Writeup: Sala *DFIR: An Introduction*

Autor: Ismaeldevs

Plataforma: TryHackMe

4 de julio de 2025

Índice

1. Introducción

Esta sala nos ayudara a proporcionar una base sólida en el campo de la respuesta a incidentes y la informática forense. Conoceremos qué es DFIR, por qué es una disciplina crítica dentro de la ciberseguridad, y cuáles son sus conceptos fundamentales, herramientas principales y metodologías.

2. Sala

2.1. Tarea 1 – Introducción

En esta primera comprenderemos qué es **DFIR (Digital Forensics and Incident Response)** y por qué es vital en seguridad defensiva.

Respuesta: **No requiere respuesta** (Hacemos clic en **Submit**).

2.2. Tarea 2 - La necesidad del DFIR

Aprenderemos que DFIR combina dos disciplinas: **Digital Forensics** y **Incident Response**. Su importancia radica en recopilar evidencia de activos digitales infestados, determinar el alcance de una brecha, eliminar amenazas y mejorar la seguridad futura.

Una vez que comprendemos la necesidad del DFIR, pasaremos a responder las siguientes preguntas. **0.5cm**

Pregunta: What does DFIR stand for?

Respuesta: **Digital Forensics and Incident Response**

Pregunta: DFIR requires expertise in two fields. One of the fields is Digital Forensics. What is the other field?

Respuesta: **Incident Response**

2.3. Tarea 3 - Conceptos básicos del DFIR

Ahora nos introduciremos en fundamentos esenciales como:

- **Qué son los artefactos forenses**
- **La preservación de evidencia (evitar contaminación)**
- **La cadena de custodia (mantener integridad legal)**

- **El orden de volatilidad (priorizar RAM antes que disco)**
- **La creación de cronologías de eventos para entender el incidente**

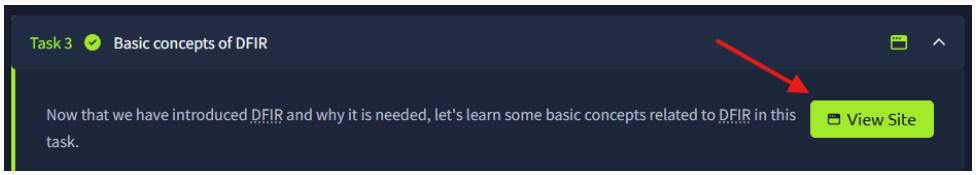
Una vez comprendido estos fundamentos, procederemos a responder las siguientes preguntas.

Pregunta: From amongst the RAM and the hard disk, which storage is more volatile?

