TryHackMe Investigating with ELK 101 Write-Up

Toumo · Follow
7 min read · Aug 5, 2023

Image from tryhackme.com

Now that we're all done with Endpoint Security Monitoring, we are moving on to Security Information and Event Management (SIEM). I mentioned this before but I have already done the Splunk labs, so redoing them and creating a write-up *at this current time* is low on my priority list. That being said, I am always up for more hands-on experience so I do want to do more Splunk labs in preparation for BTL1. We're going to be using ELK for our SIEM. I never heard of ELK before admittedly, so as always, being exposed to more tools is great for a beginner like me. Let's get started!

Task 3 ElasticStack Overview

1: Logstash is used to visualize the data. (yay / nay)

This is Kibana's function.

Answer: Nay

2: Elasticstash supports all data formats apart from JSON. (yay / nay)

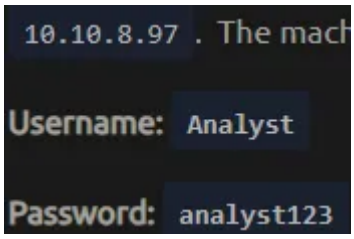
It's actually the opposite. It supports JSON. Both the answers can be found in the reading.

Answer: Nay

Task 4 Kibana Overview

Make sure you're connected to TryHackMe's network using a VPN. You can read how over here. I downloaded my configuration file and connected using OpenVPN on my Kali Linux VM.

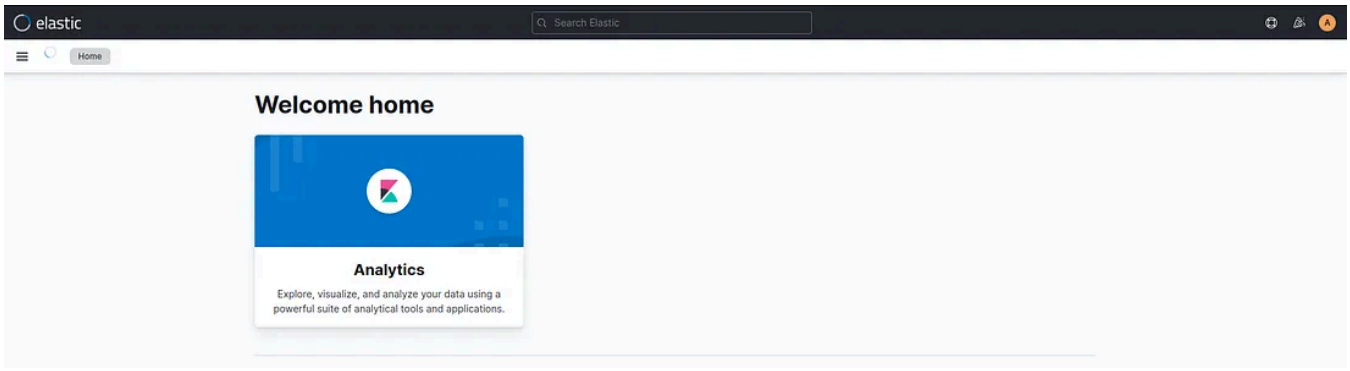
Once you're connected, open a browser and then type in the IP address that should populate when you start the machine. For me, mine was 10.10.8.97.

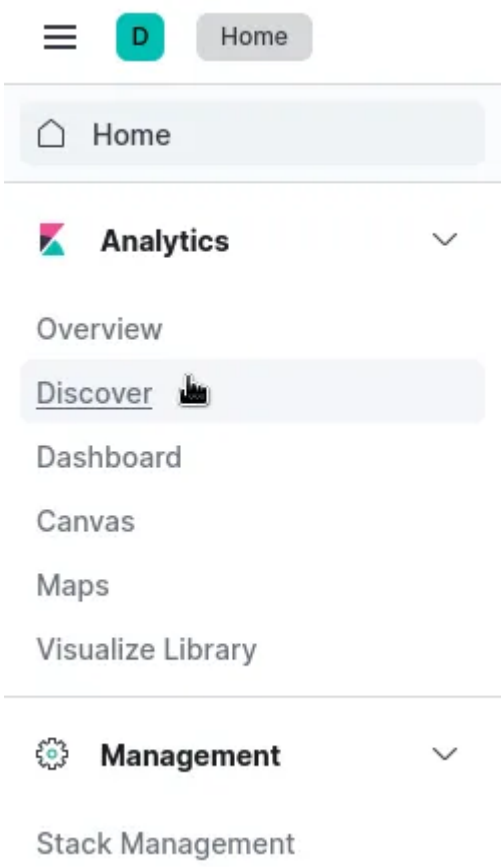


Task 5 Discover Tab

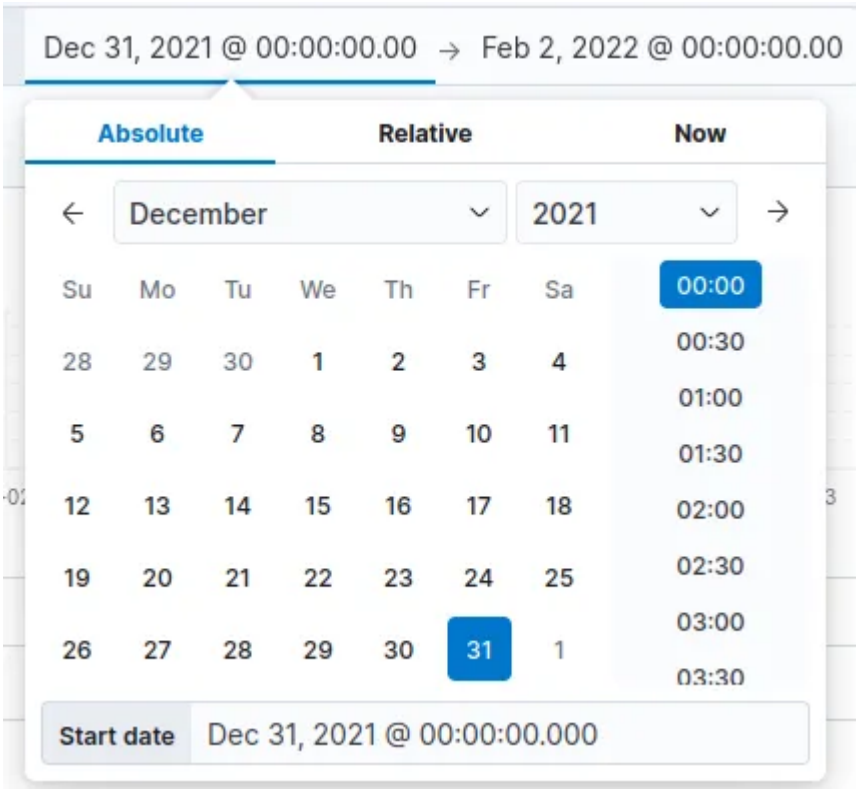
1: Select the index **vpn_connections** and filter from 31st December 2021 to 2nd Feb 2022. How many hits are returned?

Once you typed the IP of the machine, you should be greeted with this screen. Click on the hamburger sign at the top left and then click on "Discover."





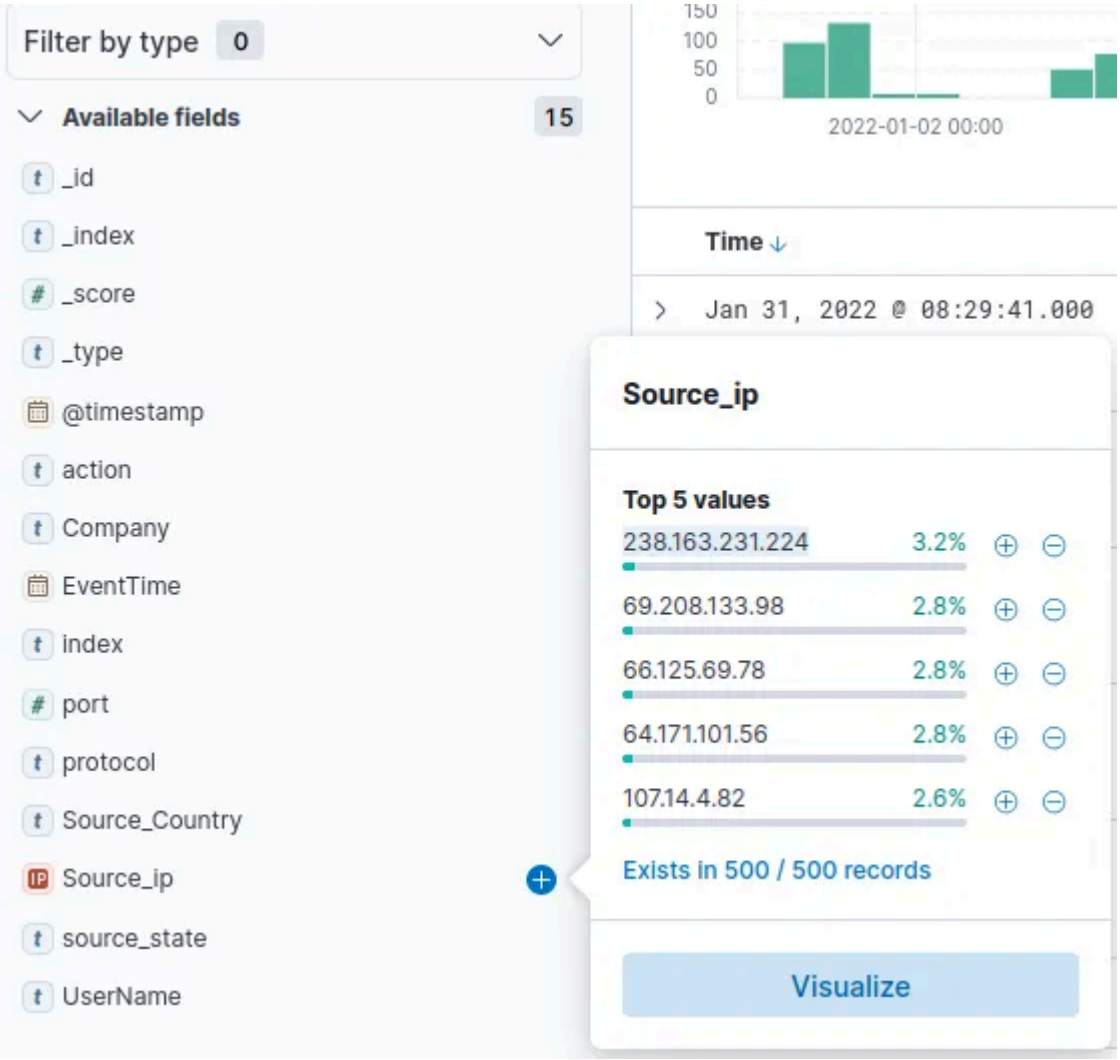
From here, you should be greeted with a search bar. There may or may not be any results currently, but it's ok. We are going to change it to get our answer. On the top right, there should be some dates or time references. We will be changing that to match what we need for our answer. Click on "Refresh" to populate the new results.



Answer: 2861

2: Which IP address has the max number of connections?

