TryHackMe Intro to Malware Analysis Write-Up

Toumo · Follow
4 min read · Aug 9, 2023

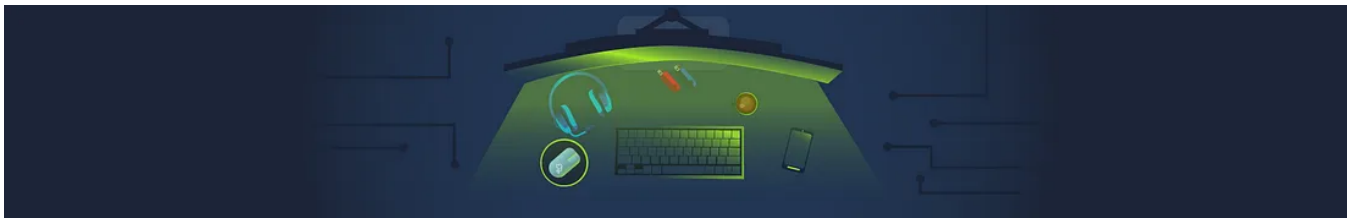


Image from tryhackme.com

This one seems to be a room more focused on Malware Analysis rather than artifacts left behind. I'm actually pretty interested in Malware Analysis too, so hopefully this will give me some basic idea and steps on how to proceed.

Task 2 Malware Analysis

1: Which team uses malware analysis to look for IOCs and hunt for malware in a network?

The answer can be found in the reading.

Answer: Threat hunt team

Task 3 Techniques of malware analysis

1: Which technique is used for analyzing malware without executing it?

The answer can be found in the reading.

Answer: Static analysis

2: Which technique is used for analyzing malware by executing it and observing its behavior in a controlled environment?

The answer can be found in the reading.

Answer: Dynamic analysis

Task 4 Basic Static Analysis

1: In the attached VM, there is a sample named ‘redline’ in the Desktop/Samples directory. What is the md5sum of this sample?

We’re going to navigate to where the Samples are. I did this with `cd ~/Desktop/Samples/` . Now we should be where the files are at. Type `md5sum redline` and it should output the md5 hash for redline.

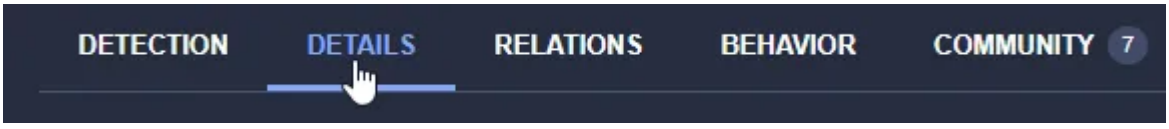
```
ubuntu@ip-10-10-231-62:~/Desktop/Samples$ md5sum redline
ca2dc5a3f94c4f19334cc8b68f256259  redline
```

You can highlight the hash and use Shift+Ctrl+C to copy it and then paste it with Ctrl+V to the answer page.

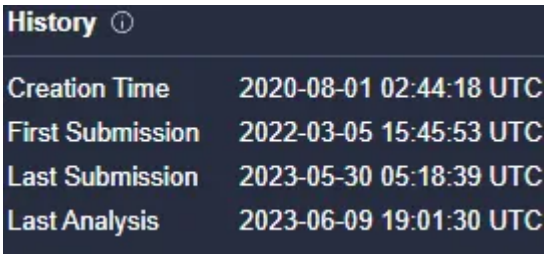
Answer: ca2dc5a3f94c4f19334cc8b68f256259

2: What is the creation time of this sample?

I copied the hash and went over to VirusTotal. I pasted the md5 hash and searched. Head over to the Details section.



Scroll down a little and you’ll come across the history. Creation time can be found there.



Answer: 2020–08–01 02:44:18 UTC

Task 5 The PE file Header

1: In the attached VM, there is a sample named ‘redline’ in the directory Desktop/Samples. What is the entropy of the .text section of this sample?

