# Reporte de Incidente de Ciberseguridad

## Escenario



Revise el siguiente escenario. A continuación, complete las instrucciones paso a paso.

Usted trabaja como analista de seguridad para una agencia de viajes que anuncia ventas y promociones en el sitio web de la empresa. Los empleados de la empresa acceden regularmente a la página web de ventas de la empresa para buscar paquetes vacacionales que puedan gustar a sus clientes.

Una tarde, recibe una alerta automática de su sistema de supervisión que le indica un problema con el servidor web. Intenta visitar la página web de la empresa, pero recibe un mensaje de error de tiempo de espera de conexión en su navegador.

Utiliza un rastreador de paquetes para capturar los paquetes de datos en tránsito hacia y desde el servidor web. Observa un gran número de solicitudes TCP SYN procedentes de una dirección IP desconocida. El servidor web parece estar desbordado por el volumen de tráfico entrante y está perdiendo su capacidad para responder al número anormalmente elevado de peticiones SYN. Usted sospecha que el servidor está siendo atacado por un actor malicioso.

Usted desconecta temporalmente el servidor para que la máquina pueda recuperarse y volver a un estado operativo normal. También configura el cortafuegos de la empresa para que bloquee la dirección IP que estaba enviando el número anormal de peticiones SYN. Sabe que su solución de bloqueo de IP no durará mucho, ya que un atacante puede suplantar otras direcciones IP para burlar este bloqueo. Tiene que alertar rápidamente a su jefe sobre este problema y discutir los pasos a seguir para detener a este atacante y evitar que este problema se repita. Tendrá que estar preparado para contarle a su jefe el tipo de ataque que ha descubierto y cómo estaba afectando al servidor web y a los empleados.

|  |
| --- |
| **Seccion 1: Identificar el tipo de ataque que puede haber causado esta interrupción en la red** |
| Una posible explicación para el mensaje de error de tiempo de espera de conexión del sitio web es un ataque de Denegación de Servicio Distribuido (DDoS).  Los registros muestran un volumen significativo de paquetes SYN entrantes desde múltiples direcciones IP en un corto período, lo que sobrecarga los recursos del servidor y dificulta su capacidad de responder a solicitudes legítimas.  Este evento podría ser un ataque diseñado para interrumpir el servicio del sitio web saturando el servidor con tráfico falso, impidiendo que los usuarios legítimos accedan a la página. |
|

|  |
| --- |
| **Section 2: Explicar cómo el ataque está causando el mal funcionamiento del sitio web** |
| Cuando los visitantes del sitio intentan establecer una conexión con el servidor web, ocurre un protocolo de enlace de tres pasos (three-way handshake) utilizando TCP:  El cliente envía un paquete SYN al servidor para iniciar la comunicación.  El servidor responde con un paquete SYN-ACK indicando que está listo para establecer la conexión.  El cliente completa el proceso enviando un paquete ACK.  Sin embargo, cuando un atacante envía un gran número de paquetes SYN de manera simultánea sin completar el handshake, el servidor queda esperando el tercer paso, lo que consume recursos del sistema.  Impacto según los registros:  Los registros muestran patrones de tráfico anómalos con un incremento significativo de paquetes SYN no completados. Esto hace que el servidor alcance su capacidad máxima de conexiones simultáneas, generando retrasos y errores de tiempo de espera para los usuarios legítimos.  Consecuencias:   * Disminución en la funcionalidad del sitio web. * Pérdida de confianza de los usuarios. * Impacto financiero debido a la interrupción del servicio.   Medidas para prevenir ataques futuros:  Implementar un firewall de aplicaciones web (WAF).  Configurar un sistema de detección y prevención de intrusiones (IDS/IPS).  Limitar las conexiones TCP simultáneas por dirección IP. |