Incident report analysis

Summary	Recientemente la empresa sufrió un ataque a sus redes internas, lo que produjo que los servicios de redes dejarán de funcionar repentinamente durante dos horas. Los registros indican que se han estado recibiendo una avalancha de paquetes ICMP de diferentes direcciones IP, por lo que el equipo deduce que se trata de un ataque DDoS.
Identify	El equipo audita los sistemas de la empresa, específicamente las redes de esta misma realizando una investigación, descubriendo que un actor malicioso había enviado una avalancha de paquetes ICMP a través de un firewall no configurado, esta vulnerabilidad produjo que la red se saturara mediante un ataque de denegación de servicios distribuido (DDoS).
Protect	El equipo de seguridad de red implementará una nueva regla de firewall para limitar la tasa de paquetes ICMP entrantes, la verificación de la dirección IP de origen en el cortafuegos para comprobar si hay direcciones IP falsificadas en los paquetes ICMP entrantes. Por último, un sistema IPS para filtrar parte del tráfico de paquetes ICMP basado en características sospechosas.
Detect	Para detectar futuros ataques, se implementó un software de monitoreo de red para detectar patrones de tráfico anormales, y por último, un sistema IDS para alertar sobre tráfico de paquetes ICMP inusuales.
Respond	El equipo de gestión de incidentes responderá bloqueando los paquetes ICMP entrantes, deteniendo todos los servicios de red no críticos fuera de línea y restableciendo los servicios de red críticos. Finalmente informarán a las altas direcciones y/o autoridades correspondientes.
Recover	• Bloqueo de paquetes ICMP y las direcciones IP del actor malicioso

	mediante Firewall. ● Bloquear todos los servicios no críticos para reducir el tráfico interno de la red. ● Restablecerá los servicios críticos para su funcionamiento normal dentro de la empresa. ● El equipo activará los servicios de red no críticos detenidos.

Reflections/Notes: