Actividad de ejemplo: Analiza un ataque a la red

Sección 1: Identifica el tipo de ataque que puede haber causado esta interrupción de la red
Una posible explicación para el mensaje de error de tiempo de espera de conexión del sitio web es un ataque DoS. Los registros muestran que el servidor web deja de responder después de que se sobrecarga con solicitudes de paquetes SYN. Este evento podría ser un tipo de ataque DoS llamado inundación sincronizada (SYN).

Sección 2: Explica cómo el ataque está causando el mal funcionamiento del sitio web
Cuando las/los visitantes del sitio web intentan establecer una conexión con el servidor, se produce un 3-way handshake (acuerdo de 3 vías) mediante el protocolo TCP. El proceso de enlace consta de tres pasos: 1. Se envía un paquete SYN de origen a destino, solicitando la conexión. 2. El destino responde al origen con un paquete SYN-ACK para aceptar la solicitud de conexión. El destino reservará recursos para que el origen se conecte. 3. El origen envía un paquete ACK al destino para confirmar el permiso de conexión. En el caso de un ataque de inundación sincronizada, un agente de amenaza enviará una gran cantidad de paquetes SYN a la vez, lo cual saturará los recursos disponibles del servidor a reservar para la conexión. Cuando esto sucede, no quedan recursos del servidor para las solicitudes de conexión TCP legítimas. Los registros indican que el servidor web se ha saturado y es incapaz de procesar las solicitudes SYN de los visitantes. El servidor no puede abrir una nueva conexión a nuevos/as visitantes, quienes reciben un mensaje de tiempo de espera de conexión.