TryHackMe ItsyBitsy Write-Up

Toumo · Follow
4 min read · Aug 6, 2023

Listen Share More

Image from tryhackme.com

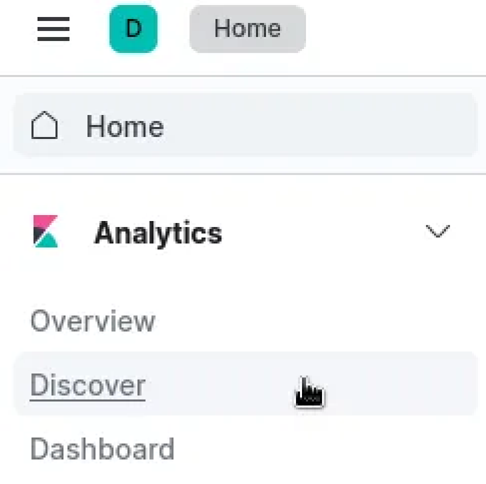
After finishing the last room, it's time to try our hands in solving a few questions! Try to do your best without looking for help. If you do need help, try to only look at the question you are stuck on and then try to solve the rest yourself again!

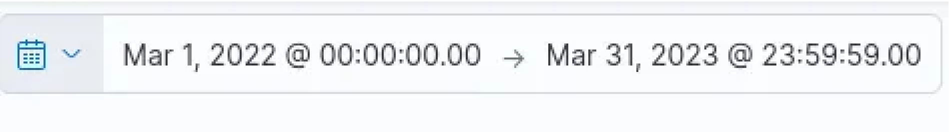
Task 2 Scenario — Investigate a potential C2 communication alert

Similar to the last room, I connected to THM's network using OpenVPN on my Kali. Partial directions are given in my RDP room on how to connect to the network. Once you are in THM's network, open a browser and then type in the IP address that should populate when you start the machine. In this instance, mine was 10.10.34.200.

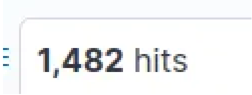
1: How many events were returned for the month of March 2022?

Similar to the previous room where we learned about the ELK Stack, I clicked on the hamburger icon and went to "Discover" to go to the page where I can view the logs. From there, I changed the date on the top right to fit the criteria as stated in the question. Finally, I just had to update the results and got my answer.





Mar 1, 2022 @ 00:00:00.00 → Mar 31, 2023 @ 23:59:59.00

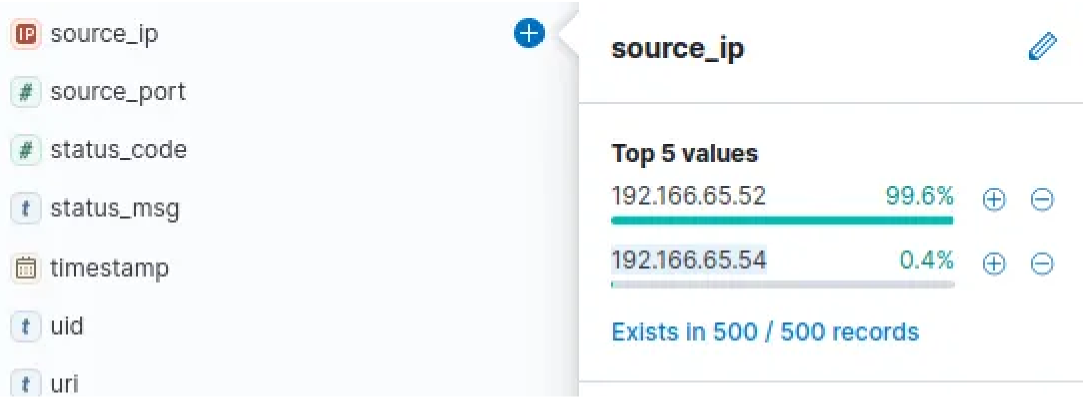


1,482 hits

Answer: 1482

2: What is the IP associated with the suspected user in the logs?

With the results, I went to the left side to start filtering some results. I clicked on "source_ip" and looked at what IP addresses came up. Looks like we have only two, so one of these is the answer!



source_ip

Top 5 values

192.166.65.52	99.6%
192.166.65.54	0.4%

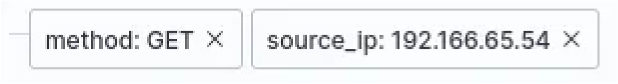
Exists in 500 / 500 records

Naturally I picked the one that had the largest hits but it was wrong.

