Práctica windows.

La primera parte de la práctica consiste en hacer un análisis de dicha máquina utilizando las herramientas proporcionadas a lo largo del curso.Además es muy importante indicar las herramientas utilizadas y cómo se ha llegado a obtener el resultado.

Tenemos la sospecha de que el usuario del equipo está sacando información de la compañía de su equipo y además el equipo de monitorización ha levantado una alerta indicando comportamientos extraños en el equipo, por ello nos han llamado para que analicemos el equipo y podamos determinar qué indicios y evidencias existen sobre las sospechas fundadas.

Además deberéis de registraros en la página **ctf.sancastell.me** utilizando el código de registro **Keepcoding2023/***

Dentro encontrareis una serie de retos que responder.

Es necesario al finalizar los retos entregar una memoria indicando cómo se han hallado y las herramientas utilizadas.

Práctica memoria Ram

Para este apartado de la práctica, debéis de hacer una adquisición de memoria ram sobre el sistema operativo a vuestra elección.

Se deberán indicar los pasos seguidos para la realización de la adquisición, así como la ejecución de mínimo dos comandos con volatility.

Práctica Metadatos

La idea de este ejercicio es examinar cómo las plataformas de mensajería quitan una serie de metadatos cuando las enviamos entre unas y otras.
Necesito que hagáis una prueba con una foto vuestra:

1. Miréis los metadatos que tiene inicialmente
2. La envíen por whatsapp y los volváis a mirar
3. La envíen por telegram y lo volváis a comparar
4. La enviéis por email y la comparais

Yo os he dado 3 ejemplos, si se os ocurre otro mecanismo en el que podáis probar, usado, se valorará positivamente.