Simply type `pecheck redline` and then look for “.text entropy.”

```
ubuntu@ip-10-10-231-62:~/Desktop/Samples$ pecheck redline
PE check for 'redline':
Entropy: 7.999627 (Min=0.0, Max=8.0)
MD5     hash: ca2dc5a3f94c4f19334cc8b68f256259
SHA-1   hash: ce9943d9efc7d5f10cac4ab0b5aa48d62a063852
SHA-256 hash: e8ba49a75de083cb786e8ed84972affa11542dd913f1a07b0d44e1d45e5e22e9
SHA-512 hash: 8c774f64631342c2465d166cd4c374356c40c1cf6bae13b2e0b003ce6c85e397da799f111cbbed638d548029c555f31156c2633d531fa1b20160d7904fa17d75
.text entropy: 6.453919 (Min=0.0, Max=8.0)
.rdata entropy: 5.136718 (Min=0.0, Max=8.0)
.data entropy: 4.096809 (Min=0.0, Max=8.0)
.ndata entropy: 0.000000 (Min=0.0, Max=8.0)
.rsrc entropy: 4.209687 (Min=0.0, Max=8.0)
```

Answer: 6.453919

2: The sample named ‘redline’ has five sections. .text, .rdata, .data and .rsrc are four of them. What is the name of the fifth section?

This can be found in the same section as the entropy value we just looked at.

Answer: .ndata

3: From which dll file does the sample named ‘redline’ import the RegOpenKeyExW function?

I typed in `pecheck redline | grep -i “regopenkey”` to help display results that has “regopenkey” in it. Grep has been really helping me a lot!

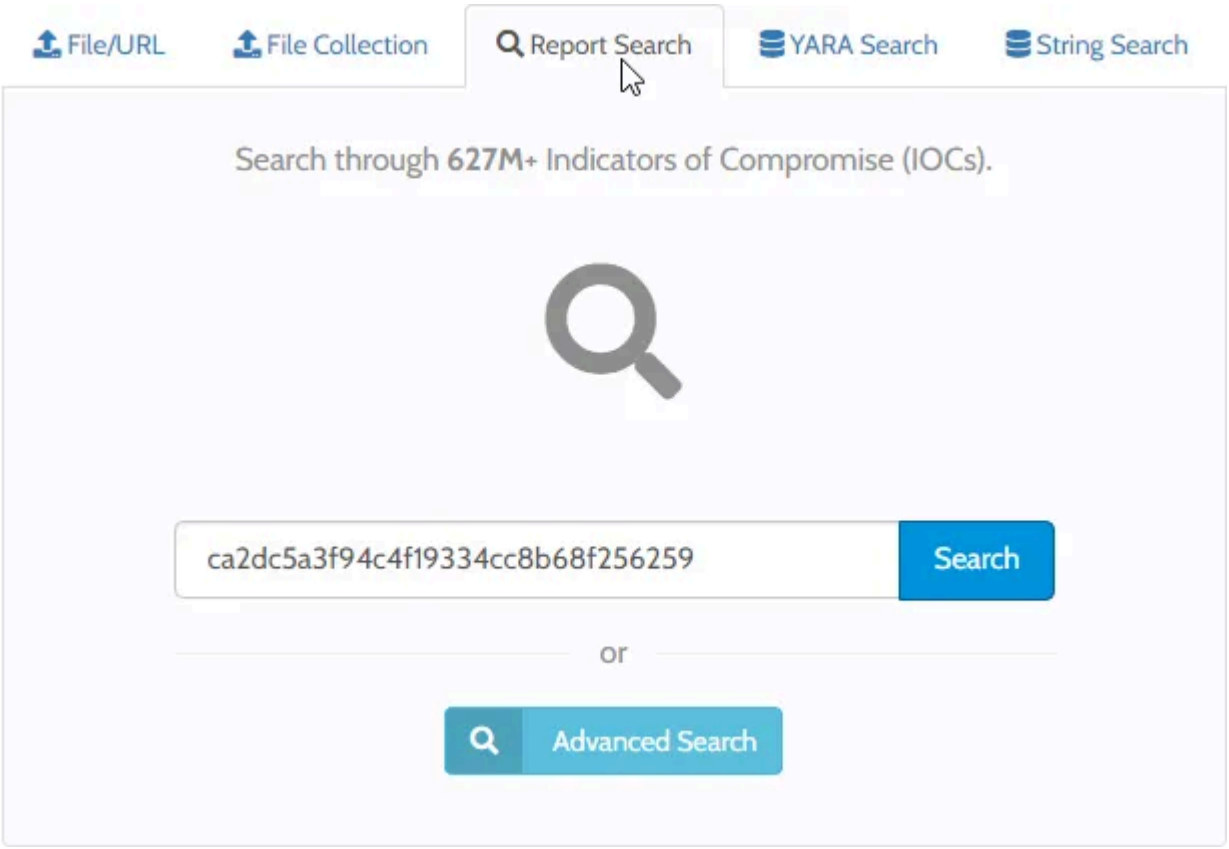
```
ubuntu@ip-10-10-231-62:~/Desktop/Samples$ pecheck redline | grep -i "regopenkey"
ADVAPI32.dll.RegOpenKeyExW Hint[493]
```