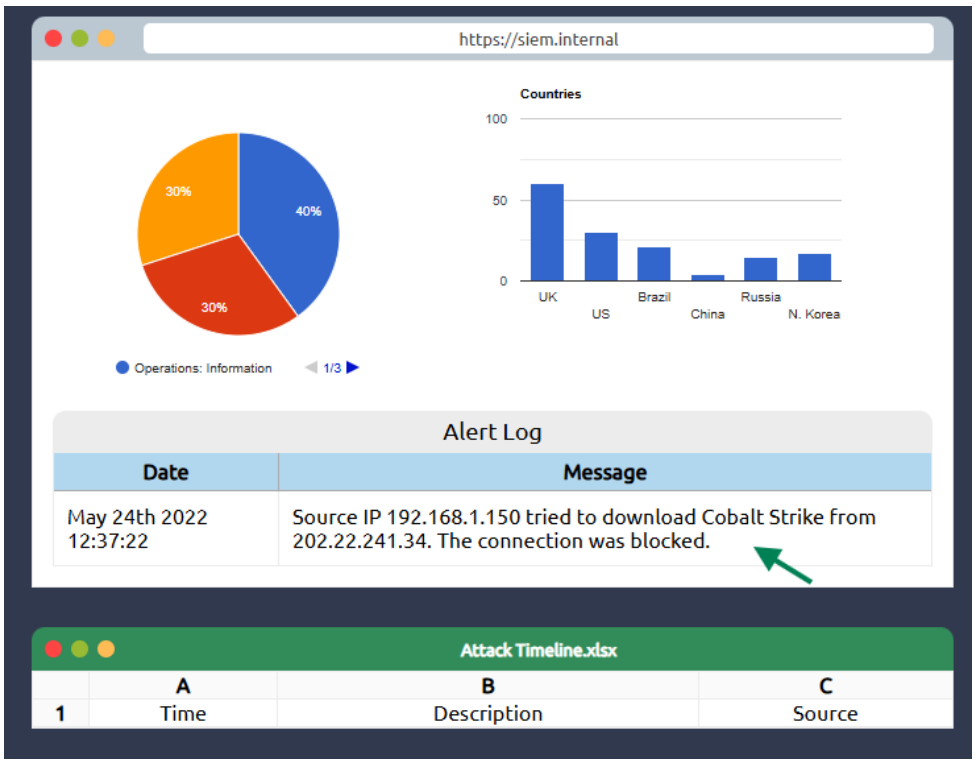
Respuesta: **RAM**

Pregunta: Complete the timeline creation exercise in the attached static site. What is the flag that you get after completion?

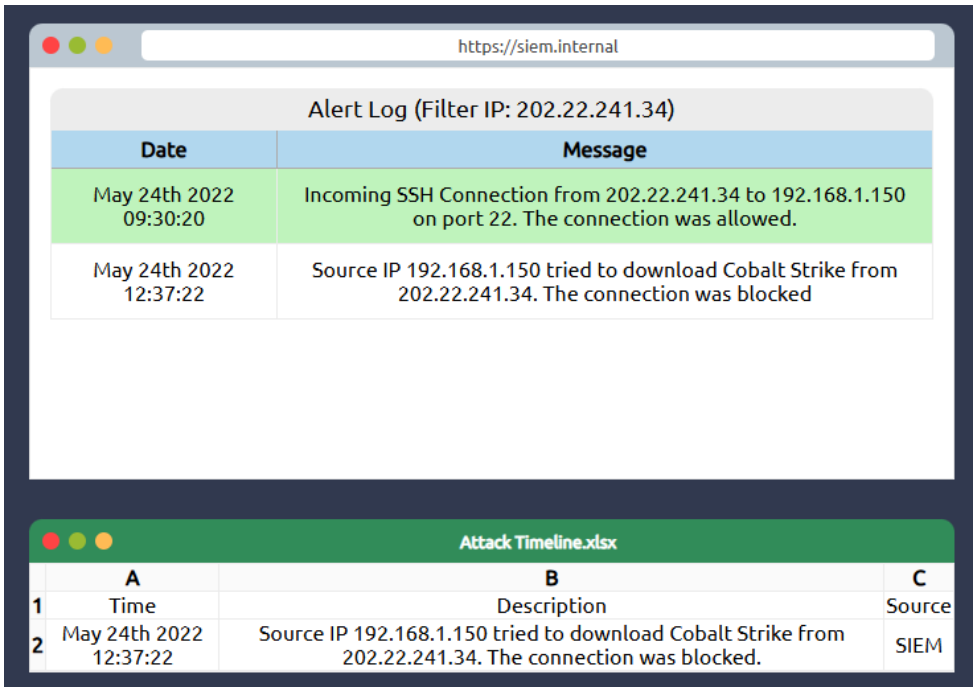
Para completar esta tarea, debemos desplegar el sitio de práctica que se encuentra en el lado superior de la tarea, haremos clic en **View Site**.



