CÁTEDRA DE CIBERSEGURIDAD CIBERUGR, INCIBE-UGR

Nombre	Injection Breach
Categoría	Forense
Dificultad	Medio
Puntos	300

DESCRIPCIÓN DEL RETO

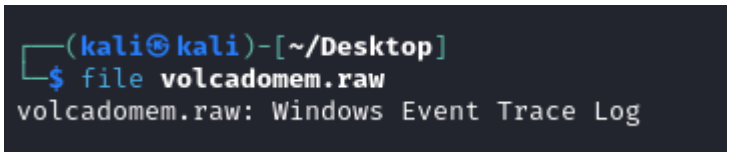
Se ha obtenido un volcado de memoria de un sistema comprometido. Hay indicios de actividad sospechosa en uno de los procesos, pero los detalles aún son desconocidos. Tu objetivo es analizar la memoria y revelar lo que sucedió.

WRITEUP

El análisis se va a realizar con la herramienta volatility3: (https://github.com/volatilityfoundation/volatility3)

1. Comprueba que tipo de archivo es el proporcionado. En función del resultado, usaremos volatility con comandos para Windows o Linux.

```
file volcadomem.raw
```



2. Lista los procesos que estaban en ejecución cuando se realizó el volcado:

```
vol -f volcadomem.raw windows.pslist
```

```
6732    4536    msedgewebview2  0xe505011a7080  14      -       1       False   2025-02-24 11:59:29.000000 UTC  N/A     Disabled
6920    776     RuntimeBroker.  0xe50501c61240  12      -       1       False   2025-02-24 11:59:30.000000 UTC  N/A     Disabled
3664    776     SearchApp.exe   0xe50501ad9340  30      -       1       False   2025-02-24 11:59:31.000000 UTC  N/A     Disabled
7492    776     UserOOBEBroker  0xe50501fce0c0  5       -       1       False   2025-02-24 11:59:34.000000 UTC  N/A     Disabled
7576    776     TextInputHost.  0xe505018b5080  12      -       1       False   2025-02-24 11:59:35.000000 UTC  N/A     Disabled
7940    776     backgroundTask  0xe505014b4300  15      -       1       False   2025-02-24 11:59:37.000000 UTC  N/A     Disabled
8100    776     WmiPrvSE.exe    0xe505019b40c0  13      -       0       False   2025-02-24 11:59:40.000000 UTC  N/A     Disabled
8152    776     RuntimeBroker.  0xe5050144c0c0  6       -       1       False   2025-02-24 11:59:40.000000 UTC  N/A     Disabled
8184    648     svchost.exe     0xe50501acb0c0  10      -       0       False   2025-02-24 11:59:40.000000 UTC  N/A     Disabled
5436    648     WmiApSrv.exe    0xe504fff9c080  5       -       0       False   2025-02-24 11:59:46.000000 UTC  N/A     Disabled
5584    648     NisSrv.exe      0xe50501748080  7       -       0       False   2025-02-24 11:59:46.000000 UTC  N/A     Disabled
6124    776     smartscreen.ex  0xe50500732080  9       -       1       False   2025-02-24 11:59:49.000000 UTC  N/A     Disabled
4792    4080    SecurityHealth  0xe5050076e080  6       -       1       False   2025-02-24 11:59:49.000000 UTC  N/A     Disabled
5980    648     SecurityHealth  0xe5050066c080  15      -       0       False   2025-02-24 11:59:49.000000 UTC  N/A     Disabled
6052    4080    vmtoolsd.exe    0xe50501a33080  10      -       1       False   2025-02-24 11:59:49.000000 UTC  N/A     Disabled
6084    4080    OneDrive.exe    0xe505018da080  45      -       1       False   2025-02-24 11:59:50.000000 UTC  N/A     Disabled
