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. Keep in mind, password is unencrypted and it´s related to the use logs in the Skytech Flight Authorization Server.

Mission Description

Your goal is to analyse a memory dump from a computer connected to Skytech Flight Authorization System and get a password. This memory dump contains a password that allow to modify Claire and Ethan permissions to fly and it´s related with user who logs in the computer. You should analyse memory deeply, in order to get the unencrypted password.

Location

SYLVARCON | PORT 2 | INTERNATIONAL TRANSIT ZONE

Tools

- Volatility 3
- Floss

Questions

Which is the process identifier (PID) of process who is listening on RDP port?

- 3460

Which is the Hostname that belongs to the memory provided?

- DESKTOP-B7AUQEA

Which is the local IP address that belongs to the memory provided?

- 192.168.211.148

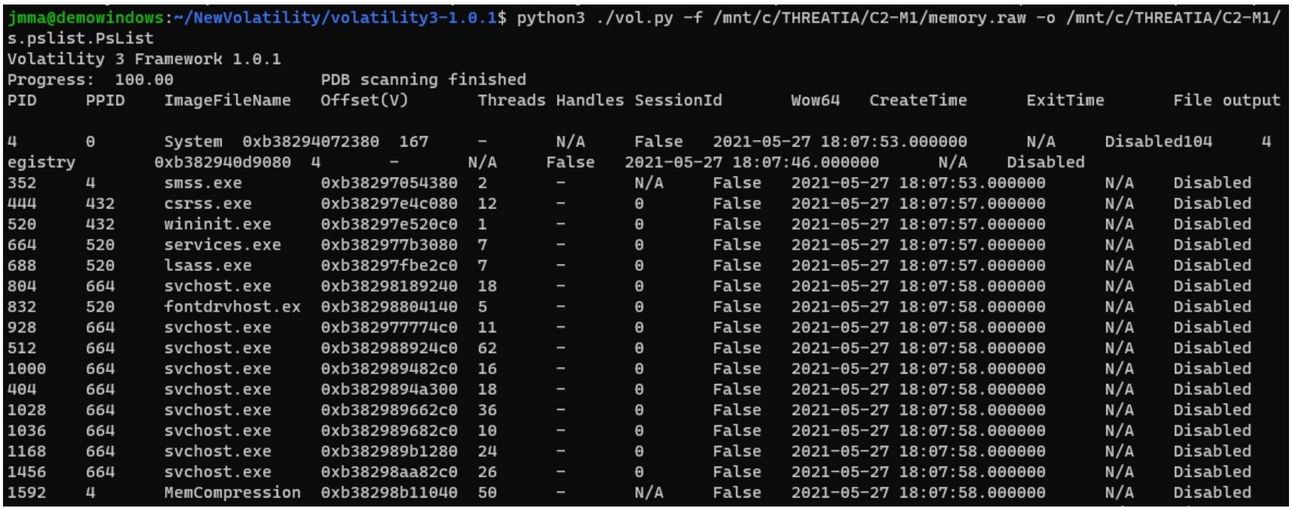
Hints

1. Use Volatility3 to identify the PID of the process to is using RDP protocol.
2. Extract memory of the previous PID using Volatility 3.
3. Use floss tool to extract all strings related to the user who is logged.

Write Up

First step would be to check Volatility with provided memory dump. This new version downloads all necessary symbols, and it´s not required to identify the profile related to the Windows Operating System.

- python3 ./vol.py -f /mnt/c/THREATIA/C2-M1/memory.raw -o /mnt/c/THREATIA/C2-M1/ windows.pslist.PsList



