Facultad de Informática	Módulo 1 (Curso 2020/21): Análisis forense de sistemas. Auditoría Informática II	

Nombre y Apellidos: ……..

Tarea1

1. Prácticas de Análisis Memoria
   - **a.** Objetivo
     - i. Adquirir área de memoria de un proceso.
     - ii. Analizar información área memoria de un proceso.
   - **b.** Documentación principal
     - i. PMDUMP (wwww.ntsecurity.nu)
     - ii. STRINGS (Sysinternal de Microsoft)
     - iii. MEMPASS.EXE (www.securitytube.net)
   - **c.** Documentación auxiliar
     - i. www.ntsecurity.nu
     - ii. www.securitytube.net
     - iii. https://docs.microsoft.com/es-es/sysinternals/
     - iv. Presentación módulo AI2_01

Desarrollo

1. Logística

Los alumnos podrán realizar la Tarea por equipos de 2-3 personas. Si se desea la práctica se puede realizar de forma individual. Descargarán las aplicaciones, programas y utilidades necesarias de las direcciones indicadas u otras que estime el alumno.

2. Desarrollo. Análisis de Memoria
   a. Proceso
      i. Se ejecutará el proceso MEMPASS introduciendo como contraseña el segundo apellido de uno de los miembros del equipo.
      ii. Se obtendrá una imagen de la evidencia digital "área de memoria del proceso MEMPASS".
      iii. Se obtendrá un hash de la evidencia con la utilidad que seleccione cada equipo.
      iv. Se analizará la evidencia digital intentando constatar información sensible (contraseña)
      v. Se generará un informe con los resultados detallados explicando los métodos y acciones seguidos en el análisis forense realizado.
   b. Uno de los miembros del equipo subirá un ZIP con el informe de resultados. Es deseable que se ponga gran interés tanto en el contenido como en el continente. En el informe se incluirá, además de lo indicado en el punto anterior, la siguiente información:
      i. Identificación de los alumnos.
      ii. Explicación y análisis detallado del laboratorio o escenario de análisis forense.

iii. Explicación detallada de las acciones realizadas en las fases:
    1. Evaluar
    2. Adquirir
    3. Analizar
    4. Informar
iv. Evidencias digitales, hash de las mismas y método para obtener estos hash. Los ficheros de cada una de las evidencias se incluirán en el ZIP.

c. Entregable. ZIP con al menos:
    i. Informe
    ii. Evidencias digitales