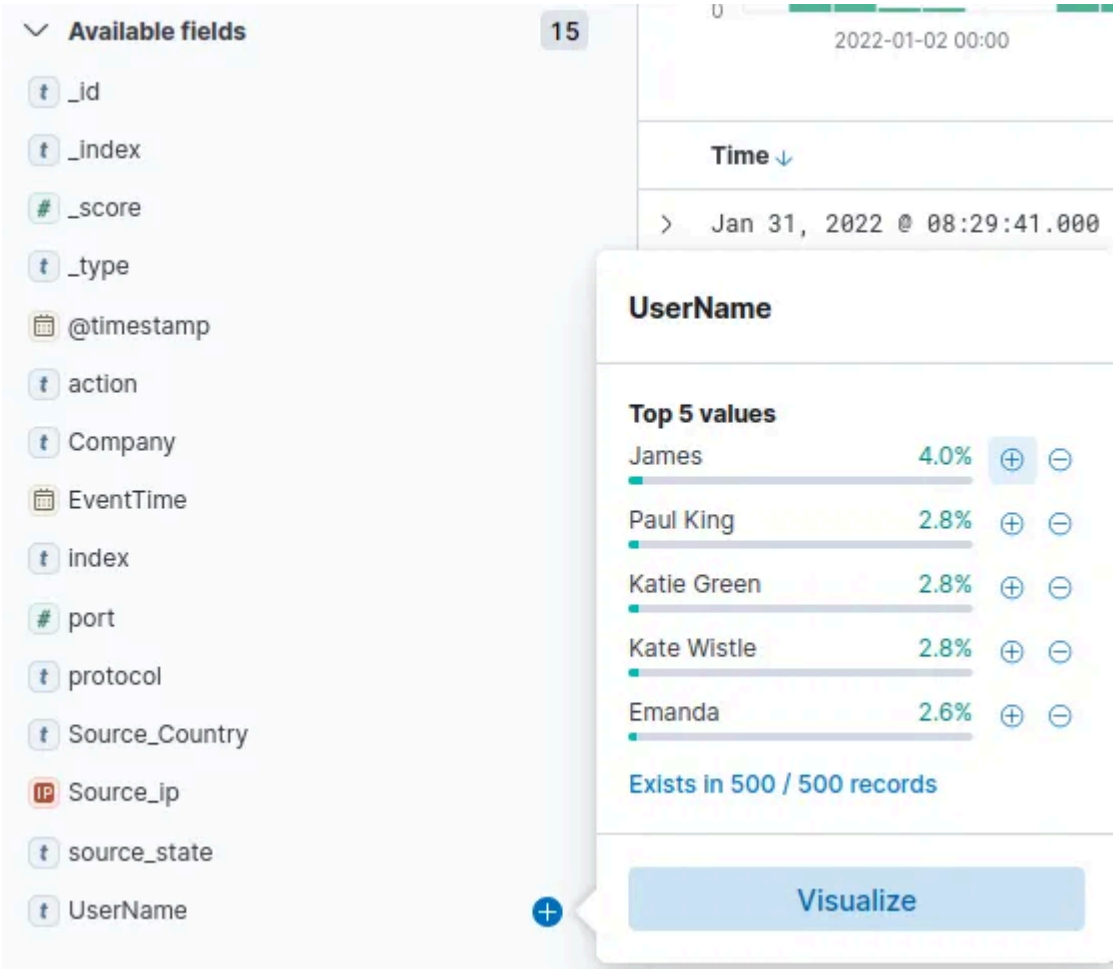
With the results, we can filter it to match what we are looking for. In this case, we are looking for IP addresses and most connections. Click on “Source_ip” and look at which IP address shows up the most. By default, it shows the top 5 values.



Answer: 238.163.231.224

3: Which user is responsible for max traffic?

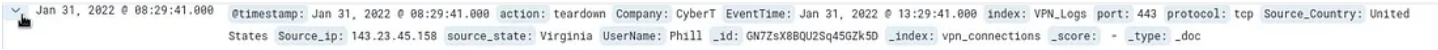
Very similar to above, but we will look at UserName instead.



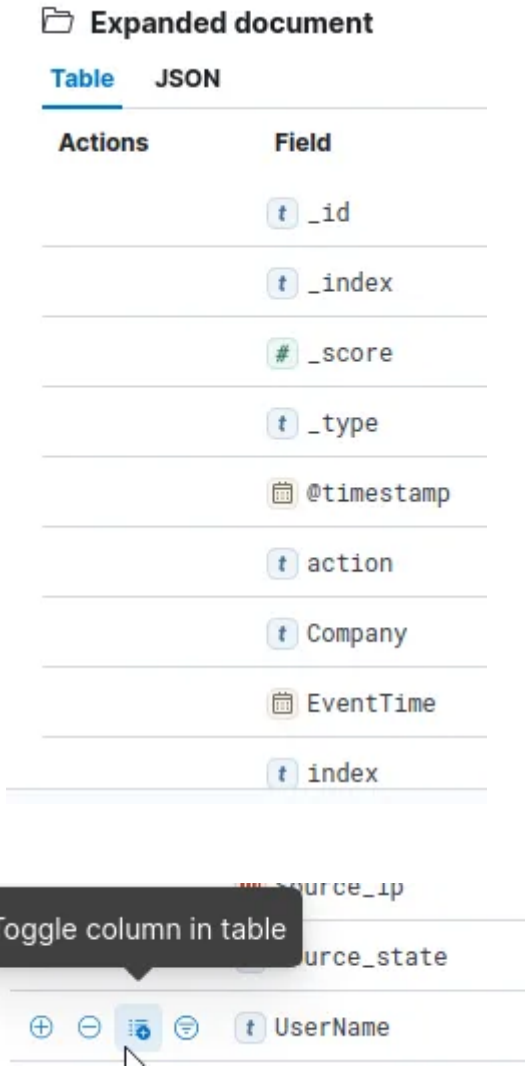
Answer: James

4: Create a table with the fields IP, UserName, Source_Country and save.

I thought this was useful, so I added this in despite having no answer.



From here, you can create a new table for yourself to display what you want to see. In our case, we want to create one with IP, UserName, and Source_Country. What we will do is find the appropriate fields and then click the third from the left icon. It should say “Toggle column in table.”

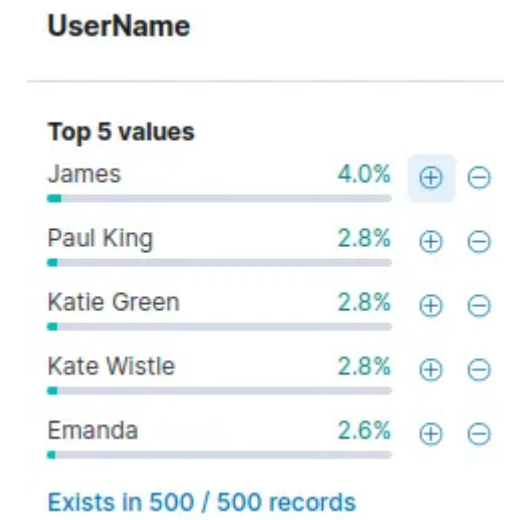


Once done, just collapse the result and our results will only display what we asked!

