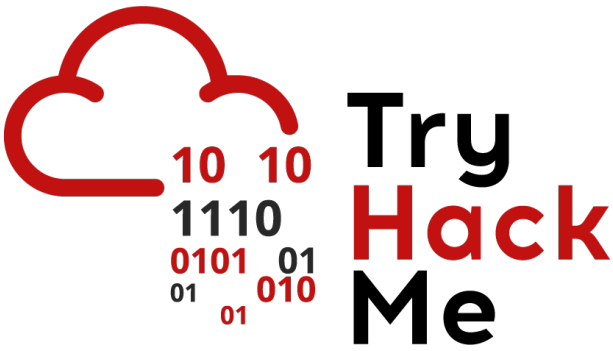
Writeup: Sala *Intro to Cyber Threat Intel*

Autor: Ismaeldevs

Plataforma: TryHackMe

4 de julio de 2025



Índice

1. Introducción

En esta sala nos introduciremos en los conceptos fundamentales de la inteligencia de amenazas cibernéticas (CTI), un pilar clave en la defensa proactiva dentro de la ciberseguridad. Aprenderemos qué es el CTI, sus diferentes niveles (estratégico, táctico, técnico y operacional), cómo se estructura su ciclo de vida, y qué estándares y marcos permiten intercambiar y analizar información sobre amenazas.

2. Sala

2.1. Tarea 1 – Introducción

En esta primera tarea nos introduce en la **inteligencia de amenazas cibernéticas (CTI)** y su papel estratégico en la seguridad. Aprendemos que como analistas de seguridad, el CTI ayuda a investigar ataques y comunicar hallazgos tanto a equipos técnicos como a tomadores de decisiones.

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

2.2. Tarea 2 - Inteligencia sobre ciberamenazas

Descubriremos que se define al CTI como el conocimiento basado en evidencia sobre adversarios, además, se clarifica la evolución desde datos (IP, hashes), a información (tendencias), y finalmente a inteligencia contextualizada, que responde preguntas como quién ataca, por qué y cómo. También se describen las clasificaciones de CTI:

- **Estratégico**
- **Operacional**
- **Táctico**
- **Técnico**

Ahora que entendemos sobre **CTI**, pasamos a responder las siguientes preguntas.

Pregunta: What does CTI stand for?
Respuesta: **Cyber Threat Intelligence**

Pregunta: IP addresses, Hashes and other threat artefacts would be found under which Threat Intelligence classification?
Respuesta: **Technical Intel**

2.3. Tarea 3 - Ciclo de vida de CTI

Conoceremos el ciclo de vida del CTI, este se desglosa en seis fases:

1. **Dirección**: definición de objetivos y preguntas clave.
2. **Recolección**: obtención de datos de fuentes diversas.
3. **Procesamiento**: limpieza, normalización y preparación para análisis.
4. **Análisis**: interpretación para generar inteligencia accionable.
5. **Diseminación**: entrega de informes adaptados al público destinatario.
6. **Retroalimentación**: ajuste del proceso en base a resultados

Ahora, procedemos a responder las siguientes preguntas:

Pregunta: At which phase of the CTI lifecycle is data converted into usable formats through sorting, organising, correlation and presentation?
Respuesta: **Processing**

Pregunta: During which phase do security analysts get the chance to define the questions to investigate incidents?
Respuesta: **Direction**

2.4. Tarea 4 - Normas y marcos de CTI

En esta tarea aprenderemos sobre marcos y estándares claves como:

- **MITRE ATT&CK**
- **TAXII**
- **STIX**
- **Cyber Kill Chain**
- **Diamond Model**

Una vez que comprendemos estas normas y marcos, podemos responder las siguientes preguntas.