Answer: 192.166.65.54

3: The user's machine used a legit windows binary to download a file from the C2 server. What is the name of the binary?

My thought process was that since we are downloading a file, we may want to use a filter. I filtered the method and looked for "GET" with our IP address. This was the filter I used.



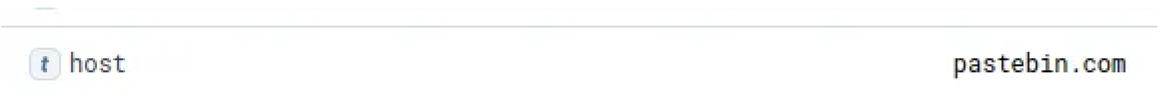
method: GET ×   source_ip: 192.166.65.54 ×

With only one result, I looked into the log and saw bitsadmin as user_agent. I searched what it was, and Microsoft states that it is "a command-line tool used to create, download or upload jobs, and to monitor their progress." Seems like we may have found what we are looking for.

Answer: bitsadmin

4: The infected machine connected with a famous filesharing site in this period, which also acts as a C2 server used by the malware authors to communicate. What is the name of the filesharing site?

With the same 1 result, I looked further to see what site it tried to connect to.

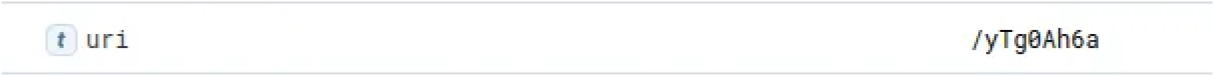


t host	pastebin.com

Answer: pastebin.com

5: What is the full URL of the C2 to which the infected host is connected?

In the same 1 result, I found the URI. Combining this with the site from above, our end result should be pastebin.com/yTg0Ah6a.

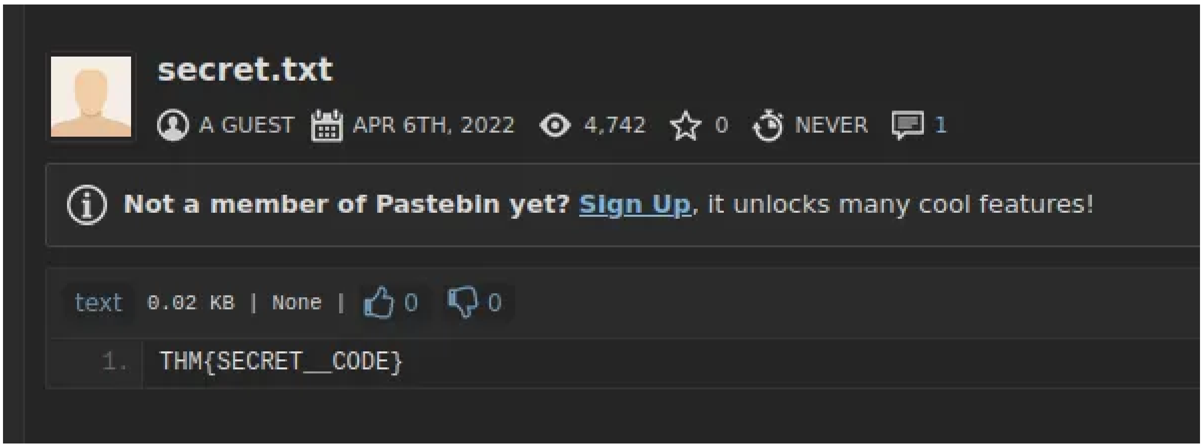


t uri	/yTg0Ah6a

Answer: pastebin.com/yTg0Ah6a

6: A file was accessed on the filesharing site. What is the name of the file accessed?

After combining both, I pasted the link into my address bar and went to see where the link will take me.



secret.txt

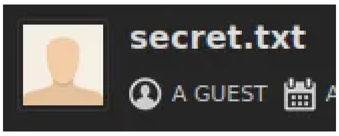
A GUEST APR 6TH, 2022 4,742 0 NEVER 1

Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

text 0.02 KB | None | 0 0

```
THM{SECRET__CODE}
```

Looks like we are at the end of the room. The name of the file can be found on the top.



secret.txt

A GUEST

Answer: secret.txt

7: The file contains a secret code with the format THM{_____}.

