# 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 that the website could be under an attack by a malicious actor, which is preventing SYN packets from the users from reaching the intended IP addresses of the website.<br><br>The logs show that there are multiple requests from the same IP address to the website which is overwhelming the website with the huge amount of SYN packets.<br><br>This event could be a type of Denial of Service attack called SYN flood attack since there are so many SYN packets from the same IP address. |

| 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:<br>1. The [SYN] packet is the initial request from an employee visitor trying to connect to a web page hosted on the web server. SYN stands for “synchronize.”<br><br>2. 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.”<br><br>3. 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.”<br><br>Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a malicious actor sends multiple SYN packets at once, the website takes all those packets to process them to the second step of the handshake which is [SYN, ACK]. Since there are so many SYN packets, the website will spend so much time trying to agree with each and every SYN packet which will slow down the website’s response and eventually make it unresponsive to any other SYN packets from users. This is a form of Denial of Service attack called SYN packet flooding.<br><br>Explain what the logs indicate and how that affects the server: The logs show that there are so many SYN packets from the same IP address which indicates that SYN packet flooding attack, a form of Denial of Service attack, is happening towards the website. This attack is |

causing the website to malfunction and be unresponsive to any other SYN packets from other users. This greatly affects the website's security by making it more vulnerable to other potential future attacks. One way to stop this attack is to block the attacker's IP address and notify the team of security analysts to take further action regarding the situation. Blocking the attacker's IP address is a temporary solution as the attacker may do the attack again by using a different IP address, so taking action as soon as possible is necessary.