5484    776     FileCoAuth.exe  0xe50500669080  10      -       1       False   2025-02-24 11:59:53.000000 UTC  N/A     Disabled
7996    6084    Microsoft.Shar  0xe50501f0b240  0       -       1       False   2025-02-24 12:00:01.000000 UTC  2025-02-24 12:00:13.000000 UTC  Disabled
4480    776     PhoneExperienc  0xe5050279a300  26      -       1       False   2025-02-24 12:00:11.000000 UTC  N/A     Disabled
1096    776     dllhost.exe     0xe504ffdb7080  12      -       1       False   2025-02-24 12:00:31.000000 UTC  N/A     Disabled
2092    4080    cmd.exe 0xe505019e8080  2       -       1       False   2025-02-24 12:00:32.000000 UTC  N/A     Disabled
4736    2092    conhost.exe     0xe5050ece0080  5       -       1       False   2025-02-24 12:00:33.000000 UTC  N/A     Disabled
8036    776     backgroundTask  0xe505018f2080  12      -       1       False   2025-02-24 12:00:58.000000 UTC  N/A     Disabled
4500    776     backgroundTask  0xe50501f1c080  18      -       1       False   2025-02-24 12:00:58.000000 UTC  N/A     Disabled
5816    776     backgroundTask  0xe5050189e080  12      -       1       False   2025-02-24 12:00:58.000000 UTC  N/A     Disabled
4388    776     backgroundTask  0xe50501f20080  17      -       1       False   2025-02-24 12:00:58.000000 UTC  N/A     Disabled
1048    776     backgroundTask  0xe50501f15080  11      -       1       False   2025-02-24 12:00:58.000000 UTC  N/A     Disabled
768     776     RuntimeBroker.  0xe50501ee0080  8       -       1       False   2025-02-24 12:00:59.000000 UTC  N/A     Disabled
3612    776     RuntimeBroker.  0xe50501f2c080  6       -       1       False   2025-02-24 12:00:59.000000 UTC  N/A     Disabled
2596    1732    audiodg.exe     0xe505018d7300  7       -       0       False   2025-02-24 12:01:18.000000 UTC  N/A     Disabled
5528    4080    DumpIt.exe      0xe50501632080  3       -       1       True    2025-02-24 12:01:19.000000 UTC  N/A     Disabled
6012    648     svchost.exe     0xe50500fe2080  11      -       0       False   2025-02-24 12:01:19.000000 UTC  N/A     Disabled
3056    5528    conhost.exe     0xe505017f1080  6       -       1       False   2025-02-24 12:01:20.000000 UTC  N/A     Disabled
1284    648     sppsvc.exe      0xe505017e1080  8       -       0       False   2025-02-24 12:01:21.000000 UTC  N/A     Disabled
544     648     svchost.exe     0xe50501fcf080  9       -       0       False   2025-02-24 12:01:21.000000 UTC  N/A     Disabled
1556    648     svchost.exe     0xe50500d7e080  16      -       0       False   2025-02-24 12:01:22.000000 UTC  N/A     Disabled
4760    4080    secret_loader.  0xe50501f2e080  3       -       1       False   2025-02-24 12:01:29.000000 UTC  N/A     Disabled
4908    4760    conhost.exe     0xe505017e7080  6       -       1       False   2025-02-24 12:01:29.000000 UTC  N/A     Disabled
```

