

✦ Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)



# TryHackMe Volatility Write-Up



Toumo · [Follow](#)

7 min read · Aug 9, 2023



Listen



Share

... More



Image from tryhackme.com

I remember about the order of volatility when I was studying for Sec+. It looks like Volatility is going to focus more on RAM, which is generally very volatile and should be collected earliest as possible. I think this is the first tool that we've worked with in SOC Level 1 training path that is focused on RAM. The others seem to be working with storage devices, so I wonder how different it would be.

## Task 4 Memory Extraction

I did not use my virtual machine here. I used the machine given by THM.

While there isn't a question here, I want to write how I got volatility to work as I wanted to follow the examples. It was very subtle but we are actually supposed to go to `/opt/volatility3` then input the commands.

We have an Ubuntu machine with Volatility and Volatility 3 already present in the `/opt` directory,

From the reading in Task 3

```
thmanalyst@ubuntu:~$ cd /opt/volatility3/
```

Go to the folder with this command

Once you're in the volatility3 folder, you can run the help command.

```
thmanalyst@ubuntu:/opt/volatility3$ python3 vol.py -h
Volatility 3 Framework 1.0.1
Usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]]
               [-e EXTEND] [-p PLUGIN DIRS] [-s SYMBOL DIRS] [-v] [-l LOG]
               [-o OUTPUT DIR] [-q] [-r RENDERER] [-f FILE]
               [--write-config] [--clear-cache] [--cache-path CACHE PATH]
               [--single-location SINGLE LOCATION]
               [--stackers [STACKERS [STACKERS ...]]]
               [--single-swap-locations [SINGLE SWAP LOCATIONS [SINGLE SWAP LOCATIONS ...]]]
               plugin ...

An open-source memory forensics framework
```

## Task 6 Identifying Image Info and Profiles

I took note of another set of folders and files we have for practice.

```
thmanalyst@ubuntu:/opt/volatility3$ cd /Scenarios/Investigations/
thmanalyst@ubuntu:/Scenarios/Investigations$ ls
Investigation-1.vmem  Investigation-2.raw
thmanalyst@ubuntu:/Scenarios/Investigations$
```

Then I typed in `vol -f /Scenarios/Investigations/Investigation-1.vmem windows.info`, that was modified from the example given in the reading, and got the following output.

```
thmanalyst@ubuntu:/opt/volatility3$ vol -f /Scenarios/Investigations/Investigation-1.vmem windows.info
Volatility 3 Framework 1.0.1
Progress: 100.00 PDB scanning finished
Variable Value
Kernel Base 0x804d7000
DTB 0x2fe000
Symbols file:///opt/volatility3/volatility3/symbols/windows/ntkrnlpa.pdb/30B5FB31AE7E4ACAABA750AA241FF331-1.json.xz
Is64Bit False
IsPAE True
primary 0 WindowsIntelPAE
memory layer 1 FileLayer
KdDebuggerDataBlock 0x80545ae0
NTBuildLab 2600.xpsp.080413-2111
CSDVersion 3
KdVersionBlock 0x80545ab8
Major/Minor 15.2600
MachineType 332
KeNumberProcessors 1
SystemTime 2012-07-22 02:45:08
NtSystemRoot C:\WINDOWS
NtProductType NtProductWinNt
NtMajorVersion 5
NtMinorVersion 1
PE MajorOperatingSystemVersion 5
PE MinorOperatingSystemVersion 1
PE Machine 332
PE TimeDateStamp Sun Apr 13 18:31:06 2008
```

Curiously enough, typing in `vol -f 'dump.vmem' windows info` gives the same output for me. Not sure why.

## Task 10 Practical Investigations

I used Shift+Ctrl+C/V to copy and paste from the machine to the site and vice versa. It may be helpful for everyone too.

1: What is the build version of the host machine in Case 001?

Going back to the very first time we used Volatility, we will enter `vol -f /Scenarios/Investigations/Investigation-1.vmem windows.info` again in order to get the build information.

```
NTBuildLab 2600.xpsp.080413-2111
```

Answer: 2600.xpsp.080413-2111

2: At what time was the memory file acquired in Case 001?