Answer: THM{SECRET__CODE}

Thoughts:

I enjoyed it. I'm no expert but I personally felt it was on the easier side. That being said, I still did mess up by choosing the 99% IP presence instead of the 0.4%, so there's still some things for me to learn, such as the thinking process of an expert.

I won't be doing the next few Splunk rooms as I've already completed them. I will eventually come back and do those again and do a write-up to complete the SOC Level 1 learning path, and to remember how to use Splunk. The next part of my write-ups will be forensics!

Cybersecurity Tryhackme Siem Kibana Elk Stack

T

Follow

Written by Toumo

151 Followers · 1 Following

Responses (1)

What are your thoughts?

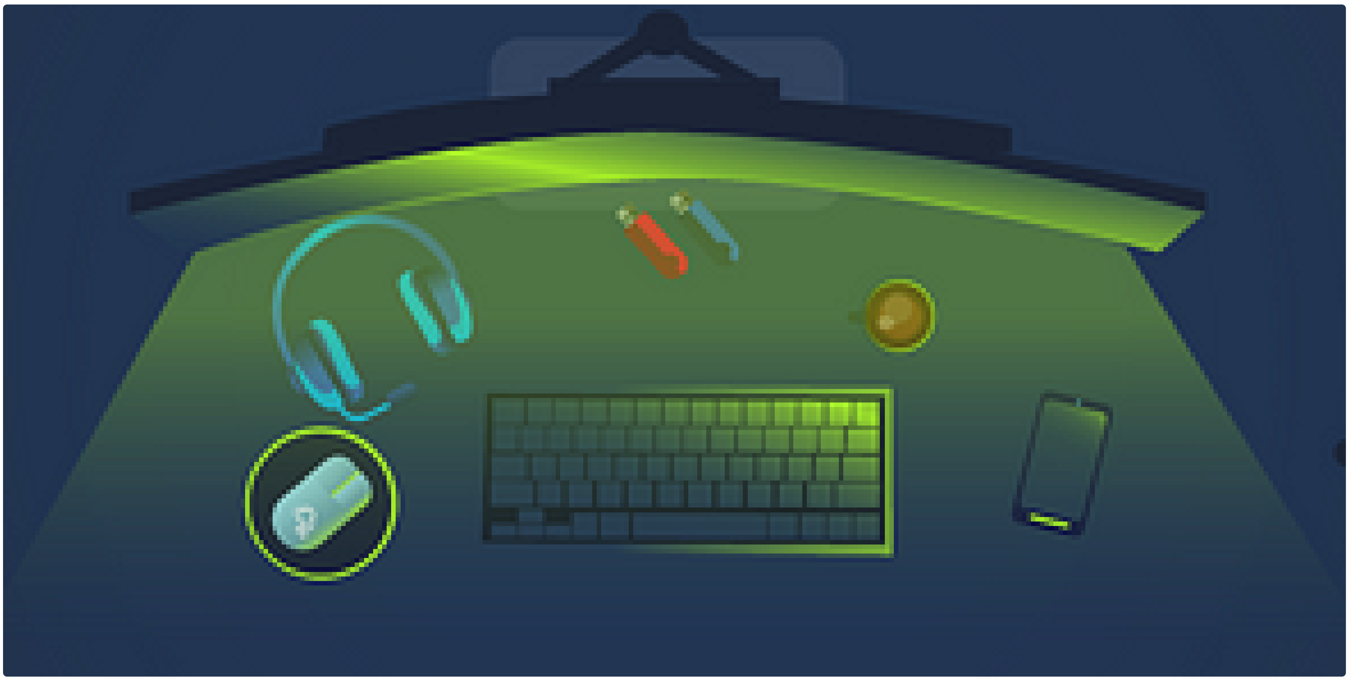
Respond

Samar
about 2 months ago

thanks

Reply

More from Toumo



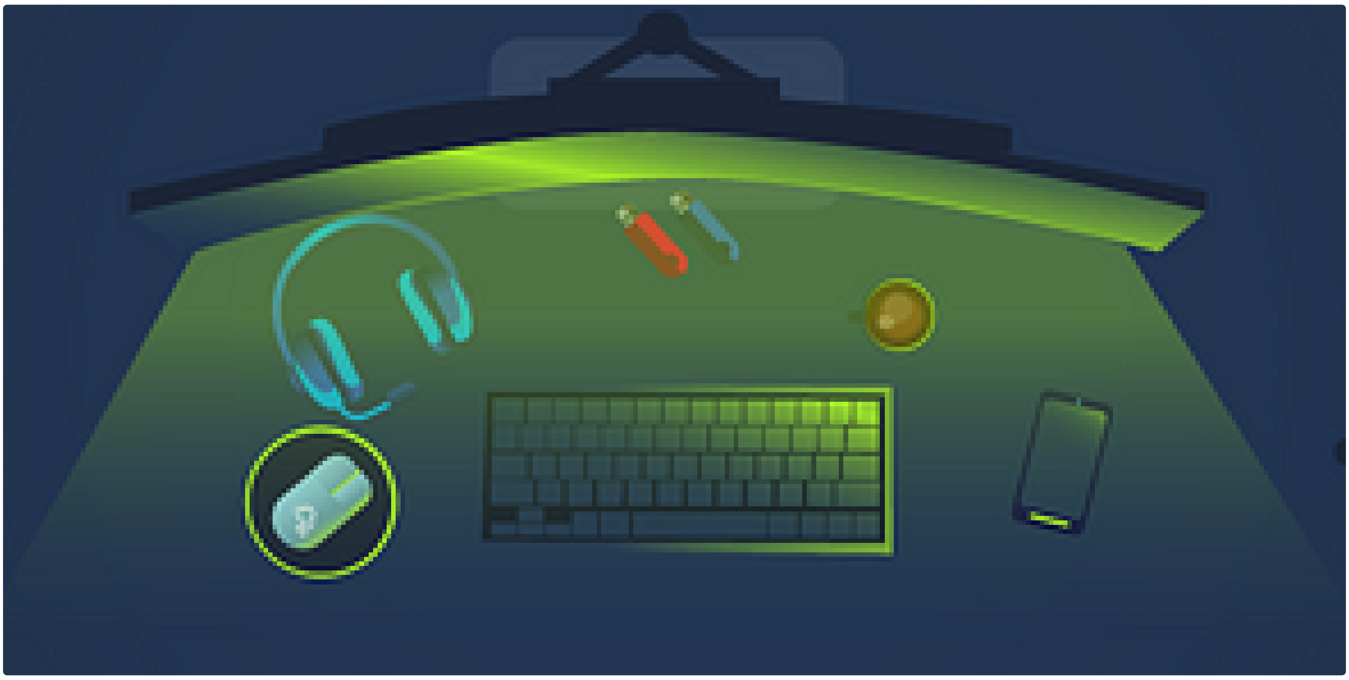
T Toumo

TryHackMe Redline Write-Up

We just finished the Autopsy room and now we will be learning how to use Redline. I've never

