TryHackMe Room Write-up

Title: Memory Forensics

Description: Perform memory forensics to find the flags

Author: Igor Buszta

Login

Description: *The forensic investigator on-site has performed the initial forensic analysis of John's computer and handed you the memory dump he generated on the computer. As the secondary forensic investigator, it is up to you to find all the required information in the memory dump.*

Objective: What is John's password?

Data: Memory dump of John's computer (.vmem file).

Tools used: macOS, Volitality3

First things first, let's create virtual environment in cloned directory and install required tools - following volatile3's github's instructions, so that thing's run smoothly.

```
> cd volatility3
> python3 -m venv venv
```

```
> source venv/bin/activate
```

Picture 1&2: Creating virtual environment.

```
> pip install -e ".[dev]"
Obtaining file:///Users/igorrob/volatility3
```

Picture 3: Obtaining essential libraries.

In order to find hashed passwords on memory dump of John's computer, the following command was used:

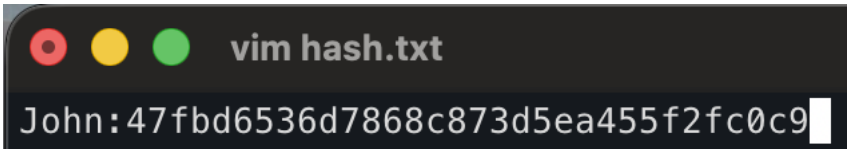
python3 vol.py -f Snapshot1.vmem windows.hashdump

And on image below (Picture 4) are the results.

```
Administrator   500     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
Guest   501     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
John    1001    aad3b435b51404eeaad3b435b51404ee        47fbd6536d7868c873d5ea455f2fc0c9
HomeGroupUser$  1002    aad3b435b51404eeaad3b435b51404ee        91c34c06b7988e216c3bfeb9530cabfb
```

Picture 4: Found hashes.

The hashes have been saved to text file.



Picture 5: Hash saved in format for later cracking.

To crack hash and see what's John's password, Jack-the-ripper was used and rockyou.txt file which contains known, cracked passwords.

```
> john --format=NT --wordlist=~/rockyou/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 ASIMD 4x2])
Press 'q' or Ctrl-C to abort, almost any other key for status
charmander999    (John)
1g 0:00:00:01 DONE (2026-02-04 12:57) 0.8000g/s 7344Kp/s 7344Kc/s 7344KC/s charmarn..charmaine21
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed
```

Picture 6: Using jack-the-ripper to crack password.

The password is: **charmander999.**

Analysis

Description: *On arrival a picture was taken of the suspect's machine, on it, you could see that John had a command prompt window open. The picture wasn't very clear, sadly, and you could not see what John was doing in the command prompt window.*

To complete your forensic timeline, you should also have a look at what other information you can find, when was the last time John turned off his computer?

Objectives**:** When was the machine last shutdown? What did John write?

Data: Memory dump of John's computer (.vmem file).

Tools used: macOS, Volitality3

In order to find the time in which computer was last shut down, we need to look into \Control\Windows directory, where these kind of infromations are stored.

```
> python3 vol.py -f /Users/igorrob/Downloads/Snapshot19_1609159453792.vmem windows.registry.printkey --key "ControlSet001\Control\Windows"
```

Picture 7: Command used to find system shutdown time.

In the results we get, there's one line we're looking for.

```
2020-12-27 22:50:12.000000 UTC  0xf8a000024010  REG_BINARY      \REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Windows  ShutdownTime
```

Picture 8: Results of the „... windows.registry.key [...]" command.

The exact time of system shutdown is **2020-12-27 22:50:12**.

To find what John wrote into the command line, we need to find the proccess ID of it and extract as much information as possible from it. First things first we type in the command:

```
> python3 vol.py -f /Users/igorrob/Downloads/Snapshot6_1609157562389.vmem windows.pslist
```

Picture 9: Command used to list PIDs.

We manage to find demanded results.

```
1920    cmd.exe "C:\Windows\System32\cmd.exe"
2488    conhost.exe     \??\C:\Windows\system32\conhost.exe
```

Picture 10: PIDs of vital processes.

We then dump the information of Virtual Adress into designated directory.

```
~/volatility3 develop ?1 > mkdir output-dump
```

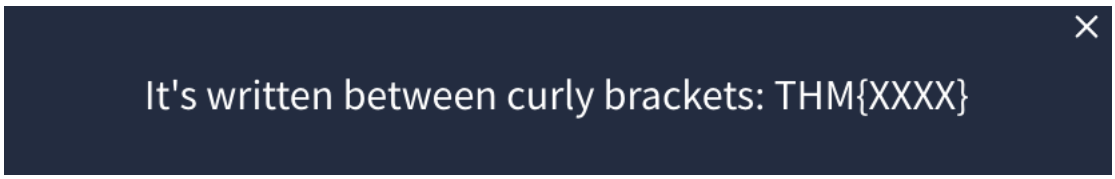
Picture 11: Creating a directory for information.

We add new flags: -o for output of command. We also specify PID and --dump.

```
~/volatility3 develop ?1 > python3 vol.py -f /Users/igorrob/Downloads/Snapshot19_1609159453792.vmem -o ./output-dump windows.memmap --pid 1920 --dump
```

Picture 12: Command for output of memory mapping.

We know in fact, from the tip on tryhackme, that the info is hidden in specific format. We use that information to our advantage.



Picture 13: Tip to finding what john typed in the cmd.

```
> strings ./output-dump/pid.1920.dmp| grep "THM"
THM{You_found_me}
BTHMODEM
BTHMODEM
FIPSALGORITHMPOLICY
COPYASPATHMENU
THM{You_found_me}
THMMOF"Z
```

Picture 14: Grepping all strings from a file with „THM" in them.

The anwser is **You_found_me**.

TrueCrypt

Description: *A common task of forensic investigators is looking for hidden partitions and encrypted files, as suspicion arose when TrueCrypt was found on the suspect's machine and an encrypted partition was found. The interrogation did not yield any success in getting the passphrase from the suspect, however, it may be present in the memory dump obtained from the suspect's computer*.

Objective: What is the TrueCrypt passphrase?

Data: Memory dump of John's computer (.vmem file).

Tools used: macOS, Volitality3

Advice: To solve this puzzle, you need to fix one bug in Volitality3's code. Follow instructions on https://github.com/volatilityfoundation/volatility3/issues/1159

We're lucky to have a command for extracting TrueCrypt passphrases in Volitality3.

```
> python3 vol.py -f /Users/igorrob/Downloads/Snapshot14_1609164553061.vmem windows.truecrypt.Passphrase
```

Picture 15: Command for extracting truecrypt passphrases.

The anwser is seen in the results plain as day.

```
0xf8800512bee4  11      forgetmenot
```

Picture 16: Passphrase with it's hex.

The anwser is **forgetmenot**.