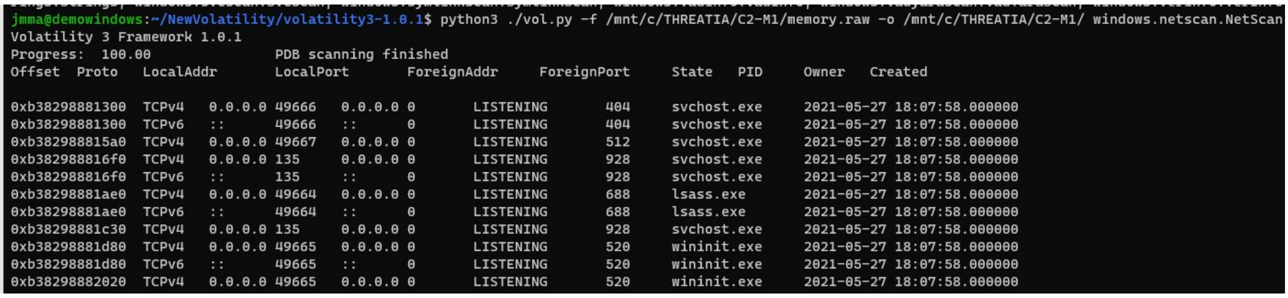
```
jmma@demowindows:~/NewVolatility/volatility3-1.0.1$ python3 ./vol.py -f /mnt/c/THREATIA/C2-M1/memory.raw -o /mnt/c/THREATIA/C2-M1/
s.pslist.PsList
Volatility 3 Framework 1.0.1
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0xb38294072380  167     -       N/A     False   2021-05-27 18:07:53.000000      N/A     Disabled104     4
egistry        0xb382940d9080  4       -       N/A     False   2021-05-27 18:07:46.000000      N/A     Disabled
352     4       smss.exe        0xb38297054380  2       -       N/A     False   2021-05-27 18:07:53.000000      N/A     Disabled
444     432     csrss.exe       0xb38297e4c080  12      -       0       False   2021-05-27 18:07:57.000000      N/A     Disabled
520     432     wininit.exe     0xb38297e520c0  1       -       0       False   2021-05-27 18:07:57.000000      N/A     Disabled
664     520     services.exe    0xb382977b3080  7       -       0       False   2021-05-27 18:07:57.000000      N/A     Disabled
688     520     lsass.exe       0xb38297fbe2c0  7       -       0       False   2021-05-27 18:07:57.000000      N/A     Disabled
804     664     svchost.exe     0xb38298189240  18      -       0       False   2021-05-27 18:07:58.000000      N/A     Disabled
832     520     fontdrvhost.ex  0xb38298804140  5       -       0       False   2021-05-27 18:07:58.000000      N/A     Disabled
928     664     svchost.exe     0xb382977774c0  11      -       0       False   2021-05-27 18:07:58.000000      N/A     Disabled
512     664     svchost.exe     0xb382988924c0  62      -       0       False   2021-05-27 18:07:58.000000      N/A     Disabled
1000    664     svchost.exe     0xb382989482c0  16      -       0       False   2021-05-27 18:07:58.000000      N/A     Disabled
404     664     svchost.exe     0xb3829894a300  18      -       0       False   2021-05-27 18:07:58.000000      N/A     Disabled
1028    664     svchost.exe     0xb382989662c0  36      -       0       False   2021-05-27 18:07:58.000000      N/A     Disabled
1036    664     svchost.exe     0xb382989682c0  10      -       0       False   2021-05-27 18:07:58.000000      N/A     Disabled
1168    664     svchost.exe     0xb382989b1280  24      -       0       False   2021-05-27 18:07:58.000000      N/A     Disabled
1456    664     svchost.exe     0xb38298aa82c0  26      -       0       False   2021-05-27 18:07:58.000000      N/A     Disabled
1592    4       MemCompression  0xb38298b11040  50      -       N/A     False   2021-05-27 18:07:58.000000      N/A     Disabled
```

Figure 1

This challenge is based on the following research:

- https://www.n00py.io/2021/05/dumping-plaintext-rdp-credentials-from-svchost-exe/

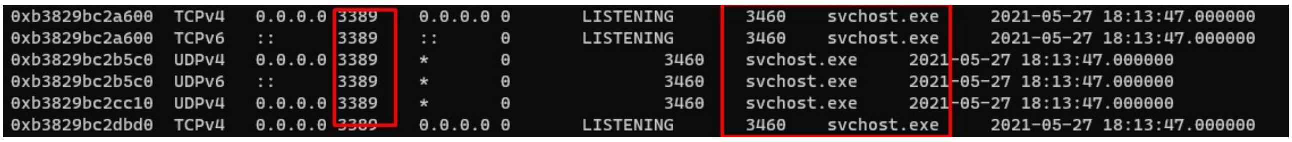
Considering that the player must check RDP connection, it´s essential to identify the process associated:



```
jmma@demowindows:~/NewVolatility/volatility3-1.0.1$ python3 ./vol.py -f /mnt/c/THREATIA/C2-M1/memory.raw -o /mnt/c/THREATIA/C2-M1/ windows.netscan.NetScan
Volatility 3 Framework 1.0.1
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0xb38298881300  TCPv4   0.0.0.0 49666   0.0.0.0 0       LISTENING       404     svchost.exe     2021-05-27 18:07:58.000000
0xb38298881300  TCPv6   ::      49666   ::      0       LISTENING       404     svchost.exe     2021-05-27 18:07:58.000000
0xb382988815a0  TCPv4   0.0.0.0 49667   0.0.0.0 0       LISTENING       512     svchost.exe     2021-05-27 18:07:58.000000
0xb382988816f0  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       928     svchost.exe     2021-05-27 18:07:58.000000
0xb382988816f0  TCPv6   ::      135     ::      0       LISTENING       928     svchost.exe     2021-05-27 18:07:58.000000
0xb38298881ae0  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       688     lsass.exe       2021-05-27 18:07:58.000000
0xb38298881ae0  TCPv6   ::      49664   ::      0       LISTENING       688     lsass.exe       2021-05-27 18:07:58.000000
0xb38298881c30  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       928     svchost.exe     2021-05-27 18:07:58.000000
0xb38298881d80  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       520     wininit.exe     2021-05-27 18:07:58.000000
0xb38298881d80  TCPv6   ::      49665   ::      0       LISTENING       520     wininit.exe     2021-05-27 18:07:58.000000
0xb38298882020  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       520     wininit.exe     2021-05-27 18:07:58.000000
```

