# 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 attacker is sending several SYN requests every second. The rows highlighted and labeled yellow are failed communications between legitimate employee website visitors and the web server.  The logs show that: Only one IP address is attacking the web server by sending multiple Syn request every second.  This event could be: DDOS 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 [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.”  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.”  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.”  Explain what happens when a malicious actor sends a large number of SYN packets all at once: When the malicious actor send number of SYN packet, The server will become overwhelmed and unable to respond to the requests. The visitors receive more error messages indicating that they cannot establish or maintain a connection to the web server.  Explain what the logs indicate and how that affects the server: The logs indicate that the IP address 203.0.113.0 is sending multiple SYN request to the server which is most likely called DDOS SYN flood attack. The server at first was able to respond to the normal visitor traffic but after the attack, It got difficult which make it to crash out. |