This will be in the same output as the previous command, so look around a bit.

```
SystemTime 2012-07-22 02:45:08
```

Answer: 2012-07-22 02:45:08

3: What process can be considered suspicious in Case 001?

Note: Certain special characters may not be visible on the provided VM. When doing a copy-and-paste, it will still copy all characters.

I used the following command to look at the processes `vol -f /Scenarios/Investigations/Investigation-1.vmem windows.psscan` and saw some processes I wasn't familiar with. After searching up online what they were, I came to the conclusion that `reader_sl.exe` was the one that was suspicious as it's an unnecessary program, and that malware can rename themselves to this. Windows also doesn't need this to function.

```
1640 1484 reader_sl.exe
```

Answer: `reader_sl.exe`

4: What is the parent process of the suspicious process in Case 001?

I ran the following command to see the parent process `vol -f /Scenarios/Investigations/Investigation-1.vmem windows.pstree`. The asterisk indicate

one level down the tree.

```
1484    1464    explorer.exe
* 1640    1484    reader_sl.exe
```

Answer: explorer.exe

5: What is the PID of the suspicious process in Case 001?

I went back to the output of .psscan since the asterisk were a bit disruptive.

```
PID      PPID      ImageFileName
908      652      svchost.exe
664      608      lsass.exe
652      608      services.exe
1640     1484     reader_sl.exe
```

Answer: 1640

6: What is the parent process PID in Case 001?

Going down a little bit more, we can see the process ID of explorer.exe, the parent. Alternatively, you can look at the PPID of reader\_sl.exe since that's the parent process ID.

```
PID      PPID      ImageFileName
908      652      svchost.exe
664      608      lsass.exe
652      608      services.exe
1640     1484     reader_sl.exe
1512     652      spoolsv.exe
1588     1004     wuaucvt.exe
788      652      alg.exe 0x22e8
1484     1464     explorer.exe
```

Answer: 1484

7: What user-agent was employed by the adversary in Case 001?

This took me a little while. I had to use the hint because I had no idea what to do. First, I edited the command from the hint to fit what I need. `vol -f`

`/Scenarios/Investigations/Investigation-1.vmem -o /home/thmanalyst`

`windows.memmap.Memmap - pid 1640 - dump` . A dump file will be created in

/home/thmanalyst. Once I did that, `strings /home/thmanalyst/*.dmp | grep -i "user-agent"` to search the dump file for anything that references "user-agent."

```
User-Agent
User-Agent: Mozilla/5.0 (Windows; U; MSIE 7.0; Windows NT 6.0; en-US)
cs(User-Agent)
USER-AGENT:
User-Agent:
```

Answer: Mozilla/5.0 (Windows; U; MSIE 7.0; Windows NT 6.0; en-US)

8: Was Chase Bank one of the suspicious bank domains found in Case 001? (Y/N)

My assumption was to scan the dump file again but this time, modify `grep` to mention chase. I used the following command `strings /home/thmanalyst/*.dmp | grep -i "chase"` and a lot of results regarding Chase comes up.

Answer: Y

9: What suspicious process is running at PID 740 in Case 002?

This time, we are going to be working on investigation 2. So I did a psscan on investigation 2 with the following `vol -f /Scenarios/Investigations/Investigation-2.raw windows.psscan .`

PID	PPID	ImageFileName
860	1940	taskdl.exe
536	1940	taskse.exe
424	1940	@WanaDecryptor@
1768	1024	wuaclt.exe
576	1940	@WanaDecryptor@
260	664	svchost.exe
740	1940	@WanaDecryptor@

Answer: @WanaDecryptor@

10: What is the full path of the suspicious binary in PID 740 in Case 002?

I looked back at the reading and used `dlllist` and added `grep` to help me filter out the output. `vol -f /Scenarios/Investigations/Investigation-2.raw windows.dlllist | grep -i "WanaDecryptor"` is what I used.

```
thmanalyst@ubuntu:/opt/volatility3$ vol -f /Scenarios/Investigations/Investigation-2.raw windows.dlllist | grep -i "WanaDecryptor"
740gress@WanaDecryptor@ 0x400000 0x3d000 @WanaDecryptor@.exe C:\Intel\Ivecuqmanpnirk615\@WanaDecryptor@.exe N/A Disabled
```

Answer: C:\Intel\ivecuqmanpnirkt615\@WanaDecryptor@.exe

11: What is the suspicious parent process PID connected to the decryptor in Case 002?