Answer: ADVAPI32.dll

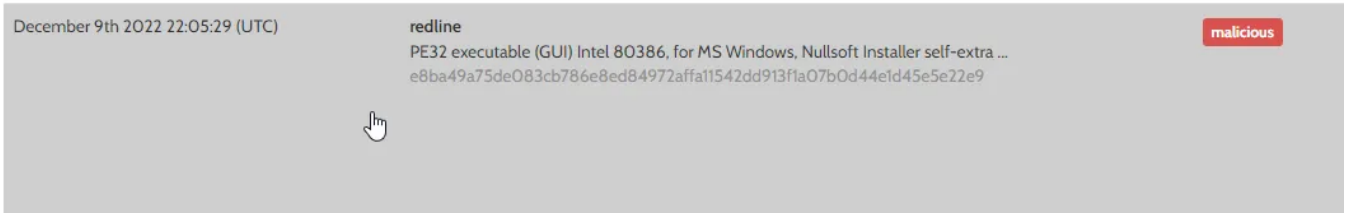
Task 6 Basic Dynamic Analysis

1: Check the hash of the sample ‘redline’ on Hybrid analysis and check out the report generated on 9 Dec 2022. Check the Incident Response section of the report. How many domains were contacted by the sample?

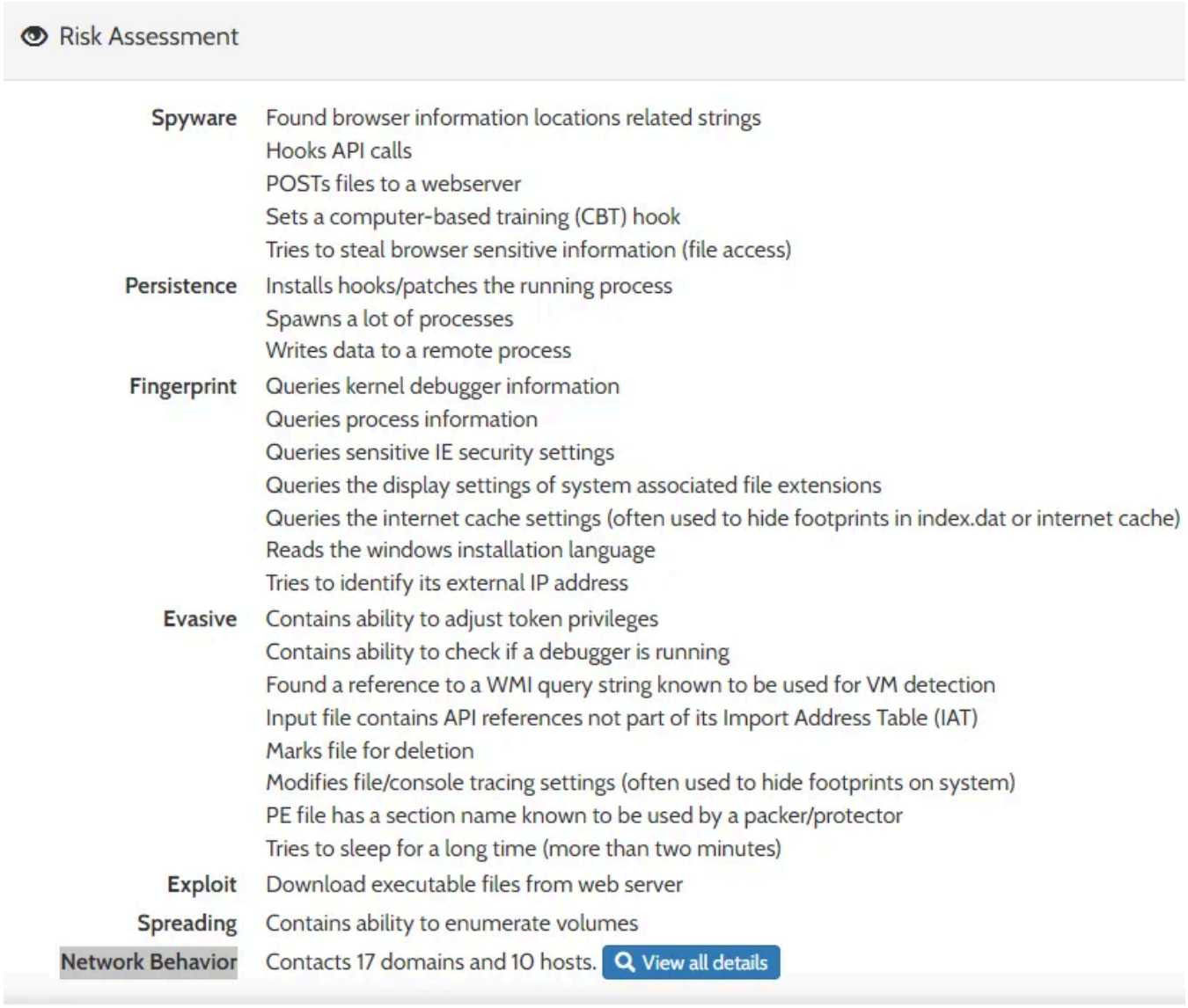
Head over to HybridAnalysis and input the hash and then search.



Look for the result that matches the date we need.



Once you click it, you should be presented with this information immediately. Scroll down a little to look for the number of domains.



Answer: 17

2: In the report mentioned above, a text file is accessed by the sample. What is the name of that text file?

Since it is a text file, I just searched for a .txt file with Ctrl+F and inputting .txt.

Answer: fj4ghga23_fsa.txt

Task 7 Anti-analysis techniques

1: Which of the techniques discussed above is used to bypass static analysis?

The answer can be found in the reading.

Answer: packing

2: Which technique discussed above is used to time out a sandbox?

The answer can be found in the reading.

Answer: long sleep calls

Thoughts:

This was a pretty light room. I'm pretty interested in the Malware Analysis series in THM. I think I saw it being mentioned when I was reading this room and browsing related rooms. I think I'll be adding HybridAnalysis into my bookmarks so I can read what some malware does occasionally.

I'm done with the entire THM SOC Level 1 Learning Module as I've already done the phishing rooms before doing my write-ups. I plan on redoing the ones I did pre-write-up to complete my write-up collection too! It'll probably be later in the future but before the end of the year (2023)!

Cybersecurity Tryhackme Malware Analysis Soc

Responses (1)

What are your thoughts?

Respond

Samar
about 2 months ago

thanks

Reply

More from Toumo

Toumo

TryHackMe Windows Event Logs Write-Up

After learning about the tool suite, Sysinternals, we are now going to be learning about logs, specifically Windows Event Logs. I'm...

