DFIR: Una introducción

Tarea 1: Introducción

Objetivos de aprendizaje
Las brechas e incidentes de seguridad ocurren a pesar de que los equipos de seguridad se esfuerzan al máximo por evitarlos en todo el mundo. La estrategia prudente en este escenario es prepararse para el momento en que ocurra un incidente para evitar ser tomados por sorpresa. Por ello, la Investigación Forense Digital y la Respuesta a Incidentes (DFIR) se han convertido en una materia esencial en la Seguridad Defensiva. En esta sesión, abordaremos algunos conceptos básicos de DFIR y presentaremos salas que amplían nuestro conocimiento sobre DFIR . La sesión abordará los siguientes temas:

- Introducción del DFIR
- Algunos conceptos básicos utilizados en el campo DFIR
- Los procesos de respuesta a incidentes utilizados en la industria
- Algunas de las herramientas utilizadas para DFIR

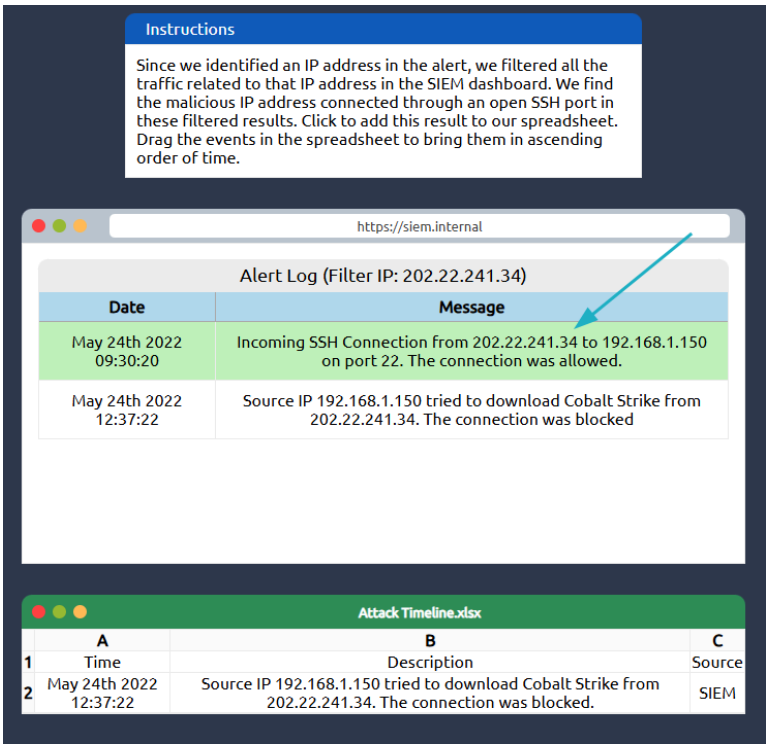
P: Lea los objetivos de aprendizaje
R: No se necesita respuesta

Tarea 2: La necesidad del DFIR
P1: ¿Qué significa DFIR?
R1: Digital Forensics and Incident Response

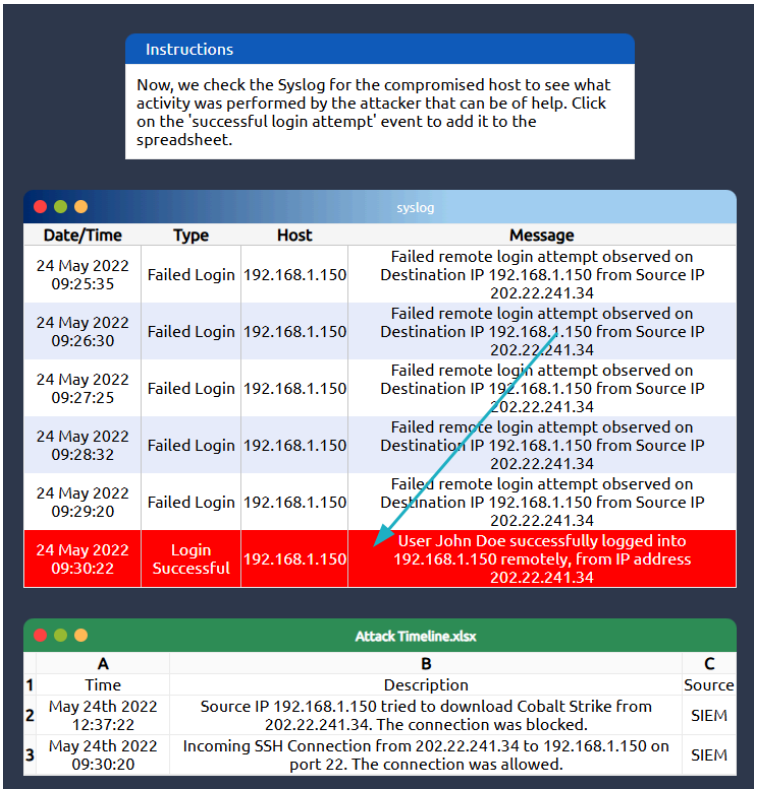
P2: El DFIR requiere experiencia en dos campos. Uno de ellos es la informática forense. ¿Cuál es el otro?
R2: Incident Response