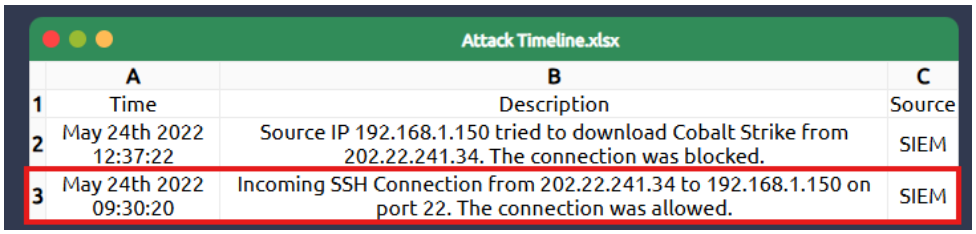
Una vez desplegado, para continuar haremos clic en la alerta que nos aparecere en el Alert Log para agregarla en la línea de tiempo de ataque.

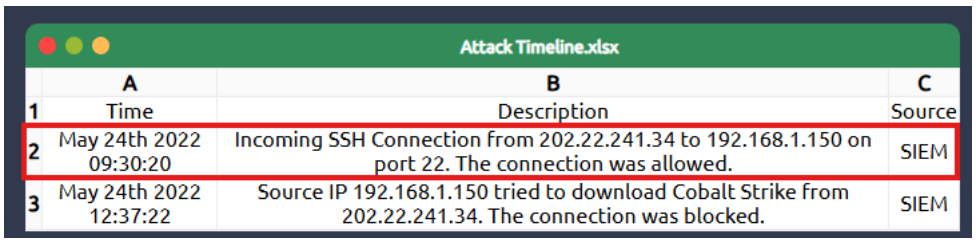


Después, nos aparecerán nuevas alertas, debemos añadir la alerta sospechosa a la línea de tiempo haciendo clic en ella.

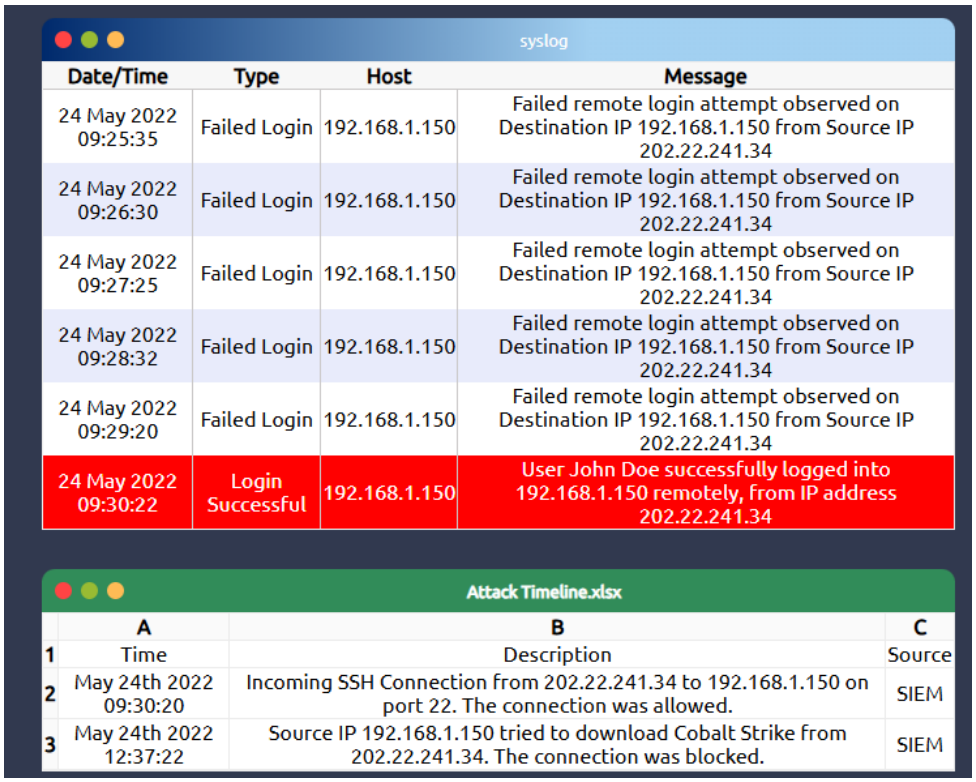


Posterior a eso, vamos a ordenar la línea de tiempo del ataque arrastrando un ítem sobre el otro.





