

volatility CTF

Working on Sift workstation using VMware

Challenge 1

Challenge Description

My friend John is an "environmental" activist and a humanitarian. He hated the ideology of Thanos from the Avengers: Infinity War. He sucks at programming. He used too many variables while writing any program. One day, John gave me a memory dump and asked me to find out what he was doing while he took the dump. Can you figure it out for me?

Challenge file: [Google drive](#)

Initial Thoughts

In most beginner level CTFs whenever we are provided with a memory forensics challenge, we also have a description which gives out certain clues. Identifying these clues can be quite tricky at first but becomes easier if you go on playing more & more CTFs.

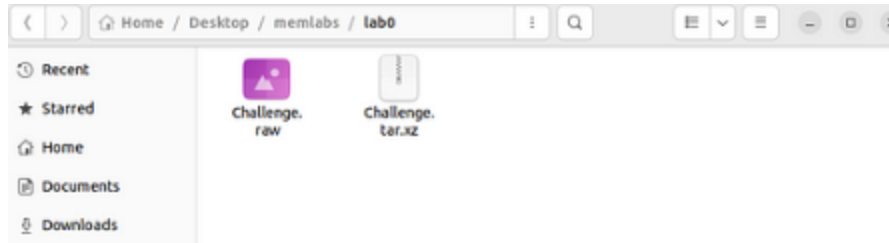
Now the clues that we can pick from this description are as follows:

- Environmental Activist (Since the word is quoted)
- John hates Thanos (Maybe useless but let us see)
- John sucks at programming and used too many variables.

Now let us move into analyzing the memory dump.

Activate Windows
Go to Settings to activate Windows.

Downloaded zip file , which after extraction , it was in raw format



Using volatility 2

First using image info to get the details of file

vol.py -f '/path/Challenge.raw' imageinfo

Output

```
$ vol.py -f '/home/sansforensics/Desktop/memlabs/lab0/Challenge.raw' imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_24000, Win7SP1x86
      AS Layer1 : IA32PagedMemoryPae (Kernel AS)
      AS Layer2 : FileAddressSpace (/home/sansforensics/Desktop/memlabs/lab0/Challenge.raw)
      PAE type : PAE
                   DTB : 0x185000L
                   KDBG : 0x8273cb78L
      Number of Processors : 1
      Image Type (Service Pack) : 1
                   KPCR for CPU 0 : 0x80b96000L
                   KUSER_SHARED_DATA : 0xffdf0000L
      Image date and time : 2018-10-23 08:30:51 UTC+0000
      Image type and time : 2018-10-23 14:00:51 UTC+0000
```

Now i am using Win7SP1x86 profile

Now will check the list of process running using pslist

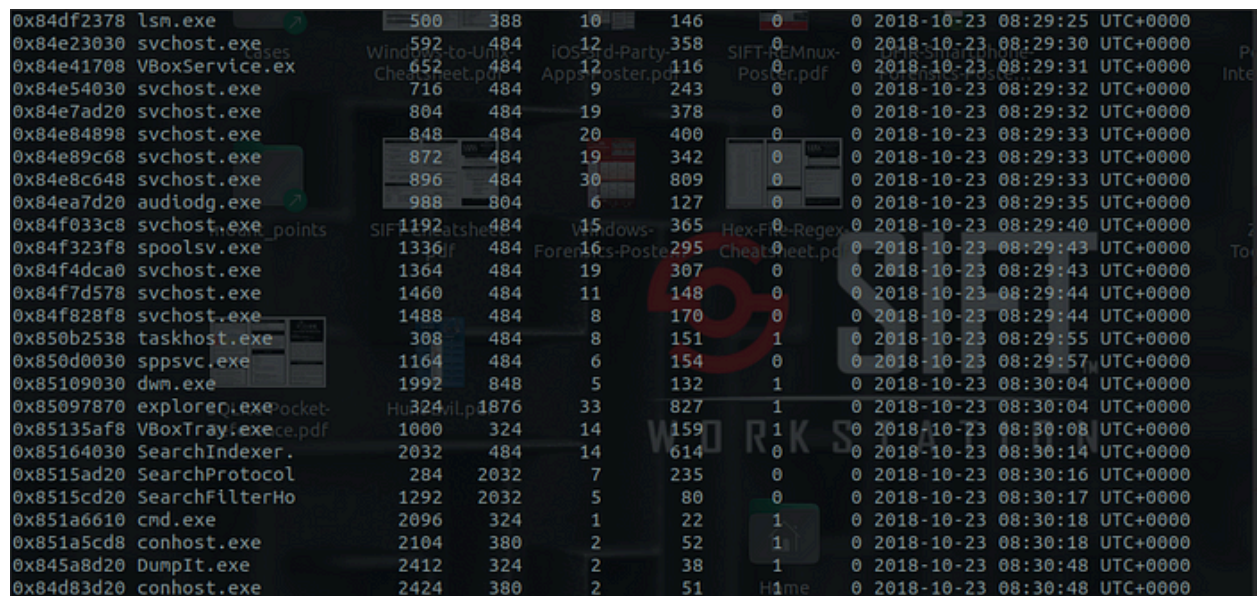
vol.py -f

‘/home/sansforensics/Desktop/memlabs/lab0/Challenge.ra

w’ — profile=Win7SP1x86 pslist

Multiple process are running , but i have some doubt on

dump.exe



0x84df2378	lsm.exe	500	388	10	146	0	0	2018-10-23 08:29:25	UTC+0000
0x84e23030	svchost.exe	592	484	12	358	0	0	2018-10-23 08:29:30	UTC+0000
0x84e41708	VBoxService.exe	652	484	12	116	0	0	2018-10-23 08:29:31	UTC+0000
0x84e54030	svchost.exe	716	484	9	243	0	0	2018-10-23 08:29:32	UTC+0000
0x84e7ad20	svchost.exe	804	484	19	378	0	0	2018-10-23 08:29:32	UTC+0000
0x84e84898	svchost.exe	848	484	20	400	0	0	2018-10-23 08:29:33	UTC+0000
0x84e89c68	svchost.exe	872	484	19	342	0	0	2018-10-23 08:29:33	UTC+0000
0x84e8c648	svchost.exe	896	484	30	809	0	0	2018-10-23 08:29:33	UTC+0000
0x84ea7d20	audiodg.exe	988	804	6	127	0	0	2018-10-23 08:29:35	UTC+0000
0x84f033c8	svchost.exe	1192	484	15	365	0	0	2018-10-23 08:29:40	UTC+0000
0x84f323f8	spoolsv.exe	1336	484	16	295	0	0	2018-10-23 08:29:43	UTC+0000
0x84f4dca0	svchost.exe	1364	484	19	307	0	0	2018-10-23 08:29:43	UTC+0000
0x84f7d578	svchost.exe	1460	484	11	148	0	0	2018-10-23 08:29:44	UTC+0000
0x84f828f8	svchost.exe	1488	484	8	170	0	0	2018-10-23 08:29:44	UTC+0000
0x850b2538	taskhost.exe	308	484	8	151	1	0	2018-10-23 08:29:55	UTC+0000
0x850d0030	sppsvc.exe	1164	484	6	154	0	0	2018-10-23 08:29:57	UTC+0000
0x85109030	dwm.exe	1992	848	5	132	1	0	2018-10-23 08:30:04	UTC+0000
0x85097870	explorer.exe	324	1876	33	827	1	0	2018-10-23 08:30:04	UTC+0000
0x85135af8	VBoxTray.exe	1000	324	14	159	1	0	2018-10-23 08:30:08	UTC+0000
0x85164030	SearchIndexer.exe	2032	484	14	614	0	0	2018-10-23 08:30:14	UTC+0000
0x8515ad20	SearchProtocolHost.exe	284	2032	7	235	0	0	2018-10-23 08:30:16	UTC+0000
0x8515cd20	SearchFilterHost.exe	1292	2032	5	80	0	0	2018-10-23 08:30:17	UTC+0000
0x851a6610	cmd.exe	2096	324	1	22	1	0	2018-10-23 08:30:18	UTC+0000
0x851a5cd8	conhost.exe	2104	380	2	52	1	0	2018-10-23 08:30:18	UTC+0000
0x845a8d20	DumpIt.exe	2412	324	2	38	1	0	2018-10-23 08:30:48	UTC+0000
0x84d83d20	conhost.exe	2424	380	2	51	1	0	2018-10-23 08:30:48	UTC+0000

Now I will check process tree so that i can check the parent child relationship

vol.py -f

‘/home/sansforensics/Desktop/memlabs/labo/Challenge.ra

w’ — profile=Win7SP1x86 pstree

0x85097870:explorer.exe	324	1876	33	827	2018-10-23	08:30:04	UTC+0000
0x845a8d20:DumpIt.exe	2412	324	2	38	2018-10-23	08:30:48	UTC+0000
0x851a6610:cmd.exe	2096	324	1	22	2018-10-23	08:30:18	UTC+0000

