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	Ayer varios trabajadores experimentaron problemas a la hora de realizar sus tareas. Durante el ataque se produjo una paralización durante dos horas de los servidores de red. El ataque fue clasificado en un primer momento como DDos.
Identificar	El equipo de Ciberseguridad de la empresa haciendo las comprobaciones necesarias descubrieron que un hacker había envidado una avalancha de pings ICMP a la red de la empresa a través del firewell que estaba sin configurar. El ataque provocó la saturación de la red de la empresa mediante un ataque de denegación de servicio distribuido (DDoS) Acciones de Identificación • Análisis de tráfico de red: Se identificaron patrones anómalos de paquetes ICMP. • Revisión de configuración del firewall: Se descubrió la falta de configuración que permitió el ataque.
Proteger	Las medidas que se han adoptado para solventar este problema de seguridad han sido las siguientes: Nueva regla de firewall para limitar la tasa de paquetes ICMP entrantes. Verificación de la dirección IP de origen en el firewall para comprobar si hay direcciones IP falsas en los paquetes ICMP entrantes. Un software de monitoreo de red para detectar patrones de tráfico anómalos. Un sistema IDS/IPS para filtrar parte del tráfico ICMP basándose en características sospechosas.

Detectar	• Para detectar ataques futuros el equipo de seguridad utilizará herramienta de: registro por firewall • Un sistema de detección de intrusos (IDS) para monitorear todo el tráfico entrante de Internet.
Responder	El equipo de seguridad restableció el tráfico de red normal. Siguiendo los protocolos de seguridad hemos: • Bloqueado los paquetes ICMP entrantes. • Desactivar los servicios no críticos • Restablecer los servicios críticos. • Comunicado el incidente a la dirección del centro.
Recuperar	El equipo de seguridad estableció el siguiente plan de recuperación: • Recuperará el tráfico normal de la red. • Establecer que cualquier incidencia que se vuelva a producir se comunique lo antes posible. • Cerciorarse que las tareas que iban realizando nuestros usuarios se puedan realizar de forma correcta y de haber alguna perdida de información solucionarlo mediante una copia de seguridad. En el caso de no existir esta copia volvimos a recordar a los empleados la importancia de las copias de seguridad.

Reflexiones/Notas:

Hemos establecido unas serie de recomendaciones:

- Revisión periódica de configuración de seguridad.
- Capacitación continua del personal en ciberseguridad.
- Realización de simulacros de respuesta a incidentes para mejorar la preparación del equipo de seguridad.