Ahora tenemos nuevas alertas, pero una es la relevante sobre el resto de alertas, para ello, haremos clic en la alerta sospechosa marcada en rojo para añadirla en la línea.



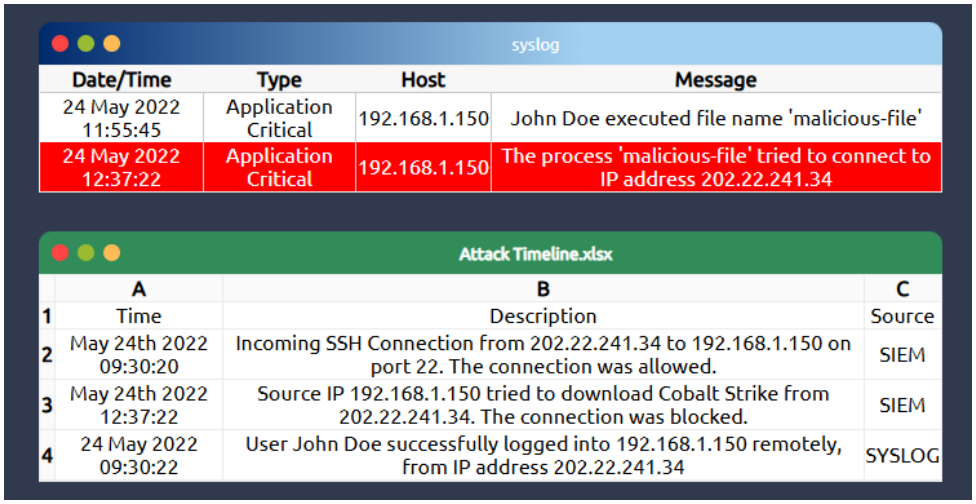
syslog

Date/Time	Type	Host	Message
24 May 2022 09:25:35	Failed Login	192.168.1.150	Failed remote login attempt observed on Destination IP 192.168.1.150 from Source IP 202.22.241.34
24 May 2022 09:26:30	Failed Login	192.168.1.150	Failed remote login attempt observed on Destination IP 192.168.1.150 from Source IP 202.22.241.34
24 May 2022 09:27:25	Failed Login	192.168.1.150	Failed remote login attempt observed on Destination IP 192.168.1.150 from Source IP 202.22.241.34
24 May 2022 09:28:32	Failed Login	192.168.1.150	Failed remote login attempt observed on Destination IP 192.168.1.150 from Source IP 202.22.241.34
24 May 2022 09:29:20	Failed Login	192.168.1.150	Failed remote login attempt observed on Destination IP 192.168.1.150 from Source IP 202.22.241.34
24 May 2022 09:30:22	Login Successful	192.168.1.150	User John Doe successfully logged into 192.168.1.150 remotely, from IP address 202.22.241.34

Attack Timeline.xlsx

	A	B	C
1	Time	Description	Source
2	May 24th 2022 09:30:20	Incoming SSH Connection from 202.22.241.34 to 192.168.1.150 on port 22. The connection was allowed.	SIEM
3	May 24th 2022 12:37:22	Source IP 192.168.1.150 tried to download Cobalt Strike from 202.22.241.34. The connection was blocked.	SIEM

Una vez añadida, nos aparecerá otra alerta sospechosa marcada en rojo, haremos lo mismo anteriormente en hacer clic en ella para añadirla a la línea de tiempo.