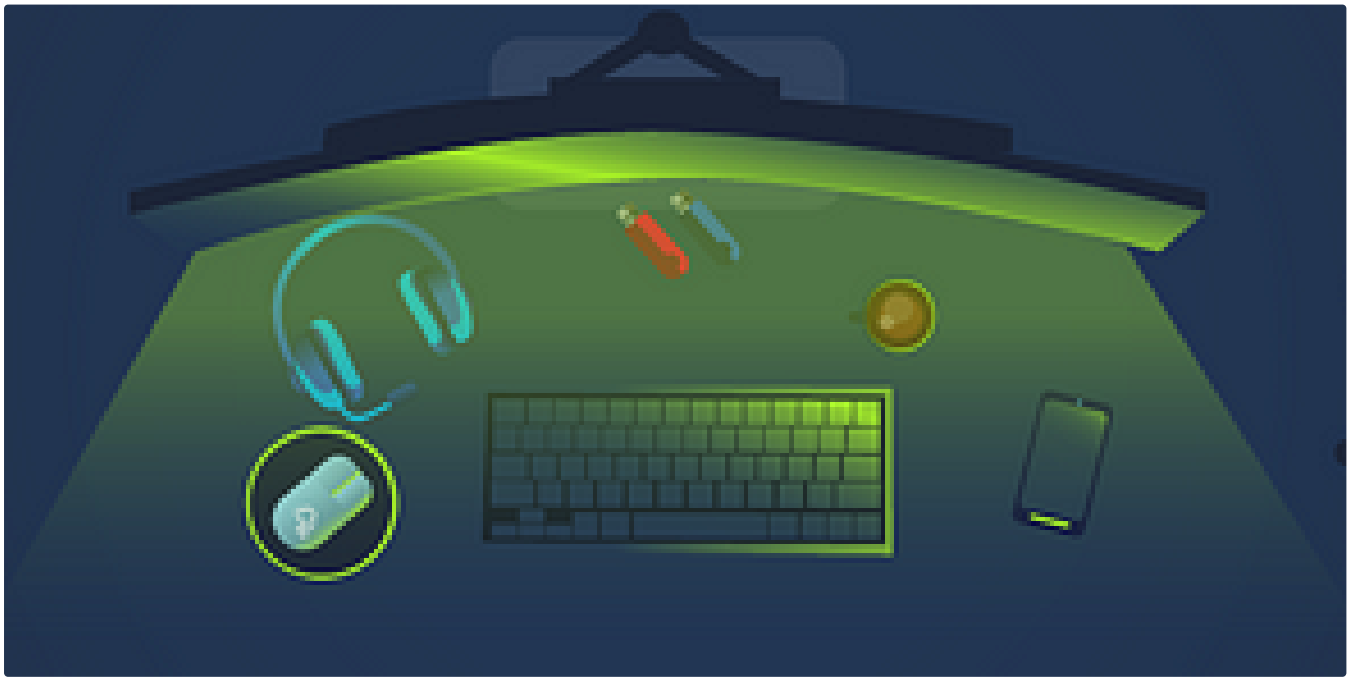
Jul 17, 2023 13

Toumo

How to RDP Into a TryHackMe Windows Machine With Your Kali VM

I will give a step by step instruction on how to use your own Kali VM and remote desktop protocol (RDP) into a Windows machine that you...