I went back to the process tree. I looked at our suspicious process which had a PID of 740. I looked at the corresponding PPID, which is 1940. I then looked for 1940 under PID and found tasksche.exe.

PID	PPID	ImageFileName
860	1940	taskdl.exe
536	1940	taskse.exe
424	1940	@WanaDecryptor@
1768	1024	wuauclt.exe
576	1940	@WanaDecryptor@
260	664	svchost.exe
740	1940	@WanaDecryptor@
1168	1024	wscntfy.exe
544	664	alg.exe 0x201002
1084	664	svchost.exe
596	348	csrss.exe
348	4	smss.exe
620	348	winlogon.exe
676	620	lsass.exe
664	620	services.exe
1024	664	svchost.exe
904	664	svchost.exe
1152	664	svchost.exe
1636	1608	explorer.exe
1484	664	spoolsv.exe
1940	1636	tasksche.exe
836	664	svchost.exe
1956	1636	ctfmon.exe

Answer: tasksche.exe

12: What is the suspicious parent process PID connected to the decryptor in Case 002?

I could not parse this question that I even had to use the hint. It's asking what is the PPID of our suspicious process or PID of our parent process.

Answer: 1940

13: From our current information, what malware is present on the system in Case 002?

I essentially looked up what was WanaDecryptor. I had an idea already but I wanted to double check.

Answer: Wannacry

14: What DLL is loaded by the decryptor used for socket creation in Case 002?

I used the following command to filter only results that has Decryptor to start me off  
`vol -f /Scenarios/Investigations/Investigation-2.raw windows.dlllist | grep -i "decryptor"` . After that, it was basically me just searching up each individual dlls to know what they do. Admittedly, I counted the asterisks to reduce my searching a bit.

```
740 @WanaDecryptor@ 0x71ab0000 0x17000 WS2_32.dll C:\WINDOWS\system32\WS2_32.dll N/A Disabled
```

WS2\_32.dll can be used by trojans for network connections, so it may be a backdoor.

Answer: WS2\_32.dll

15: What mutex can be found that is a known indicator of the malware in question in Case 002?

I used the hint for this. I used the following command `vol -f /Scenarios/Investigations/Investigation-2.raw windows.handles | grep "1940"` . There were a few mutexes mentioned so I tried them all.

```
1940 tasksche.exe 0x821883e8 0x40 Mutant 0x120001 ShimCacheMutex
1940 tasksche.exe 0xe16644e0 0x44 Section 0x2 ShimSharedMemory
1940 tasksche.exe 0x822386a8 0x48 File 0x100001 \Device\KsecDD
1940 tasksche.exe 0x823d54d0 0x4c Semaphore 0x1f0003 shell.{A48F1A32-A340-11
1940 tasksche.exe 0x823a0cd0 0x50 File 0x100020 \Device\HarddiskVolume1\WINDOWS
202
1940 tasksche.exe 0x8224f180 0x54 Mutant 0x1f0001 MsWinZonesCacheCounterMutexA
1940 tasksche.exe 0x822e3b08 0x58 Mutant 0x1f0001 MsWinZonesCacheCounterMutexA0
1940 tasksche.exe 0x822344f0 0x5c Event 0x1f0003
```

Answer: MsWinZonesCacheCounterMutexA

16: What plugin could be used to identify all files loaded from the malware working directory in Case 002?

I used the hint again. I should have thought about using the manual in hindsight. Simply type `vol -h` to look at the help menu and explanation what each command does. It'll take a bit of looking, but I only read the windows section.

Answer: windows.filescan

Thoughts:



Personally I initially thought the preparation was very light and that I was not prepared for it. I think I did pretty well at the end. Some of them I had absolutely no idea though, so I think that would come with time. I really enjoyed using volatility since it allowed me to further remember my Linux commands, although I do enjoy using a GUI a whole lot more. There was a lot more research needed for this hands on challenge than others I believe. I had to research dlls and executables to understand what they do, and if they are necessary or not. I can't say it's fun but it is necessary.

