**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** | La red de la empresa multimedia sufrió una caída debido a una avalancha de paquetes ICMP entrantes, lo que provocó la interrupción de servicios no críticos durante al menos 2 horas. Los servicios críticos se mantuvieron operativos mientras se resolvía el problema de red.  El equipo de ciberseguridad identificó un firewall no configurado adecuadamente, que permitió a un actor malicioso realizar un ataque DDoS. El tráfico normal de datos se vio afectado debido a la inundación de múltiples paquetes ICMP. **Medidas tomadas**: - Implementación de una nueva regla de firewall para limitar los paquetes ICMP entrantes.  - Monitoreo de la red para detectar patrones de tráfico anómalos.  - Implementación de un sistema IDS/IPS. |
| Identificar | **Auditoría de Equipos y Conexiones:**  - Se auditó el hardware de red (router, switch, módem) y la configuración de la conexión a la red.  - Se revisaron los protocolos de firewall y los involucrados en el ataque.  **Descubrimiento del Problema:** - Un firewall no configurado permitió el ataque DDoS, afectando algunos servicios y manteniendo solo los necesarios para el funcionamiento web. |
| Proteger | **Protección de Servidores:**  - Apagado de algunos servicios durante aproximadamente 2 horas.  - Configuración de un firewall para limitar la tasa de paquetes ICMP entrantes.  - Implementación de un software de monitoreo para controlar el tráfico de datos sospechosos.  - Agregado de un sistema IDS/IPS para filtrar el tráfico ICMP basado en características sospechosas. |
| Detectar | 1.Herramientas SIEM:   * Utilizadas para recopilar datos de eventos y registros de dispositivos conectados a la red.   2. Monitoreo de Red en Tiempo Real:   * Observación del tráfico de red en tiempo real mediante software de monitoreo.   3. IDS/IPS y Firewall:   * Utilizados para detectar y filtrar el tráfico malicioso |
| Responder | **Monitoreo de Red:**   * Configurado para establecer un comportamiento base del tráfico de red normal.   **Herramientas SIEM:**   * Recopilación de datos de registros o eventos anteriores.   **Ajuste de Monitoreo**:   * Monitoreo de red ajustado para notificar a la herramienta SIEM ante una subida anómala del tráfico de datos.   **Respuesta Automática:**   * La herramienta SIEM puede instruir a un firewall o IPS para mitigar la dirección IP sospechosa. |
| Recuperar | **Verificación de Sistemas y Datos:**   * Asegurarse de que los sistemas y datos no hayan sido afectados.   **Reactivación de Servicios:**   * Reactivar los servicios no críticos necesarios para el funcionamiento web.   **Comunicación con Clientes**:   * Informar a los clientes sobre la restauración del servicio y el funcionamiento normal de la web. |

|  |
| --- |
| Reflexiones/Notas: Las medidas tomadas durante el ataque DDoS permitieron identificar y mitigar la amenaza, restaurar los servicios críticos y proteger la red contra futuros incidentes. La implementación de nuevas reglas de firewall, sistemas IDS/IPS y herramientas SIEM han fortalecido la postura de seguridad de la organización.  Acciones Preventivas: - Realización de auditorías regulares de la configuración de seguridad.  - Monitoreo continuo y ajuste de las políticas de seguridad.  - Capacitación continua del personal en prácticas de ciberseguridad. |