Nota: Hay dos que llaman la atención, “cmd.exe” y “secret_loader.exe”.

3. Como el proceso “cmd.exe” se estaba ejecutando, vamos a comprobar los comandos que se ejecutaron:

```
vol -f volcadomem.raw windows.cmdscan
```

```
m.raw windows.cmdscan
rk 2.11.0
        PDB scanning finished
oleInfo     Property        Address Data

    0x1bb860a73d0   _COMMAND_HISTORY        0x1bb860a73d0   None
    0x1bb860a73d0   _COMMAND_HISTORY.Application    0x1bb860a7400   cmd.exe
    0x1bb860a73d0   _COMMAND_HISTORY.ProcessHandle  0x1bb840c4cf0   0x138
    0x1bb860a73d0   _COMMAND_HISTORY.CommandCount   N/A     2
    0x1bb860a73d0   _COMMAND_HISTORY.LastDisplayed  0x1bb860a742c   1
    0x1bb860a73d0   _COMMAND_HISTORY.CommandCountMax        0x1bb860a73f8   50
    0x1bb860a73d0   _COMMAND_HISTORY.CommandBucket  0x1bb860a73e0
    0x1bb860a73d0   _COMMAND_HISTORY.CommandBucket_Command_0        0x1bb86356560   cd C:\Users\agran\OneDrive\Escritorio\dllinjector\DLL-Injector\Source\x64\Debug
    0x1bb860a73d0   _COMMAND_HISTORY.CommandBucket_Command_1        0x1bb86356580   "DLL Injector.exe" "C:\Users\agran\OneDrive\Escritorio\injection\payload.dll" secret_loader.exe
    0x1bb860a73d0   _COMMAND_HISTORY.CommandBucket_Command_8        0x1bb86356660
    0x1bb860a73d0   _COMMAND_HISTORY.CommandBucket_Command_23       0x1bb86356840
    0x213a877ea80   _COMMAND_HISTORY        0x213a877ea80   None
    0x213a877ea80   _COMMAND_HISTORY.Application    0x213a877eab0   DumpIt.exe
    0x213a877ea80   _COMMAND_HISTORY.ProcessHandle  0x213a67b58e0   0x12c
    0x213a877ea80   _COMMAND_HISTORY.CommandCount   N/A     0
    0x213a877ea80   _COMMAND_HISTORY.LastDisplayed  0x213a877eadc   -1
    0x213a877ea80   _COMMAND_HISTORY.CommandCountMax        0x213a877eaa8   50
    0x213a877ea80   _COMMAND_HISTORY.CommandBucket  0x213a877ea90
    0x1c59fd91b80   _COMMAND_HISTORY        0x1c59fd91b80   None
    0x1c59fd91b80   _COMMAND_HISTORY.Application    0x1c59fd91bb0   secret_loader.exe
    0x1c59fd91b80   _COMMAND_HISTORY.ProcessHandle  0x1c59dd56760   0x130
    0x1c59fd91b80   _COMMAND_HISTORY.CommandCount   N/A     0
    0x1c59fd91b80   _COMMAND_HISTORY.LastDisplayed  0x1c59fd91bdc   -1
```

Nota: Se puede ver que se ha utilizado un ejecutable, “DLL Injector.exe”, una DLL, “payload.dll” y un proceso “secret_loader.exe” (el que hemos visto antes en la lista de procesos). Parece ser que lo que se ha hecho es utilizar una herramienta para inyectar una DLL en un proceso.

