Mission Name

DumperClearance

History Background

Ethan and Claire hack their clearance status to grant them a global departure with their own recon car.

Technical High-Level Overview

A memory dump from a computer connected to a system that manages authorizations is provided to the player. This memory dump contains a password that allow to modify Claire and Ethan permissions to fly.

Short Description

Your goal is to analyse a memory dump from a computer connected to Skytech Flight Authorization System and get a password inside a file created with Notepad.

Mission Description

Your goal is to analyse a memory dump from a computer connected to Skytech Flight Authorization System and get a password inside a file created with Notepad. This memory dump contains a password that allow to modify Claire and Ethan permissions to fly.

Location

SYLVARCON | PORT 2 | INTERNATIONAL TRANSIT ZONE

Tools

- Volatility

Questions

Which is the parent process identifier (PPID) of cmd.exe?

- 2304

Which is process identifier of notepad.exe?

- 732

Which is the IP address used to connect to port 80?

- 93.184.220.29

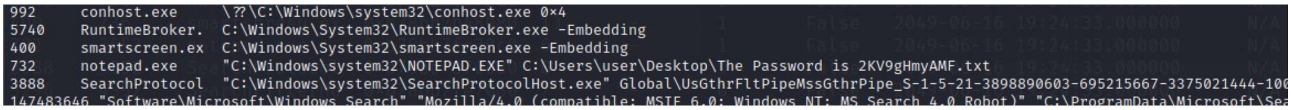
Hints

1. Use image command on Volatility to identify Volatility´s Memory Profile
2. Use the following profile Win10x64_18362
3. Use cmdline command on volatility to identify the password on Notepad.

Write Up

LinuxMethod—Vol3

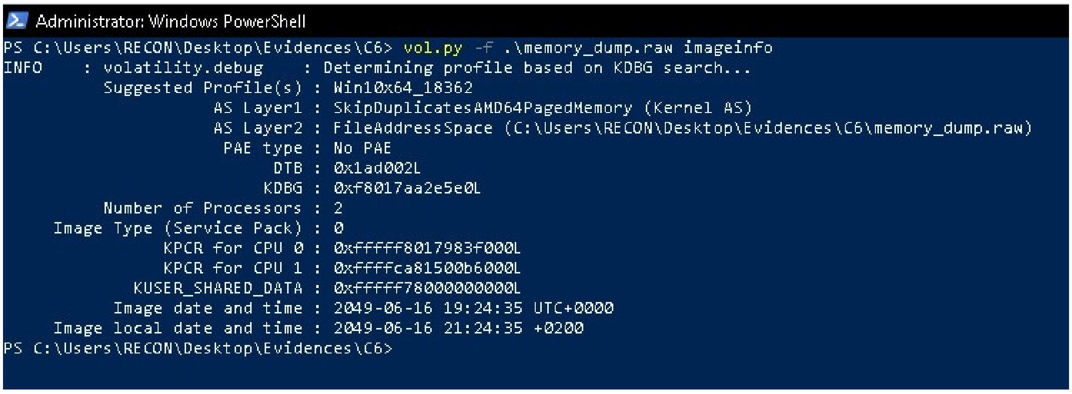
- https://book.hacktricks.xyz/forensics/basic-forensic-methodology/memory-dump-analysis/volatility-examples
- python3 vol.py -f file.dmp windows.pstree.PsTree # Get processes tree (not hidden)
- python3 vol.py -f file.dmp windows.pslist.PsList # Get process list (EPROCESS)
- python3 vol.py -f file.dmp windows.psscan.PsScan # Get hidden process list(malware)
- python3 vol.py -f file.dmp windows.cmdline.CmdLine



```
992      conhost.exe     \??\C:\Windows\system32\conhost.exe 0×4
5740     RuntimeBroker.  C:\Windows\System32\RuntimeBroker.exe -Embedding
400      smartscreen.ex  C:\Windows\System32\smartscreen.exe -Embedding
732      notepad.exe     "C:\Windows\system32\NOTEPAD.EXE" C:\Users\user\Desktop\The Password is 2KV9gHmyAMF.txt
3888     SearchProtocol  "C:\Windows\system32\SearchProtocolHost.exe" Global\UsGthrFltPipeMssGthrPipe_S-1-5-21-3898890603-695215667-3375021444-100
147483646 "Software\Microsoft\Windows Search" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT; MS Search 4.0 Robot)" "C:\ProgramData\Microsoft\Sea
```