We can see that explorer.exe is parent process of both cmd & DumpIT.exe

So checking cmd.exe what command is executed through terminal using cmdscan plugin

```
$ vol.py -f '/home/sansforensics/Desktop/memlabs/lab0/Challenge.raw' --profile=Win7SP1x86 cmdscan
Volatility Foundation Volatility Framework 2.6.1
*****
CommandProcess: conhost.exe Pid: 2104
CommandHistory: 0x300498 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
Cmd #0 @ 0x2f43c0: C:\Python27\python.exe C:\Users\hello\Desktop\demon.py.txt
Cmd #12 @ 0x2d0039: ???
Cmd #19 @ 0x300030: ???
Cmd #22 @ 0xff818488: ?
Cmd #25 @ 0xff818488: ?
Cmd #36 @ 0x2d00c4: /?0?-???-
Cmd #37 @ 0x2fd058: 0?-????
*****
CommandProcess: conhost.exe Pid: 2424
CommandHistory: 0x2b04c8 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
Cmd #22 @ 0xff818488: ?
Cmd #25 @ 0xff818488: ?
Cmd #36 @ 0x2800c4: *?+?(???(
Cmd #37 @ 0x2ad070: +?(????
```

We can see demon.py.txt is getting executed through cmd .

So lets check the o/p using consoles plugin

vol.py -f

‘/home/sansforensics/Desktop/memlabs/lab0/Challenge.ra

w’ — profile=Win7SP1x86 consoles

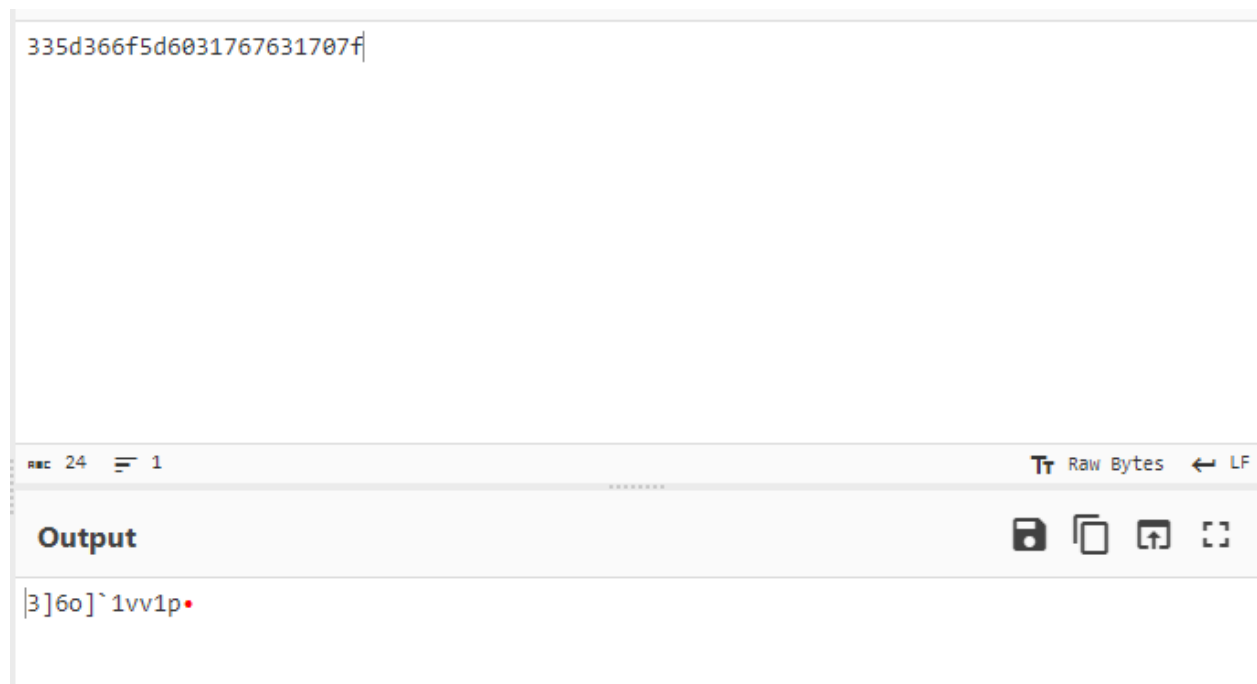
```
CommandHistory: 0x300498 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
Cmd #0 at 0x2f43c0: C:\Python27\python.exe C:\Users\hello\Desktop\demon.py.txt
Screen 0x2e6368 X:80 Y:300
Dump: master
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\hello>C:\Python27\python.exe C:\Users\hello\Desktop\demon.py.txt
335d366f5d6031767631707f

C:\Users\hello>
```

now we can see, some hex values, so now will use cyberchef,
getting some random values