Time	Source_Country	Source_ip	UserName
Jan 31, 2022 @ 08:29:41.000	United States	143.23.45.158	Phill
Jan 31, 2022 @ 08:27:38.000	United States	107.14.110.254	Nathon Lyon
Jan 31, 2022 @ 08:25:45.000	United States	64.169.223.215	Sammy
Jan 31, 2022 @ 08:22:08.000	United States	107.14.182.38	Smith

5: Apply Filter on UserName Emanda; which SourceIP has max hits?

I clicked on “UserName” And clicked on the “+” next to Emanda’s name to display only results that has her name. From there, I clicked on “Source_ip” to display IP addresses that is under the UserName “Emanda.”

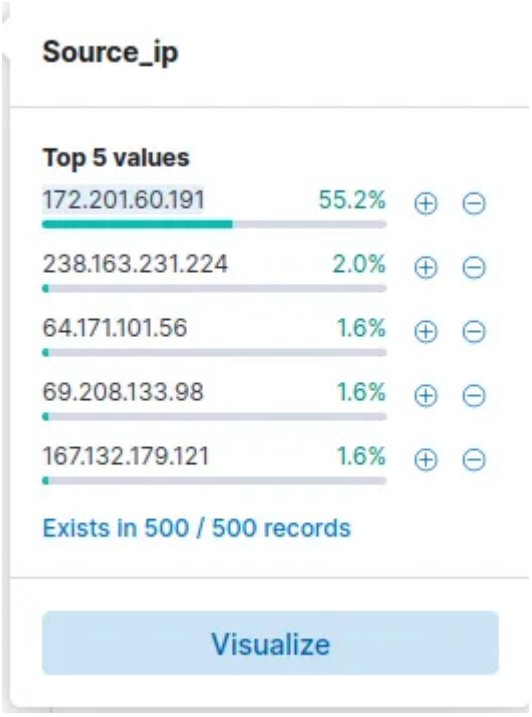


Answer: 107.14.1.247

6: On 11th Jan, which IP caused the spike observed in the time chart?

I changed the filter to search for only activities that happened on January 11, 2021. Then I removed the filter that was searching for only Emanda by clicking on “x.”

Refresh to display the new results. Then click on “Source_ip” to look at the top 5 values of the new results.

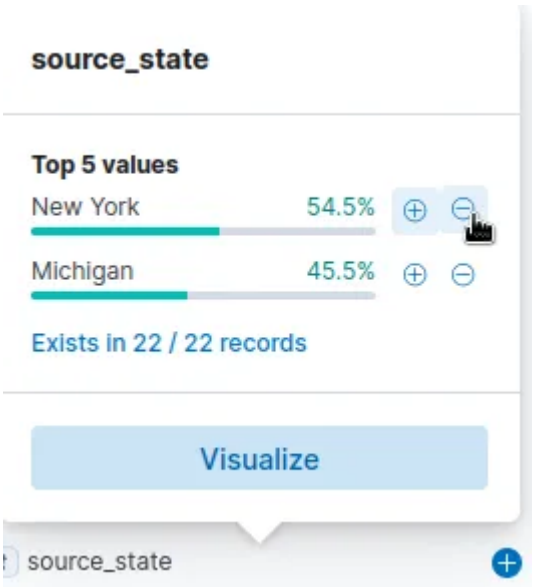


Answer: 172.201.60.191

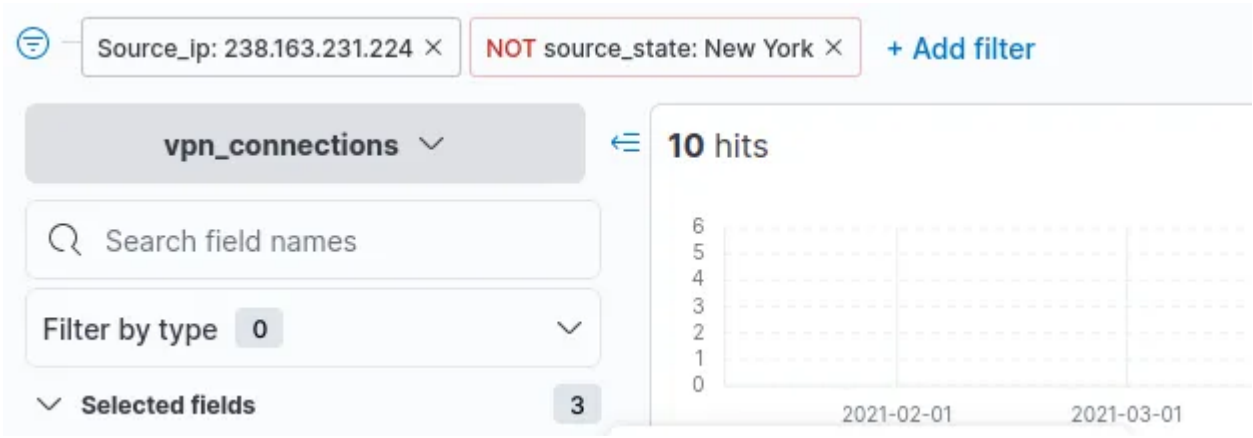
7: How many connections were observed from IP **238.163.231.224**, excluding the **New York** state?

What I did first is click on the “+” icon on the correct IP address to add it to our filter.

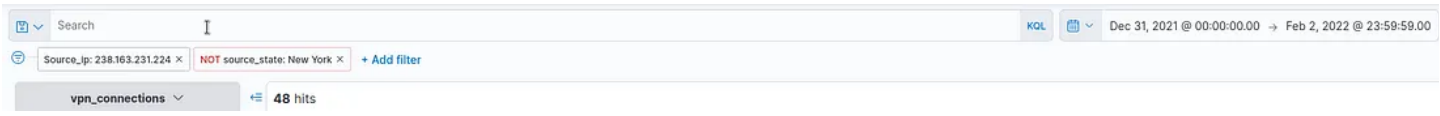
Next, I head over to “source_state” and clicked on “-” icon next to New York, which means to display results coming from the states **excluding** New York.



An overview of my filters used and the number of hits that resulted.