Open in app ↗

Medium Search

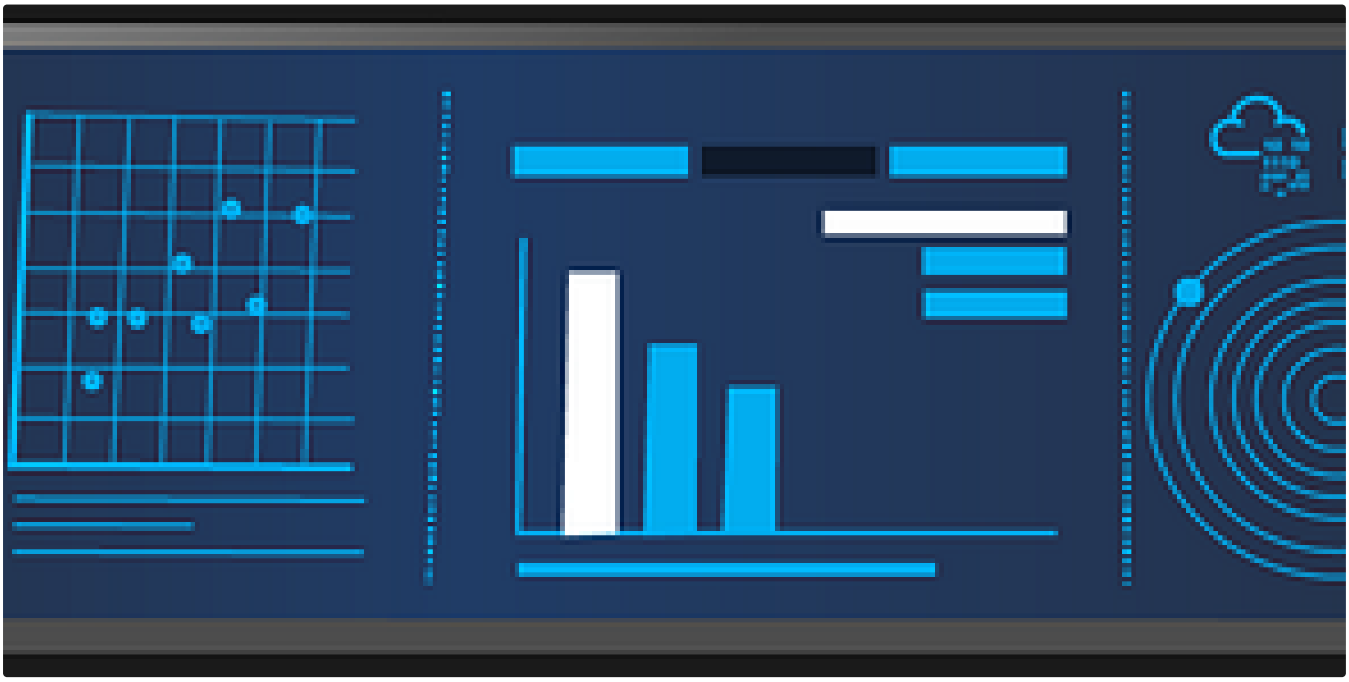


T Toumo

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

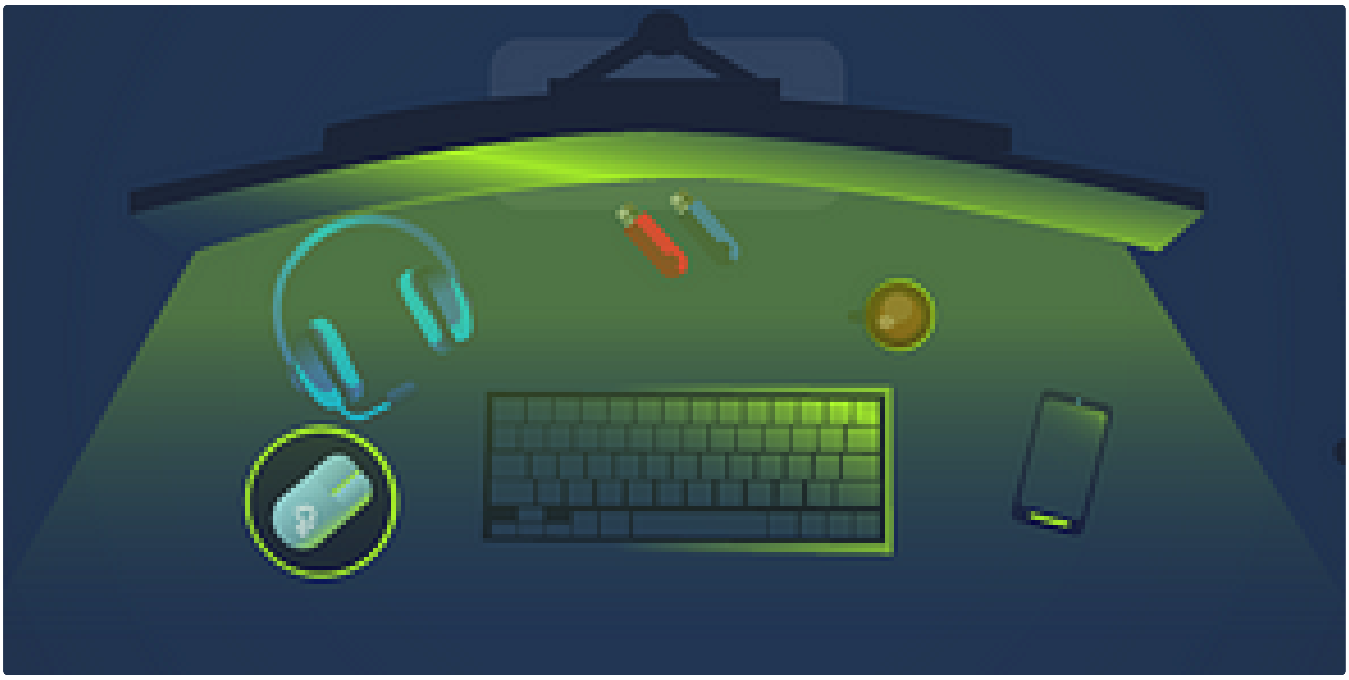


Toumo

TryHackMe Incident handling with Splunk Write-Up

I did the introductory Splunk room after a long break. I felt like the introductory room was pretty basic the second time around but it...

