**Incident report analysis**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

|  |  |
| --- | --- |
| **Summary** | Un ataque de Denegación de Servicio Distribuido (DDoS) afectó a la red interna de la empresa durante dos horas. El ataque consistió en una avalancha de paquetes ICMP entrantes que saturaron la red, impidiendo el acceso a los recursos internos. El equipo de gestión de incidentes respondió bloqueando los paquetes ICMP, deteniendo servicios no críticos y restableciendo los servicios críticos. Tras la investigación, se descubrió que el ataque se originó debido a una configuración incorrecta del cortafuegos, lo que permitió al atacante enviar una gran cantidad de pings ICMP y sobrecargar la red. |
| Identify | Objetivo: Identificar los riesgos de seguridad y las brechas en la red.  Acciones Tomadas:  - Auditoría de la red interna, sistemas y dispositivos para identificar la vulnerabilidad en el cortafuegos.  - Identificación de los servicios críticos y no críticos afectados durante el ataque.  - Análisis del tráfico de red para determinar el origen del ataque (paquetes ICMP entrantes).  Brechas Identificadas:  - Configuración incorrecta del cortafuegos que permitió el tráfico ICMP excesivo.  - Falta de monitoreo continuo del tráfico de red para detectar patrones anormales. |
| Protect | Objetivo: Implementar medidas para proteger los activos de la red.  Acciones Tomadas:  - Implementación de una nueva regla en el cortafuegos para limitar la tasa de paquetes ICMP entrantes.  - Verificación de direcciones IP de origen para detectar IPs falsificadas.  - Instalación de un sistema de detección y prevención de intrusiones (IDS/IPS) para filtrar tráfico ICMP sospechoso.  Medidas de Protección Futuras:  - Actualización de las políticas de seguridad del cortafuegos para bloquear tráfico no autorizado.  - Implementación de autenticación multifactor (MFA) para accesos críticos.  - Capacitación del personal en prácticas de seguridad para prevenir ataques de phishing y otros vectores de ataque. |
| Detect | Objetivo: Mejorar la capacidad de detectar amenazas y actividades sospechosas en la red.  Acciones Tomadas:  - Implementación de software de monitoreo de red para detectar patrones de tráfico anormales.  - Configuración de alertas en tiempo real para tráfico ICMP excesivo o sospechoso.  Mejoras Futuras:  - Integración de un Sistema de Gestión de Eventos e Información de Seguridad (SIEM) para centralizar el monitoreo y análisis de logs.  - Realización de pruebas periódicas de penetración para identificar nuevas vulnerabilidades. |
| Respond | Objetivo: Contener, neutralizar y analizar el incidente para mejorar los procedimientos de respuesta.  Acciones Tomadas:  - Bloqueo inmediato de los paquetes ICMP entrantes para contener el ataque.  - Desconexión de servicios no críticos para reducir la carga en la red.  - Restablecimiento de servicios críticos para minimizar el impacto en las operaciones.  Mejoras en la Respuesta:  - Desarrollo de un plan de respuesta a incidentes detallado que incluya pasos claros para contener y neutralizar futuros ataques.  - Comunicación efectiva con las partes interesadas (empleados, clientes y gerencia) durante y después del incidente. |
| Recover | Objetivo: Restaurar los sistemas afectados y mejorar los procesos de recuperación.  Acciones Tomadas:  - Restauración de los servicios de red críticos utilizando copias de seguridad recientes.  - Verificación de la integridad de los datos y sistemas después del ataque.  Mejoras en la Recuperación:  - Implementación de un plan de recuperación ante desastres que incluya copias de seguridad automatizadas y pruebas regulares de restauración.  - Capacitación del personal en procedimientos de recuperación para garantizar una respuesta rápida y efectiva en futuros incidentes. |

|  |
| --- |
| Reflections/Notes: Identificar: La auditoría de la red reveló que la configuración incorrecta del cortafuegos fue la principal brecha de seguridad. Es fundamental realizar revisiones periódicas de la configuración de los dispositivos de red para evitar vulnerabilidades similares.  Proteger: La implementación de nuevas reglas en el cortafuegos y la instalación de un IDS/IPS son medidas efectivas para prevenir futuros ataques DDoS. Sin embargo, es necesario fortalecer las políticas de seguridad y capacitar al personal para evitar errores humanos.  Detectar: El monitoreo continuo del tráfico de red es esencial para detectar patrones anormales. La integración de un SIEM mejorará la capacidad de la organización para identificar y responder a amenazas en tiempo real.  Responder: La respuesta rápida del equipo de gestión de incidentes fue clave para contener el ataque. Sin embargo, es necesario desarrollar un plan de respuesta más detallado y realizar simulacros regulares para mejorar la preparación.  Recuperar: La restauración de los servicios críticos fue exitosa, pero se debe implementar un plan de recuperación más robusto que incluya copias de seguridad automatizadas y pruebas regulares de restauración. |

**Conclusión**

El incidente de DDoS resalta la importancia de aplicar el Marco de Ciberseguridad del NIST (NIST CSF) para gestionar los riesgos de seguridad de manera proactiva. Las cinco funciones principales (Identificar, Proteger, Detectar, Responder y Recuperar) permitieron a la organización contener el ataque, mitigar el impacto y mejorar sus defensas contra futuras amenazas. La implementación de medidas como la actualización del cortafuegos, la instalación de un IDS/IPS y la capacitación del personal son pasos esenciales para fortalecer la seguridad de la red.