**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** | El equipo de ciberseguridad de la organización descubrió un ataque DDoS de inundación ICMP. |
| Identificar | Un agente o unos agentes de amenaza atacaron la empresa con un ataque de inundación ICMP, el cual llegó a afectar a la totalidad de la red interna. Los recursos más críticos de la red necesitaban asegurarse y restaurarse a un estado funcional. |
| Proteger | Para mitigar el ataque se implementó una regla en el Firewall para limitar el número de paquetes ICMP entrantes. Esto, sumado a un sistema IDS/IPS con el objetivo de filtrar el tráfico sospechoso. |
| Detectar | Para detectar el ataque, se configuró la verificación de direcciones IP de origen para identificar IP falsas en los paquetes ICMP entrantes. Posteriormente se implementó un software de monitoreo de red con el objetivo de detectar tráfico sospechoso. |
| Responder | Los pasos a seguir en un futuro consistirán en aislar los sistemas afectados, para posteriormente restaurar los sistemas y servicios críticos. Se analizarán los logs del registro de la red para investigar actividad potencialmente sospechosa. Finalmente se informarán todos los incidentes a los entes competentes. |
| Recuperar | Para recuperarse de un ataque DDoS de este tipo, el primer paso es restaurar la red a un estado normal y seguro. A raíz de las estrategias que serán adoptadas de ahora en adelante, el Firewall permitirá bloquear gran parte del tráfico potencialmente sospechoso |

|  |
| --- |
| Reflexiones/Notas: |