Jul 24, 2023 48 1

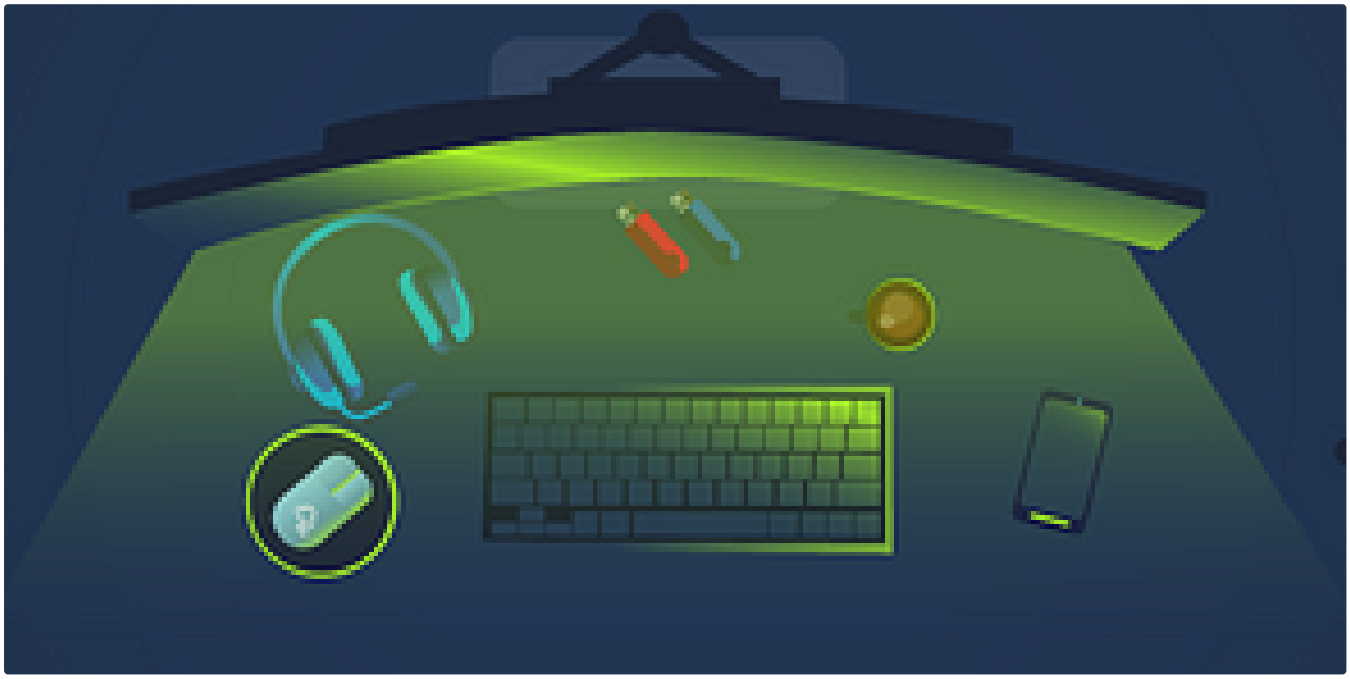


Toumo

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



Toumo

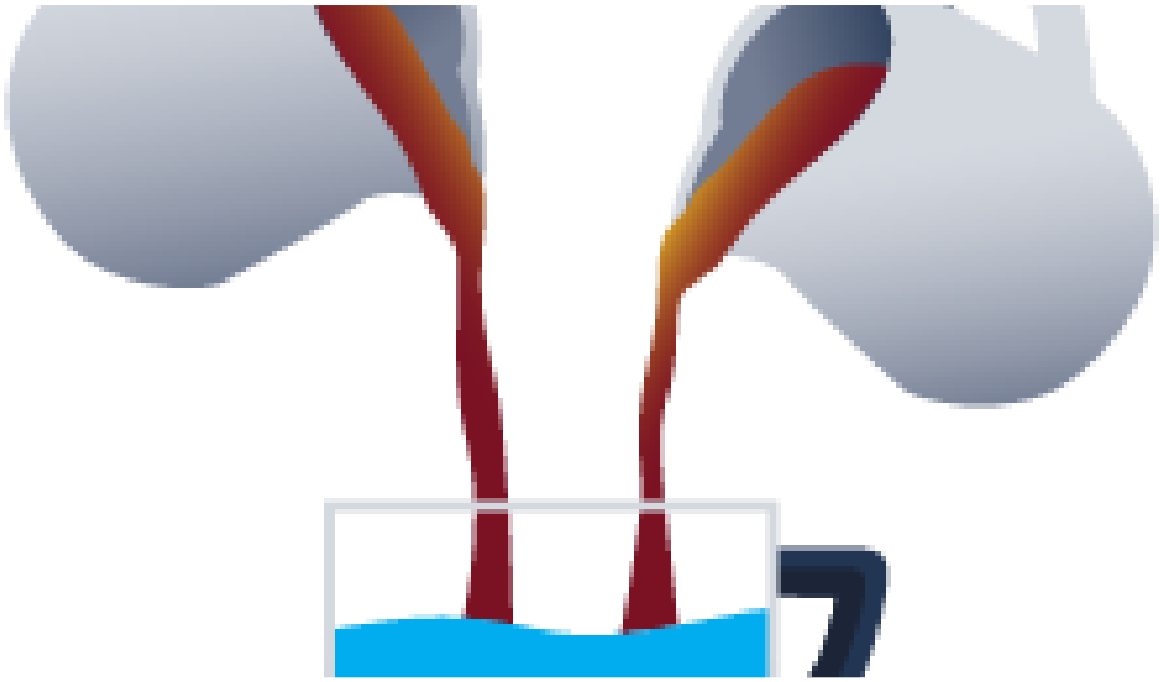
TryHackMe Windows Forensics 1 Write-Up

