# 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/ Una posible explicación para el mensaje de error de tiempo de espera de conexión del sitio web es:  Se está identificando un tipo de ataque tipo DoS que simula la conexión TCP/IP e inunda el servidor con paquetes SYN dado que se observa un gran número de solicitudes TCP SYN procedentes de una dirección IP desconocida.  Lo que ha hecho que el puerto se sature y no funcione, recibiendo un mensaje de error de tiempo de espera de conexión en el navegador.  Esto esta afectando a la empresa dejando inaccesible la pagina web y que los empleados no puedan mostrar a los clientes los paquetes de viajes a los que pueden optar, perdiendo así posibles contratos de viajes.  The logs show that/Los registros muestran que:  Los registros muestran un número elevado de solicitudes TCP SYN.  This event could be/Este evento puede ser:  Un ataque SYN flood |
|

|  |
| --- |
| **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/Cuando los visitantes del sitio web tratan de establecer una conexión con el servidor, se produce un protocolo de enlace de tres vías mediante el protocolo TCP. Explique los tres pasos del protocolo de enlace:   1. Se envía una solicitud SYN o sincronizar al servidor  * El paquete [SYN] es la solicitud inicial de un empleado visitante que intenta conectarse a una página web alojada en el servidor web. SYN significa "sincronizar".  1. El servidor responde con un paquete SYN/ACK para confirmar la recepción de la solicitud del dispositivo, dejando un puerto abierto para el paso final del protocolo de enlace  * El paquete [SYN, ACK] es la respuesta del servidor web a la solicitud del visitante que acepta la conexión. El servidor reservará los recursos del sistema para el paso final del protocolo de enlace. SYN, ACK significa "sincronizar reconocimiento".  1. Se establece una conexión TCP  * El paquete [ACK] es la máquina del visitante que reconoce el permiso para conectarse. Este es el paso final necesario para realizar una conexión TCP exitosa. ACK significa "reconocimiento".   Explain what happens when a malicious actor sends a large number of SYN packets all at once/Explique qué pasa cuando un actor malicioso envía un largo número de paquetes SYN a la vez:  Si el número de solicitudes SYN es, mayor que el número de puertos disponibles en el servidor, el servidor se saturará y no podrá funcionar y no responderá a las solicitudes.  Explain what the logs indicate and how that affects the server/Explique que indican los registros y como afectan el servidor:  Los registros indican que el puerto afectado es el 443, siendo afectado el protocolo de la capa de transporte del modelo TCP/IP  Este tipoi de ataque DoS se origina en una sola fuente, dado que se identifica la IP 192.0.2.1 repetidas veces enviando solicitudes |

* Se sugiere mantener los firewalls activos y vigentes para evitar este tipo de ataques en el futuro.