Figure 1

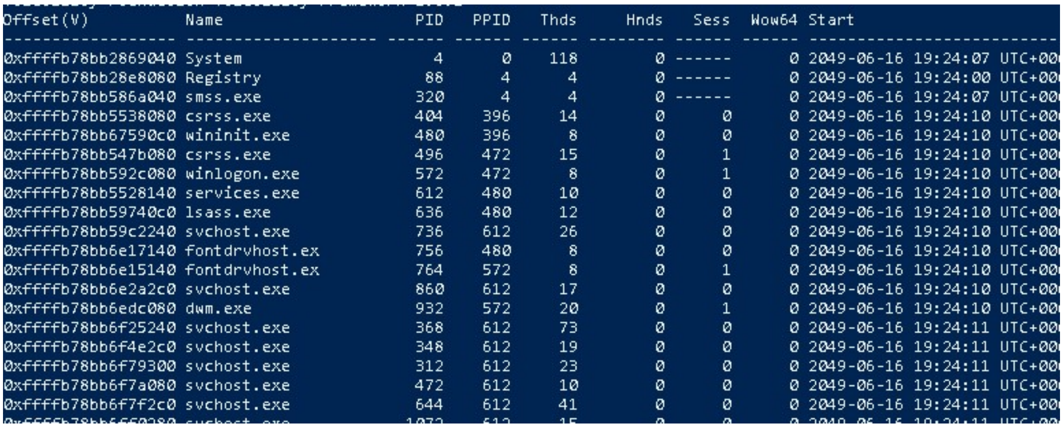
Player should use Volatility application instead of string command to get the password. First of all, player should identify which Version of Windows, launching the following command: vol.py -f .\memory_dump.raw imageinfo



```
PS C:\Users\RECON\Desktop\Evidences\C6> vol.py -f .\memory_dump.raw imageinfo
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win10x64_18362
                     AS Layer1 : SkipDuplicatesAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\Users\RECON\Desktop\Evidences\C6\memory_dump.raw)
                      PAE type : No PAE
                           DTB : 0x1ad002L
                          KDBG : 0xf8017aa2e5e0L
          Number of Processors : 2
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0xfffff8017983f000L
                KPCR for CPU 1 : 0xffffca81500b6000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2049-06-16 19:24:35 UTC+0000
     Image local date and time : 2049-06-16 21:24:35 +0200
PS C:\Users\RECON\Desktop\Evidences\C6>
```

Figure 2

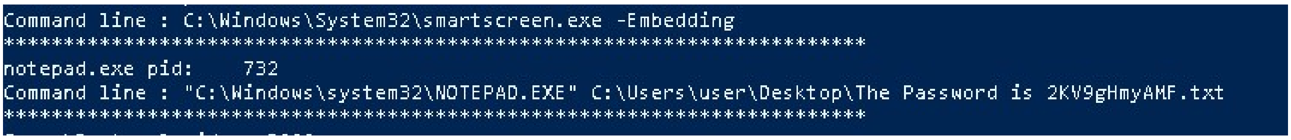
We check that profile works, launching pslist command: vol.py -f .\memory_dump.raw --profile=Win10x64_18362 pslist



```
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------
0xffffb78bb2869040 System                    4      0    118        0 ------      0 2049-06-16 19:24:07 UTC+00
0xffffb78bb28e8080 Registry                 88      4      4        0 ------      0 2049-06-16 19:24:00 UTC+00
0xffffb78bb586a040 smss.exe                320      4      4        0 ------      0 2049-06-16 19:24:07 UTC+00
0xffffb78bb5538080 csrss.exe               404    396     14        0      0      0 2049-06-16 19:24:10 UTC+00
0xffffb78bb67590c0 wininit.exe             480    396      8        0      0      0 2049-06-16 19:24:10 UTC+00
0xffffb78bb547b080 csrss.exe               496    472     15        0      1      0 2049-06-16 19:24:10 UTC+00
0xffffb78bb592c080 winlogon.exe            572    472      8        0      1      0 2049-06-16 19:24:10 UTC+00
0xffffb78bb5528140 services.exe            612    480     10        0      0      0 2049-06-16 19:24:10 UTC+00
0xffffb78bb59740c0 lsass.exe               636    480     12        0      0      0 2049-06-16 19:24:10 UTC+00
0xffffb78bb59c2240 svchost.exe             736    612     26        0      0      0 2049-06-16 19:24:10 UTC+00
0xffffb78bb6e17140 fontdrvhost.ex          756    480      8        0      0      0 2049-06-16 19:24:10 UTC+00
0xffffb78bb6e15140 fontdrvhost.ex          764    572      8        0      1      0 2049-06-16 19:24:10 UTC+00
0xffffb78bb6e2a2c0 svchost.exe             860    612     17        0      0      0 2049-06-16 19:24:10 UTC+00
0xffffb78bb6edc080 dwm.exe                 932    572     20        0      1      0 2049-06-16 19:24:10 UTC+00
0xffffb78bb6f25240 svchost.exe             368    612     73        0      0      0 2049-06-16 19:24:11 UTC+00
0xffffb78bb6f4e2c0 svchost.exe             348    612     19        0      0      0 2049-06-16 19:24:11 UTC+00
0xffffb78bb6f79300 svchost.exe             312    612     23        0      0      0 2049-06-16 19:24:11 UTC+00
0xffffb78bb6f7a080 svchost.exe             472    612     10        0      0      0 2049-06-16 19:24:11 UTC+00
0xffffb78bb6f7f2c0 svchost.exe             644    612     41        0      0      0 2049-06-16 19:24:11 UTC+00
```

Figure 3

Considering, player knows that password must be located in a file created with Notepad, the easy way to achieve this challenge would be launching Volatility with "cmdline" option. vol.py -f .\memory_dump.raw --profile=Win10x64_18362 cmdline



```
Command line : C:\Windows\System32\smartscreen.exe -Embedding
************************************************************************
notepad.exe pid:    732
Command line : "C:\Windows\system32\NOTEPAD.EXE" C:\Users\user\Desktop\The Password is 2KV9gHmyAMF.txt
************************************************************************
```

Figure 4

Finally player could get the password: 2KV9gHmyAMF

Flag Information

flag{2KV9gHmyAMF}