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

See all from Toumo

Recommended from Medium

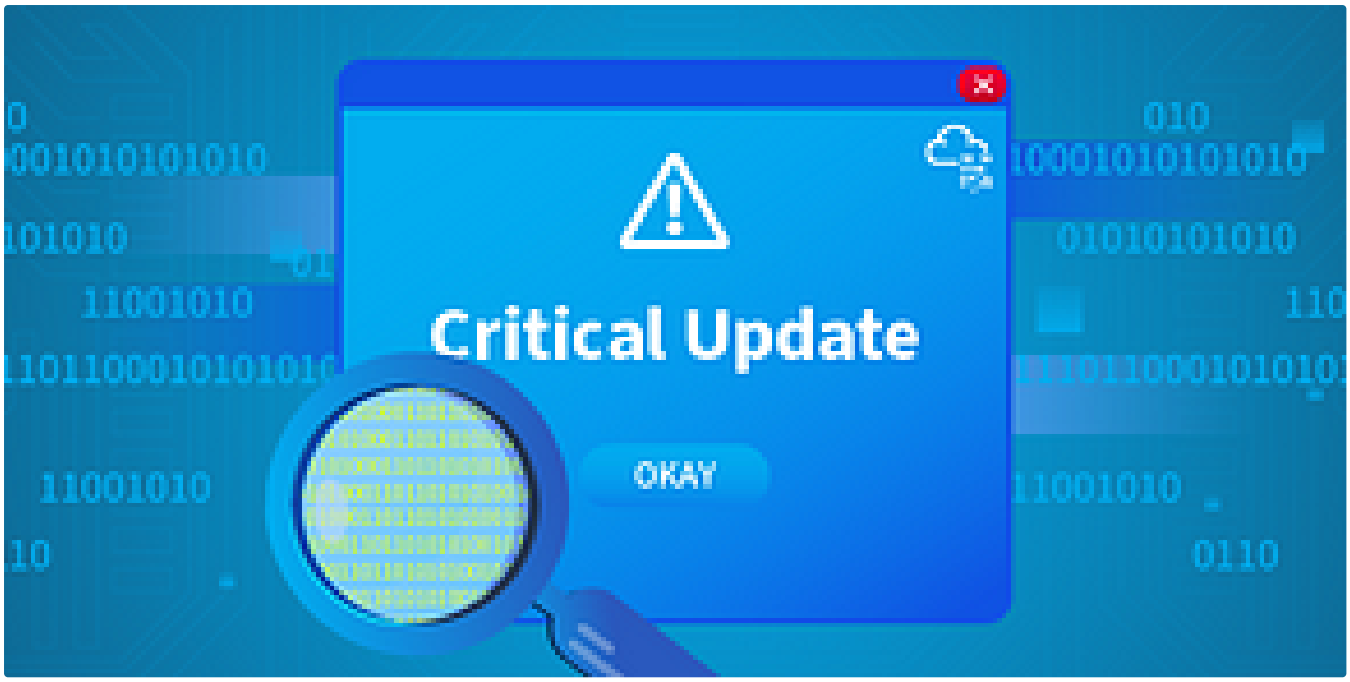


MAGESH

Secret Recipe-Tryhackme Writeup

Perform Registry Forensics to Investigate a case.

