**Informe de incidente de ciberseguridad.**

**Tiempo de espera en la red.**

El error de tiempo de espera de conexión del sitio web podría deberse a que el servidor web se vio abrumado por una gran cantidad de paquetes SYN de un atacante. Como resultado, el servidor no pudo procesar solicitudes legítimas de manera oportuna, lo que provocó errores de tiempo de espera para los visitantes del sitio web.

**Los registros muestran que:**

* Ataque de inundación SYN: los registros revelan un gran volumen de paquetes SYN desde una única dirección IP (203.0.113.0) al puerto 443 del servidor. El servidor responde inicialmente a estos paquetes SYN, pero el atacante continúa enviando más solicitudes SYN a un ritmo rápido. paso. Este tráfico excesivo abruma la capacidad del servidor para gestionar las conexiones.
* Impacto en el tráfico legítimo: los registros también muestran que durante el ataque, los intentos de conexión de los visitantes legítimos se interrumpen o agotan el tiempo de espera. Esto es evidente a partir de las entradas de registro resaltadas en amarillo que indican errores de tiempo de espera de puerta de enlace HTTP 504 y paquetes [RST, ACK], que sugieren que el servidor no pudo completar la conexión con usuarios legítimos.

**Este evento podría ser:**

Ataque de denegación de servicio (DoS): específicamente, este es un tipo de ataque DoS conocido como ataque de inundación SYN. El atacante inunda el servidor con una gran cantidad de paquetes SYN, lo que inmoviliza los recursos del servidor y le impide manejar solicitudes de conexión legítimas. Como resultado, los usuarios experimentan tiempos de espera de conexión y errores porque el servidor no puede procesar sus solicitudes debido a que está abrumado por el tráfico malicioso

**Que está ocurriendo:**

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. Los tres pasos son:

1. Solicitud SYN (Sincronizar)
   * El visitante (cliente) envía un paquete con el indicador SYN (Sincronizar) al servidor web. Este paquete inicial solicita establecer una conexión y sincroniza números de secuencia entre el cliente y el servidor.
2. Respuesta SYN-ACK (Sincronización-Reconocimiento)
   * El servidor web responde al cliente con un paquete que tiene configurados los indicadores SYN y ACK (Reconocimiento). Esto indica que el servidor acepta establecer la conexión y también sincroniza su propio número de secuencia con el cliente.
3. Confirmación ACK (Reconocimiento)
   * El cliente responde con un paquete ACK, confirmando que ha recibido la respuesta SYN-ACK del servidor. Esto completa el protocolo de enlace de tres vías y establece una conexión TCP completa entre el cliente y el servidor.

### Cuando un actor malintencionado envía una gran cantidad de paquetes SYN al servidor, se produce un ataque de inundación SYN. En este ataque, el servidor web recibe muchas solicitudes SYN simultáneamente y reserva recursos para cada una de estas solicitudes. Sin embargo, si el número de solicitudes SYN excede la capacidad del servidor para manejar conexiones, el servidor se satura. Esto impide que el servidor procese solicitudes legítimas y puede provocar una falla en el manejo de nuevas conexiones, lo que genera errores de tiempo de espera para los usuarios legítimos.

**Información de los registros:**

Los registros indican que el servidor web está siendo objetivo de un ataque de inundación SYN, como lo demuestra una gran cantidad de paquetes SYN provenientes de una dirección IP maliciosa. A medida que el servidor intenta manejar estas solicitudes SYN, no puede procesar solicitudes legítimas de los visitantes del sitio web debido a la sobrecarga. Esto genera mensajes de error, como HTTP 504 Gateway Timeout, porque el servidor no puede responder a las solicitudes de manera oportuna. Con el tiempo, el servidor puede dejar de responder por completo a solicitudes legítimas, lo que resulta en una denegación de servicio para usuarios reales