Cybersecurity

Tryhackme

Dfir

Digital Forensics

Volatility



Follow

## Written by Toumo

152 Followers · 1 Following

## Responses (2)



What are your thoughts?

Respond



Samar

about 2 months ago



thanks



Reply



**.nobody#**

8 months ago

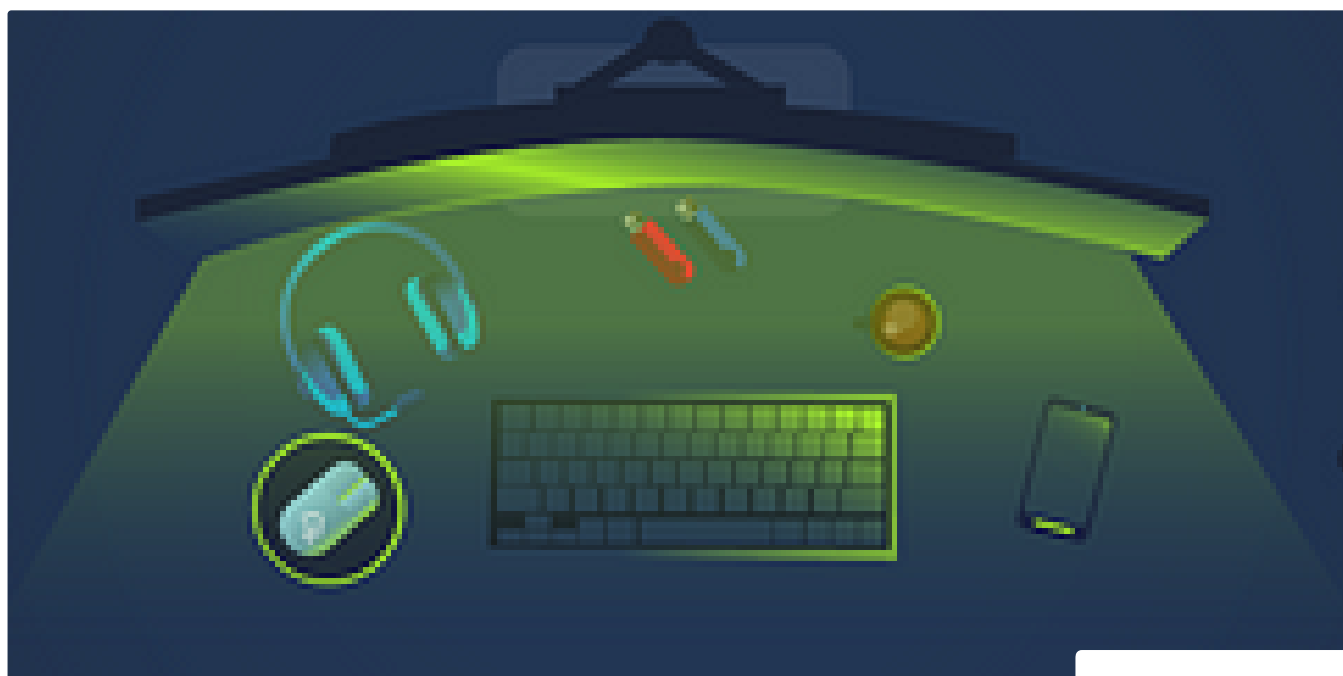


for i am using volatility 2, and stuck at finding the user agent. how do i achieve this?!



Reply

## More from Toumo

**Toumo**

## TryHackMe Redline Write-Up

We just finished the Autopsy room and now we will be learning how to use Redline. I've never used it, nor have I heard of it before, so...