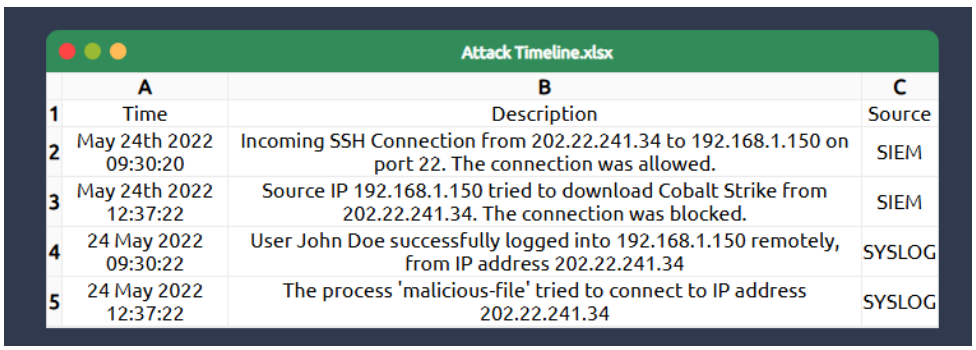
syslog

Date/Time	Type	Host	Message
24 May 2022 11:55:45	Application Critical	192.168.1.150	John Doe executed file name 'malicious-file'
24 May 2022 12:37:22	Application Critical	192.168.1.150	The process 'malicious-file' tried to connect to IP address 202.22.241.34

Attack Timeline.xlsx

	A	B	C
1	Time	Description	Source
2	May 24th 2022 09:30:20	Incoming SSH Connection from 202.22.241.34 to 192.168.1.150 on port 22. The connection was allowed.	SIEM
3	May 24th 2022 12:37:22	Source IP 192.168.1.150 tried to download Cobalt Strike from 202.22.241.34. The connection was blocked.	SIEM
4	24 May 2022 09:30:22	User John Doe successfully logged into 192.168.1.150 remotely, from IP address 202.22.241.34	SYSLOG

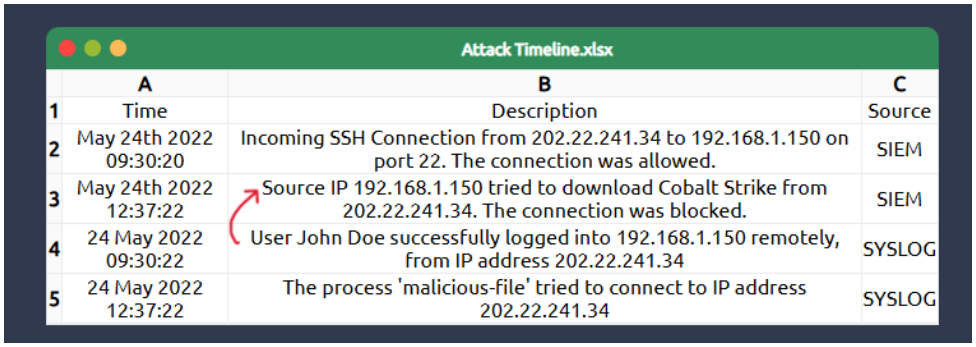
Ahora, ya solo nos queda ordenar la línea de tiempo del ataque con los eventos que fuimos registrando.