… Except it was wrong because it didn't use results from **ONLY** January 11. I changed the dates back to how it was originally and the answer was accepted.



Answer: 48

Task 6 KQL Overview

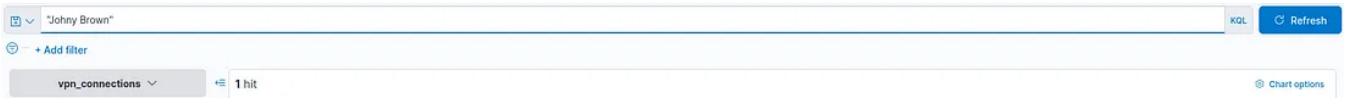
1: Create a search query to filter out the logs from Source_Country as the **United States** and show logs from User James or Albert. How many records were returned?

I followed the example and attempted to create my own. I typed in `Source_Country : United States AND UserName : James OR Albert` into the search bar. The important thing is to remember that there is a space between the field name and colon.

Answer: 161

2: As User **Johny Brown** was terminated on 1st January 2022, create a search query to determine how many times a VPN connection was observed after his termination.

I changed the date range and made it start on January 1, 2022. I typed in his name and waited for the results. Admittedly, I thought this wasn't the answer because it felt too little, but it was the answer!



Answer: 1

Task 7 Creating Visualizations

1: Which user was observed with the greatest number of failed attempts?

The reading will tell you exactly how to do it. I didn't notice until after I did my attempt. What I did was using 3 fields first. I chose Source_ip, UserName, and action. From there, I was presented with a lot of data. I didn't know how to filter yet, but on a whim, I decided to hover over failed to see if I can filter it this way, and I can!

Top values of Source_ip	Top values of UserName	Top values of action	Count of records
238.163.231.224	Rafique M	teardown	24
238.163.231.224	Suleman	teardown	24
69.208.133.98	Paul King	teardown	29
64.171.101.56	Kate Wistle	teardown	28
157.109.0.102	James	teardown	28
Other	Maleena	teardown	30
Other	Rock	teardown	30
Other	Bentle	teardown	29
Other	Other	teardown	1,069
172.201.60.191	Simon	failed	274

You can see on the top left with a new filter where actions has to have a value of "failed." This resulted in only one line of result, very easy to read.

Answer: Simon

2: How many wrong VPN connection attempts were observed in January?

Answer: 274

Thoughts:

This was a really nice room that exposed me to another SIEM tool. I personally felt like it's easier than Splunk but this is really just an introduction room, so it is deFsigned to be easy. What I really enjoyed about it was just how intuitive the filter is. It seems beginner friendly when trying to find what you need. Can't wait to utilize what we learned in the next room!

Cybersecurity Siem Tryhackme Elk Stack Kibana

Follow

Written by Toumo

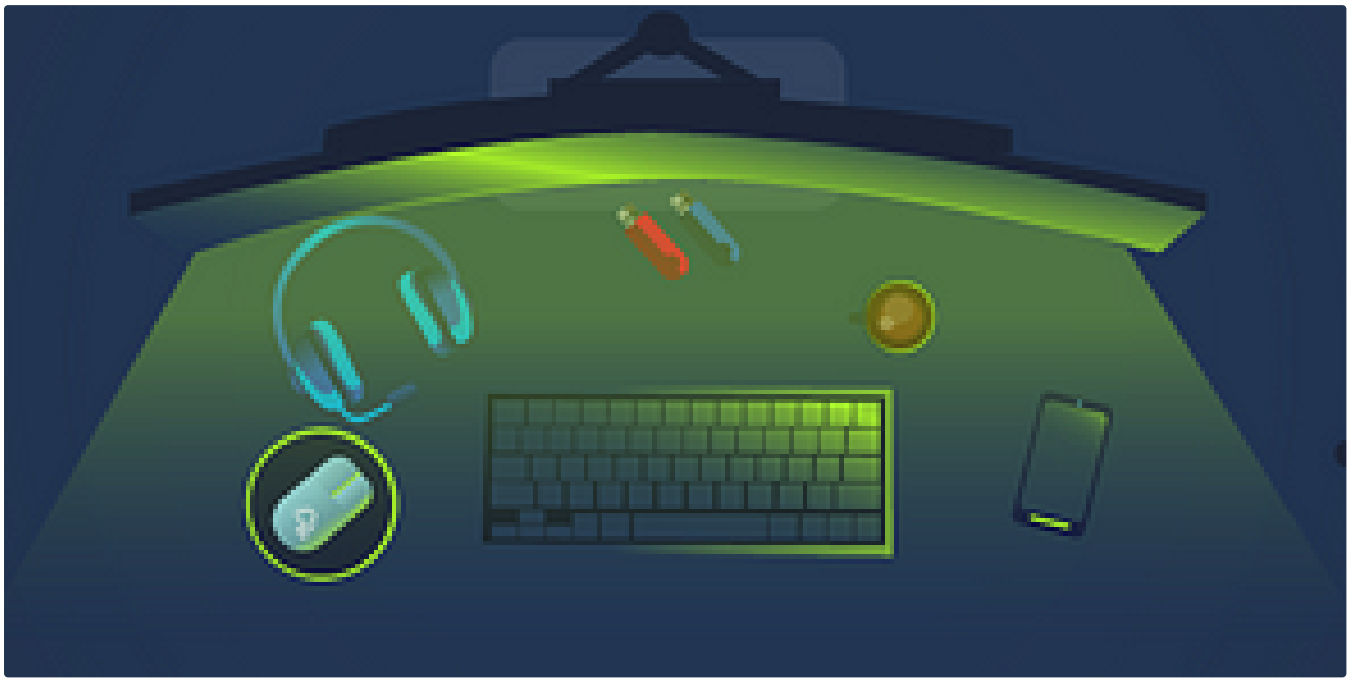
151 Followers · 1 Following

No responses yet

What are your thoughts?

