
ATTACK
DEFENSE
by PentesterAcademy

Name	Volatility: Binary II
URL	https://attackdefense.com/challengedetails?cid=1131
Type	Forensics: Memory Forensics

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

A program "authenticator" was executed on a Windows machine. This program contains a token which is encrypted using the local user's password. The program fetches the name of the encryption scheme from the environment variables.

Objective: Recover the plaintext token.

Answer: this_is_plaintext_token

Solution:

Step 1: Check process list to get the PID of the authenticator program

Command: vol.py -f memory_dump.mem --profile=Win81U1x64 pslist

```
0xffffe001d8b3d080 conhost.exe            3408   3444      2        0      1      0 2019-07-13 07:03:19 UTC+0000
0xffffe001d8a04080 authenticator.         3532   3444      1        0      1      0 2019-07-13 07:03:20 UTC+0000
0xffffe001d8bfa080 audiodg.exe            3356    848      6        0      0      0 2019-07-13 07:03:23 UTC+0000
```

Step 2: Dump the process memory using PID and extract strings from it

Commands:
vol.py -f memory_dump.mem --profile=Win81U1x64 memdump -p 3532 --dump-dir .
strings 3532.dmp > strings_file

```
root@attackdefense:~#
root@attackdefense:~# vol.py -f memory_dump.mem --profile=Win81U1x64 memdump -p 3532 --dump-dir .
Volatility Foundation Volatility Framework 2.6.1
************************************************************************
Writing authenticator. [  3532] to 3532.dmp
root@attackdefense:~#
```

```
root@attackdefense:~#
root@attackdefense:~# strings 3532.dmp > strings_file
root@attackdefense:~#
```

Step 3: Look for “token” keyword in strings_file and locate the token

```
{=^%l
'token' : 'QlHLOtEYzgYRsRLLWh4ujMcM9h2Fw/54Hmkyueu2w2A='}
@=^%l
>Y%l
```

Step 4: Use lsadump to dump the logged in user’s password

Command: vol.py -f memory_dump.mem --profile=Win81U1x64 lsadump

```
root@attackdefense:~# vol.py -f memory_dump.mem --profile=Win81U1x64 lsadump
Volatility Foundation Volatility Framework 2.6.1
DefaultPassword
0x00000000  12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00000010  50 00 61 00 73 00 73 00 77 00 30 00 72 00 64 00   P.a.s.s.w.0.r.d.
0x00000020  21 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   !...............
```

Step 5: Get the encryption method/mode information from environment variables available to process

Command: vol.py -f memory_dump.mem --profile=Win81U1x64 envars -p 3532

```
root@attackdefense:~# vol.py -f memory_dump.mem --profile=Win81U1x64 envars -p 3532
Volatility Foundation Volatility Framework 2.6.1
Pid      Process              Block              Variable                       Value
-------- -------------------- ------------------ ------------------------------ -----
    3532 authenticator.       0x0000006c25230860 ALLUSERSPROFILE                C:\ProgramData
    3532 authenticator.       0x0000006c25230860 APPDATA                        C:\Users\IEUser\AppData\Roaming
    3532 authenticator.       0x0000006c25230860 ChocolateyInstall              C:\ProgramData\chocolatey
    3532 authenticator.       0x0000006c25230860 ChocolateyLastPathUpdate       Wed Jan 10 14:19:36 2018
    3532 authenticator.       0x0000006c25230860 CommonProgramFiles             C:\Program Files\Common Files
    3532 authenticator.       0x0000006c25230860 CommonProgramFiles(x86)        C:\Program Files (x86)\Common Files
    3532 authenticator.       0x0000006c25230860 CommonProgramW6432             C:\Program Files\Common Files
    3532 authenticator.       0x0000006c25230860 COMPUTERNAME                   IE11WIN8_1
    3532 authenticator.       0x0000006c25230860 ComSpec                        C:\Windows\system32\cmd.exe
    3532 authenticator.       0x0000006c25230860 CYGWIN                         mintty
    3532 authenticator.       0x0000006c25230860 ENC_METHOD                     aes-256-cbc
```

Step 6: Use OpenSSL to decrypt the token

Command: echo 'QlHLOtEYzgYRsRLLWh4ujMcM9h2Fw/54Hmkyueu2w2A=' | openssl enc -base64 -d -aes-256-cbc -nosalt -pass pass:Passw0rd!

```
root@attackdefense:~#
root@attackdefense:~# echo 'QlHLOtEYzgYRsRLLWh4ujMcM9h2Fw/54Hmkyueu2w2A=' |   openssl enc -base64 -d -aes-256-cbc -n
osalt -pass pass:Passw0rd!
this_is_plaintext_token
root@attackdefense:~#
```

Decrypted token: this_is_plaintext_token

References:

1. Volatility (https://github.com/volatilityfoundation/volatility)