# 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 server is overwhelmed  The logs show that one IP is making a lot of requests to the server in a short time lapse  This event could be Denial of Service |
|

|  |
| --- |
| **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 visitor sends a TCP segment with the flag SYNCHRONIZE in that segment includes Initial Sequence Number (ISN) 2. SYN-ACK: When the server receives a new segment responds back the initial segment adding ACK flag and own ISN is greater than the client 3. ACK: The client who sent that segment now receives back the SYN-ACK segment. Finally, this segment is sent again to the server but now it has got a new ACK flag, once the server has the segment with the new flag the connection is complete.   Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a malicious actor makes a lot of requests with SYN packets the server can be overwhelmed and the performance decreases, this way the server cannot respond to other clients, this could be considered a DoS attack.  Explain what the logs indicate and how that affects the server: Logs indicate the server was working great until the malicious actor makes DoS attack with the same IP in a short period of time. The malicious actor always sends SYN segment, and the server changes the flags when trying to respond RST-ACK an unusual flag. |

# Potential consequences

The potential consequences of this attack can be listed:

* Financial: the overloading of the server will be seen in the monthly billing increasing resources quota like CPU
* Reputation: The company's image with investors and customers would fall due to the lack of competence and confidence in handling threats.

# Suggest potential ways to secure the network

We can configurate a system that can block the requests to the server when the malicious actor makes 10 requests in 10 seconds or less. This block could work 10 min after unblocking that IP, the final step is this event repeat again it will add to blacklist.