Aug 8, 2023



45



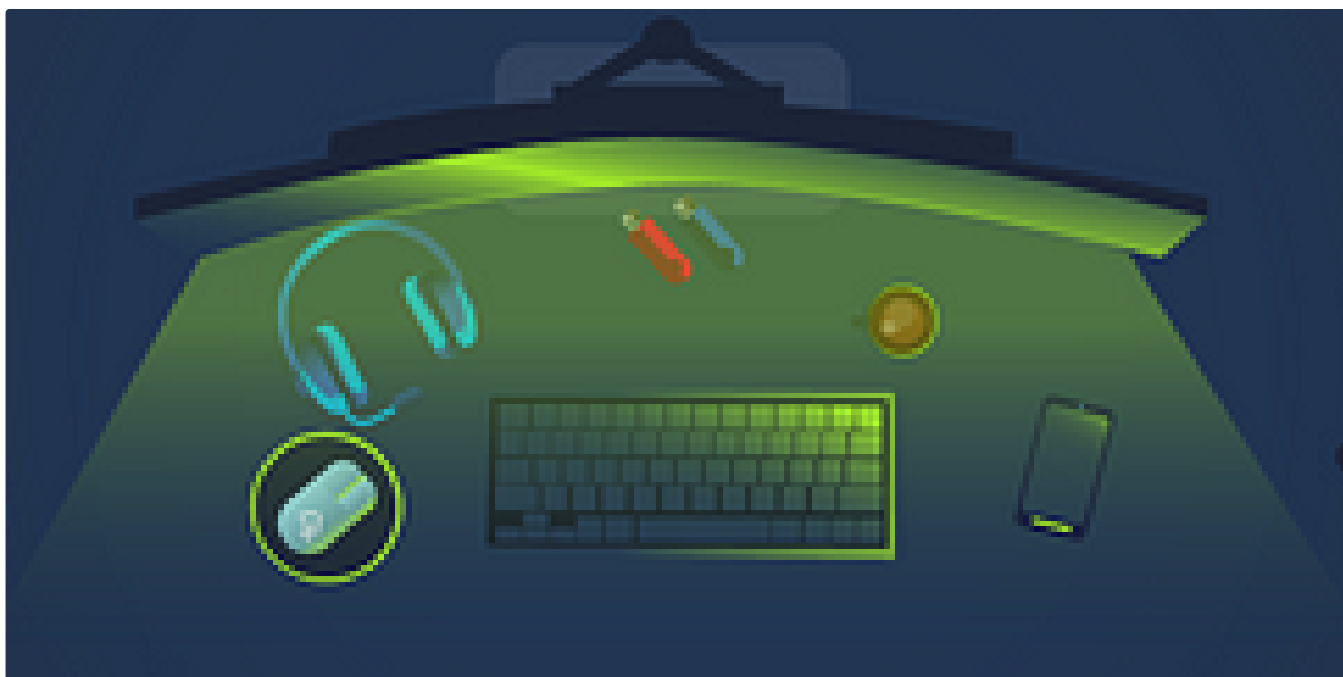
4




[Open in app ↗](#)**Medium** Search

For me, it's the final stretch to completing the SOC Level 1 learning path. I have completed all the phishing rooms already early on before...

Aug 6, 2023  39  1

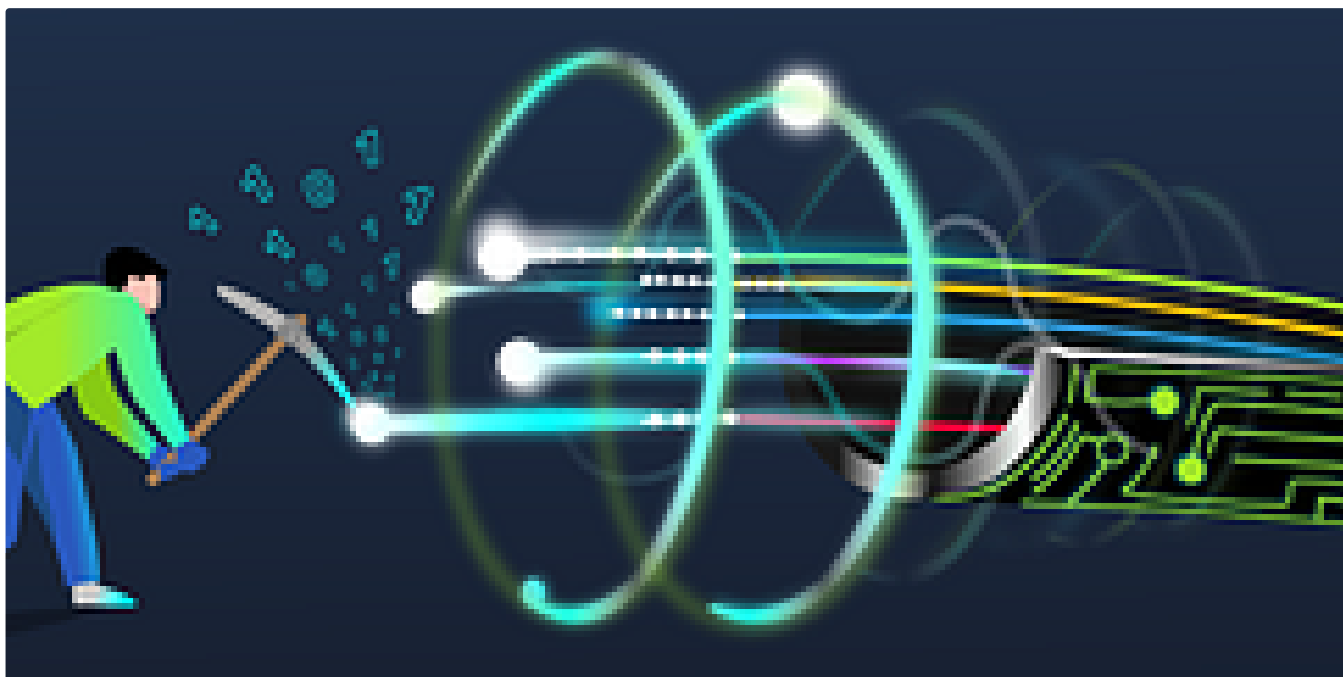


 Toumo

## TryHackMe Velociraptor Write-Up

We'll be learning about Velociraptor now. Another tool that I never heard of but I wonder how this will be different compared to the rest...

Aug 9, 2023 🖱 20 💬 1



 Toumo

## TryHackMe NetworkMiner Write-Up

This time, we will be using a new tool called NetworkMiner. My assumption is that we're being exposed to many tools as we do not know what...

Jul 5, 2023 🖱 6 💬 1



See all from Toumo

## Recommended from Medium

```
rd.img.old  lib64      media  opt    root  sbin  srv  tmp  var      vmlinuz.old
            lost+found mnt    proc   run   snap  sys  usr      vmlinuz

var/log
log# ls
cloud-init-output.log  dpkg.log          kern.log          lxd              unattended-upgrades
cloud-init.log         fontconfig.log    landscape         syslog           wtmp
dist-upgrade          journal           lastlog          tallylog

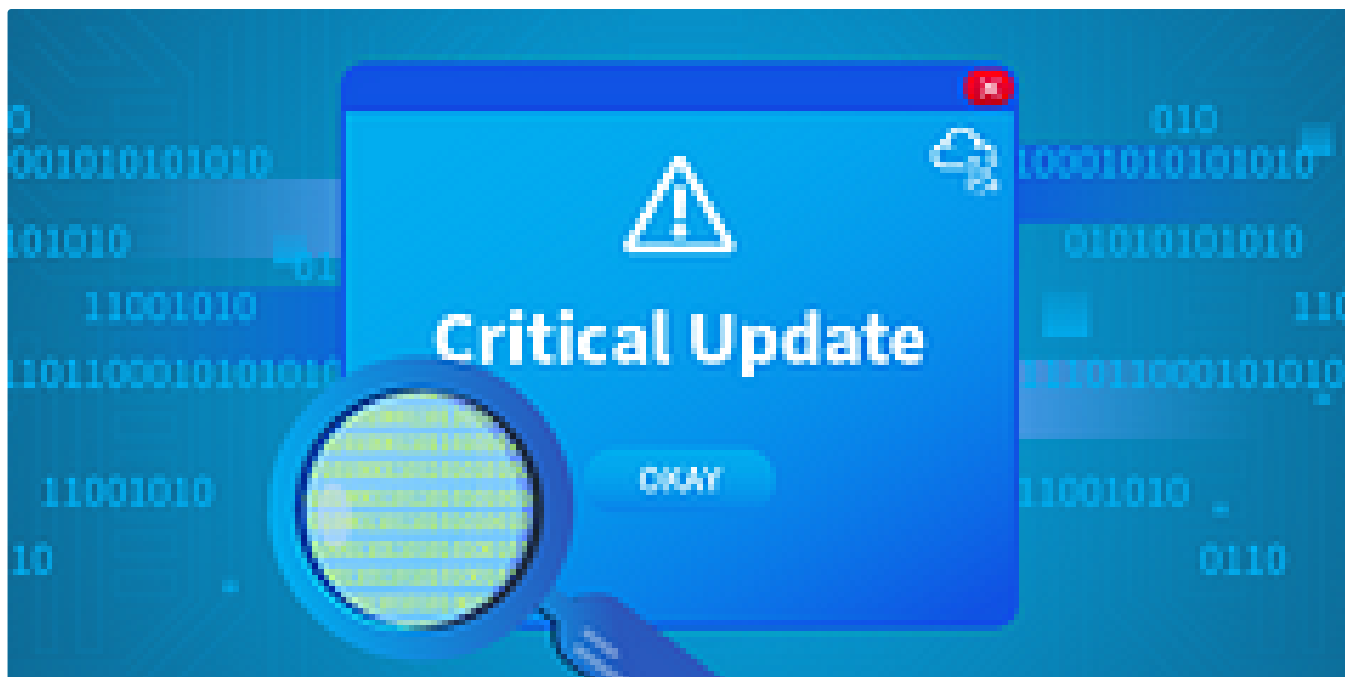
log# cat auth.log | grep install
8-55 sudo: cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/
8-55 sudo: cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/
8-55 sudo: cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/chow
hare/dokuwiki/bin /usr/share/dokuwiki/doku.php /usr/share/dokuwiki/feed.php /usr/s
hare/dokuwiki/install.php /usr/share/dokuwiki/lib /usr/share/dokuwiki/vendor -R
log#
```

T Dan Molina

## Disgruntled CTF Walkthrough

This is a great CTF on TryHackMe that can be accessed through this link here:  
<https://tryhackme.com/room/disgruntled>

Oct 22, 2024



In T3CH by Axoloth

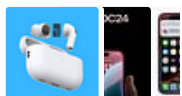
## TryHackMe | Critical | WriteUp

Acquire the basic skills to analyze a memory dump in a practical scenario.

★ Jul 21, 2024 🖱 104

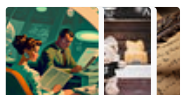


## Lists



### Tech & Tools

22 stories · 380 saves



### Medium's Huge List of Publications Accepting Submissions

377 stories · 4345 saves



### Staff picks

796 stories · 1561 saves



### Natural Language Processing

1884 stories · 1529 saves



 In T3CH by Axoloth

## TryHackMe | Snort Challenge—The Basics | WriteUp

Put your snort skills into practice and write snort rules to analyse live capture network traffic

