Analizar ataques a la red

Sección 1: Identifique el tipo de ataque que pudo haber causado esto interrupción de la red
Una posible explicación para el problema del sitio web es el tiempo de espera de conexión/error. El mensaje es un ataque DoS. Los registros muestran que el servidor web deja de responder tras una sobrecarga con solicitudes de paquetes SYN. Este evento podría ser un tipo de ataque DoS llamado inundación SYN.

Sección 2: Explique cómo el ataque está provocando el mal funcionamiento del sitio web
Cuando los visitantes del sitio web intentan establecer una conexión con el servidor web, se produce un protocolo de enlace de tres vías mediante TCP. Este protocolo consta de tres pasos: 1. Se envía un paquete SYN desde el origen al destino solicitando 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. Se envía un paquete ACK final desde el origen al destino reconociendo el permiso para conectarse. En caso de un ataque de inundación SYN, un agente malicioso enviará una gran cantidad de paquetes SYN a la vez, lo que satura los recursos disponibles del servidor para la conexión. Cuando esto sucede, no quedan recursos del servidor para solicitudes de conexión TCP legítimas. Los registros indican que el servidor web se ha saturado y no puede procesar las solicitudes SYN de los visitantes. El servidor no puede abrir una nueva conexión para los nuevos visitantes que reciben un tiempo de espera de conexión mensaje.