INFORME PRÁCTICA 1

Markel Alvarez Martinez

Pablo Alvarez Garcia

1. **Evaluar**

   Vamos a evaluar la información almacenada en el espacio de memoria reservado para el proceso de *mempass*. Una vez tengamos esa información podemos observar los datos y ver que información sensible que no debería mostrarse encontramos.

2. **Adquirir**

   Ejecutamos en un terminal el programa mempass.exe con la contraseña:

```
C:\Users\Administrator\Desktop>mempass.exe
Please enter your password:ALVAREZ
```

   Ejecutamos en otra terminal el comando tasklist, para conocer el PID (ID del proceso) de mempass.exe:

```
C:\Users\Administrator\Desktop>tasklist

Nombre de imagen                PID Nombre de sesión Núm. de ses Uso de memor
========================= ======== ================ =========== ============
System Idle Process               0 Services                   0          8 KB
System                            4 Services                   0      2.412 KB
Registry                        124 Services                   0     43.660 KB
smss.exe                        516 Services                   0      1.188 KB
```

```
Taskmgr.exe                   14884 Console                    1     52.960 KB
cmd.exe                        9396 Console                    1      5.028 KB
conhost.exe                   13124 Console                    1     20.040 KB
mempass.exe                    7568 Console                    1      4.236 KB
cmd.exe                        7204 Console                    1      5.076 KB
cmd.exe                       15348 Console                    1      4.776 KB
```

3. Analizar

Ejecutamos en otra terminal el programa pmdump, generando el informe (informe.txt) de la región de memoria de mempass (paso 2):

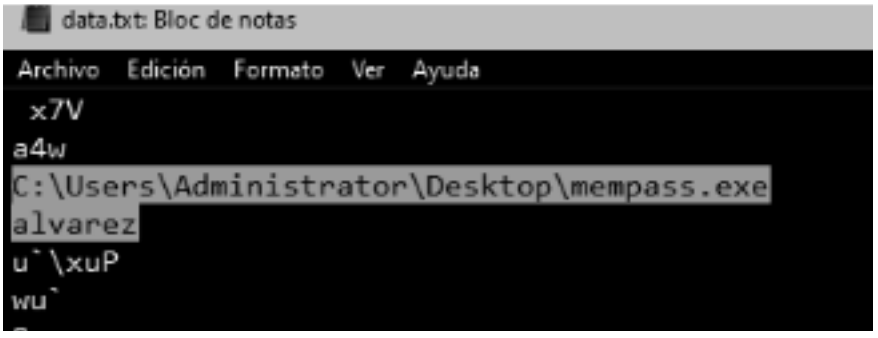
```
C:\Users\Administrator\Desktop>pmdump.exe 7568 Informe.txt
```

```
Name      Informe.txt
Size      8118272 bytes (7928 KiB)
CRC32     6D7E8DDF
CRC64     EB8FE2BD2DCA3D84
SHA256    8471676681D45A6361AD0A588B447893255FEDE6B20FF9229E0EA10065A00A23
SHA1      A3CAEE5FDAD71B42221CB38448DFC34B29D69644
BLAKE2sp  BB2268F5860A99440A7E4371BDFABF2F676DBB2345ACFB9D135C1A868DE12499
```

Ejecutamos en otra terminal el programa strings, redirigido a otro archivo de texto (data.txt), que será el archivo a analizar para el informe:

```
C:\Users\Administrator\Desktop>strings.exe Informe.txt > data.txt
```

Abrimos el archivo de texto generado (data.txt) con cualquier editor de texto, por ejemplo en bloc de notas, y lo analizamos en búsqueda de información sensible :




```
Name      data.txt
Size      2228860 bytes (2176 KiB)
CRC32     F602DBB1
CRC64     D969F1AA64488900
SHA256    5B41B3731DCE24A932ADE4EBD6AAEA379289BE01E16BEA483D4D0D49DA84E36E
SHA1      A37477E6FD7345B836517A5FD427E273CDE90FBB
BLAKE2sp  9EA7BBD76AB56361B792C632EDB9963D9C5F74B39E0C628557CC65DD2AB6939B
```

4. **Informar**

   Se crea el informe con los hallazgos pertinentes para ser entregado al cliente y pueda subsanar el problema.

   Para generar los hashes usamos la herramienta 7-Zip: