**Análisis del informe del incidente**

**Instrucciones**

A medida que avances en el curso, puedes usar esta plantilla para registrar tus conclusiones tras completar una actividad o para tomar notas sobre lo que aprendiste acerca de una herramienta o concepto específico. También puedes usar esta tabla como una forma de practicar la aplicación del marco CSF del NIST a diferentes situaciones que te encuentres.

|  |  |
| --- | --- |
| **Resumen** |  |
| Identificar | * **Tipo de ataque:** DDoS (basado en ICMP flood). * **Sistemas afectados:** red interna, servicios de red críticos (acceso a internet, servidores de aplicaciones, recursos internos de diseño y marketing). * **Causa raíz:** firewall sin reglas adecuadas para limitar o filtrar tráfico ICMP. * **Impacto:** interrupción de servicios durante dos horas, afectación en la productividad y reputación de la empresa. |
| Proteger | ** Configuración de nuevas reglas de firewall para limitar la tasa de paquetes ICMP entrantes.**  ** Verificación de IP de origen en el firewall para bloquear direcciones falsas o suplantadas.**  ** Implementación de capacitación al personal técnico sobre configuración de seguridad en firewalls y monitoreo de red.**  ** Aplicación de políticas de hardening en dispositivos de red y segmentación del tráfico crítico.** |
| Detectar | * Instalación de **software de monitoreo de red** para detectar patrones de tráfico anómalos. * Configuración de un **IDS/IPS** (Sistema de Detección/Prevención de Intrusiones) que identifique tráfico ICMP sospechoso. * Habilitar **alertas tempranas** a través de un SIEM para notificar anomalías de tráfico en tiempo real. |
| Responder | * **Acciones inmediatas:** bloqueo de tráfico ICMP en firewall, desconexión temporal de servicios no críticos, restablecimiento de servicios críticos. * Comunicación al equipo directivo sobre la causa y resolución del incidente. * Documentación del evento en el registro de incidentes de seguridad. * Plan de contingencia: disponer de procedimientos estandarizados para aislamiento de tráfico malicioso en caso de ataques futuros. |
| Recuperar |  Restablecimiento completo de los servicios afectados tras detener el ataque.   Verificación de integridad en los sistemas internos para asegurar que no se comprometieron datos.   Plan de recuperación actualizado:   * Mantener respaldos y redundancia de servicios críticos. * Establecer pruebas periódicas de resiliencia frente a ataques DDoS.    Comunicación interna: informar a los empleados sobre las medidas implementadas y reforzar la cultura de seguridad. |

|  |
| --- |
| Reflexiones/Notas:   * El incidente puso en evidencia la importancia de una correcta configuración inicial del firewall. * El uso de herramientas de detección temprana habría reducido la duración del ataque. * Es necesario mantener auditorías periódicas y simulacros de incidentes DDoS para fortalecer la resiliencia organizacional. |