Figure 2

Check 3389 local port:



```
0xb3829bc2a600  TCPv4   0.0.0.0 3389    0.0.0.0 0       LISTENING       3460    svchost.exe     2021-05-27 18:13:47.000000
0xb3829bc2a600  TCPv6   ::      3389    ::      0       LISTENING       3460    svchost.exe     2021-05-27 18:13:47.000000
0xb3829bc2b5c0  UDPv4   0.0.0.0 3389    *       0                       3460    svchost.exe     2021-05-27 18:13:47.000000
0xb3829bc2b5c0  UDPv6   ::      3389    *       0                       3460    svchost.exe     2021-05-27 18:13:47.000000
0xb3829bc2cc10  UDPv4   0.0.0.0 3389    *       0                       3460    svchost.exe     2021-05-27 18:13:47.000000
0xb3829bc2dbd0  TCPv4   0.0.0.0 3389    0.0.0.0 0       LISTENING       3460    svchost.exe     2021-05-27 18:13:47.000000
```

Figure 3

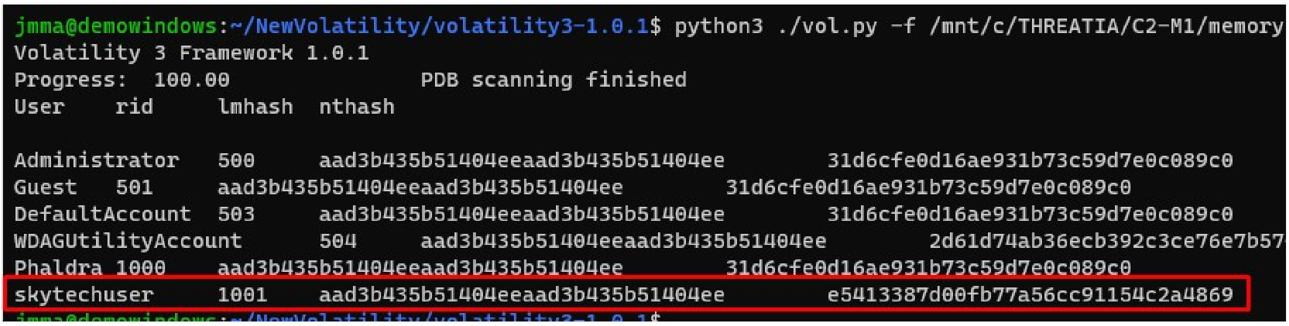
This PID, 3460 related to RDP protocol. Now player must extract memory related to this PID, using the following command:

- python3 ./vol.py -f /mnt/c/THREATIA/C2-M1/memory.raw -o /mnt/c/THREATIA/C2-M1/ windows.memmap.Memmap --pid 3460 –dump

It´s essential to know which is the user who logged into this system. One command to identify users would be:

- python3 ./vol.py -f /mnt/c/THREATIA/C2-M1/memory.raw windows.hashdump.Hashdump

With this, you will be able to know NTLM hashes and accounts stored. The key to this challenge is to locate the unencrypted password, so player doesn´t have to crack any NTLM password.



