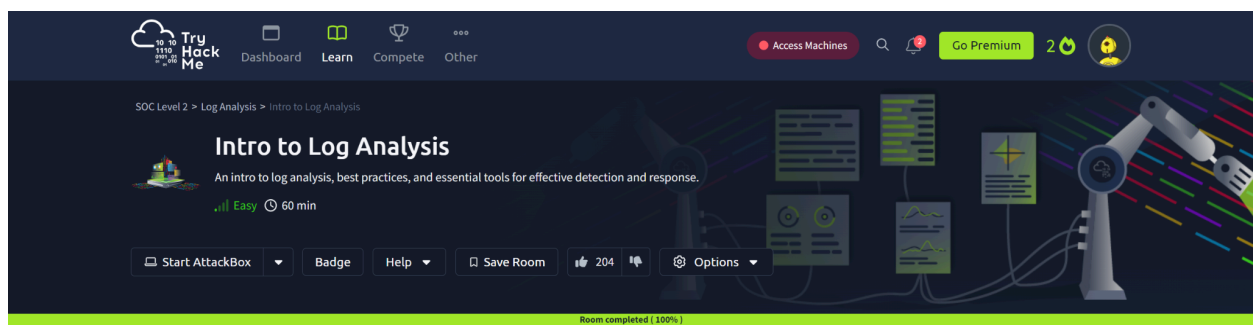


# INTRO TO LOG ANALYSIS

## ASSIGNMENT REPORT



**Peter Kinyumu,**  
**cs-sa07-24067,**  
**July 9th, 2024.**

# 1. INTRODUCTION

This room teaches log analysis, an essential skill for a security analyst to identify, detect and respond to security incidents. It teaches foundational investigation theory for effective log analysis investigations and the common tools used for log analysis including command line ones, cybercheff, sigma and yara.

## 2. ANSWERS TO QUESTIONS

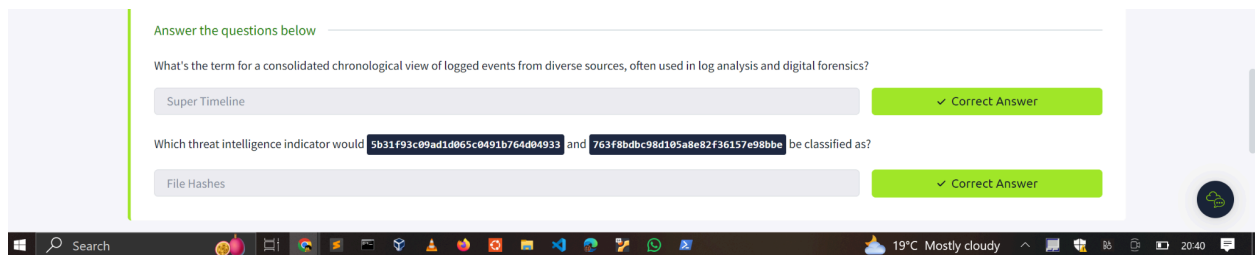
### Investigation theory

- a. What's the term for a consolidated chronological view of logged events from diverse sources, often used in log analysis and digital forensics?

- **Super Timeline**

- b. Which threat intelligence indicator would 5b31f93c09ad1d065c0491b764d04933 and 763f8bdbc98d105a8e82f36157e98bbe be classified as?

- **File Hashes**



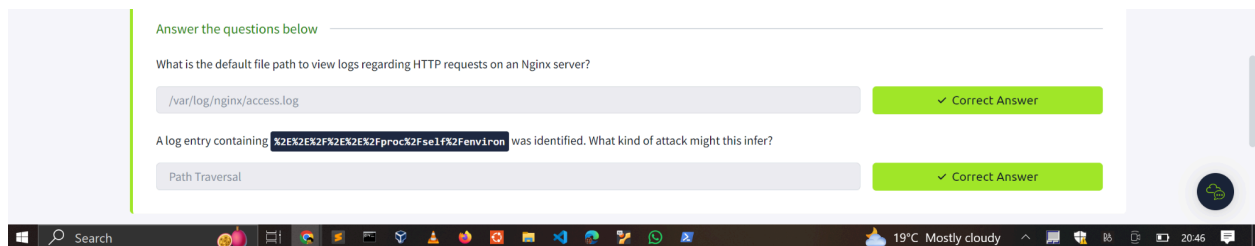
### Detection Engineering

- a. What is the default file path to view logs regarding HTTP requests on an Nginx server?

- **/var/log/nginx/access.log**

- b. A log entry containing %2E%2E%2F%2E%2E%2Fproc%2Fself%2Fenviron was identified. What kind of attack might this infer?

- **Path traversal**



## Automated Vs Manual Analysis

- A log file is processed by a tool which returns an output. What form of analysis is this?
  - **Automated**
- An analyst opens a log file and searches for events. What form of analysis is this?
  - **Manual**

Answer the questions below

A log file is processed by a tool which returns an output. What form of analysis is this?

Automated

✓ Correct Answer

An analyst opens a log file and searches for events. What form of analysis is this?

Manual

✓ Correct Answer

## Log Analysis tools: Command Line

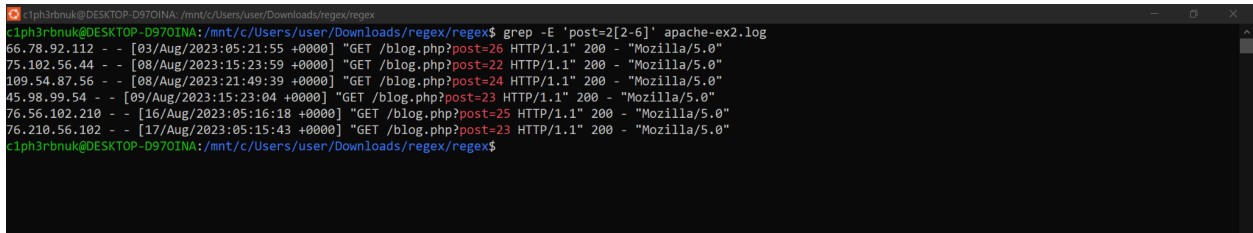
```
Select c1ph3rbnuk@DESKTOP-D970INA: /mnt/c/Users/user/Downloads
c1ph3rbnuk@DESKTOP-D970INA: /mnt/c/Users/user/Downloads$ cut -d ' ' -f 7 apache-1691435735822.log | grep flag
/index.php?flag=c701d43cc5a3acb9b5b04db7f1be94f6
c1ph3rbnuk@DESKTOP-D970INA: /mnt/c/Users/user/Downloads$
c1ph3rbnuk@DESKTOP-D970INA: /mnt/c/Users/user/Downloads$ cut -d ' ' -f 9 apache-1691435735822.log | grep 200 | wc -l
52
c1ph3rbnuk@DESKTOP-D970INA: /mnt/c/Users/user/Downloads$
c1ph3rbnuk@DESKTOP-D970INA: /mnt/c/Users/user/Downloads$ cut -d ' ' -f 1 apache-1691435735822.log | uniq -c | sort -r | head -n 1
2 145.76.33.201
c1ph3rbnuk@DESKTOP-D970INA: /mnt/c/Users/user/Downloads$
c1ph3rbnuk@DESKTOP-D970INA: /mnt/c/Users/user/Downloads$
c1ph3rbnuk@DESKTOP-D970INA: /mnt/c/Users/user/Downloads$ cut -d ' ' -f 1,4,5,7 apache-1691435735822.log | grep 'login.php' | grep '110.122.65.76'
110.122.65.76 [31/Jul/2023:12:34:40 +0000] /login.php
c1ph3rbnuk@DESKTOP-D970INA: /mnt/c/Users/user/Downloads$
c1ph3rbnuk@DESKTOP-D970INA: /mnt/c/Users/user/Downloads$
```

- Use cut on the apache.log file to return only the URLs. What is the flag that is returned in one of the unique entries?
  - **c701d43cc5a3acb9b5b04db7f1be94f6**

- b. In the apache.log file, how many total HTTP 200 responses were logged?
- 52
- c. In the apache.log file, which IP address generated the most traffic?
- 145.76.33.201
- d. What is the complete timestamp of the entry where 110.122.65.76 accessed /login.php?
- 31/Jul/2023:12:34:40 +0000

## Log Analysis tools: Regular Expression

- a. How would you modify the original grep pattern above to match blog posts with an ID between 22-26?
- post=2[2-6]

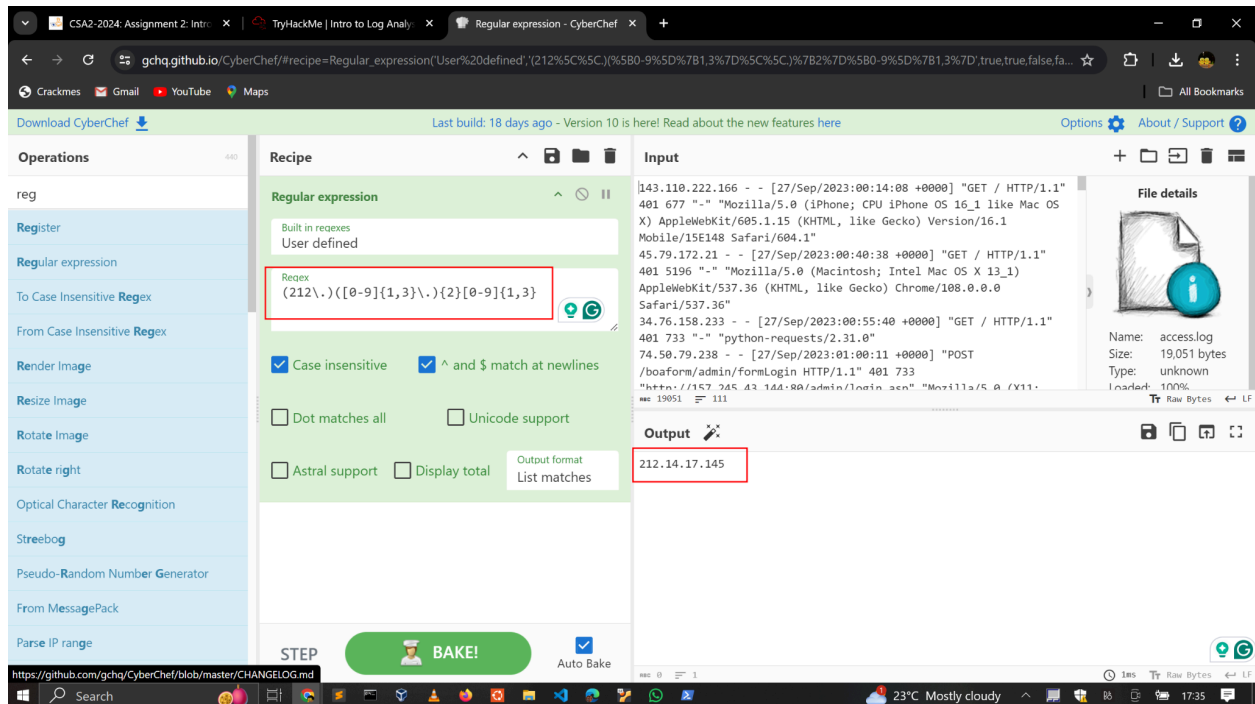


```
k1ph3rbnuke@DESKTOP-D970INA: /mnt/c/Users/user/Downloads/regex/regex$ grep -E 'post=2[2-6]' apache-ex2.log
66.78.92.112 - - [03/Aug/2023:05:21:55 +0000] "GET /blog.php?post=26 HTTP/1.1" 200 - "Mozilla/5.0"
75.102.56.44 - - [08/Aug/2023:15:23:59 +0000] "GET /blog.php?post=22 HTTP/1.1" 200 - "Mozilla/5.0"
109.54.87.56 - - [08/Aug/2023:21:49:39 +0000] "GET /blog.php?post=24 HTTP/1.1" 200 - "Mozilla/5.0"
45.98.99.54 - - [09/Aug/2023:15:23:04 +0000] "GET /blog.php?post=23 HTTP/1.1" 200 - "Mozilla/5.0"
76.56.102.210 - - [16/Aug/2023:05:16:18 +0000] "GET /blog.php?post=25 HTTP/1.1" 200 - "Mozilla/5.0"
76.210.56.102 - - [17/Aug/2023:05:15:43 +0000] "GET /blog.php?post=23 HTTP/1.1" 200 - "Mozilla/5.0"
k1ph3rbnuke@DESKTOP-D970INA: /mnt/c/Users/user/Downloads/regex/regex$
```

- b. What is the name of the filter plugin used in Logstash to parse unstructured log data?
- Grok

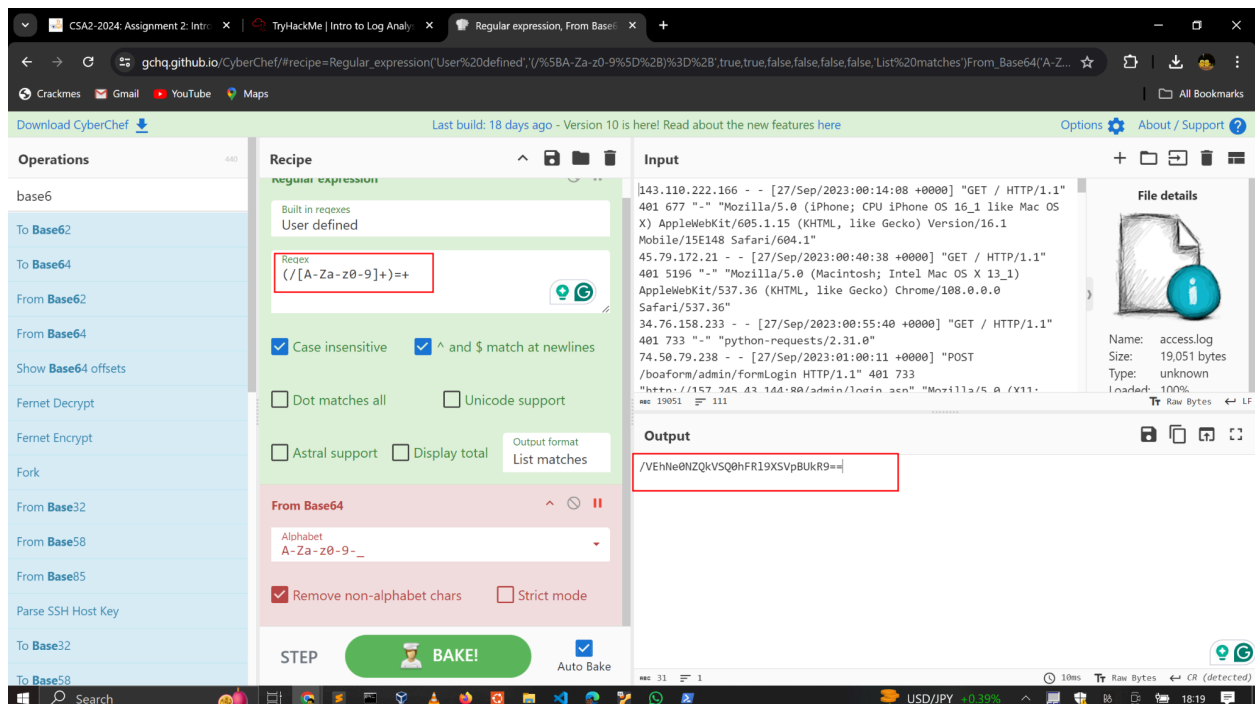
## Log Analysis tools: CyberChef

- a. Upload the log file named "access.log" to CyberChef. Use regex to list all of the IP addresses. What is the full IP address beginning in 212?
- 212.14.17.145
  - The regex below will match an IP address beginning with 212.

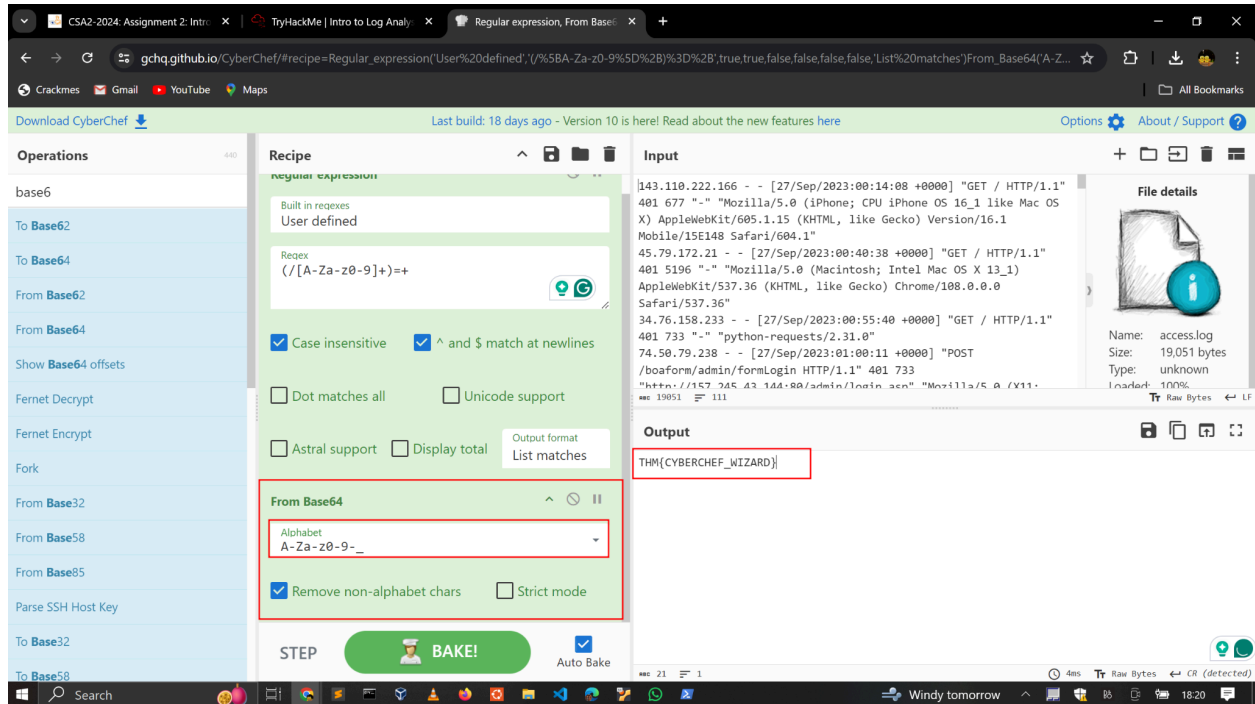


b. Using the same log file from Question #2, a request was made that is encoded in base64. What is the decoded value?

- **THM{CYBERCHEF\_WIZARD}**
- We can use the highlighted regex below to match the base64 request

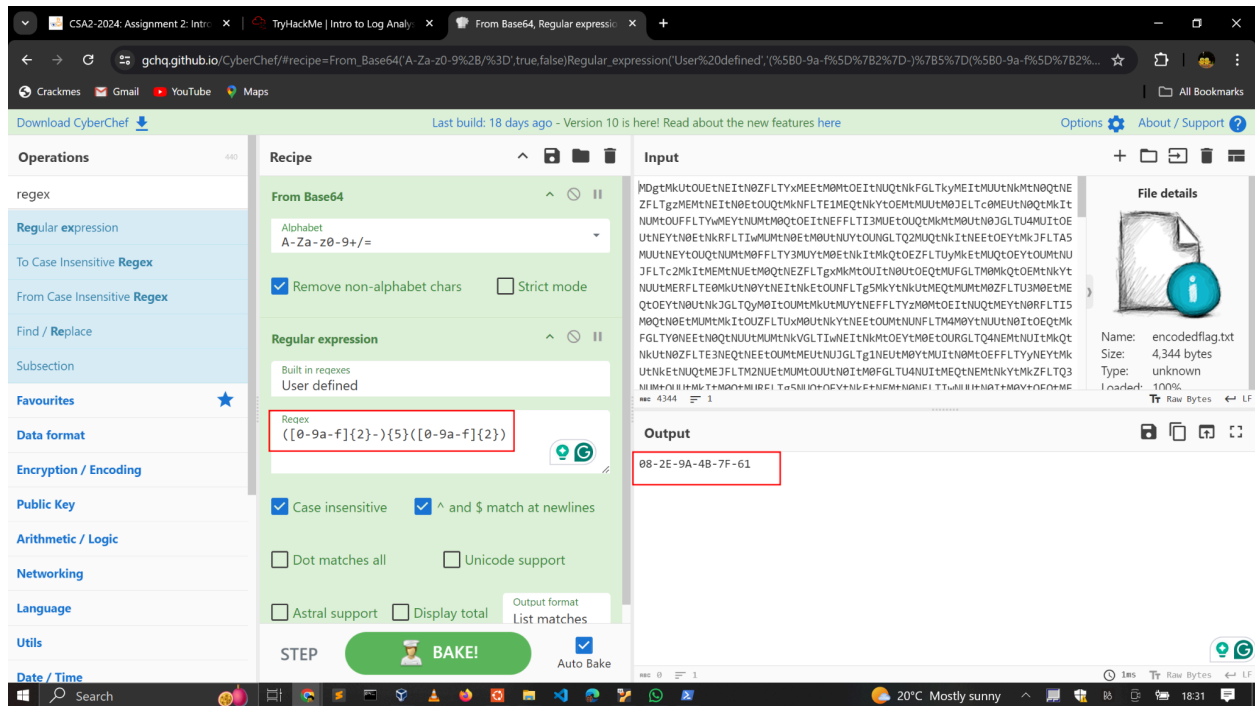


- After which we can then use base64 to decode the string and retrieve the flag.



c. Using CyberChef, decode the file named "encodedflag.txt" and use regex to extract by MAC address. What is the extracted value?

- **08-2E-9A-4B-7F-61**
- The regex below will match a Mac address format of 5 pairs of hexadecimal characters followed by a hyphen then followed by a last pair of hexadecimal characters.



## Log Analysis tools: Yara and Sigma

a. What languages does Sigma use?

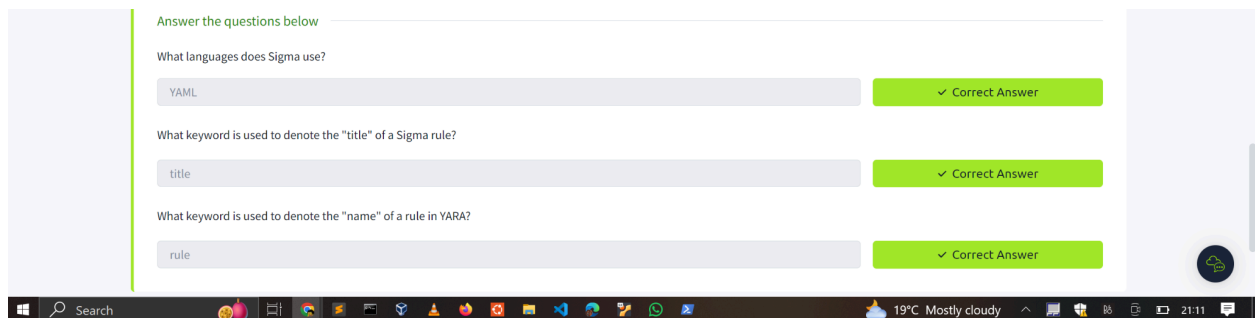
- **YAML**

b. What keyword is used to denote the "title" of a Sigma rule?

- **title**

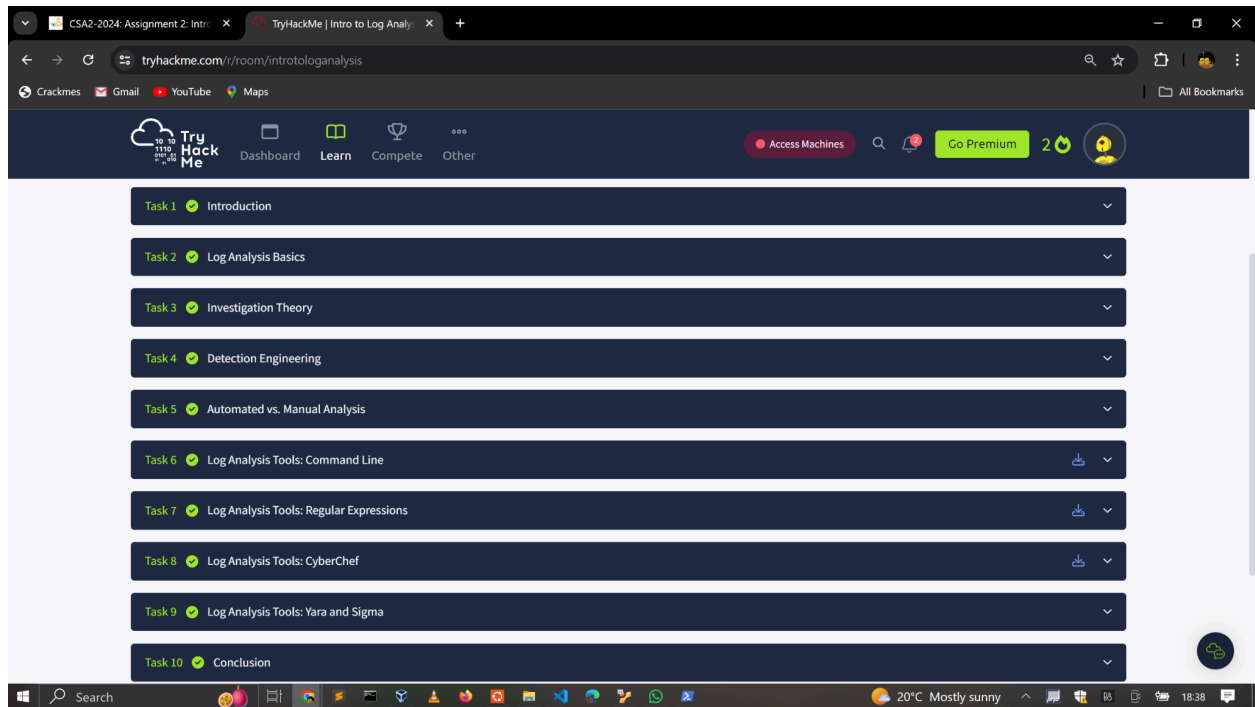
c. What keyword is used to denote the "name" of a rule in YARA?

- **rule**



### 3. MODULE COMPLETION

<https://tryhackme.com/p/c1ph3rbnuk>



### 4. CONCLUSION

This assignment has taught me how to analyze apache logs using three techniques. Firstly, I have learned to use the **cut**, **grep**, **wc**, **sort**, **head**, **uniq** utilities to filter and extract informations of interest from log files. Secondly, I have learned to use regular expressions and the cybercheff tool to extract information and decode it. Lastly, i have learned how to use Sigma and Yara rules to perform pattern matching in log files.