Respond

More from Toumo

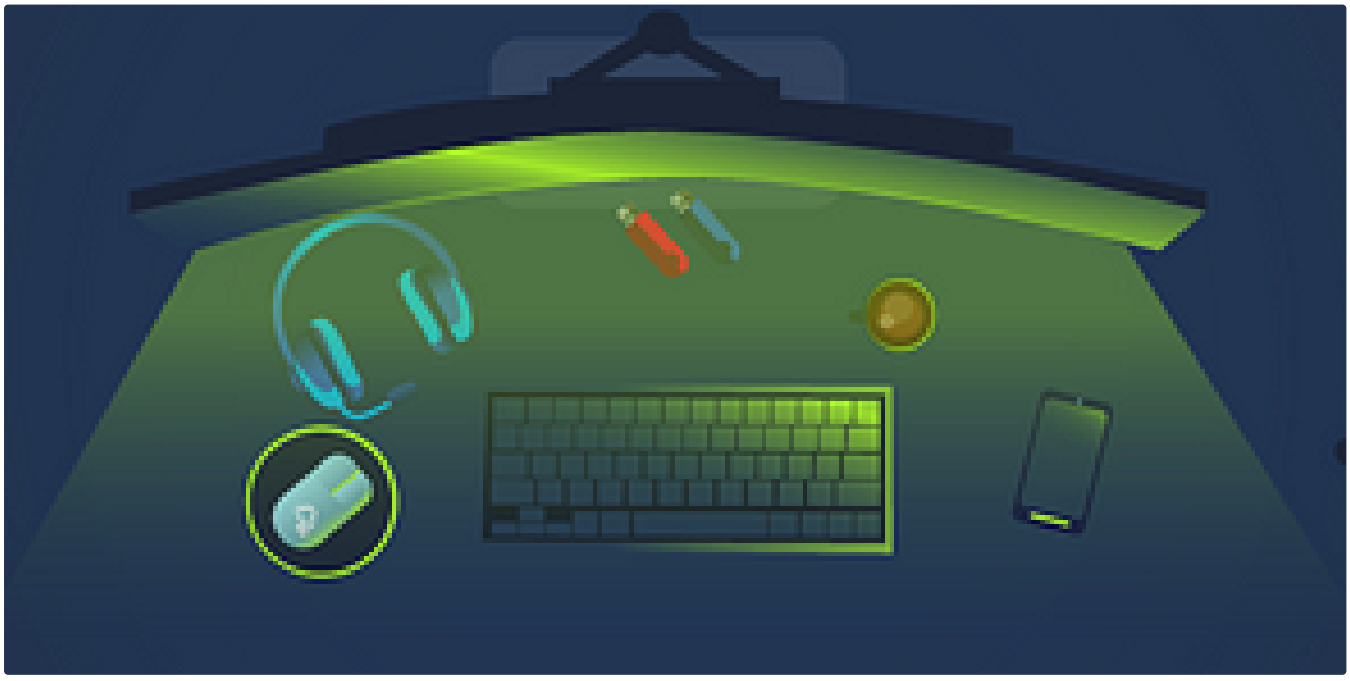


Toumo

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

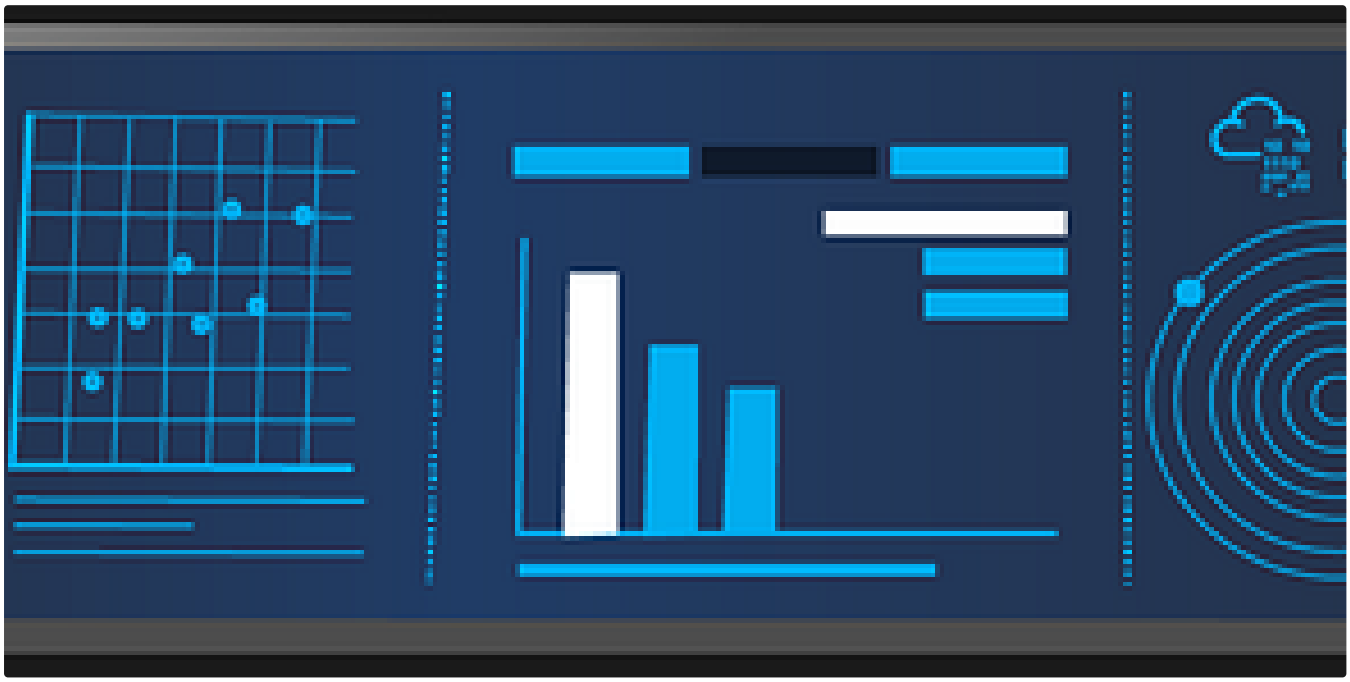


Toumo

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

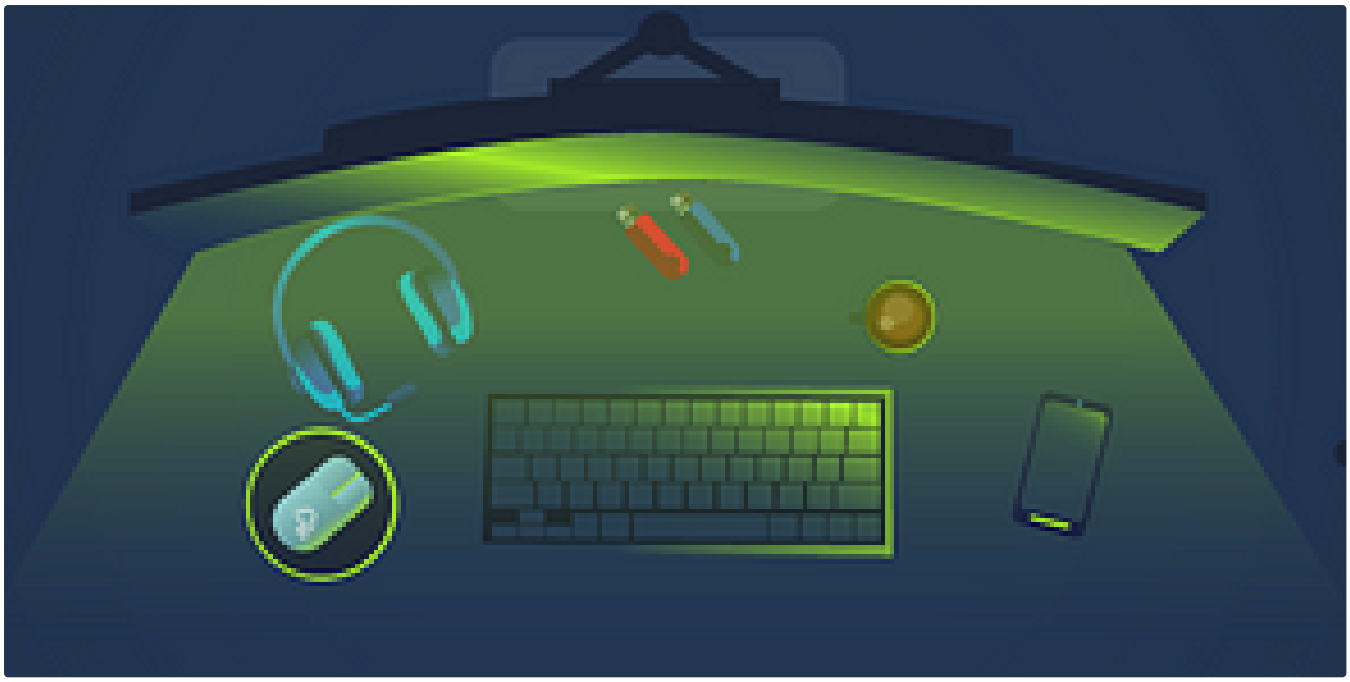


Toumo

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