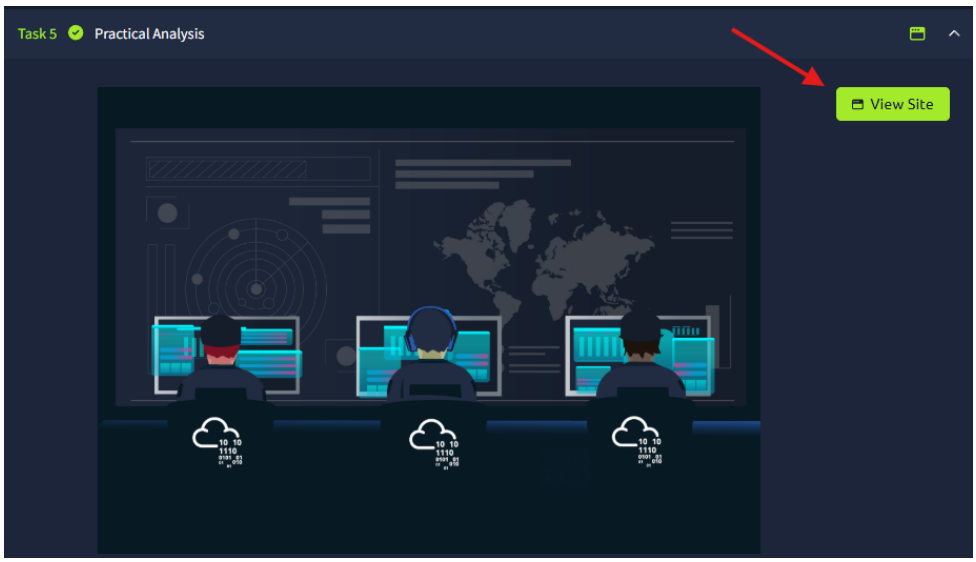
Pregunta: What sharing models are supported by TAXII?
Respuesta: **Collection and Channel**

Pregunta: When an adversary has obtained access to a network and is extracting data, what phase of the kill chain are they on?