Sep 12, 2023 4



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

See all from Toumo

Recommended from Medium

In T3CH by Axoloth

TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

Nov 28, 2024 50

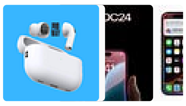
In T3CH by Axoloth

TryHackMe | Search Skills | WriteUp

Learn to efficiently search the Internet and use specialized search engines and technical docs

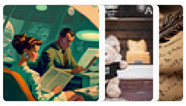
✦ Oct 26, 2024 61

Lists



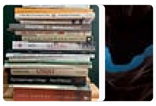
Tech & Tools

22 stories · 377 saves



Medium's Huge List of Publications Accepting Submissions

377 stories · 4321 saves



Staff picks

793 stories · 1549 saves

Natural Language Processing

1883 stories · 1524 saves

Fritzadriano

Retracted — TryHackMe WriteUp

IInvestigate the case of the missing ransomware. After learning about Wazuh previously, today's task is a bit different.

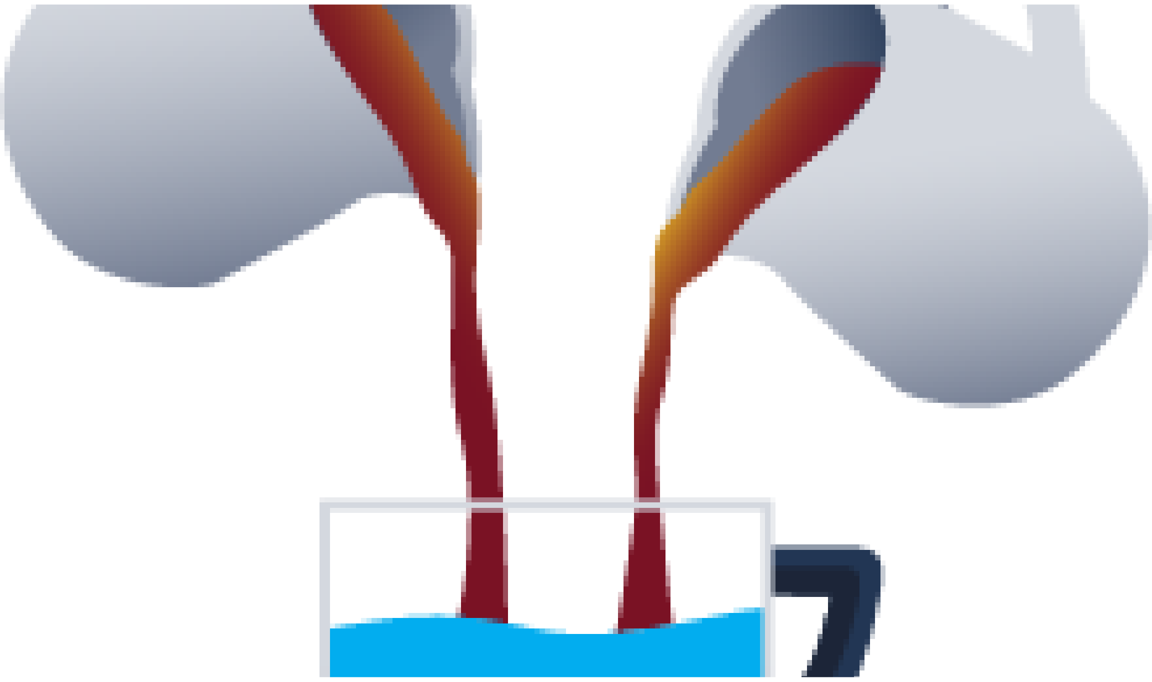
Sep 4, 2024 50

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



MAGESH

Secret Recipe-Tryhackme Writeup

Perform Registry Forensics to Investigate a case.

Aug 21, 2024 2

Daouda Diallo

TryHackMe : Trooper Writeup

Synopsis : " A global tech company has suffered several cyber attacks recently, leading to stolen intellectual property and operational…

Aug 15, 2024 👏 1

See more recommendations