3]6o]`1vv1p



To get the environment variables of a process you can use the `envvars` plugin

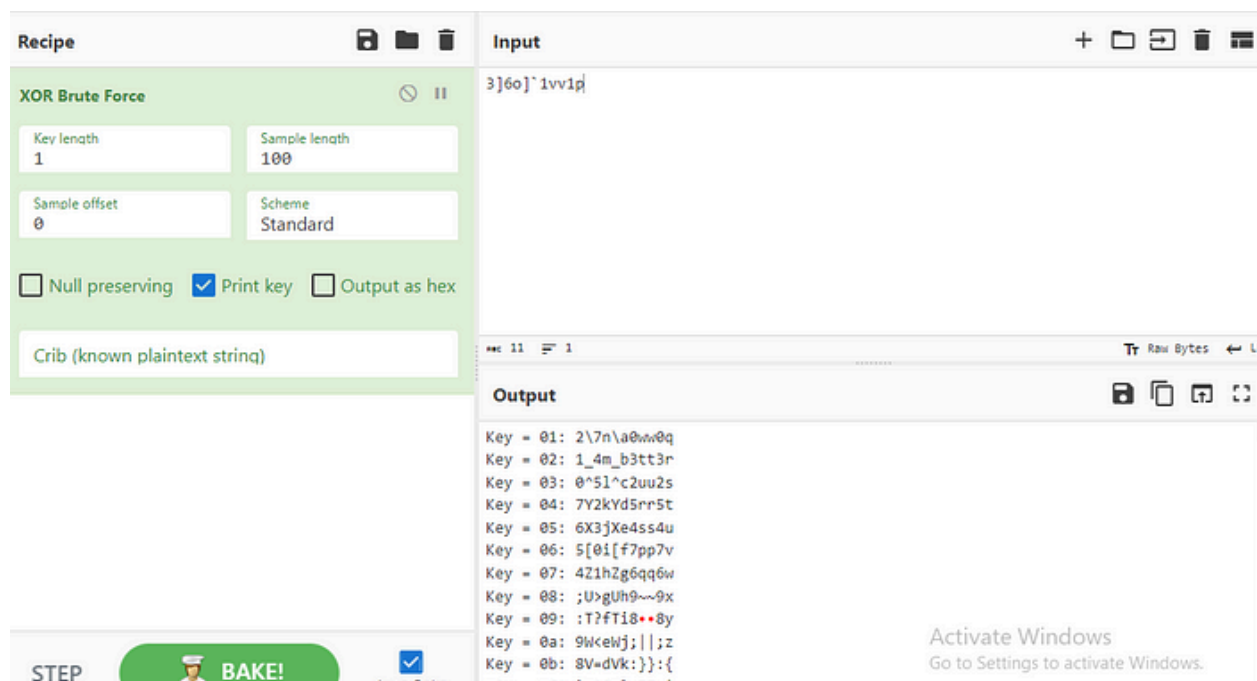
As per hints, using envvars plugin



2424	conhost.exe	0x002934b0	SystemRoot	C:\	You opened • 18:04	Ab
2424	conhost.exe	0x002934b0	SystemRoot	C:\Windows		
2424	conhost.exe	0x002934b0	TEMP	C:\Windows\TEMP		
2424	conhost.exe	0x002934b0	Thanos	xor and password	ov 2023	m

As per hints we can see that Thanos & xor and password

Now will try to use this hint & complete above task using cyberchef



So I am taking hashdump to look for some password

we found one user

```
$ vol.py -f '/home/sanstorensics/Desktop/memlabs/lab0/Challenge.raw' --profile=Win7SP1x86 has
Volatility Foundation Volatility Framework 2.6.1
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
hello:1000:aad3b435b51404eeaad3b435b51404ee:101da33f44e92c27835e64322d72e8b7:::
```

Trying to break ntlm hashvalue not able to find. Checked with creator & issue was there in the hash.

So completing this challenge here.