Aug 21, 2024 2



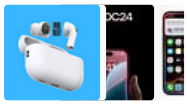
In T3CH by Axoloth

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 · 377 saves

Medium's Huge List of Publications Accepting Submissions

377 stories · 4318 saves

Staff picks

793 stories · 1549 saves

Natural Language Processing

1883 stories · 1521 saves

Trnty

TryHackMe | Introduction To Honeypots Walkthrough

A guided room covering the deployment of honeypots and analysis of botnet activities

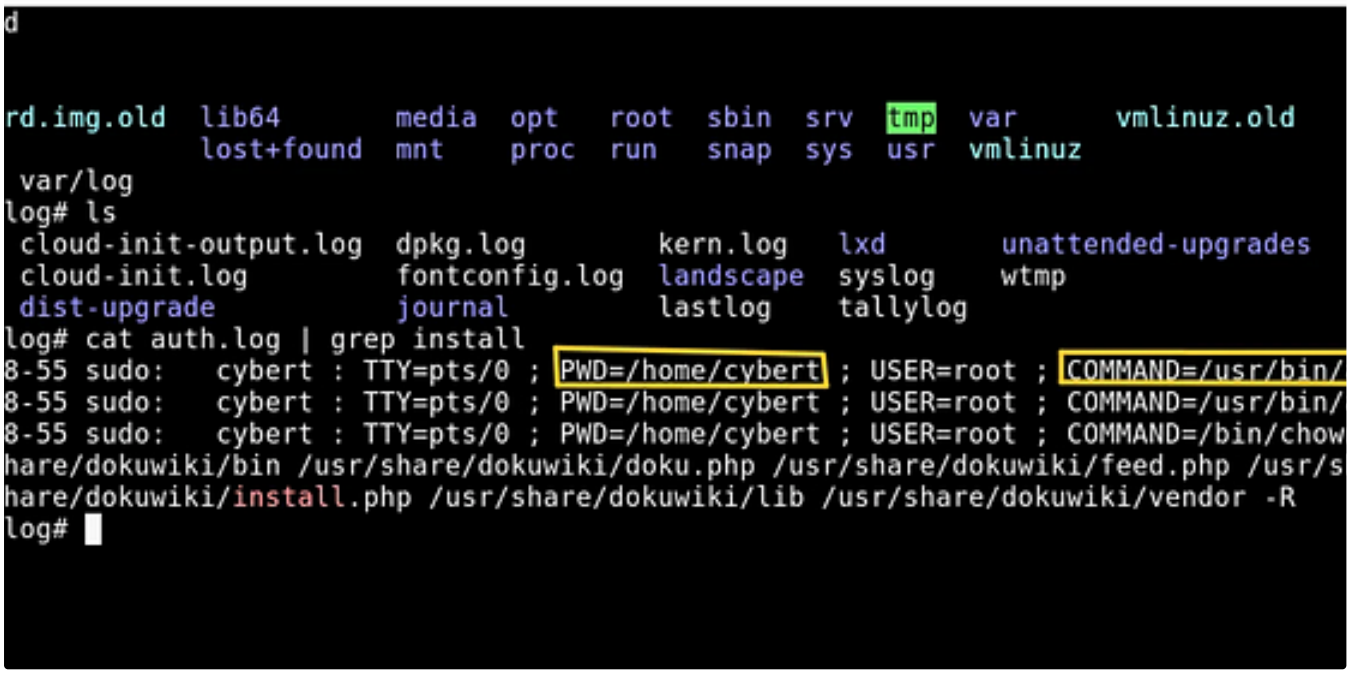
Sep 7, 2024 10

In T3CH by Axoloth

TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

Nov 28, 2024 50



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 System Weakness by Joseph Alan

TryHackMe Critical Write-Up: Using Volatility For Windows Memory Forensics

This challenge focuses on memory forensics, which involves understanding its concepts, accessing and setting up the environment using tools...

Jul 18, 2024 46 1