Meta4Sec, k.eii's official WU

LapisLegit [FINAL]

Meta4Sec{th1s_B1rB_l0v3_t0_l3aRn_F0ren51cS}

```
Volatility 3 Framework 2.7.1
Progress:  100.00               PDB scanning finished
Variable        Value

Kernel Base     0xf80745a1f000
DTB     0x1aa000
Symbols file:///home/jons/tools/volatility3/volatility3/sy
json.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 WindowsCrashDump64Layer
base_layer      2 FileLayer
KdVersionBlock  0xf8074662e400
Major/Minor     15.19041
MachineType     34404
KeNumberProcessors      1
SystemTime      2024-08-01 08:03:28
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion  10
PE MinorOperatingSystemVersion  0
PE Machine      34404
PE TimeDateStamp        Mon Dec  9 11:07:51 2019
```

k.eii's POC:

Firstly, scan the processes, notice there are 2 programs running (notepad and MS paint). I intendedly add MS paint as a decoy, the main objective is in the notepad

using vol notepad plugin, notice that it contains docker

```
torage.dll,-21770 5 .txt F C:\Users\Doli\Pictures\desktop.ini 8 ; 3 @ 2 TextInputServer TextInputServer r C:\Windows\sys
tem32\urlmon.dll CoreUIComponents ParkedProxyOwner C:\Windows\system32\iertutil.dll C:\Windows\system32\netutils.dll 0 C
:\Windows\system32\srvcli.dll 0 ExternalComOwner > ! fy + r Ed Memory Mapped Cache Mgr D O ; / # / / # # / url / / url #
 H % / ; G Y k $ , 4U 7 L [m )     C:\Users\Doli\Documents\data\notes.txt C:\Users\Doli\Documents\data\notes.txt ' ) < >
f h /C:/Users/Doli/Documents/data/notes.txt /C:/Users/Doli/Documents/data/notes.txt 8 windowspropertydescriptions C:\Win
dows\SYSTEM32\policymanager.dll C:\Windows\system32\msvcp110_win.dll -1001 210 53 01    \BaseNamedObjects C:\Users\Doli\D
ocuments\data\notes.txt 1001     @ C:\Users\Doli\Music\desktop.ini   3 L -f S S \BaseNamedObjects\[CoreUI]-PID(3204)-TID
(3252) 9ea23626-ffdb-4dd7-84a4-30c9ebe9bf29 7 \BaseNamedObjects\[CoreUI]-PID(4460)-TID(6164) a64f6972-532f-4d36-97af-f50
f4664f7db     ) @ lor   .txt @ ( @ dummy://url/ Notepad          8 8 8 8 Consolas nsole ER\S 6371-756753964-2940938769-
1001 ` ' k.eii ganteng i need to decrypt it FROM ubuntu:20.04 LABEL maintainer="k.eii.sni@gmail.com" RUN apt-get update
&& \     apt-get install -y openssl coreutils && \     rm -rf /var/lib/apt/lists/* COPY "MyProject" /app/MyProject WORKD
IR /app/My_Project CMD ["bash"] < d3-8 \DosDevices\D: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\System Tools\
desktop.ini Notepad ` `     ' ' . . & i :< 7 7 C:\Windows\SYSTEM32\ole32.dll l o C D r t j C h m s A p f ( q P1 s< . Use
rs N1 : . Doli \1 sD . Documents k g n C:\Windows\system32\NOTEPAD.EXE # = & 2  # > )   = ) ) 2 = dummy://url C:\Windows
 r NTFS calendar Contact Microsoft er dummy document NTFS file .txt about:blank document Contact email Email NOTEPAD.EXE
 text/plain Calendar E-mail Game r feed Feed contact about folder Feed Document Folder Folder Calendar C:\Windows Docume
nt blank about:blank game blank Game Change Software\Policies\Microsoft\Internet Explorer\Main ff Software\Policies\Micr
osoft\Internet Explorer\Main ff 2 C:\Users\Doli\Documents\desktop.ini C:\Windows\System32\COMDLG32.dll C:\Windows\system
```

from the dockerfile readed by notepad try to look for the files "MyProject"

when searching for it, found '25fqjks81ce9sowwz0x9u1ouj' folder, dump the files from it (disk.enc and key.bin)

```
┌──(jons㉿01-20-jonathans)-[~/tools/volatility3]
└─$ sudo python3 vol.py -f memory.dmp windows.filescan | grep "MyProject"
0x8a8ebdf9e9b0.0\Users\Doli\Documents\data\25fqjks81ce9sowwz0x9u1ouj\diff\app\MyProject\disk.enc       216
0x8a8ebeb7b7a0  \Users\Doli\Documents\data\25fqjks81ce9sowwz0x9u1ouj\diff\app\MyProject 216
0x8a8ebeb7c100  \Users\Doli\Documents\data\25fqjks81ce9sowwz0x9u1ouj\diff\app\MyProject 216
0x8a8ebf525460  \Users\Doli\Documents\data\25fqjks81ce9sowwz0x9u1ouj\diff\app\MyProject\key.bin 216
```

poc:

1. analyze the key.bin's length (64 byte), it was encrypted using 256 bit aes.

```
┌──(jons㉿01-20-jonathans)-[~/tools/volatility3]
└─$ sudo xxd file.0x8a8ebf525460.0x8a8ebafb4d10.DataSectionObject.key.bin.dat
00000000: 2599 0e93 498d fc1c e72b 1100 12b3 57e0  %...I....+....W.
00000010: 46f4 c5c5 cbf7 894b b9e0 a2c6 882f ea19  F......K...../..
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
```

2. openssl enc -d -aes-256-cbc -in disk.enc -out decrypted -pass file:./key.bin

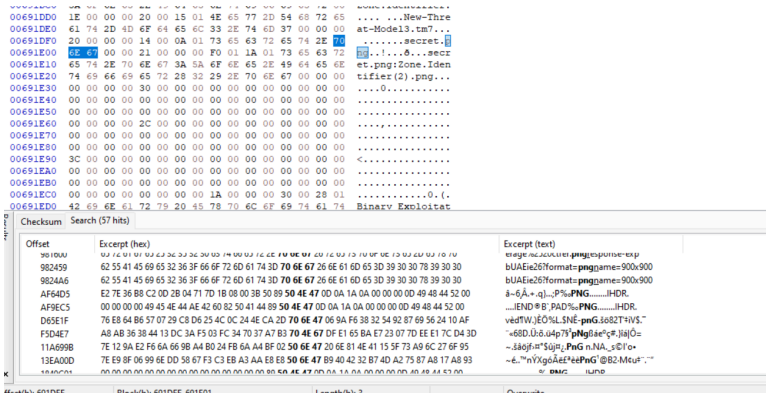
3. because of ram parsing, the key and encrypted file is padded with null bytes (00s), don’t forget to clean it before decrypting or else you wont be able to decrypt it

```
┌──(jons㉿01-20-jonathans)-[~/tools/volatility3]
└─$ sudo xxd file.0x8a8ebf525460.0x8a8ebafb4d10.DataSectionObject.key.bin.dat
00000000: 2599 0e93 498d fc1c e72b 1100 12b3 57e0  %...I....+....W.
00000010: 46f4 c5c5 cbf7 894b b9e0 a2c6 882f ea19  F......K...../..
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000030: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000040: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000050: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000060: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000070: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000080: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000090: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000b0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000c0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000d0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000e0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000f0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000100: 0000 0000 0000 0000 0000 0000 0000 0000  ................
```

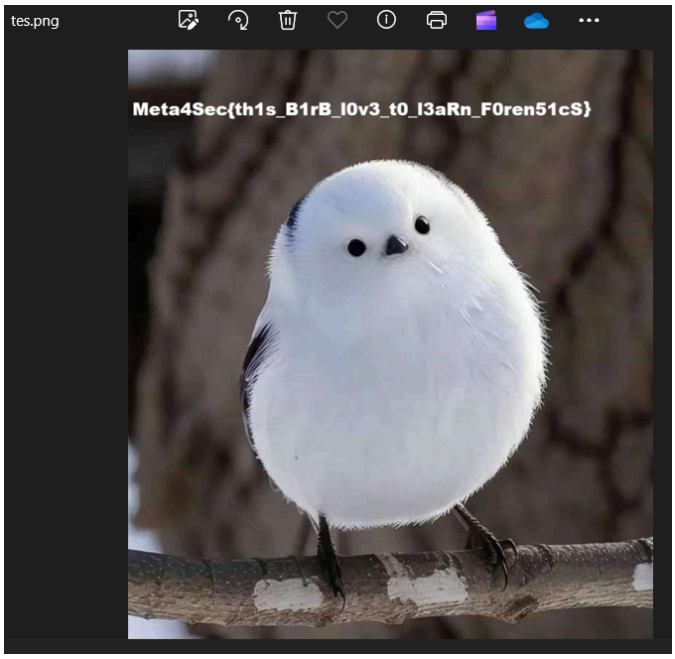
4. got .rar file from disk.enc

5. after extracting it you'll get a .dd file

6. there are some files in it some of them is images, dump the files by parsing the hexes (i use HxD, copy and paste the hex of the files and create a new file with it)



