**Informe de incidentes de ciberseguridad**

|  |
| --- |
| 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: es que el servidor está recibiendo un volumen anómalo de solicitudes, lo que genera saturación de recursos y provoca la interrupción de la red.  Los registros muestran que: además del tráfico legítimo proveniente del rango corporativo 198.51.100.0/24, se identificó una dirección IP externa (203.0.113.0) que envía un número excesivo de solicitudes en milésimas de segundo. Este comportamiento es consistente con un ataque de Denegación de Servicio (DoS), cuyo objetivo es sobrecargar al servidor hasta que no pueda responder a usuarios legítimos.  Este evento podría ser: Se identifica un ataque de Denegación de Servicio (DoS) directo, probablemente de tipo SYN flood, que satura la cola de conexiones y agota recursos del servidor, interrumpiendo el flujo de trabajo y degradando la disponibilidad de los servicios.  El evento analizado corresponde a un ataque DoS directo, que interrumpe el flujo normal de trabajo del servidor, degrada su rendimiento y compromete la disponibilidad de los servicios críticos de la empresa. |
|  |

|  |
| --- |
| Sección 2: Explique cómo el ataque está provocando el mal funcionamiento del sitio web |
| Cuando los visitantes de un sitio web intentan establecer una conexión con el servidor web, se produce un protocolo de enlace de tres vías mediante el protocolo TCP. Explique los tres pasos del protocolo de enlace:     1. SYN (Synchronize): El cliente envía un paquete SYN al servidor solicitando iniciar una conexión. 2. SYN-ACK (Synchronize-Acknowledge): El servidor responde con un SYN-ACK, confirmando la recepción de la solicitud y ofreciendo establecer la sesión. 3. ACK (Acknowledge): El cliente responde con un paquete ACK, cerrando el ciclo y estableciendo así una conexión TCP válida.   Explique qué sucede cuando un actor malicioso envía una gran cantidad de paquetes SYN a la vez: En un ataque DoS de tipo SYN flood, un actor malicioso envía de manera masiva paquetes SYN sin completar el proceso de handshake. Esto genera que:   * El servidor reserve recursos para conexiones que nunca se finalizan. * La tabla de sesiones activas (backlog) se sature rápidamente. * Los usuarios legítimos experimenten tiempos de espera, lentitud o inaccesibilidad total al sitio web.   Explique qué indican los registros y cómo afecta eso al servidor: Los registros analizados indican que la IP 203.0.113.0 está ejecutando este tipo de actividad, enviando múltiples paquetes SYN en intervalos extremadamente cortos. Esto provoca que el servidor entre en un estado de sobrecarga de recursos, afectando directamente la disponibilidad del servicio y deteniendo la continuidad operativa de la empresa. |