# Informe sobre incidentes de ciberseguridad

|  |
| --- |
| **Sección 1: Identifica el tipo de ataque que puede haber causado esta**  **interrupción de la red** |
| El tipo de ataque que se logra identificar luego de hacer un escaneo con la aplicación Wireshark es un enorme número de solicitudes TCP SYN procedentes de una IP desconocida. |
|

|  |
| --- |
| **Sección 2: Explica cómo el ataque está provocando que el sitio web no funcione como debería** |
| Al hacer múltiples peticiones, se satura el servidor, lo que no da cabida a las peticiones de los otros usuarios, brindando un mensaje de tiempo de conexión agotado. |

* ¿Qué entiendes actualmente sobre los ataques a la red?

Los ataques de Red están didseñados para interrumpir el funcionamiento normal de los sistemas y servicios.

* ¿Con qué tipo de ataque es probable que se produzcan los síntomas descritos en el escenario?

El comportamiento observado, con un gran volumen de solicitudes TCP SYN provenientes de una IP desconocida, es característico de Inundación SYN (SYN Flood).

* ¿Cuál es la diferencia entre una denegación de servicio (DoS) y una denegación de servicio distribuida (DDoS)?

**DoS:** Proviene de un único origen (dispositivo o servidor). Es más fácil de mitigar porque solo involucra una dirección IP que se puede bloquear directamente.

**DDoS:** Utiliza múltiples dispositivos distribuidos, a menudo comprometidos a través de botnets. Es más difícil de bloquear debido a la variedad de direcciones IP que genera el tráfico malicioso.

* ¿Por qué el sitio web tarda tanto en cargarse e informa de un error de tiempo de espera de conexión?

El sitio web está sobrecargado debido al alto número de solicitudes SYN no resueltas. Esto provoca que el servidor:

* Agote sus recursos (memoria, CPU, sockets disponibles).
* No pueda manejar solicitudes legítimas de empleados o clientes, lo que resulta en tiempos de espera prolongados o en un error de tiempo de espera de conexión (timeout).