Diario del gestor de incidentes

Instrucciones

A medida que avanza en este curso, puede usar esta plantilla para registrar sus hallazgos después de completar una actividad o para tomar notas sobre lo que ha aprendido sobre una herramienta o concepto específico. También puede utilizar este diario como una forma de registrar las conclusiones clave sobre las diferentes herramientas o conceptos de ciberseguridad que encuentre en este curso.

Fecha	**23 de julio de 2024**
Entrada	#1
Descripción	Documentación de un incidente de ciberseguridad
Etapas del Incidente	**1. Detección y Análisis:** La organización detectó el ransomware y contactó a otra entidades para apoyo técnico. **2. Contención, Erradicación y Recuperación:** La empresa apagó sus sistemas par contener el incidente y solicitó ayuda externa para su erradicación y recuperació
Herramienta(s) Utilizada(s)	Ninguna
Las 5 W	**Quién:** Grupo de hackers **Qué:** Incidente de ransomware **Dónde:** Empresa de atención médica **Cuándo:** Martes, 9:00 a.m. **Por qué:** Ataque de phishing que permitió el acceso y lanzamiento del ransomware. Los atacantes buscaban un beneficio financiero.
Notas Adicionales	1. ¿Cómo prevenir futuros incidentes similares? 2. ¿Debería la empresa pagar el rescate?

Fecha	**25 de julio de 2024**
Entrada	#2
Descripción	Análisis de un archivo de captura de paquetes
Herramienta(s) Utilizada	Wireshark
Descripción de la Herramienta	Wireshark es un analizador de protocolos que permite capturar y examinar tráfico de red, útil para detectar actividades maliciosas.
Las 5 W	N/A
Notas Adicionales	Primera experiencia con Wireshark; a pesar de su interfaz compleja, pude ver su utilidad en el análisis de tráfico.

Fecha	**25 de julio de 2024**
Entrada	#3
Descripción	Capturando mi primer paquete
Herramienta(s) Utilizada(s)	tcpdump
Descripción de la Herramienta	tcpdump es un analizador de protocolos de línea de comandos que permite capturar y analizar tráfico de red.
Las 5 W	N/A
Notas Adicionales	Usar tcpdump fue desafiante debido a la línea de comandos, pero después de algunos intentos logré capturar el tráfico correctamente.

Fecha	**27 de julio de 2024**
Entrada	#4
Descripción	Investigación de un hash de archivo sospechoso
Herramienta(s) Utilizada(	VirusTotal
Descripción de la Herramienta	VirusTotal permite verificar si archivos o URLs son reportados como maliciosos.
Etapas del Incidente	El archivo sospechoso fue detectado por el sistema de seguridad, y un anális adicional confirmó su peligrosidad.
Las 5 W	**Quién:** Actor malicioso desconocido **Qué:** Archivo adjunto malicioso en un correo electrónico

	Dónde: Computadora de un empleado en una empresa de servicios financieros **Cuándo:** Alerta enviada al SOC a la 1:20 p.m. **Por qué:** El archivo malicioso fue descargado y ejecutado por un empleado.
Notas Adicionales	¿Cómo prevenir incidentes futuros? ¿Se debería fortalecer la formación en ciberseguridad?

Reflexiones/Notas	
Reto Personal	El uso de tcpdump fue complicado, pero me enseñó la importancia de seguir las instrucciones cuidadosamente.
Comprensión Mejorad	Mi comprensión sobre detección y respuesta a incidentes mejoró, especialment en cuanto a la planificación y complejidad de los procesos.
Herramienta Favorita	Disfruté aprender sobre el análisis de tráfico de red y espero profundizar en el tema. La experiencia fue desafiante y motivadora.