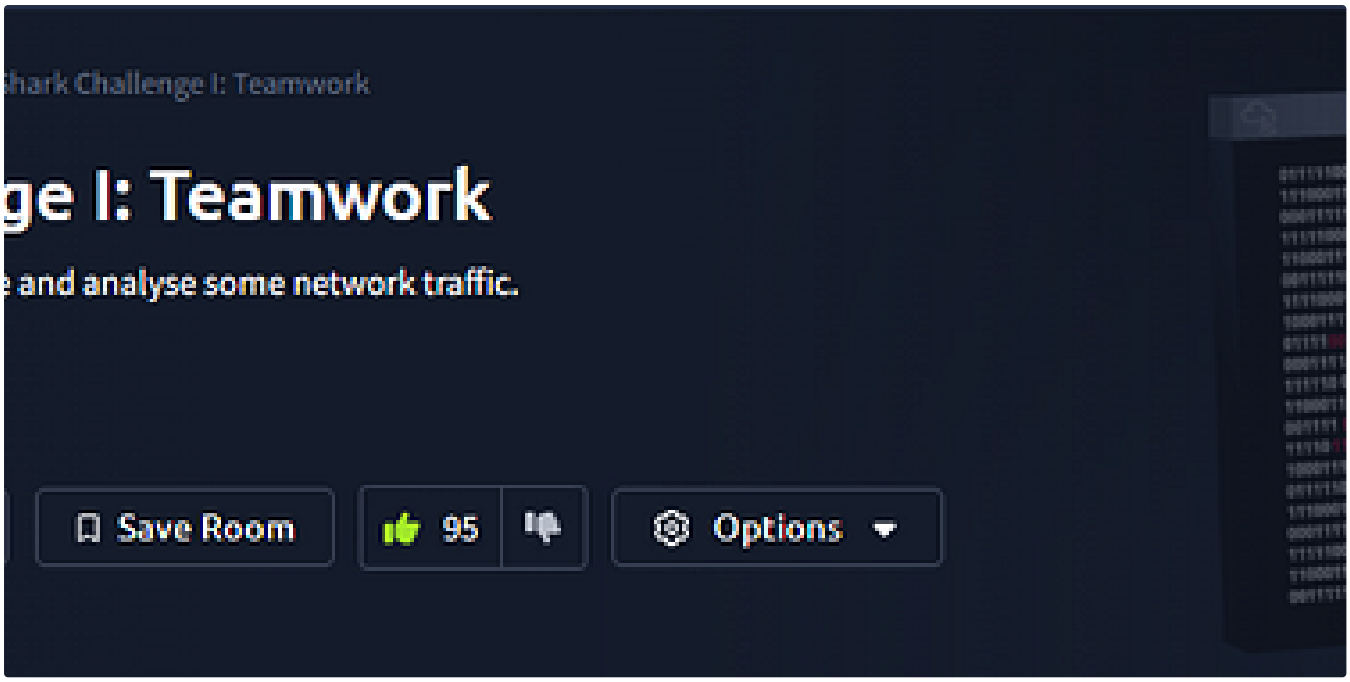
Recommended from Medium

In T3CH by Axoloth

TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

Nov 28, 2024 50



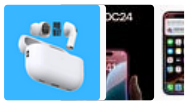
Abhijeet Singh

TShark Challenge I: Teamwork | SOC Level 1 | TryHackMe Walkthrough

Task 1 - Introduction

Nov 11, 2024

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.