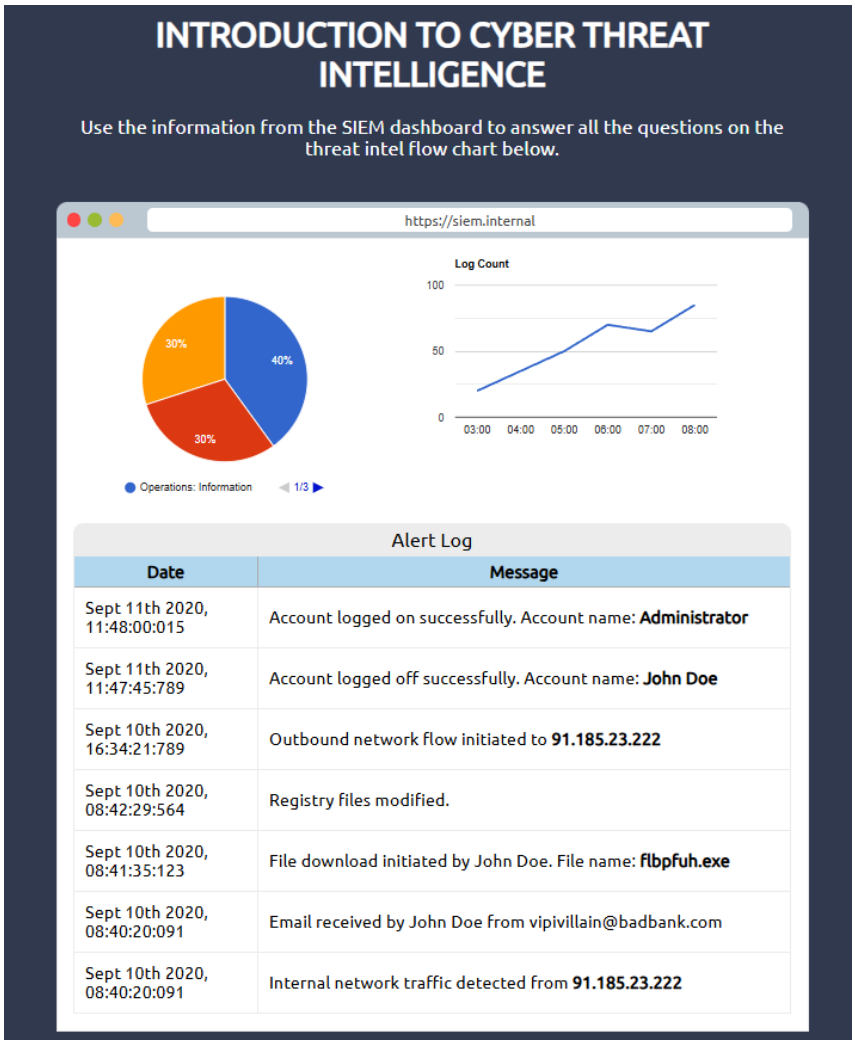
Respuesta: **Actions on Objectives**

2.5. Tarea 5 - Análisis práctico

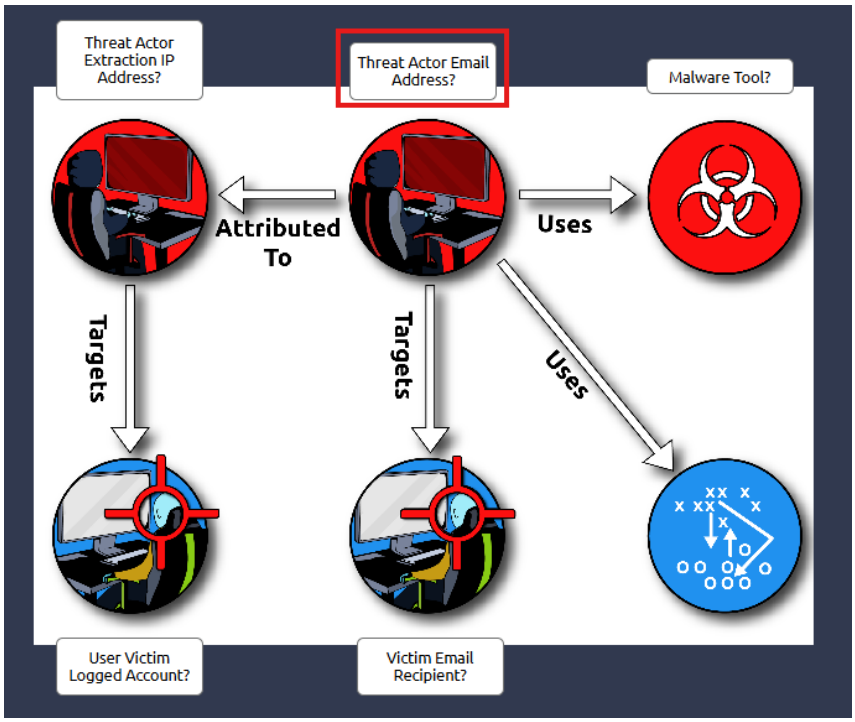
Ahora aplicaremos lo aprendido en un ejercicio práctico con una interfaz tipo SIEM. Para comenzar con la práctica, vamos a desplegar el sitio haciendo clic en **View Site** que se encuentra en el lado superior de la tarea.

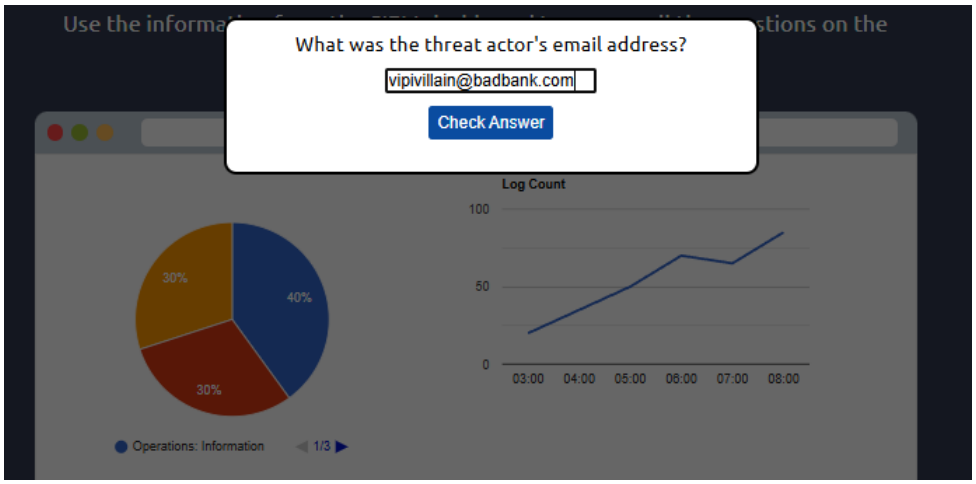


Debemos analizar los registros de alerta, una vez analizados, pasaremos a responder las diferentes preguntas que se nos presentarán en base a los registros.