Attack Timeline.xlsx

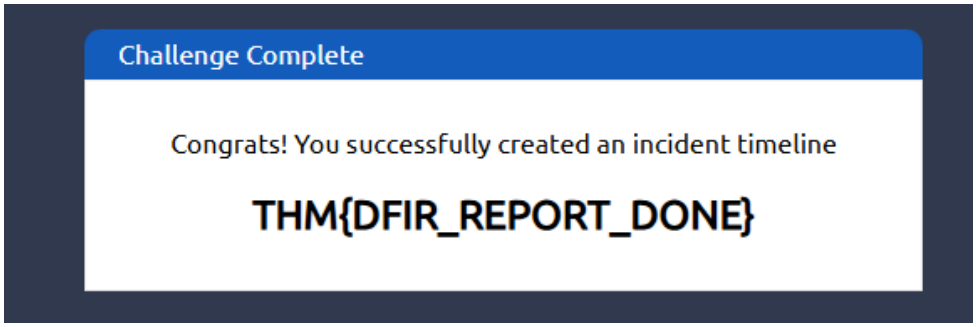
	A	B	C
1	Time	Description	Source
2	May 24th 2022 09:30:20	Incoming SSH Connection from 202.22.241.34 to 192.168.1.150 on port 22. The connection was allowed.	SIEM
3	May 24th 2022 12:37:22	Source IP 192.168.1.150 tried to download Cobalt Strike from 202.22.241.34. The connection was blocked.	SIEM
4	24 May 2022 09:30:22	User John Doe successfully logged into 192.168.1.150 remotely, from IP address 202.22.241.34	SYSLOG
5	24 May 2022 12:37:22	The process 'malicious-file' tried to connect to IP address 202.22.241.34	SYSLOG

Para resolver la línea de tiempo, simplemente pondremos en segúndo lugar la alerta del **User John**, posterior a eso, nos saltará la flag que necesitamos para resolver la tarea.



Attack Timeline.xlsx

	A	B	C
1	Time	Description	Source
2	May 24th 2022 09:30:20	Incoming SSH Connection from 202.22.241.34 to 192.168.1.150 on port 22. The connection was allowed.	SIEM
3	May 24th 2022 12:37:22	Source IP 192.168.1.150 tried to download Cobalt Strike from 202.22.241.34. The connection was blocked.	SIEM
4	24 May 2022 09:30:22	User John Doe successfully logged into 192.168.1.150 remotely, from IP address 202.22.241.34	SYSLOG
5	24 May 2022 12:37:22	The process 'malicious-file' tried to connect to IP address 202.22.241.34	SYSLOG



Respuesta: **THM{DFIR_REPORT_DONE}**

2.4. Tarae 4 -DFIR Tools

Aprenderemos sobre herramientas comunes utilizadas en DFIR: los utilitarios de Eric Zimmerman, KAPE, Autopsy, Volatility, Redline y Velociraptor, mostrando cómo ayudan en el análisis forense y la respuesta ante incidentes.

Respuesta: **No requiere respuesta** (Hacemos clic en **Submit**).

2.5. Tarea 5 - El proceso de respuesta a incidentes

Ahora, conoceremos los marcos de trabajo IR aceptados (NIST y SANS), destacando el ciclo PICERL: Preparación, Identificación, Contención, Erradicación, Recuperación y Lecciones aprendidas, explicando brevemente cada etapa.

Una vez que comprendemos estos marcos, pasaremos a responder las siguientes preguntas.

Pregunta: At what stage of the IR process are disrupted services brought back online as they were before the incident?

Respuesta: **Recovery**

Pregunta: At what stage of the IR process is the threat evicted from the network after performing the forensic analysis?

Respuesta: **Eradication**

Pregunta: What is the NIST-equivalent of the step called Lessons learned in the SANS process?

Respuesta: **Post-incident Activity**

2.6. Tarea 6 - Conclusión

Recapitulamos el aprendizaje en el cual se definió DFIR y su necesidad, se revisaron conceptos clave (cadena de custodia, volatilidad, cronologías), se exploraron herramientas fundamentales y se entendió el proceso IR.

Respuesta: **No requiere respuesta** (Hacemos clic en **Submit**).

3. Conclusión sobre la Sala

Al finalizar esta sala, habremos adquirido un conocimiento general sobre qué implica DFIR, comprendiendo conceptos clave como la cadena de custodia, el orden de volatilidad y la importancia de preservar la evidencia. Además, se habrán presentado herramientas forenses comunes y se habrá explorado el proceso de respuesta a incidentes siguiendo marcos reconocidos como el de NIST.