★ Nov 9, 2024 🖱 100





In T3CH by Axoloth

## TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

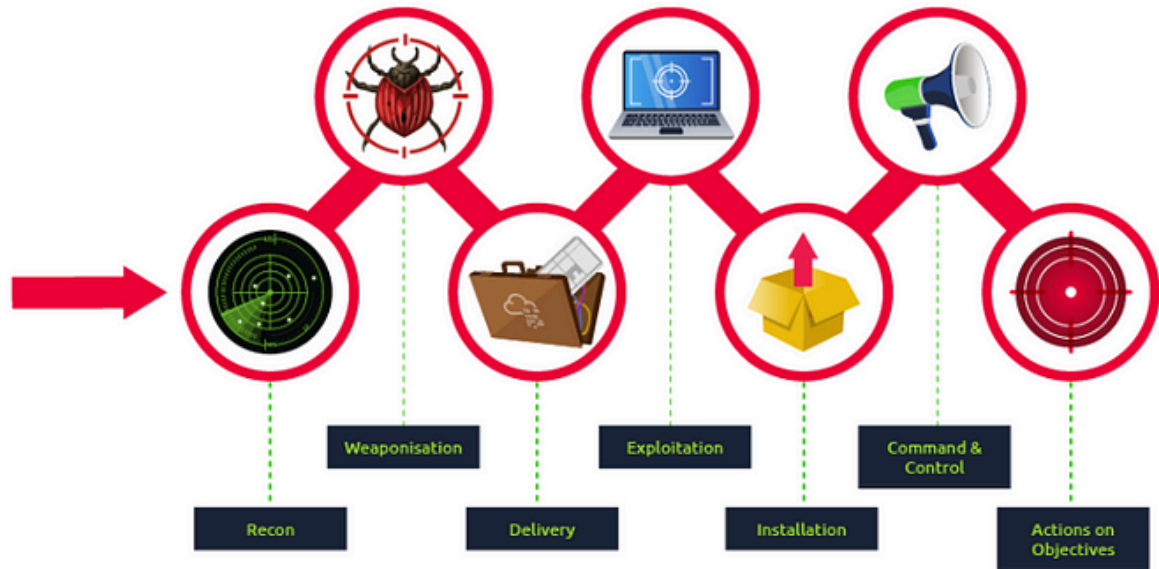



Nov 5, 2024



60





 RosanaFSS

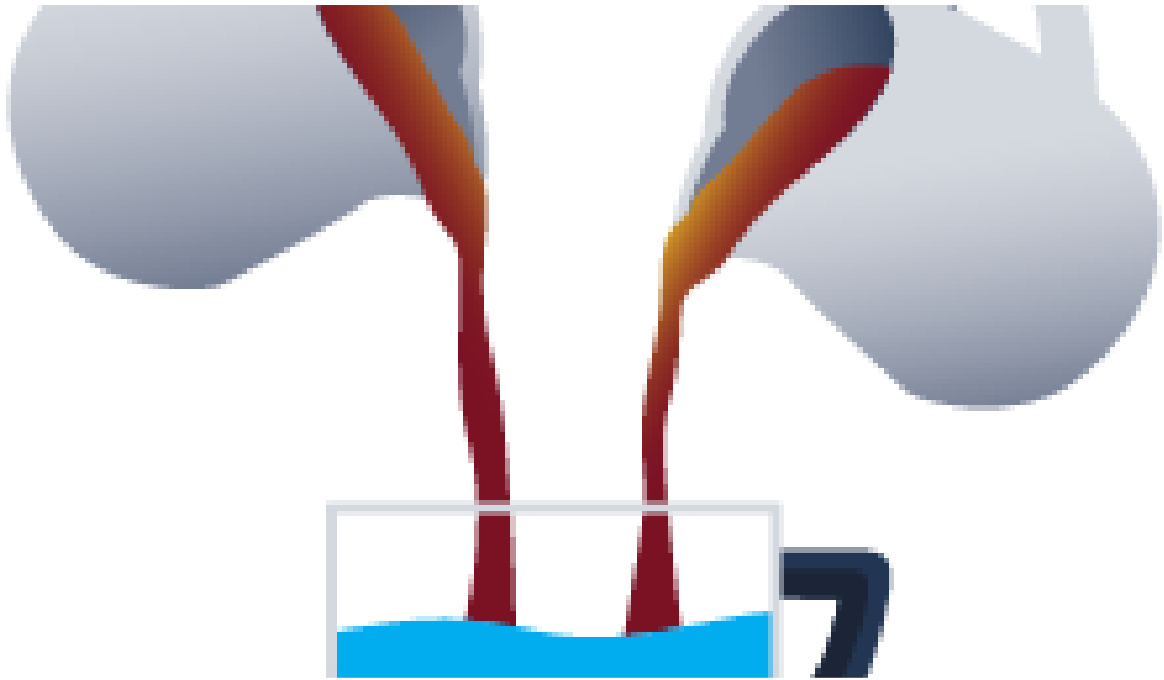
## TryHackMe: Threat Hunting With YARA, detailed Write-up

This room focuses on using YARA for threat hunting.

Nov 26, 2024







MAGESH

## Secret Recipe-Tryhackme Writeup

Perform Registry Forensics to Investigate a case.

Aug 21, 2024  2



See more recommendations