# Informe sobre incidentes de ciberseguridad

|  |
| --- |
| **Sección 1: Identifica el tipo de ataque que puede haber causado esta**  **interrupción de la red** |
| Tras el análisis de los registros capturados en Wireshark, se observó un gran número de solicitudes TCP SYN procedentes de una dirección IP desconocida hacia el servidor web de la empresa (192.0.2.1).  Este comportamiento corresponde a un ataque de denegación de servicio (DoS) tipo SYN Flood, donde el atacante envía múltiples solicitudes SYN sin completar el proceso de establecimiento de conexión TCP (three-way handshake).  **Evidencia del log:**  - Repetidas solicitudes SYN desde la misma dirección IP hacia el puerto del servidor web. - El servidor no logra completar las conexiones, quedando con recursos ocupados. - Como resultado, los empleados y clientes reciben errores de tiempo de espera de conexión.  **Diferencia entre DoS y DDoS:**  - Este caso es un ataque DoS, ya que proviene de una única dirección IP atacante. - En un DDoS, el ataque proviene de múltiples direcciones distribuidas, lo que lo hace más difícil de bloquear. |
|

|  |
| --- |
| **Sección 2: Explica cómo el ataque está provocando que el sitio web no funcione como debería** |
| **Descripción del ataque:**  El atacante envió un volumen masivo de solicitudes SYN al servidor web sin finalizar las conexiones. Esto saturó la tabla de conexiones del servidor y lo dejó incapaz de atender solicitudes legítimas.  **Impacto en la red:**  - El sitio web de la empresa dejó de responder a los usuarios. - Los navegadores mostraron errores de tiempo de espera de conexión (timeout). - Los empleados no pudieron acceder a la página de ventas para atender a los clientes.  **Consecuencias para la organización:**  - Interrupción del servicio en línea de la empresa. - Pérdida temporal de productividad de los empleados. - Impacto negativo en la confianza de los clientes y en la reputación de la empresa.  **Posibles medidas de protección:**  1. Configurar el firewall para detectar y mitigar ataques SYN Flood (técnicas de rate limiting o SYN cookies). 2. Implementar un sistema de balanceo de carga para distribuir el tráfico. 3. Utilizar soluciones de protección anti-DDoS en la nube. 4. Monitorear el tráfico en tiempo real para detectar patrones anómalos rápidamente |