7. flag is found as png

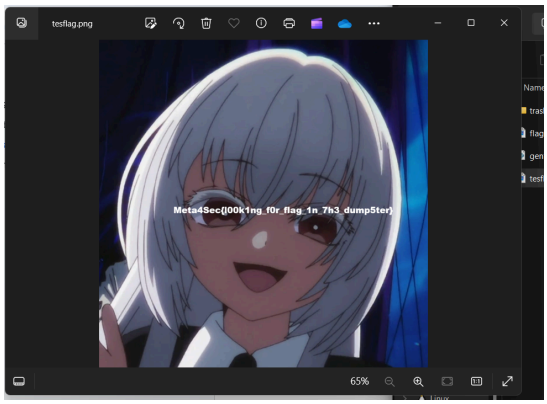


Trashbag [QUALS]

just use grep, the flag used is png and then you just need to combine the hexes

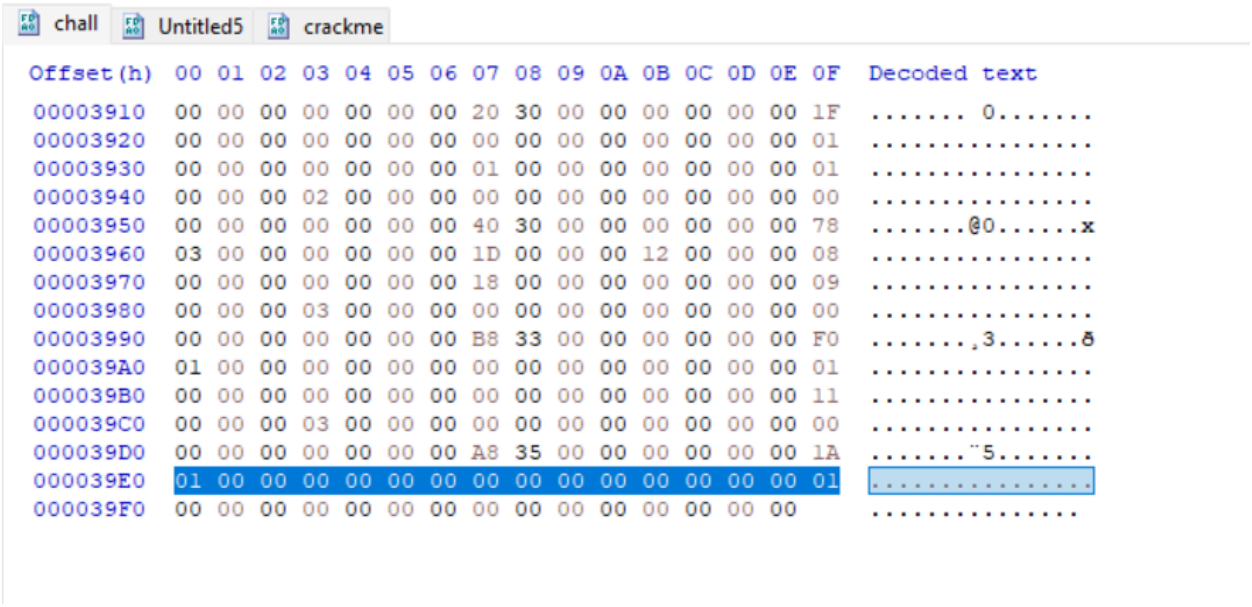
```
┌──(jons㉿01-20-jonathans)-[~/gudangchall/Meta4Sec/trashbag]
└─$ grep -r "PNG" trashbag
grep: trashbag/B3JmSUwPES/B3JmSUwPES: binary file matches

┌──(jons㉿01-20-jonathans)-[~/gudangchall/Meta4Sec/trashbag]
└─$ grep -r "IDAT" trashbag
grep: trashbag/B3JmSUwPES/B3JmSUwPES: binary file matches
grep: trashbag/JLRCWmPe1E/JLRCWmPe1E: binary file matches
grep: trashbag/O2lzPyiGZd/O2lzPyiGZd: binary file matches
```



FLE [FINAL]

EOF of an ELF is marked with 16 bytes that start with 01 ended with 01 and being continued with 15 null bytes



ELF file header, before entering the GLIBC setting will be marked with 16 bytes that contains 01 and 22. after that will be continued with null bytes and then entering the memory mapping of the ELF

Here, I just swap the position of the ELF file header under the EOF and then move the chunk of the EOF after the ELF file header. It is supposed to be easy.

if you have successfully recovered the ELF, you just need to run it and the flag will be printed out.

the flag is written in Octal, you can use cyberchef/dcode.fr

↑↓	↑↓
OCT /N	Meta4Sec{f1x1ng_a_ELF_f1le}