Tarea 3: Conceptos básicos del DFIR
P1: Entre la RAM y el disco duro, ¿qué almacenamiento es más volátil?
R1: RAM

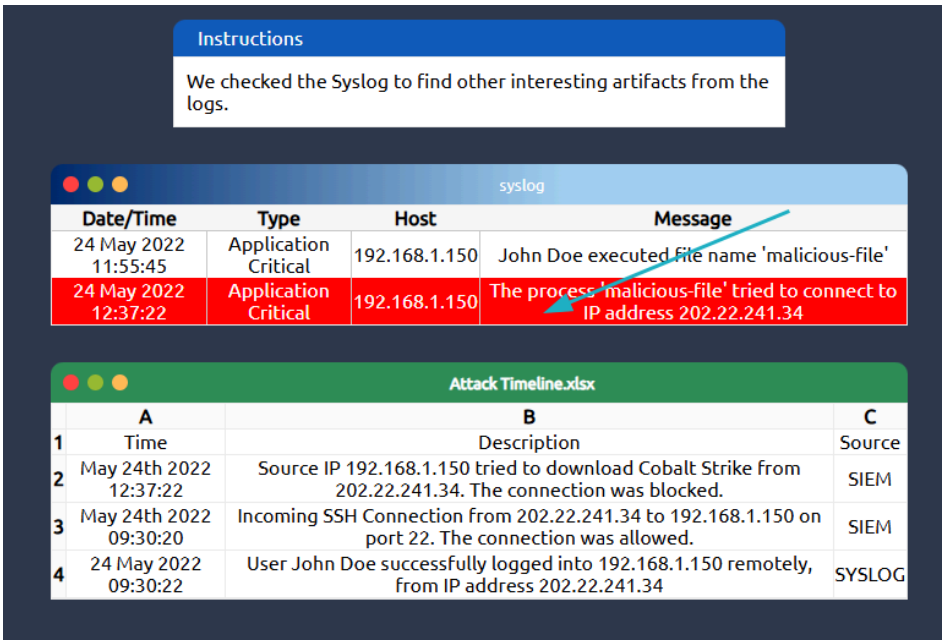
P2: Completa el ejercicio de creación de una línea de tiempo en el sitio estático adjunto. ¿Qué bandera aparece al completarlo?



Ordenamos los Timelines



Ordenamos los Timelines



R2: THM{DFIR_REPORT_DONE}

Tarea 4: Herramientas DFIR
P: Consulta las salas relacionadas con las diferentes herramientas mencionadas aquí.
R: No se necesita respuesta

Tarea 5: El proceso de respuesta a incidentes
P1: ¿En qué etapa del proceso de IR se restablecen los servicios interrumpidos a como estaban antes del incidente?
R1: Recovery

P2: ¿En qué etapa del proceso de IR se expulsa la amenaza de la red después de realizar el análisis forense?
R2: Eradication

P3: ¿Cuál es el equivalente NIST del paso denominado “Lecciones aprendidas” en el proceso SANS?
R3: Post-incident Activity

Tarea 6: Conclusión

Eso fue todo por esta sala. Repasemos lo que aprendimos aquí.

- Aprendimos qué es DFIR y dónde se utiliza.
- Aprendimos por qué necesitamos realizar DFIR .
- Aprendimos conceptos básicos como la cadena de custodia , la preservación de la evidencia y el orden de volatilidad.
- Aprendimos sobre algunas de las herramientas utilizadas en la industria como EZ tools, KAPE , Autopsy, etc.
- El proceso PICERL para respuesta a incidentes

Ahora podemos pasar a las siguientes salas de este módulo para aprender más sobre DFIR . Cuéntanos qué te pareció esta sala en nuestro canal de Discord o en nuestra cuenta de Twitter . Nos vemos.

P: Únete a la discusión en nuestros canales sociales.
R: No se necesita respuesta

💼**LinkedIn:**https://www.linkedin.com/in/mateo-rodr%C3%ADguez-suar-202695249/
💻 **GitHub:** https://github.com/MaateoSuar