4. Vamos a comprobar que efectivamente dicha DLL está cargada en el proceso. Para ello, utiliza el PID del proceso en el siguiente comando:

```
vol -f volcadomem.raw windows.dlllist --pid 4760
```

```
└─$ vol -f volcadomem.raw windows.dlllist --pid 4760
Volatility 3 Framework 2.11.0
Progress:  100.00               PDB scanning finished
PID     Process Base    Size    Name    Path    LoadTime        File output

4760    secret_loader.  0x7ff606890000  0x22000 secret_loader.exe       C:\Users\agran\OneDrive\Escritorio\injection\secre
4760    secret_loader.  0x7ffc83090000  0x1f8000        ntdll.dll       C:\Windows\SYSTEM32\ntdll.dll   2025-02-24 12:01:2
4760    secret_loader.  0x7ffc818c0000  0xc2000 KERNEL32.DLL    C:\Windows\System32\KERNEL32.DLL        2025-02-24 12:01:2
4760    secret_loader.  0x7ffc80b70000  0x2ff000        KERNELBASE.dll  C:\Windows\System32\KERNELBASE.dll      2025-02-24
4760    secret_loader.  0x7ffc82160000  0x9e000 msvcrt.dll      C:\Windows\System32\msvcrt.dll  2025-02-24 12:01:29.00000
4760    secret_loader.  0x7ffc37c80000  0x250000        libstdc++-6.dll C:\msys64\mingw64\bin\libstdc++-6.dll    2025-02-24
4760    secret_loader.  0x7ffc77db0000  0x2c000 libgcc_s_seh-1.dll      C:\msys64\mingw64\bin\libgcc_s_seh-1.dll        20
4760    secret_loader.  0x7ffc77d90000  0x15000 libwinpthread-1.dll     C:\msys64\mingw64\bin\libwinpthread-1.dll       20
4760    secret_loader.  0x7ffc80000000  0xc000  CRYPTBASE.DLL   C:\Windows\SYSTEM32\CRYPTBASE.DLL       2025-02-24 12:01:2
4760    secret_loader.  0x7ffc80ec0000  0x82000 bcryptPrimitives.dll    C:\Windows\System32\bcryptPrimitives.dll        20
4760    secret_loader.  0x7ffc6b8e0000  0x1f000 payload.dll     C:\Users\agran\OneDrive\Escritorio\injection\payload.dll
4760    secret_loader.  0x7ffc826a0000  0x19d000        USER32.dll      C:\Windows\System32\USER32.dll  2025-02-24 12:01:2
4760    secret_loader.  0x7ffc808e0000  0x22000 win32u.dll      C:\Windows\System32\win32u.dll  2025-02-24 12:01:29.00000
4760    secret_loader.  0x7ffc82200000  0x2b000 GDI32.dll       C:\Windows\System32\GDI32.dll   2025-02-24 12:01:29.00000
4760    secret_loader.  0x7ffc80910000  0x11a000        gdi32full.dll   C:\Windows\System32\gdi32full.dll       2025-02-24
4760    secret_loader.  0x7ffc80ad0000  0x9d000 msvcp_win.dll   C:\Windows\System32\msvcp_win.dll       2025-02-24 12:01:2
4760    secret_loader.  0x7ffc80730000  0x100000        ucrtbase.dll    C:\Windows\System32\ucrtbase.dll        2025-02-24
4760    secret_loader.  0x7ffc81120000  0x2f000 IMM32.DLL       C:\Windows\System32\IMM32.DLL   2025-02-24 12:01:29.00000
4760    secret_loader.  0x7ffc6b160000  0xae000 TextShaping.dll C:\Windows\SYSTEM32\TextShaping.dll     2025-02-24 12:01:2
4760    secret_loader.  0x7ffc7e0e0000  0x9e000 uxtheme.dll     C:\Windows\system32\uxtheme.dll 2025-02-24 12:01:29.00000
4760    secret_loader.  0x7ffc82a80000  0x355000        combase.dll     C:\Windows\System32\combase.dll 2025-02-24 12:01:2
4760    secret_loader.  0x7ffc81fa0000  0x123000        RPCRT4.dll      C:\Windows\System32\RPCRT4.dll  2025-02-24 12:01:2
```

5. Para poder ver el contenido de la DLL, necesitaremos volcar la memoria asignada al proceso. Utiliza el siguiente comando:

```
vol -f volcadomem.raw windows.memmap --dump --pid 4760
```

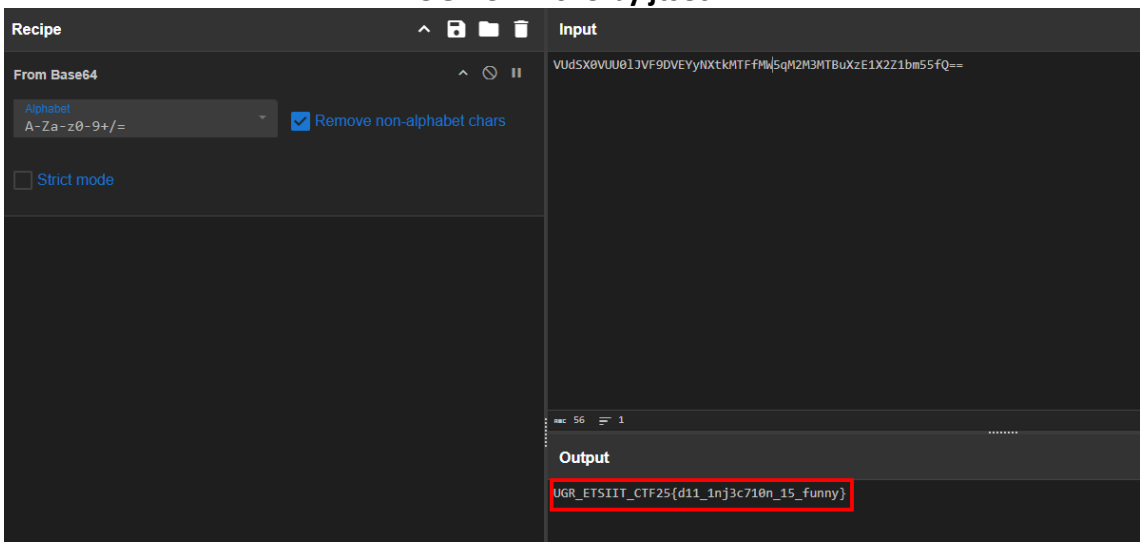
Nota: Esto creará un archivo de nombre “pid.4760.dmp” en el mismo directorio donde se ejecute el comando.

