**Diario del gestor de incidentes**

**Instrucciones**

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

|  |  |
| --- | --- |
| **Fecha:** 23 de julio de 2024 | **Entrada:**  #1 |
| Descripción | Documentar un incidente de ciberseguridad  Este incidente ocurrió en dos fases:   1. **Detección y análisis** : el escenario describe cómo la organización detectó por primera vez el incidente de ransomware. Para el paso de análisis, la organización se puso en contacto con varias organizaciones para obtener asistencia técnica. 2. **Contención, erradicación y recuperación** : el escenario detalla algunos pasos que la organización tomó para contener el incidente. Por ejemplo, la empresa apagó sus sistemas informáticos. Sin embargo, como no podían trabajar para erradicar y recuperarse del incidente por sí solas, se pusieron en contacto con otras organizaciones para solicitar ayuda. |
| Herramienta(s) utilizada(s) | Ninguno |
| Las 5 W | * **Quién** : Un grupo organizado de hackers poco éticos. * **Qué** : Un incidente de seguridad de ransomware * **Dónde** : En una empresa de atención médica. * **Cuándo** : Martes 9:00 am * **Motivo** : El incidente se produjo porque piratas informáticos poco éticos pudieron acceder a los sistemas de la empresa mediante un ataque de phishing. Tras obtener acceso, los atacantes lanzaron su ransomware en los sistemas de la empresa, cifrando archivos críticos. La motivación de los atacantes parece ser económica, ya que la nota de rescate que dejaron exigía una gran suma de dinero a cambio de la clave de descifrado. |
| Notas adicionales | 1. ¿Cómo podría la compañía sanitaria evitar que un incidente como éste volviera a ocurrir? 2. ¿Debe la empresa pagar el rescate para recuperar la clave de descifrado? |

|  |  |
| --- | --- |
| **Fecha:** 25 de julio de 2024 | **Entrada:** #2 |
| Descripción | Analizando un archivo de captura de paquetes |
| Herramienta(s) utilizada(s) | Para esta actividad, utilicé Wireshark para analizar un archivo de captura de paquetes. Wireshark es un analizador de protocolos de red que utiliza una interfaz gráfica de usuario. El valor de Wireshark en materia de ciberseguridad es que permite a los analistas de seguridad capturar y analizar el tráfico de la red. Esto puede ayudar a detectar e investigar actividades maliciosas. |
| Las 5 W | * **Quién** : N/A * **Qué** : N/A * **Dónde** : N/A * **Cuándo** : N/A * **Por qué** : N/A |
| Notas adicionales | Nunca había usado Wireshark antes, así que me entusiasmó comenzar este ejercicio y analizar un archivo de captura de paquetes. A primera vista, la interfaz me resultó abrumadora. Puedo ver por qué es una herramienta tan poderosa para comprender el tráfico de la red. |

|  |  |
| --- | --- |
| **Fecha:** 25 de julio de 2024 | **Entrada:**  #3 |
| Descripción | Capturando mi primer paquete |
| Herramienta(s) utilizada(s) | Para esta actividad, utilicé tcpdump para capturar y analizar el tráfico de red. Tcpdump es un analizador de protocolos de red al que se accede mediante la interfaz de línea de comandos. Al igual que Wireshark, el valor de tcpdump en ciberseguridad es que permite a los analistas de seguridad capturar, filtrar y analizar el tráfico de red. |
| Las 5 W | * **Quién** : N/A * **Qué** : N/A * **Dónde** : N/A * **Cuándo** : N/A * **Por qué** : N/A |
| Notas adicionales | Todavía no tengo experiencia en el uso de la interfaz de línea de comandos, por lo que usarla para capturar y filtrar el tráfico de red fue un desafío. Me quedé atascado un par de veces porque usé los comandos incorrectos. Pero después de seguir atentamente las instrucciones y rehacer algunos pasos, pude realizar esta actividad y capturar el tráfico de red. |

|  |  |
| --- | --- |
| **Fecha:** 27 de julio de 2024 | **Entrada:**  #4 |
| Descripción | Investigar un hash de archivo sospechoso |
| Herramienta(s) utilizada(s) | Para esta actividad, utilicé VirusTotal, una herramienta de investigación que analiza archivos y URL en busca de contenido malicioso, como virus, gusanos, troyanos y más. Es una herramienta muy útil para comprobar rápidamente si un indicador de riesgo, como un sitio web o un archivo, ha sido denunciado como malicioso por otros miembros de la comunidad de ciberseguridad. Para esta actividad, utilicé VirusTotal para analizar un hash de archivo que se había denunciado como malicioso.  Este incidente ocurrió en la fase de **Detección y Análisis** . El escenario me puso en el lugar de un analista de seguridad de un SOC que investigaba un hash de archivo sospechoso. Después de que los sistemas de seguridad instalados detectaran el archivo sospechoso, tuve que realizar un análisis e investigación más profundos para determinar si la alerta significaba una amenaza real. |
| Las 5 W | * **Quién** : Un actor malicioso desconocido * **Qué** : Un correo electrónico enviado a un empleado contenía un archivo adjunto malicioso con el hash de archivo SHA-256 de 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b * **Dónde** : La computadora de un empleado de una empresa de servicios financieros. * **Cuándo** : A las 13:20 horas, se envió una alerta al SOC de la organización después de que el sistema de detección de intrusiones detectara el archivo. * **Por qué** : Un empleado pudo descargar y ejecutar un archivo adjunto malicioso mediante un correo electrónico. |
| Notas adicionales | ¿Cómo se puede evitar que este incidente se repita en el futuro? ¿Deberíamos considerar mejorar la capacitación en materia de seguridad para que los empleados tengan cuidado con lo que hacen clic? |

|  |
| --- |
| Reflexiones/Notas:   1. **¿Hubo alguna actividad específica que fuera un desafío para ti? ¿Por qué sí o por qué no?**   Realmente me resultó desafiante la actividad de usar tcpdump. Soy nuevo en el uso de la línea de comandos y aprender la sintaxis de una herramienta como tcpdump fue una gran curva de aprendizaje. Al principio, me sentí muy frustrado porque no obtenía el resultado correcto. Volví a realizar la actividad y descubrí dónde me había equivocado. Lo que aprendí de esto fue leer atentamente las instrucciones y seguir el proceso lentamente.   1. **¿Ha cambiado su comprensión de la detección y respuesta a incidentes después de tomar este curso?**   Después de realizar este curso, mi comprensión de la detección y respuesta ante incidentes ha evolucionado definitivamente. Al principio del curso, tenía una comprensión básica de lo que implicaba la detección y respuesta, pero no entendía del todo la complejidad que implica. A medida que avanzaba en el curso, aprendí sobre el ciclo de vida de un incidente; la importancia de los planes, los procesos y las personas; y las herramientas utilizadas. En general, siento que mi comprensión ha cambiado y estoy equipado con más conocimientos y comprensión sobre la detección y respuesta ante incidentes.   1. **¿Hubo alguna herramienta o concepto específico que te haya gustado más? ¿Por qué?**   Disfruté mucho aprendiendo sobre el análisis del tráfico de red y aplicando lo que aprendí a través de las herramientas de análisis de protocolos de red. Fue la primera vez que aprendí sobre el análisis del tráfico de red, por lo que fue un desafío y una emoción a la vez. Me pareció realmente fascinante poder usar herramientas para capturar el tráfico de red y analizarlo en tiempo real. Definitivamente estoy más interesado en aprender más sobre este tema y espero algún día volverme más competente en el uso de herramientas de análisis de protocolos de red. |