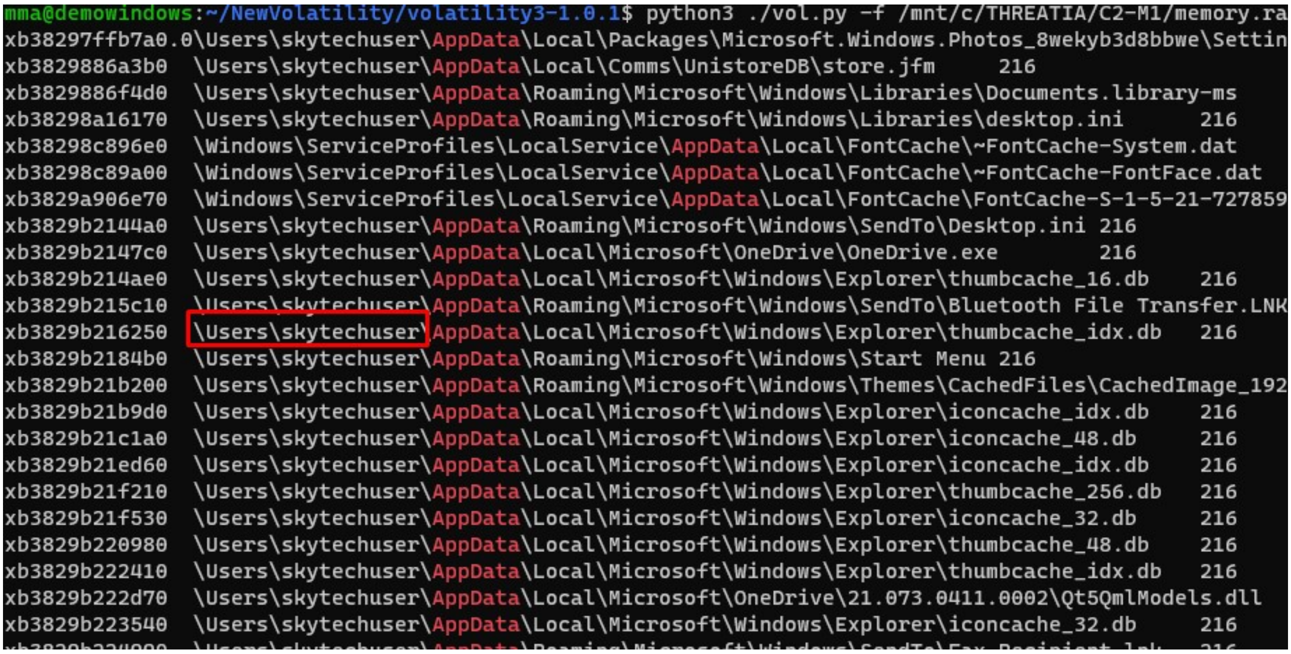
```
jmma@demowindows:~/NewVolatility/volatility3-1.0.1$ python3 ./vol.py -f /mnt/c/THREATIA/C2-M1/memory
Volatility 3 Framework 1.0.1
Progress:  100.00               PDB scanning finished
User    rid     lmhash  nthash

Administrator   500     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
Guest   501     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
DefaultAccount  503     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
WDAGUtilityAccount      504     aad3b435b51404eeaad3b435b51404ee        2d61d74ab36ecb392c3ce76e7b57
Phaldra 1000    aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
skytechuser     1001    aad3b435b51404eeaad3b435b51404ee        e5413387d00fb77a56cc91154c2a4869
jmma@demowindows:~/NewVolatility/volatility3-1.0.1$
```

Figure 4

One way to catch the user whos logged is to identify what files are being used in that moment.

- python3 ./vol.py -f /mnt/c/THREATIA/C2-M1/memory.raw windows.filescan.FileScan | grep --color "AppData"

