visitor’s machine acknowledging the permission to connect. This is the final step required to make a successful TCP connection. ACK stands for “acknowledge.”  Explain what happens when a malicious actor sends a large number of SYN packets all at once:  This kind of attack is called a DOS (denial of service) and it is an attack where the malicious threat actor sends multiple synchronization requests to the server in order to overwhelm it and crash it. The multiple requests ensure server resources are not available to authorized users. An example is sending multiple ICMP ping requests to the server by a threat actor.  Explain what the logs indicate and how that affects the server:  The logs indicated that a malicious actor with IP address 200.0.113.0 is in the middle of the attack and is using a DOS mechanism to attack the web server, freeze up services and resources and crash it. |