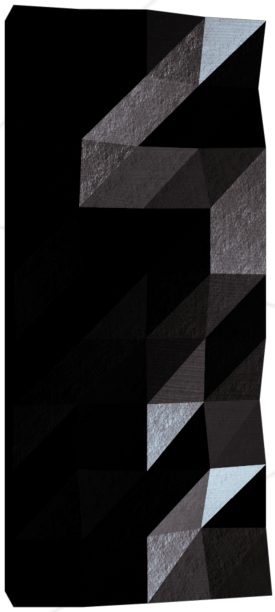

Bootcamp Ciberseguridad | 42

recovery

Resumen: Recolección de evidencias

Versión: 1

Índice general

Capítulo I

Prólogo

Creo que los virus informáticos deberían contar como vida. Creo que dice bastante sobre nosotros el hecho de que la única forma de vida que hemos logrado crear sea puramente destructiva. Hemos creado vida basada en nuestra imagen.

Source: https://es.wikipedia.org/wiki/Kevin_Mitnick

Capítulo II

Introducción

`Recovery`

La recolección de evidencias es una parte fundamental en la realización de un forense. Disponer de la información claray organizada es algo que puede facilitar la labor del forense. El objetivo de este proyecto es crear un programa que, dado un rango de fechas, sea capaz de extraer diversa información de un sistema Windows como la actividad del usuario, los programas abiertos, el historial de navegación, distinta información del registro de Windows... en dicho rango de tiempo.

`Instrucciones generales`

Trabajarás en todo momento sobre una máquina virtual de Windows 10. Puedes hacer uso de una máquina de Vagrant, por ejemplo, esta. Para desarrollar esta herramienta esta permitido usar cualquier lenguaje de programación (Recomendado Python). En caso de utilizar lenguajes compilados se debera entregar el código fuente y compilarlo durante la evaluación.

Puedes utilizar cualquier librería que te ayude a desarrollar la herramienta, siempre y cuando su uso pueda ser justificado durante la evaluación.

Capítulo III

Parte Obligatoria

III.1. Recovery

Se debe crear un programa que, dando un rango de tiempo, se pueda extraer información de interés para el forense, por ejemplo:

- Fechas de cambio de ramas de registro (CurrentVersionRun)
- Archivos recientes
- Programas instalados
- Programas abiertos
- Historial de navegación
- Dispositivos conectados
- Eventos de log

Si no se facilita un rango de tiempo, podría tomar un valor por defecto, por ejemplo, las últimas 24 horas, la última semana o el último mes.

Capítulo IV

Parte Bonus

La evaluación de los bonus se hará `SI Y SOLO SI` la parte obligatoria es `PERFECTA`. De lo contrario, los bonus serán totalmente `IGNORADOS`.

Puedes mejorar tu proyecto con las siguientes características:
Aunque la información recopilada puede ser mostrada por pantalla de manera ordenada en diferentes secciones, de manera opcional se pueden implementar las siguientes funcionalidades:

- Sealizar una línea temporal gráfica donde aparezcan todas evidencias organizadas en el tiempo y por categorías.
- Se puede mostrar el árbol de directorios del usuario de manera gráfica.

Capítulo V

Evaluación por pares

Este proyecto será corregido por tus compañeros. Entrega los archivos en el repositorio Git y asegúrate de que todo funciona como se espera.