# 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: Someone from IP address 203.0.113.0 is flooding the network with SYN packets.  The logs show that: IP address 203.0.113.0 keeps sending SYN requests to the browser which is in turn overwhelming the network and making it difficult for employees to access the site.  This event could be: a DoS attack using SYN flood packets. | |
|

| **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.There is a SYN packet, synchronize, being sent over the network, from the source IP which is 203.0.113.0 trying to connect to 192.0.2.1 - destination IP address.  2. The network acknowledges that and replies with a [syn, ack] acknowledgment saying it’s received the packet.  3.Then finally sends an ACK packet back confirming the handshake.  Explain what happens when a malicious actor sends a large number of SYN packets all at once: it overwhelms the system once the requests are greater than the server resources. This is a network level denial of service attack (DoS), that targets network bandwidth to slow traffic.  Explain what the logs indicate and how that affects the server:The logs begin to reflect the struggle the web server is having to keep up with the abnormal number of SYN requests coming in at a rapid pace.  An HTTP/1.1 504 Gateway Time-out (text/html) error message. This message is  generated by a gateway server that was waiting for a response from the web server. If  the web server takes too long to respond, the gateway server will send a timeout error  message to the requesting browser.  An [RST, ACK] packet, which would be sent to the requesting visitor if the [SYN, ACK]  packet is not received by the web server. RST stands for reset, acknowledge. The  visitor will receive a timeout error message in their browser and the connection  attempt is dropped. The visitor can refresh their browser to attempt to send a new SYN  request.  The web server stops responding to legitimate employee visitor traffic. The visitors receive more error messages indicating that they cannot establish or maintain a connection to the web server.  From log item number 125  on, the web server stops responding. The only items logged at that point are from the attack as there is only one IP address attacking the web server, you can assume this is a direct DoS SYN flood attack. |