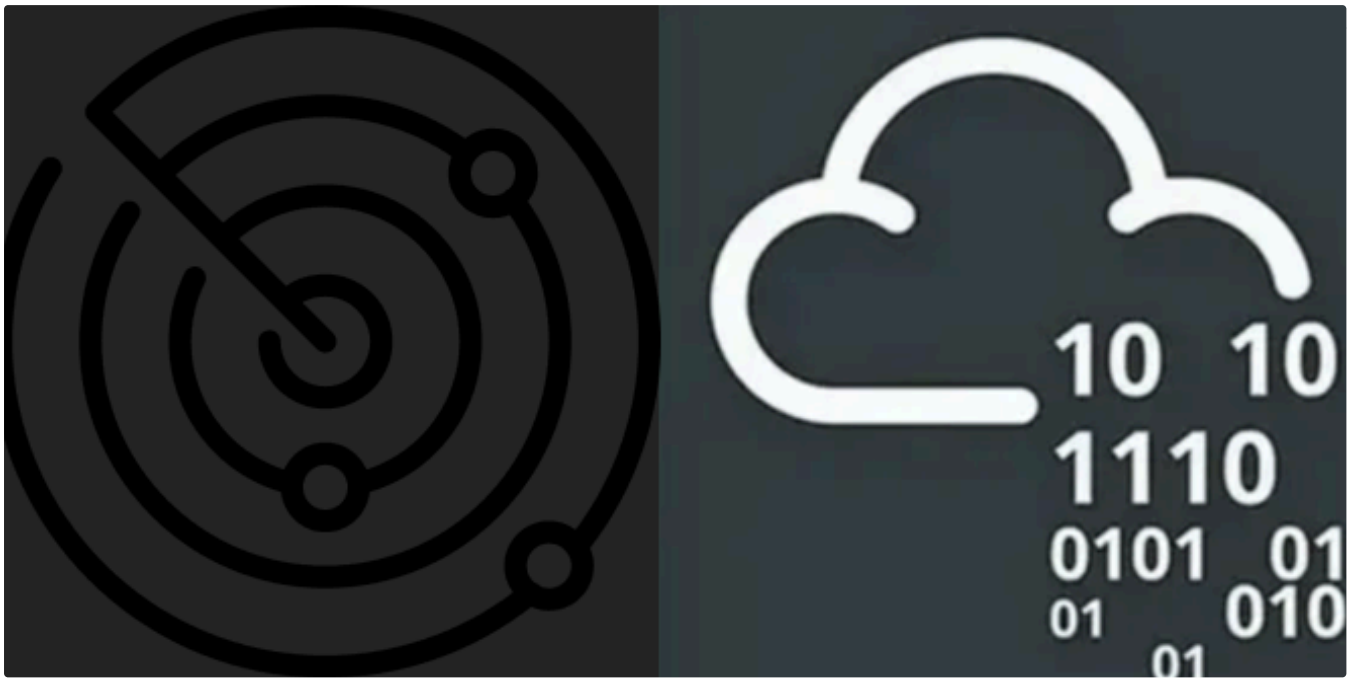
Sep 4, 2024 50

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

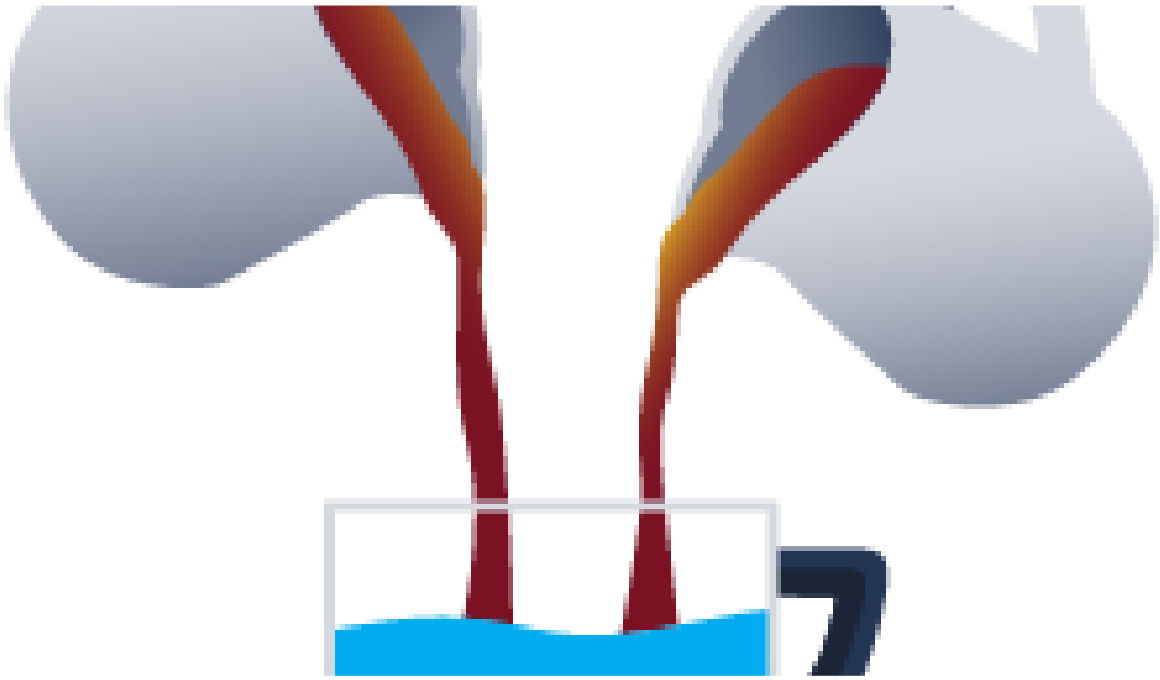


IritT

Nmap — TryHackMe Insights &Walkthrough

An in depth look at scanning with Nmap, a powerful network scanning tool.

Dec 23, 2024



MAGESH

Secret Recipe-Tryhackme Writeup

Perform Registry Forensics to Investigate a case.

Aug 21, 2024 2