# Informe sobre incidentes de ciberseguridad

|  |
| --- |
| **Sección 1: Identifica el tipo de ataque que puede haber causado esta**  **interrupción de la red** |
| El ataque es una inundación SYN, un tipo de ataque de denegación de servicio (DoS). Este ataque satura el servidor web con solicitudes SYN, lo que inicia conexiones TCP, pero no las completa. Aunque el ataque parece provenir de una única dirección IP, el atacante podría usar IP spoofing para ocultar su identidad y evitar ser bloqueado fácilmente. Los registros muestran un gran número de conexiones entrantes en el puerto 443 (HTTPS), todas con solicitudes SYN que inician el proceso de conexión, pero no lo finalizan. |
|

|  |
| --- |
| **Sección 2: Explica cómo el ataque está provocando que el sitio web no funcione como debería** |
| El ataque está colapsando el servidor web debido a una explotación del protocolo TCP, específicamente durante el handshake de tres vías. En una conexión TCP normal, el cliente envía una solicitud SYN, el servidor responde con un SYN-ACK, y finalmente el cliente envía un ACK para completar la conexión.  En este ataque, el atacante envía una gran cantidad de solicitudes SYN, pero no responde a los SYN-ACK del servidor, dejando las conexiones a medio abrir. Esto agota los recursos del servidor, que tiene que mantener una gran cantidad de conexiones abiertas sin completarse, lo que lo deja incapaz de atender nuevas conexiones legítimas y, por ende, provoca la caída del servicio. |