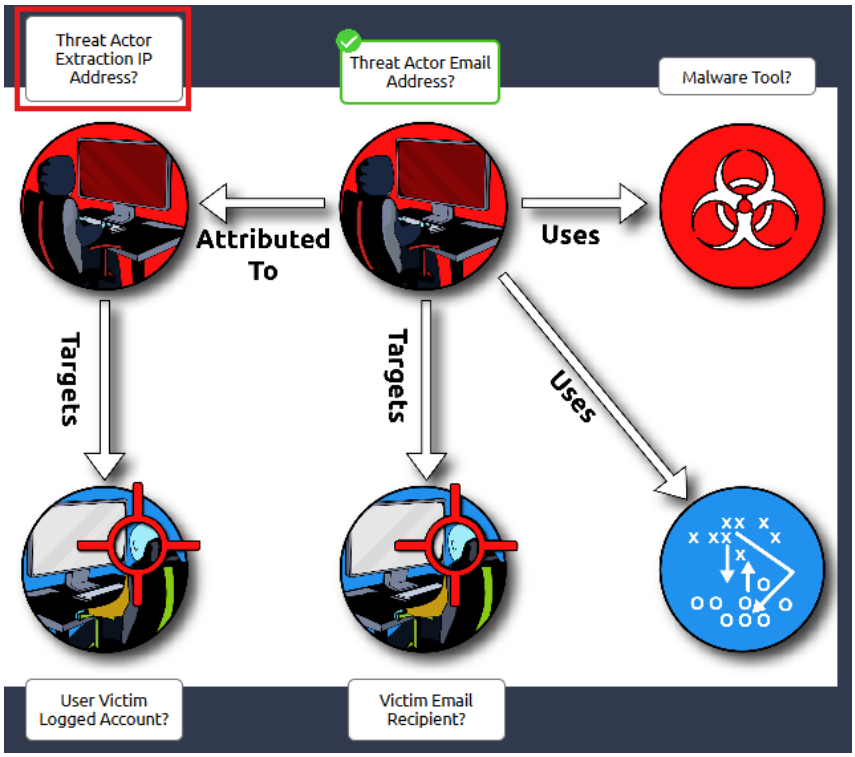


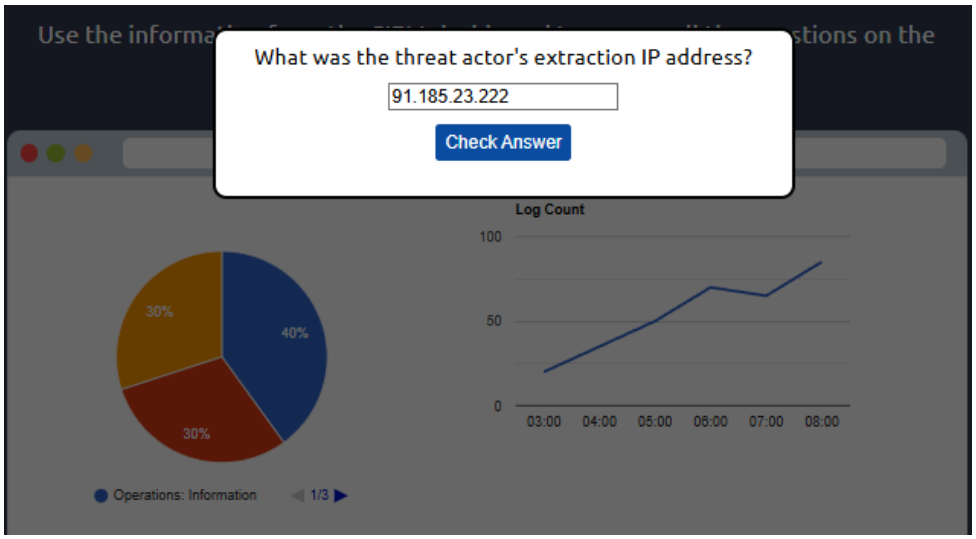
Pregunta: What was the source email address?



