TRABAJO PRÁCTICO N° 1: ANTIFORENSIA

Nombre del estudiante: Diego Castro

Fecha de elaboración: 20/04/2024

**1) Mencione un concepto distintivo del documento que Ud. haya encontrado aquí por primera vez, o sea: ¿que aprendió de nuevo?**

*The term forensics is significant and quite specific -- whatever AF is pertains to the scientific analysis of evidence for court.* La realidad es que todo me parece nuevo, lo que me ha quedado más claro el significado de anti-forensics.

**2) ¿Qué es la esteganografía? Mencione al menos 3 ejemplos**

Es la práctica de ocultar un mensaje secreto dentro (o incluso encima) de algo que no es secreto. Ejemplos: *Enmascaramiento, Algoritmos de la compresión de datos, Métodos de sustitución.*

**3) Busque en internet al menos 3 herramientas para limpieza de artefactos que no sea ninguna de las que cita el autor, señale la web de acceso a las herramientas encontradas.**

*Limpieza de disco: Darik's Boot and Nuke ( DBAN ) y Blancco Drive Eraser.*
*Eliminación de datos genéricos: CCleaner*
*Limpieza de archivos: BCWipe*

**4) Busque alguna noticia respecto de lo que el autor denomina "ofuscación del rastro", señale la web de acceso a la noticia y explique cuál fue la técnica de ofuscación utilizada.**

Consiste en ocultar o modificar el código fuente o el comportamiento de un programa malicioso para dificultar su detección o análisis por parte de los sistemas de seguridad o los expertos. La ofuscación puede emplear métodos como la compresión, el cifrado, la sustitución o la inserción de código basura.
Noticia:https://blog.segu-info.com.ar/2018/09/descubren-nuevos-modulos-para-la-botnet.html?m=0

**5) Acerca de los ataques contra las herramientas forenses, identifique las debilidades atribuibles a los desarrolladores de estas herramientas que cita el autor, y elabore una opinión al respecto, como si Ud. fuera uno de esos desarrolladores.**

Diría que es por un mal diseño del software y falta de conocimientos de algunas técnicas al momento de escribir el código y por no pasar por un proceso de testing.

**6) Explique la formulación matemática que hace el autor respecto de la "antiforensia sensible al tiempo"**

La fórmula sugiere que la información o el sistema están diseñados de tal forma que su estado o sus propiedades varían con el tiempo de una manera que dificultará la recuperación o el análisis forense. Probablemente *PSt* esté relacionado con la forma en que se almacena, se codifica o se procesa la información de manera que sea difícil de interpretar o de utilizar en un momento posterior.