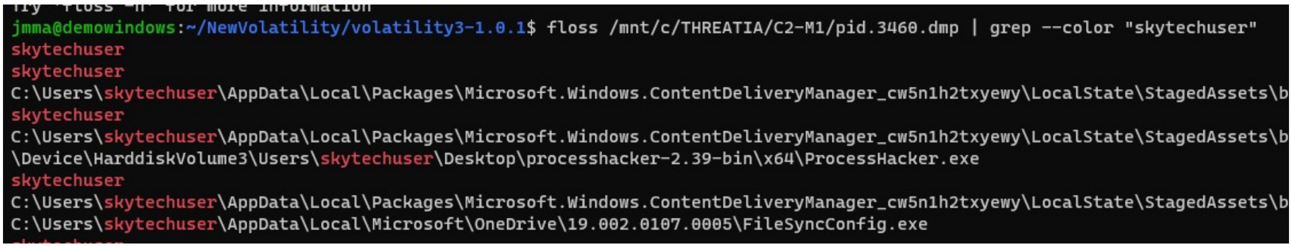
Appdata will show files related to the user: skytechuser



```
mma@demowindows:~/NewVolatility/volatility3-1.0.1$ python3 ./vol.py -f /mnt/c/THREATIA/C2-M1/memory.ra
xb38297ffb7a0.0\Users\skytechuser\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\Settin
xb3829886a3b0  \Users\skytechuser\AppData\Local\Comms\UnistoreDB\store.jfm     216
xb3829886f4d0  \Users\skytechuser\AppData\Roaming\Microsoft\Windows\Libraries\Documents.library-ms
xb38298a16170  \Users\skytechuser\AppData\Roaming\Microsoft\Windows\Libraries\desktop.ini      216
xb38298c896e0  \Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\~FontCache-System.dat
xb38298c89a00  \Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\~FontCache-FontFace.dat
xb3829a906e70  \Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\FontCache-S-1-5-21-727859
xb3829b2144a0  \Users\skytechuser\AppData\Roaming\Microsoft\Windows\SendTo\Desktop.ini 216
xb3829b2147c0  \Users\skytechuser\AppData\Local\Microsoft\OneDrive\OneDrive.exe        216
xb3829b214ae0  \Users\skytechuser\AppData\Local\Microsoft\Windows\Explorer\thumbcache_16.db    216
xb3829b215c10  \Users\skytechuser\AppData\Roaming\Microsoft\Windows\SendTo\Bluetooth File Transfer.LNK
xb3829b216250  \Users\skytechuser\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db   216
xb3829b2184b0  \Users\skytechuser\AppData\Roaming\Microsoft\Windows\Start Menu 216
xb3829b21b200  \Users\skytechuser\AppData\Roaming\Microsoft\Windows\Themes\CachedFiles\CachedImage_192
xb3829b21b9d0  \Users\skytechuser\AppData\Local\Microsoft\Windows\Explorer\iconcache_idx.db    216
xb3829b21c1a0  \Users\skytechuser\AppData\Local\Microsoft\Windows\Explorer\iconcache_48.db     216
xb3829b21ed60  \Users\skytechuser\AppData\Local\Microsoft\Windows\Explorer\iconcache_idx.db    216
xb3829b21f210  \Users\skytechuser\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db   216
xb3829b21f530  \Users\skytechuser\AppData\Local\Microsoft\Windows\Explorer\iconcache_32.db     216
xb3829b220980  \Users\skytechuser\AppData\Local\Microsoft\Windows\Explorer\thumbcache_48.db    216
xb3829b222410  \Users\skytechuser\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db   216
xb3829b222d70  \Users\skytechuser\AppData\Local\Microsoft\OneDrive\21.073.0411.0002\Qt5QmlModels.dll
xb3829b223540  \Users\skytechuser\AppData\Local\Microsoft\Windows\Explorer\iconcache_32.db     216
```

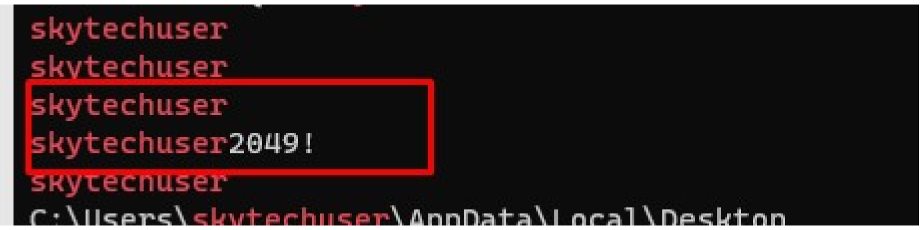
Figure 5

Finally, player must analyse previous dump of PID 3460, using tool Floss tool:



```
Try 'floss -h' for more information
jmma@demowindows:~/NewVolatility/volatility3-1.0.1$ floss /mnt/c/THREATIA/C2-M1/pid.3460.dmp | grep --color "skytechuser"
skytechuser
skytechuser
C:\Users\skytechuser\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\StagedAssets\b
skytechuser
C:\Users\skytechuser\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\StagedAssets\b
\Device\HarddiskVolume3\Users\skytechuser\Desktop\processhacker-2.39-bin\x64\ProcessHacker.exe
skytechuser
C:\Users\skytechuser\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\StagedAssets\b
C:\Users\skytechuser\AppData\Local\Microsoft\OneDrive\19.002.0107.0005\FileSyncConfig.exe
```

Figure 6



```
skytechuser
skytechuser
skytechuser
skytechuser2049!
skytechuser
C:\Users\skytechuser\AppData\Local\Desktop
```

Figure 7

The unencrypted password is skytechuser2049!

Flag Information

flag{skytechuser2049!}