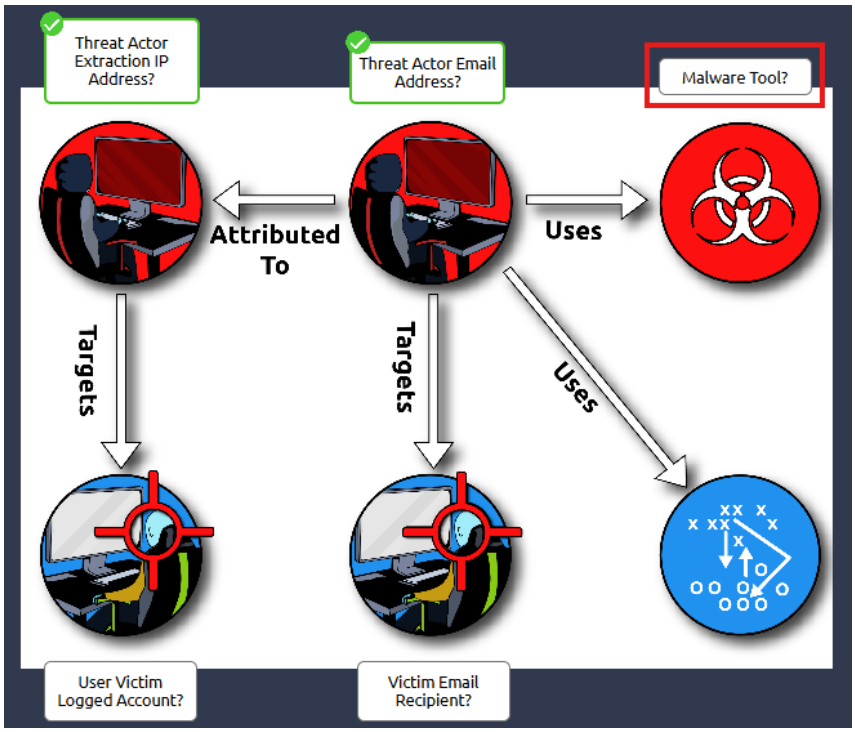


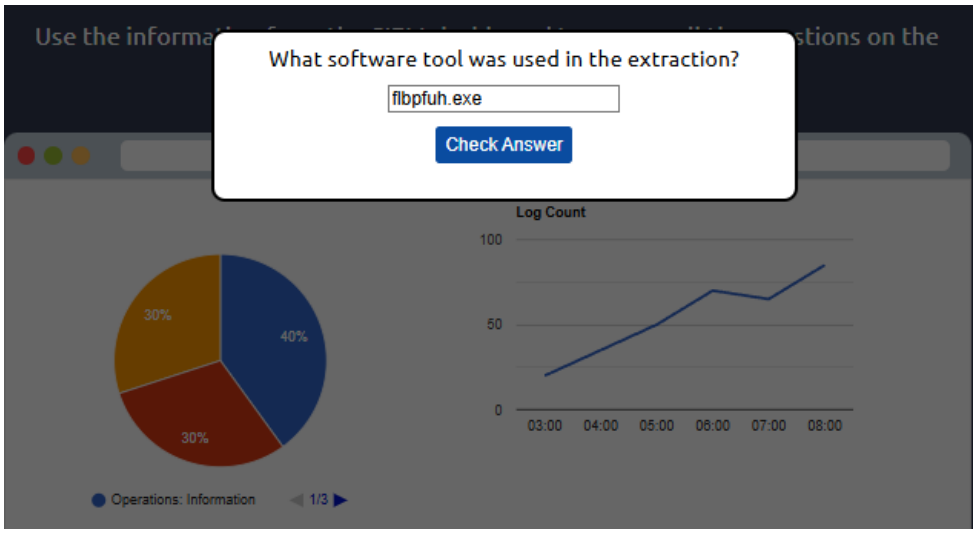
Respuesta: vipivillain@badbank.com