6. Una vez tenemos el volcado de la memoria del proceso, para ver su contenido podemos utilizar la utilidad “strings” para ver las cadenas de texto imprimibles. Analizando su contenido, podemos ver una línea que dice “Esta es la flag” y una cadena en base 64.

```
strings pid.4760.dmp
```

```
_flag
_flag
flags
_flag
_ZSt9call_onceIMSt6thread FvvEJPS0_EEvRSt9once_flagOT_DpOT0_
_ZStlsIcSt11char_traitsIcEERSt13basic_ostreamIT_T0_ES6_St12_Setios flags
Esta es la flag: VUdSX0VUU0lJVF9DVEYyNXtkMTFfMW5qM2M3MTBuXzE1X2Z1bm55fQ==
fegetexceptflag
fesetexceptflag
flags
flags
flags
SXS: %s() Bad flags/size 0x%lx/0x%lx
flag
execution_flags
execution_flags
execution_flags
execution_flags
An invalid combination of regular expression syntax flags was used.
An invalid combination of regular expression syntax flags was used.
ZlF0Cg8XYxakN3SLd5JTLUbJMGEGbTFhmP5dnprf3b29nBfDlgQ9N+0nupXSy0fr7ziddBJ8BcswXLC+Ota0K76CEUIzZ/8DNLBhMI
8VUy67Gh4IyiGb91ZynQ8TxyMD44uC4g7f7AXXWh8Iw3gqpG0hffqRCNLfmoB1Yk5hT8AbhWUQ77gLJvffo9T2DPgNNawDyh3q6AxO
/mx:renderer><sl:productIdRange xmlns:sl="http://www.microsoft.com/DRM/XrML2/SL/v2" value="{4de7cb65-c
2"><sl:type>msft:sl/externalValidator/generic</sl:type><sl:data Algorithm="msft:rm/algorithm/flags/1.0
.org/2000/09/xmldsig#"><SignedInfo><CanonicalizationMethod Algorithm="http://www.microsoft.com/xrml/lw
thm="urn:mpeg:mpeg21:2003:01-REL-R-NS:licenseTransform"/><Transform Algorithm="http://www.microsoft.co
```

7. La flag está codificada en base64, ve a Cyberchef (https://gchq.github.io/CyberChef/) y decodifícala:



8. Otra forma de obtener la flag es extraer la DLL inyectada y ver su contenido. Para ello, recuperamos los archivos que había en memoria de la siguiente forma

```
vol -f volcadomem.raw windows.filescan > data/filescan
```

Nota: El resultado se almacena en un archivo llamado “filescan”, ubicado en el directorio data.

9. Una vez que tenemos los archivos, nos aseguramos de que entre ellos figure la DLL que vimos antes:

```
cat data/filescan | grep "payload"
```

10. Vamos a volcar el contenido de la DLL. Para ello, utiliza el siguiente comando, usando el offset que aparece en el comando anterior (da igual cual utilices de los dos, son el mismo archivo):

```
vol -f volcadomem.raw -o data windows.dumpfiles --virtaddr
0xe505029f6210
```

11. Ahora, utilizamos la utilidad “strings” para analizar el contenido del archivo:

```
strings
data/file.0xe505029f6210.0xe505017c6800.ImageSectionObject
.payload.dll.img
```

```
([^_]
WVSH
 [^_
Se ha ejecutado la DLL maliciosa!
Esta es la flag: VUdSX0VUU0lJVF9DVEYyNXtkMTFfMW5qM2M3MTBuXzE1X2Z1bm55fQ==
Mingw-w64 runtime failure:
Address %p has no image-section
  VirtualQuery failed for %d bytes at address %p
  VirtualProtect failed with code 0x%x
  Unknown pseudo relocation protocol version %d.
  Unknown pseudo relocation bit size %d.
%d bit pseudo relocation at %p out of range, targeting %p, yielding the val
```

12. Como antes, decodificamos la flag: