

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



# Fixit-Tryhackme Writeup



MAGESH · Following

4 min read · Apr 22, 2024



Listen



Share

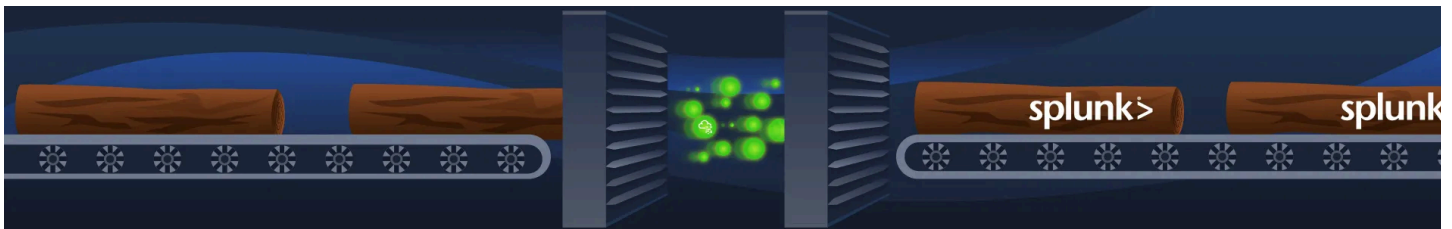


More

Fix the log parsing issue and analyze the logs in Splunk.

*This room is accessible only for subscribers, so if you wish to subscribe you can use this link and get \$5 credits 💰 🇸🇬 when you become a member.*

<https://tryhackme.com/signup?referrer=633819acb90069005f4fd623>.



Link to the room <https://tryhackme.com/r/room/fixit>

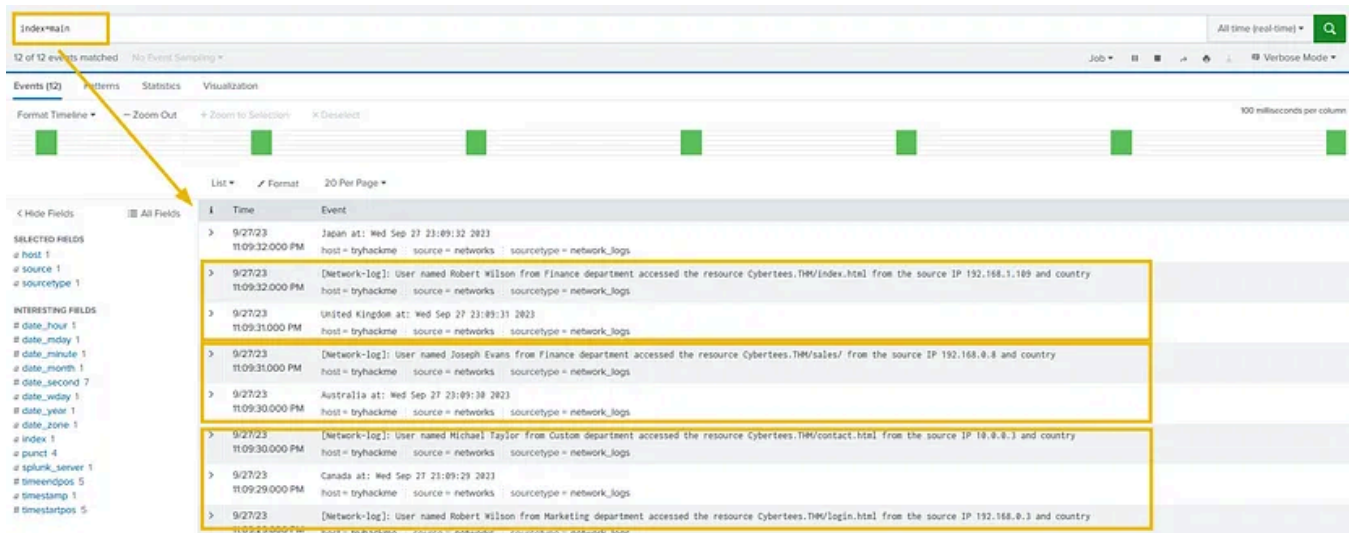
*Tip: Make sure to do the configuration changes one by one and check the results before moving on to the next one. It is recommended to complete Splunk: Data Manipulation room for better understanding.*

*Note: Splunk is installed in the `/opt/splunk` directory, and you will be working in the App called `Fixit`.*

**This challenge is divided into three levels:**

## Level 1: Fix Event Boundaries

Fix the Event Boundaries in Splunk. As the image below shows, Splunk cannot determine the Event boundaries, as the events are coming from an unknown device.



In order to fix this issue, we can use different `stanzas` in the `props.conf` file. If we run the script a few times to observe the output, we can see that each event starts with the term `[Network-log]`, indicating the start of the event. We can use this as the regex pattern with the stanza `BREAK_ONLY_BEFORE` and see if it could fix this problem. Create the `props.conf` file in default directory and copy the following lines in `props.conf` file, save the file, and then restart Splunk to apply changes.

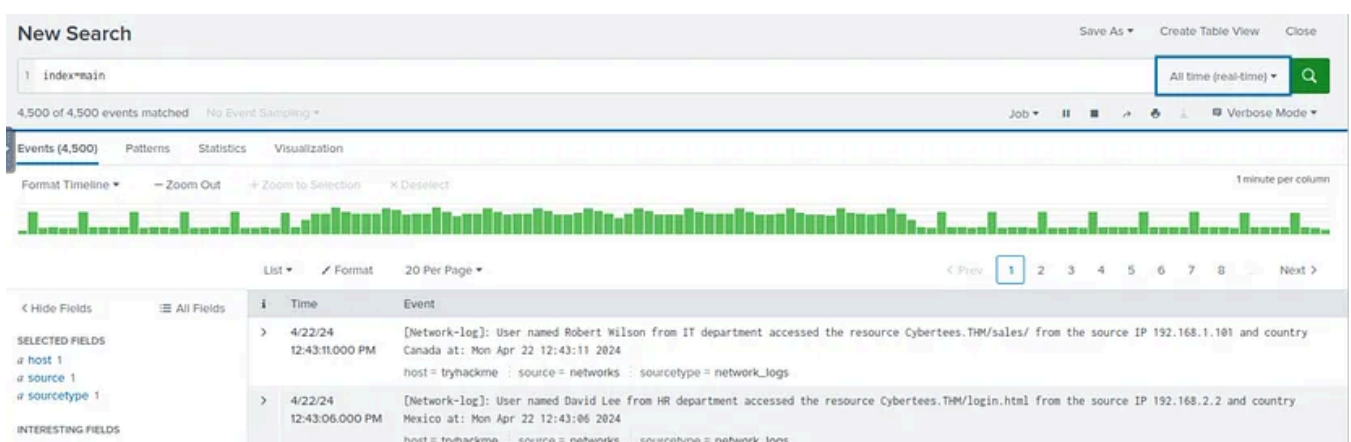
```
[network_logs]
```

```
SHOULD_LINEMERGE = true
```

```
BREAK_ONLY_BEFORE = \[Network-log\]
```

**To restart :** `/opt/splunk/bin/splunk restart.`

Use the search head option with all time(real-time).



It worked

A stanza in Splunk refers to a section of configuration settings..

*What is the full path of the FIXIT app directory?*

*Ans: /opt/Splunk/etc/apps/fixit.*

---

*What Stanza will we use to define Event Boundary in this multi-line Event case?*

*Ans: BREAK\_ONLY\_BEFORE*

---

*In the inputs.conf, what is the full path of the network-logs script?*

*Ans: /opt/splunk/etc/apps/fixit/bin/network-logs*

```
[script:///opt/splunk/etc/apps/fixit/bin/network-logs]

index = main
source = networks
sourcetype = network_logs
interval = 1
```

---

*What regex pattern will help us define the Event's start?*

*Ans: \[Network-log\]*

### **Level 2: Extract Custom Fields**

Once the event boundaries are defined, it is time to extract the custom fields to make the events searchable.

- Username
- Country
- Source\_IP
- Department
- Domain

### **Sample Logs:**

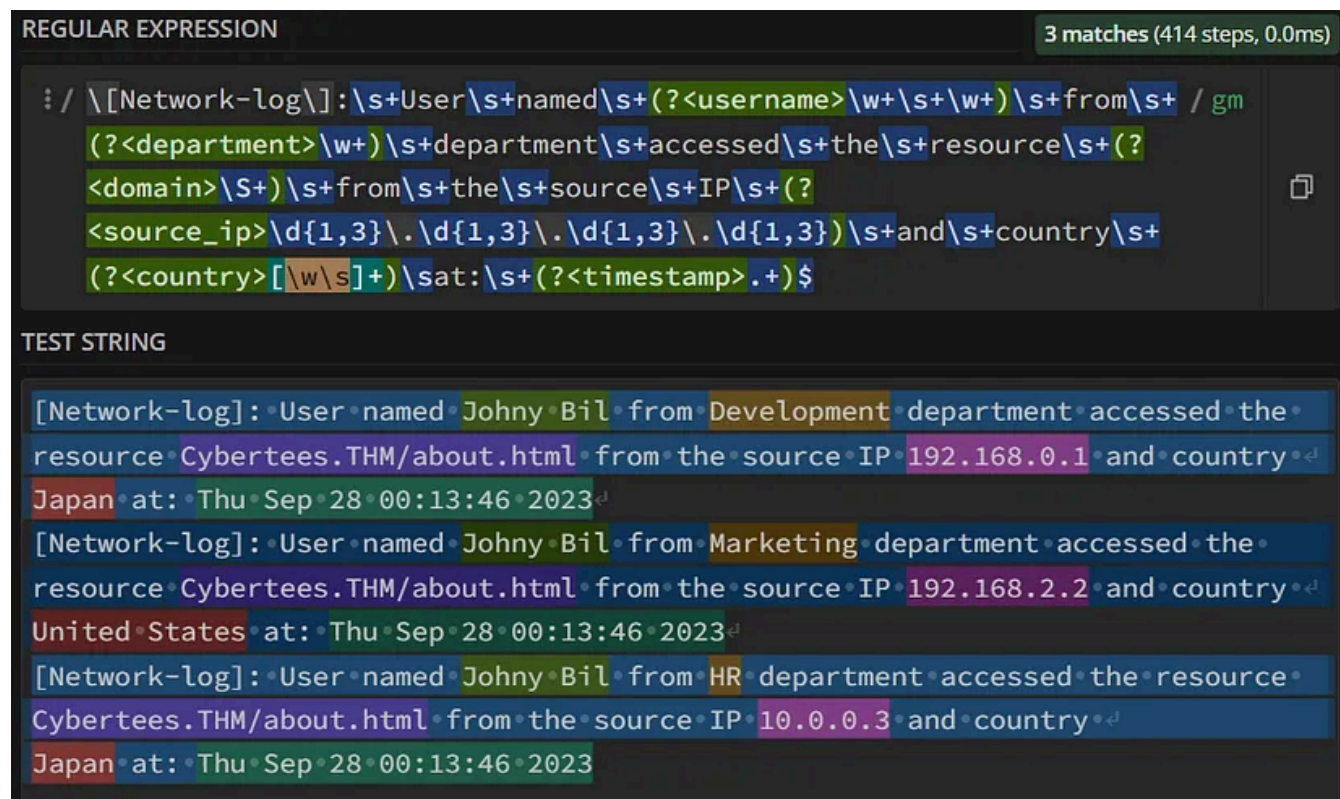
To create regex patterns, sample Network logs are shown below:

[Network-log]: User named Johny Bil from Development department accessed the resource Cybertees.THM/about.html from the source IP 192.168.0.1 and country Japan at: Thu Sep 28 00:13:46 2023

[Network-log]: User named Johny Bil from Marketing department accessed the

resource Cybertees.THM/about.html from the source IP 192.168.2.2 and country Japan at: Thu Sep 28 00:13:46 2023

[Network-log]: User named Johny Bil from HR department accessed the resource Cybertees.THM/about.html from the source IP 10.0.0.3 and country Japan at: Thu Sep 28 00:13:46 2023.



regex101

Chatgpt can help finding the regex but, it may not help you completely, you have to ask the right questions and also verify whether it works. There is another other way to extract fields using Extract Fields option in splunk fields column. This might help you but, using conf files have advantages like reusability, scalability and also when dealing with larger data.

So first we create and edit the transforms.conf file for extraction.

```
root@tryhackme:/opt/splunk/etc/apps/fixit/default# cat transforms.conf
[network_custom_fields]
REGEX = \[Network-log\]:\s+User\s+named\s+(?<username>\w+\s+\w+)\s+from\s+(?<department>\w+)\s+department\s+accessed\s+the\s+resource\s+(?<domain>\S+)\s+from\s+the\s+source\s+IP\s+(?<source_ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})\s+and\s+country\s+(?<country>[\w\s]+)\sat:\s+(?<timestamp>.+)$
FORMAT = Username::$1 Department::$2 Domain::$3 Source_IP::$4 Country::$5
WRITE_META = true
```

We need to update the props.conf to mention the recent updates we did in transforms.conf.



```
root@tryhackme:/opt/splunk/etc/apps/fixit/default# cat props.conf
[network_logs]
SHOULD_LINEMERGE = true
BREAK_ONLY_BEFORE = \[Network-log\]
TRANSFORM-network = network_custom_fields
```

The next step would be to create fields.conf and mention the field we are going to extract from the logs. INDEXED = true means we are telling Splunk to extract this field at the indexed time.

```
root@tryhackme:/opt/splunk/etc/apps/fixit/default# cat fields.conf
[Username]
INDEXED = true

[Country]
INDEXED = true

[Source_IP]
INDEXED = true

[Department]
INDEXED = true

[Domain]
INDEXED = true
```

That's all we need in order to extract the custom fields. Now, restart the Splunk instance so that the changes we have made are committed. Go to the Splunk instance and use the search query `index=main sourcetype=network_logs`

---

*What is the captured domain?*

*Ans: cybertees.thm*

---

*How many countries are captured in the logs?*

*Ans:12*

---

*How many departments are captured in the logs?*

*Ans: 6*

---

*How many usernames are captured in the logs?*

*Ans: 28*

*How many source IPs are captured in the logs?*

*Ans: 52*

*Which configuration files were used to fix our problem? [Alphabetic order: File1, file2, file3]*

*Ans: fields.conf, props.conf, transforms.conf*

*What are the TOP two countries the user Robert tried to access the domain from?  
[Answer in comma-separated and in Alphabetic Order][Format: Country1, Country2]*

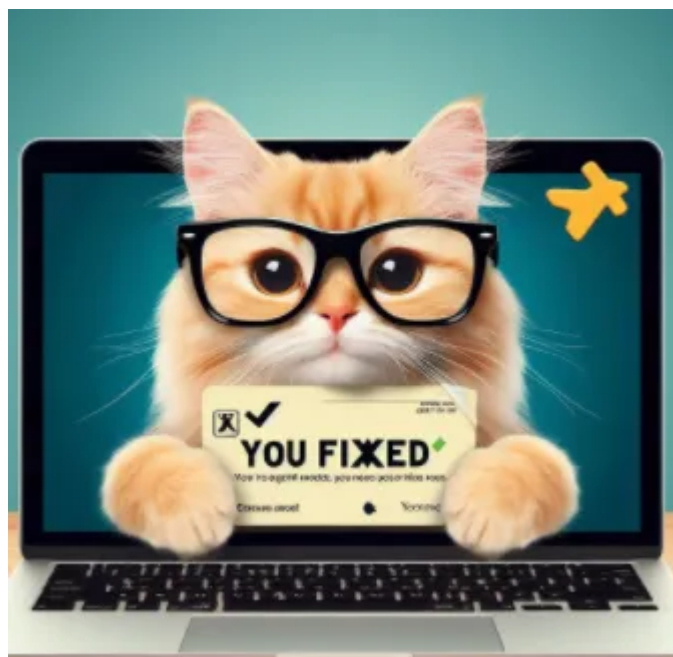
*Ans: canada, united states*

*Which user accessed the secret-document.pdf on the website?*

*Ans: sarah hall*

Search the document name in search head

THANK YOU FOR READING!!! ❤️ 🐱



Splunk

Tryhackme

Parsing



Following

## Written by MAGESH

40 Followers · 11 Following

Cybersecurity | Tryhackme

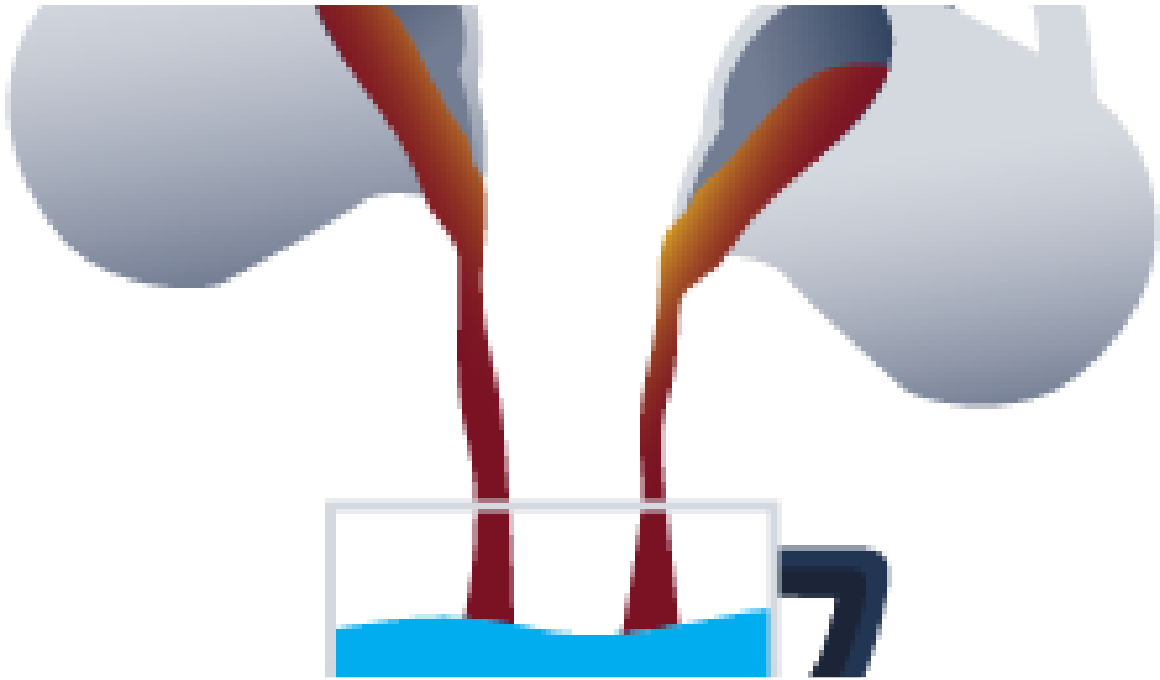
No responses yet



What are your thoughts?

Respond

More from MAGESH



 MAGESH

## Secret Recipe-Tryhackme Writeup

Perform Registry Forensics to Investigate a case.

Aug 21, 2024  2



 MAGESH

## OAuth Vulnerabilities-Tryhackme Walkthrough

Learn how the OAuth protocol works and master techniques to exploit it.

Sep 5, 2024  1





[Open in app](#) ↗**Medium** Search MAGESH

## Windows PowerShell-Tryhackme Writeup

Discover the “Power” in PowerShell and learn the basics.

Oct 23, 2024  8

 MAGESH

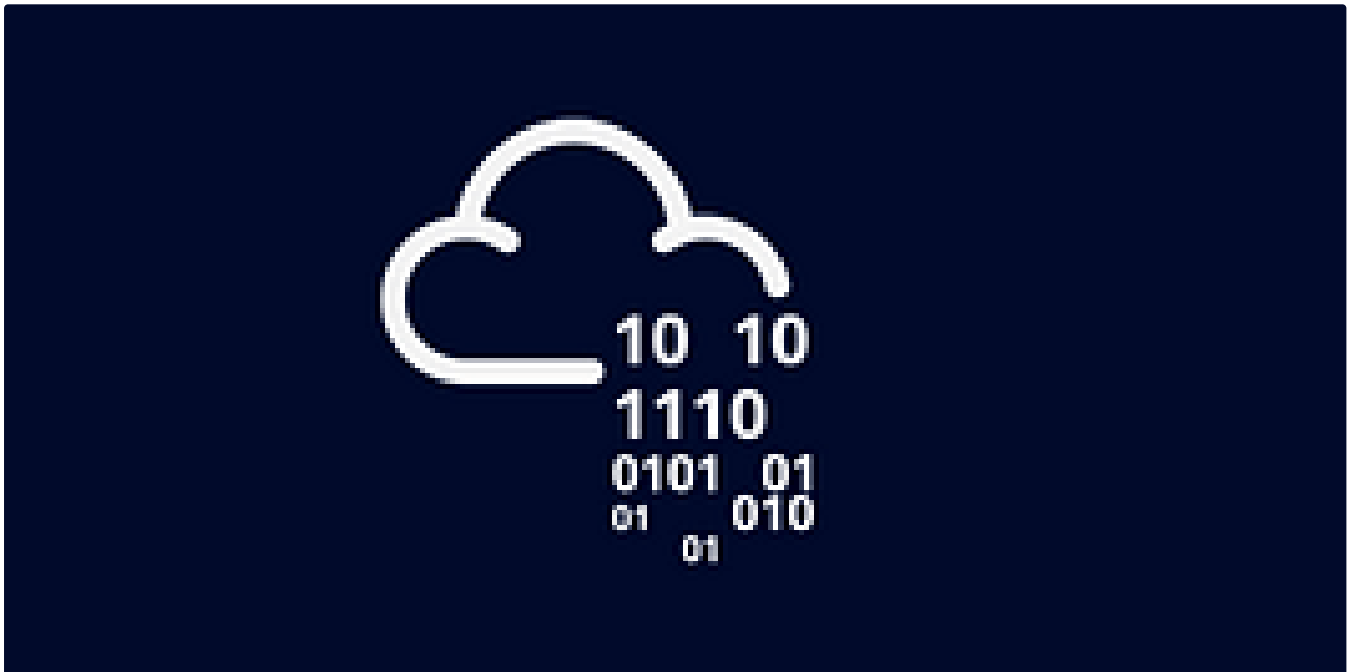
## Race Conditions -Tryhackme Writeup

Learn about race conditions and how they affect web application security

Jun 13, 2024 🖱 1

[See all from MAGESH](#)

## Recommended from Medium



In T3CH by Axoloth

### TryHackMe | Brute Force Heroes | WriteUp


Walkthrough room to look at the different tools that can be used when brute forcing, as well as the different situations that might favour...



Oct 3, 2024 🖱 51





 Berat Arslan

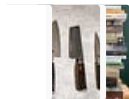
## TryHackMe—Hammer Writeup

‘Hammer’ is one of the ‘Medium’ difficulty rooms in THM.

Sep 1, 2024  69  1



### Lists



#### Staff picks

798 stories · 1566 saves



#### Stories to Help You Level-Up at Work

19 stories · 915 saves



#### Self-Improvement 101

20 stories · 3212 saves




#### Productivity 101

20 stories · 2714 saves

nts

	▼	User Name	▼	Name	▼	Surname	▼	Email
3		student1		Student1				studi
4		student2		Student2				studi
5		student3		Student3				studi
9		anatacker		Ana Tacker				
10		THM{Got.the.User}		X				
11		qweqwe		qweqwe				

<< < 1 > >>

 embosssdotar

### TryHackMe—Session Management—Writeup

Key points: Session Management | Authentication | Authorisation | Session Management Lifecycle | Exploit of vulnerable session management...

 Aug 7, 2024  27

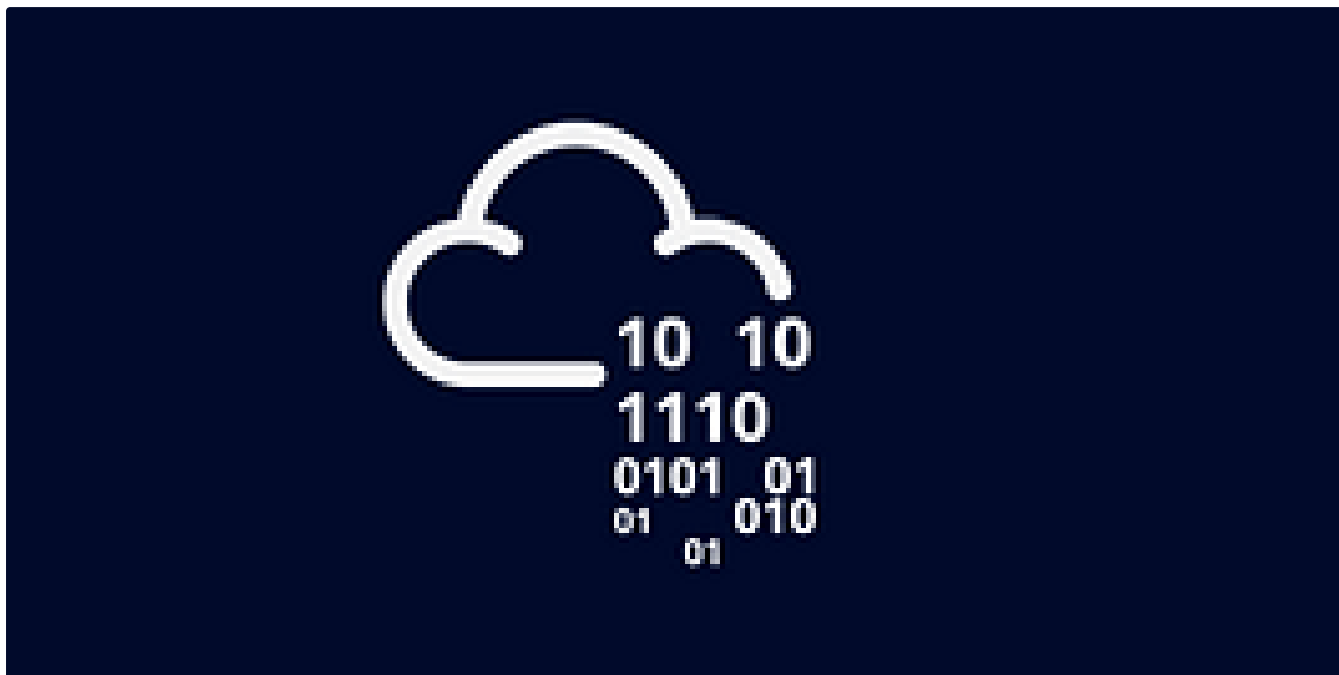


 K9ine95

### Block ~ Tryhackme ~ walkthrough

One of your junior system administrators forgot to deactivate two accounts from a pair of recently fired employees. We believe these...

Aug 12, 2024 🖱 2



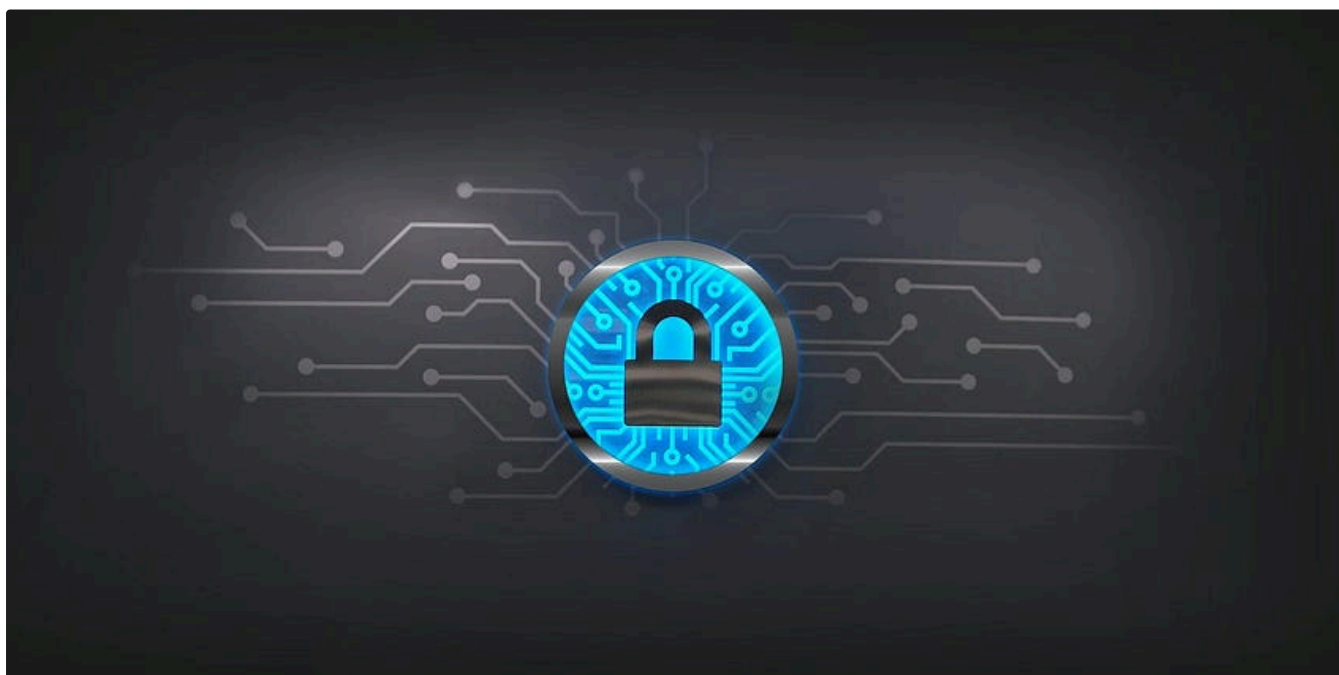
In T3CH by Axoloth

## TryHackMe | Deja Vu | WriteUp

Exploit a recent code injection vulnerability to take over a website full of cute dog pictures!



Oct 13, 2024 🖱 50



CyferNest Sec

## CSRF | TryHackMe Walkthrough

## CSRF: The Art of Sneaky Online Mischief

Jan 3  1



See more recommendations