Análisis de reporte de incidente

Resumen	Se informó que la organización experimentó un ataque DDoS basado en paquetes ICMP entrantes que provocó la interrupción de servicios durante aproximadamente 2 horas, hasta que el incidente fue mitigado. Se determinó que la causa raíz fue la ausencia de controles adecuados en el firewall para filtrar tráfico ICMP, lo que expuso a la organización a un ataque de denegación de servicio. El ataque ocasionó la interrupción total de los servicios durante 2 horas, afectando a los usuarios y generando posibles pérdidas económicas y de productividad para la organización. El equipo de gestión de incidentes implementó un bloqueo del tráfico ICMP entrante, lo que permitió detener el ataque y restablecer la operatividad de los servicios críticos de red.
Identify	Los activos afectados fueron los servicios de red que la organización brinda a sus usuarios, lo que interrumpió transacciones y operaciones en curso. La vulnerabilidad explotada fue una configuración deficiente del firewall, que permitió el ingreso masivo de tráfico ICMP. El impacto se extendió a toda la red corporativa durante aproximadamente 2 horas
Protect	Para fortalecer la seguridad se recomienda implementar una configuración de firewall reforzada, estableciendo reglas claras para filtrar y limitar el tráfico ICMP. Asimismo, aplicar mecanismos de limitación de tasa (rate limiting) que restrinjan la cantidad de paquetes ICMP por segundo para mitigar intentos de denegación de servicio. Finalmente, instaurar políticas de gestión de cambios y revisiones periódicas de configuración que permitan detectar y corregir oportunamente posibles debilidades en la infraestructura de red.
Detect	Se recomienda implementar un sistema de monitoreo de tráfico de red con alertas tempranas, como una herramienta SIEM, que permitan identificar anomalías en tiempo real. Además, la incorporación de soluciones IDS/IPS facilitaría la detección y, en algunos casos, la prevención de patrones de ataque como el DDoS basado en ICMP.
Respond	La respuesta ante un incidente de este tipo debe iniciar con una comunicación inmediata a las partes relevantes, garantizando que la gerencia y los equipos técnicos estén al tanto de la situación. En paralelo, se deben aplicar medidas de contención como el bloqueo del tráfico ICMP en el firewall para detener el ataque. Asimismo, resulta fundamental actualizar los planes de respuesta a incidentes y ajustar las configuraciones de seguridad con el fin de prevenir que el escenario vuelva a repetirse.
Recover	Una vez contenido el ataque, se procedió a restaurar la operatividad de los servicios críticos, asegurando que los usuarios pudieran retomar sus actividades normales. Como parte del proceso de mejora continua, se documentaron las lecciones aprendidas del incidente con el objetivo de fortalecer la estrategia de seguridad y optimizar la capacidad de respuesta ante futuros eventos similares.

Reflection/Notes:	Este ejercicio me permitió aplicar el marco NIST CSF en un caso práctico de DDoS. Aprendí a estructurar un informe de incidente paso a paso, identificando causas raíz, medidas de mitigación y oportunidades de mejora. Considero que este enfoque es replicable en incidentes reales para fortalecer la seguridad organizacional.