Cybersecurity Incident Report

Sección 1: Identifique el tipo de ataque que pudo haber causado esto interrupción de la red
Una posible explicación para el mensaje de error de tiempo de espera de conexión del sitio web es:esto se debe a que al mandar la petición para conectarse a algún servicio, este procedimiento tiene un tiempo máximo de espera antes de dar un error. Esto puede ser por diversos factores, caídas de sistema, saturación del servidor o actualización de servicio. Los registros muestran que: un usuario(203.0.113.0) establece una conexión con el servidor para luego volver a solicitar conexión, luego se observa otros usuarios estableciendo conexión y solicitando finalmente la web o los servicios requeridos. Este usuario repetidas veces cada segundo inunda el servidor de peticiones con lo que el servidor no da para responder y comienza a no poder dar servicio a los usuarios legítimos que buscan empezar con parte de sus obligaciones. Este evento podría ser: por el uso del protocolo de conexión y el repetido intento de este usuario de establecer conexión una y otra vez muchas veces por segundo, se entiende que es un ataque DoS que buscaba saturar el servicio de esta web.

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 utilizando el protocolo TCP. Explique los tres pasos: 1.El paquete [SYN] es la solicitud inicial de un visitante empleado que intenta conectarse a una página web alojada en el servidor web. SYN significa "sincronizar". 2.El paquete [SYN, ACK] es la respuesta del servidor web a la solicitud del visitante que acepta la conexión. El servidor reservará recursos del sistema para el paso final del protocolo de enlace. SYN, ACK significa "reconocimiento de sincronización". 3.El paquete [ACK] es la máquina del visitante que reconoce el permiso para conectarse. Este es el último paso necesario para realizar una conexión TCP exitosa. ACK significa "reconocer".

Explique qué sucede cuando un actor malintencionado envía una gran cantidad de paquetes SYN a la vez: enviar peticiones constantes al servidor no es algo raro. Pero un mismo equipo sin esperar respuesta constantemente genera que el servidor tenga que responder a todas las peticiones, hasta que por limitaciones físicas el servidor queda sobrepasado y ya no puede dar respuesta.

Explique qué indican los registros y cómo afecta eso al servidor: un servidor tiene recursos finitos, por ello puede manejar hasta un cierto número de peticiones con lo que hasta ese punto los servicios funcionarán con normalidad. Pasado este punto, las peticiones que sobrepasen este momento quedarán en espera de respuesta hasta que por las limitaciones de tiempo (Time out que se establecen los servicios para no hacer esperas eternas) dan aviso de que no pueden acceder al servicio y con ello su objetivo de que la web o servicio se ve obstruido paralizando su funcionamiento.