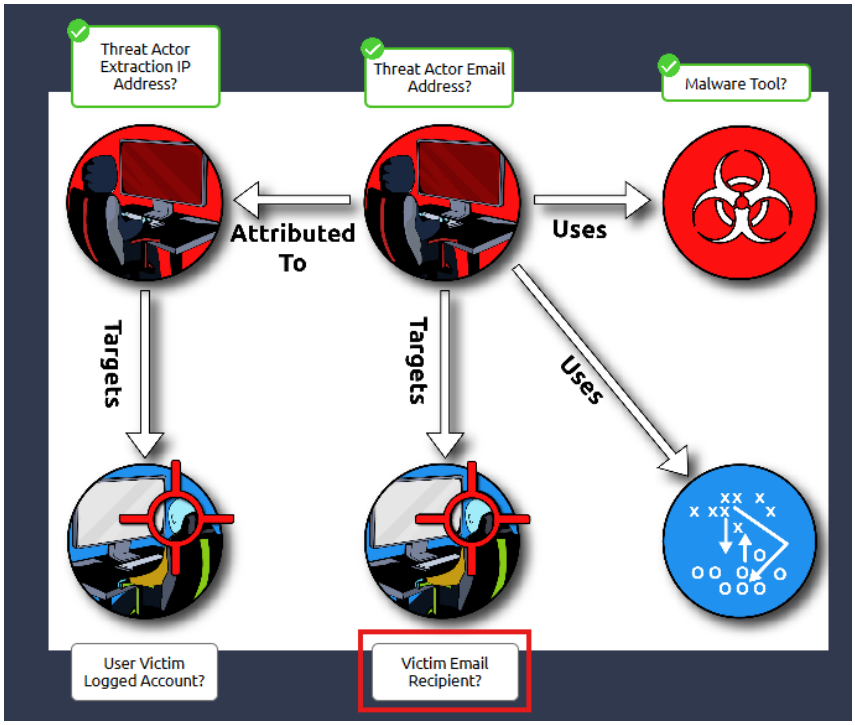


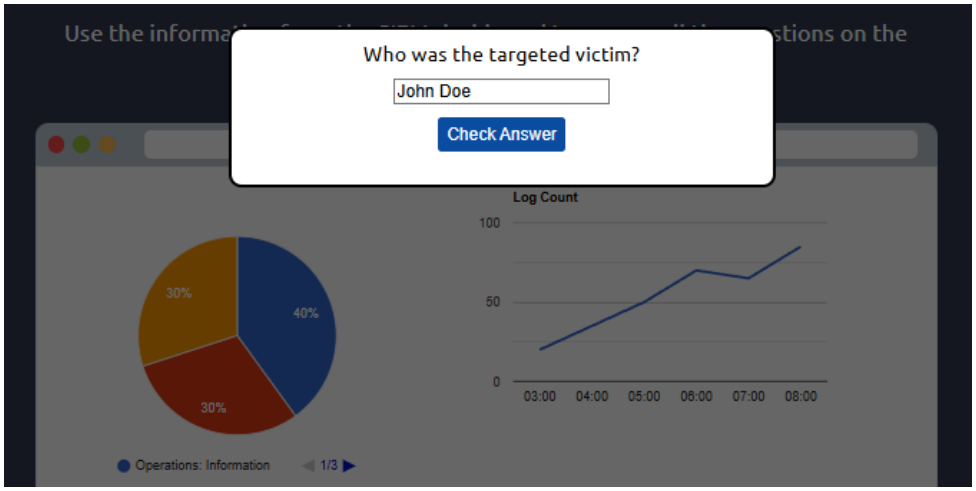
Pregunta: What was the name of the file downloaded?

