**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 sufrio una caida debido a una avalancha de paquetes ICMP entrantes, provocando que se detuvieran por almenos 2 horas los servicios no criticos y los servicios criticos mantenerlos mientras se solucionaba el problema de red.  El equipo de ciberseguridad dio con el fallo, un firewall no configurado por el cual un actor malicioso realizo un ataque de denegacion de servicios DDoS provocando que el trafico de datos normal se viera afectado y llenando de multiples paquetes ICMP. Se tomo las medidas adecuadas, una nueva regla firewall para limitar los paquetes ICMP entrantes, se monitoreo la red para detectar patrones de trafico anomalos y se implemento un sistema ISD/IPS. |
| Identificar | Se audito los equipos de red(router, switch, modem), la conexion a la red y los protocolos de firewall y los protocolos involucrados en el ataque para identificar si existen brechas de seguridad que los actores maliciosos puedan aprovechar para infiltrarse. El equipo descubrio un firewall no configurado por el cual el actor malicioso pudo hacer un ataque de denegacion de servicio distribuido(DDoS), el cual hizo que algunos servicios se apagaran y solo esten activos los necesarios para el funcionamiento de la web. |
| Proteger | Se logro proteger los servidores luego de apagar algunos servicio durante 2 horas aproximandamente, se configuro un firewall que limita la tasa de paquetes ICMP entrantes, se implemento un software de monitoreo para controlar trafico de datos que sean sospechosos, se agrego un sistema IDS/IPS para filtrar parte del tráfico ICMP basándose en características sospechosas. Implementando estas medidas se lograria una actuacion inmediata para mitigar futuras amenazas similares. |
| Detectar | Hacer uso de herramientas SIEM para recopilar datos de eventos y registros de dispositivos que esten conectados a la red. Mediante un software de monitoreo de red se observa el trafico de red en tiempo real. Uso de IDS/IPS y firewall. |
| Responder | El monitoreo de red ayuda a observar el trafico de datos y se configura para establecer un comportamiento base del tráfico de red normal. La herramienta SIEM recopila datos de registros o eventos anteriores Ajustar el monitoreo de red para notificar a la herramienta SIEM que cuando exista una extraña subida en el trafico de datos la herramienta SIEM pueda recopilar registro para detectar el problema y generar una alerta, se podria configurar la herramienta SIEM para que instruya a un firewall o IPS y mitigar la direccion IP sospechosa. |
| Recuperar | Una vez que incidente este bajo control es importante asegurarse que los sistemas y otros datos no hayan sido afectados, reactivar los servicios que se consideraron no criticos para el funcionamiento de la web, comunicacion con clientes e informar sobre el funcionamiento normal que vuelve a tener 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. |