**Diario del gestor de incidentes**

|  |  |
| --- | --- |
| **Fecha:** 23 de julio de 2024 | **Entrada:**  #1 |
| Descripción | Documentación de un incidente de ciberseguridad  Este incidente se desarrolló en dos fases:   1. **Detección y Análisis:** El escenario describe cómo la organización detectó inicialmente el incidente de ransomware. Para la fase de análisis, la organización contactó a varias entidades para recibir asistencia técnica. 2. **Contención, Erradicación y Recuperación**: El escenario detalla algunos pasos que la organización tomó para contener el incidente, como apagar sus sistemas informáticos. Sin embargo, dado que no podían erradicar ni recuperarse del incidente por sí mismos, contactaron a varias otras organizaciones para obtener ayuda. |
| Herramientas utilizadas | Ninguna |
| Las 5 W | * **Who**: Un grupo organizado de hackers poco éticos. * **What**: Un incidente de seguridad por ransomware. * **Where**: En una empresa de atención médica. * **When**: Martes, 9:00 a. m. * **Why**: El incidente ocurrió porque hackers poco éticos pudieron acceder a los sistemas de la empresa mediante un ataque de \*phishing\*. Después de obtener acceso, los atacantes lanzaron su \*ransomware\* en los sistemas de la compañía, cifrando archivos críticos. La motivación de los atacantes parece ser financiera, 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 de atención médica evitar que un incidente como este vuelva a ocurrir? 2. ¿Debería la compañía pagar el rescate para obtener la clave de descifrado? |

|  |  |
| --- | --- |
| **Date:** 25 de Julio 2024 | **Entrada:** #2 |
| Descripción | Analizando un archivo de captura de paquetes |
| Herramientas utilizadas | 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 ciberseguridad es que permite a los analistas de seguridad capturar y analizar el tráfico de red. Esto puede ayudar a detectar e investigar actividades maliciosas. |
| Las 5 W | * **Who**: N/A * **What**: N/A * **Where**: N/A * **When**: N/A * **Why**: N/A |
| Notas Adicionales | Nunca había usado Wireshark antes, así que estaba emocionado por comenzar este ejercicio y analizar un archivo de captura de paquetes. A primera vista, la interfaz fue muy abrumadora. Puedo ver por qué es una herramienta tan poderosa para comprender el tráfico de red. |

|  |  |
| --- | --- |
| **Date:** 25 de Julio 2024 | **Entrada:**  #3 |
| Descripción | Capturando mi primer paquete |
| Herramientas utilizadas | Para esta actividad, utilicé tcpdump para capturar y analizar el tráfico de red. Tcpdump es un analizador de protocolos de red que se accede mediante la interfaz de línea de comandos. Al igual que Wireshark, su valor en ciberseguridad es que permite a los analistas capturar, filtrar y analizar el tráfico de red. |
| Las 5 W | * **Who**: N/A * **What**: N/A * **Where**: N/A * **When**: N/A * **Why**: N/A |
| Notas Adicionales | Todavía soy nuevo en el uso de la interfaz de línea de comandos, así que usarla para capturar y filtrar tráfico de red fue un desafío. Me quedé atascado un par de veces porque utilicé comandos incorrectos. Pero después de seguir cuidadosamente las instrucciones y repetir algunos pasos, pude completar la actividad y capturar el tráfico de red. |

|  |  |
| --- | --- |
| **Date:** 27 de Julio 2024 | **Entrada:**  #4 |
| Descripción | Investigar un hash de archivo sospechoso |
| Herramientas utilizadas | Para esta actividad, utilicé **VirusTotal**, que es 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 si deseas verificar rápidamente si un indicador de compromiso, como un sitio web o un archivo, ha sido reportado como malicioso por otros en la comunidad de ciberseguridad. Para esta actividad, usé **VirusTotal** para analizar un hash de archivo, el cual fue reportado como malicioso.  Este incidente ocurrió en la fase de Detección y Análisis. El escenario me puso en el lugar de un analista de seguridad en un SOC investigando un hash de archivo sospechoso. Después de que los sistemas de seguridad detectaron el archivo sospechoso, tuve que realizar un análisis e investigación más profundos para determinar si la alerta representaba una amenaza real. |
| Las 5 W | * **Who**: Un actor malicioso desconocido * **What**: Un correo electrónico enviado a un empleado contenía un archivo adjunto malicioso con el hash de archivo SHA-256: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b * **Where**: La computadora de un empleado en una empresa de servicios financieros * **When**: A la 1:20 p. m., se envió una alerta al SOC de la organización después de que el sistema de detección de intrusiones detectara el archivo. * **Why**: Un empleado pudo descargar y ejecutar un archivo adjunto malicioso a través del correo electrónico. |
| Notas Adicionales | ¿Cómo se puede prevenir este incidente en el futuro? ¿Deberíamos considerar mejorar la capacitación en concienciación sobre seguridad para que los empleados sean más cuidadosos con los enlaces y archivos que abren? |