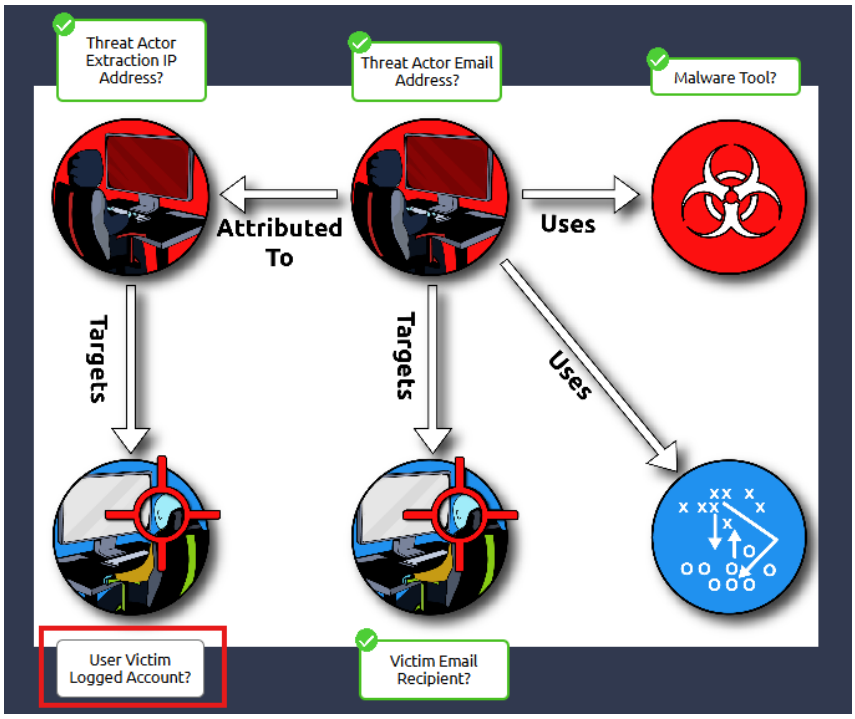


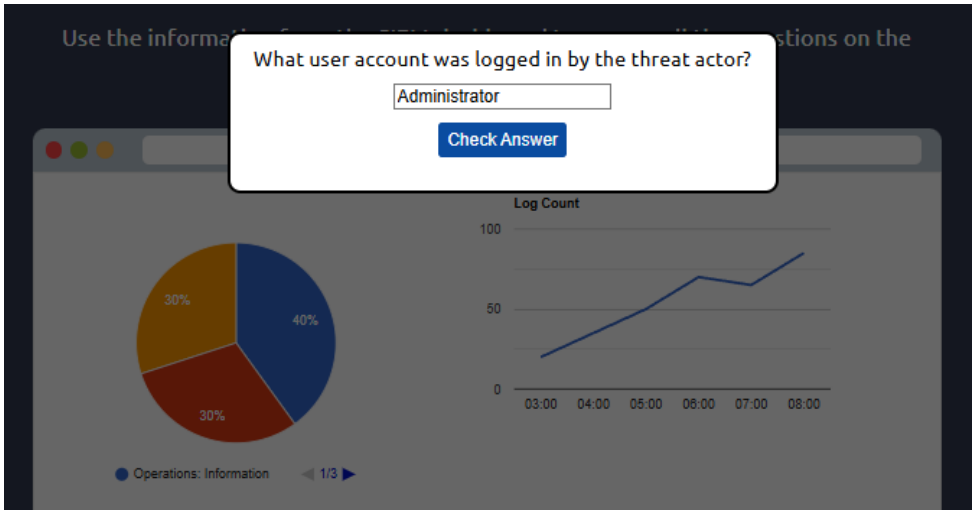


Respuesta: flbpfuh.exe

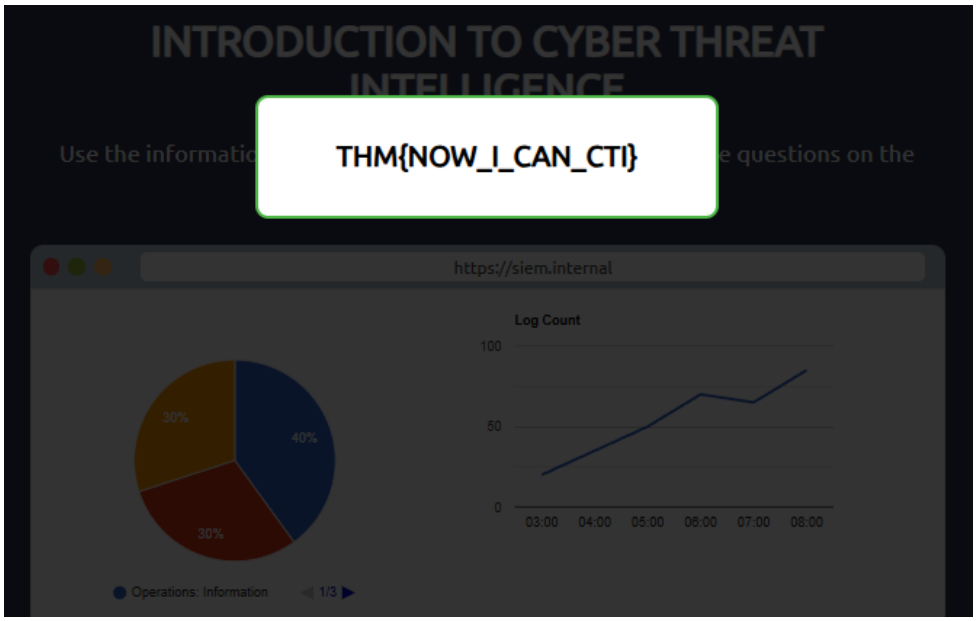








Una vez que completamos de responder correctamente todas las preguntas, obtendremos la flag para lograr completar la tarea.



Pregunta: After building the threat profile, what message do you receive?
Respuesta: **THM{NOW_I_CAN_CTI}**

3. Conclusión sobre la Sala

Al finalizar la sala, logramos aprender a diferenciar los tipos de CTI, a reconocer las etapas del ciclo de vida del análisis de amenazas, y a utilizar marcos como MITRE ATT&CK, STIX y el modelo Diamond.