# 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 gateway server was waiting for a response from the web server, and took too long to respond so the gateway server sent a timeout error message to the request browser. It took too long to respond because the server was unable to answer because it was overwhelmed with requests.  The logs show that: this attack started with the first request of the attacker (203.0.113.0) sending up approximately 47 messages in 3 seconds. In the next 20 rows of the log he kept sending SYN requests every second until the server overwhelmed and was unable to respond to requests. From log item number 125 on the web server stops responding.  This event could be: a successful denial of service (DoS) attack, specifically a direct DoS SYN flood attack. It’s a DoS attack and not a DDoS attack because the attack has been directed only from one device. |
|

|  |
| --- |
| **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 (synchronize) packet is the initial request from an employee visitor trying to connect to a web page hosted in the server. 2. The SYN/ACK (synchronize acknowledge) 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. 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.   Explain what happens when a malicious actor sends a large number of SYN packets all at once: If the quantity of SYN requests is greater than the server resources available to handle requests, the server will get overwhelmed and it is going to be unable to respond to any requests. The attacker is sending a lot of SYN requests trying to begin a handshake trying to synchronize. The server starts to respond to these requests but eventually it stops, because it can’t get over with any handshake and new requests of new handshakes are coming so it stops responding to anyone due to the high amount.  Explain what the logs indicate and how that affects the server: the logs indicate that from log item number 125 on, the web server stops responding to everyone, it has been flooded with constant SYN packets every second and it got overwhelmed by not being able to respond to those. That’s why the server shows two errors on the logs: HTTP/1.1 504 Gateway Time-out (text/html) telling that the gateway server was waiting for a response from the web server that stopped working and the RST,ACK packet that is sent when a SYN,ACK packet is not received. |