Reporte Incidente: SYN Flood Attack 2024-05-13 #2

Globe Sistemas - Av. Libertador Jardin America

| **Parte 1: Identifique el tipo de ataque que pudo haber causado esto interrupción de la red** |
| --- |
| Una posible explicación para la caída del sitio web tiempo de espera de conexión error El mensaje es un ataque DoS. Los registros muestran que el servidor web deja de responder después de sobrecargarse con solicitudes de paquetes SYN. Este evento podría ser un tipo de ataque DoS llamado inundación SYN. |

| **Parte 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. El apretón de manos consta de tres pasos:   1. Se envía un paquete SYN desde el origen al destino, solicitando conectarse. 2. El destino responde al origen con un paquete SYN-ACK para aceptar la solicitud de conexión. El destino reservará recursos para que la fuente se conecte. 3. Se envía un paquete ACK final desde el origen al destino reconociendo el permiso para conectarse.   En el caso de un ataque de inundación SYN, un actor malintencionado enviará una gran cantidad de paquetes SYN a la vez, lo que abruma los recursos disponibles del servidor para reservar 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 visto abrumado y no puede procesar las solicitudes SYN de los visitantes. El servidor no puede abrir una nueva conexión para nuevos visitantes que reciben una ctiempo de espera de conexión mensaje. |