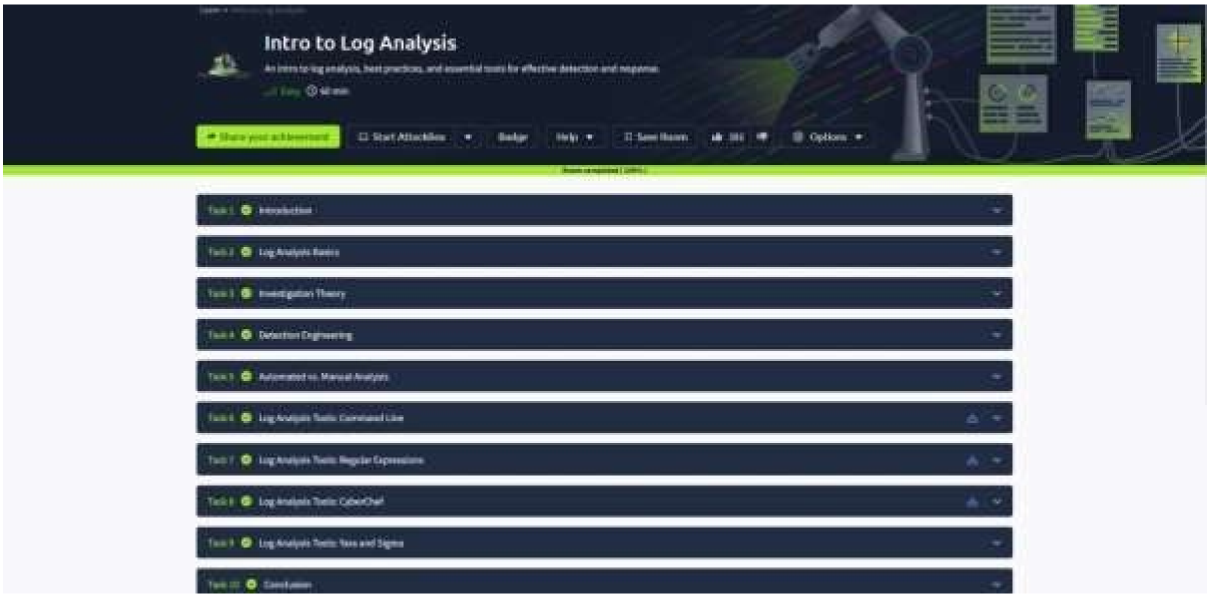
EX NO : 14 Log Analysis for detection and response 231901005

AIM:

An intro to log analysis, best practices and essential tools for effective detection and response.



Intro to Log Analysis

An intro to log analysis, best practices, and essential tools for effective detection and response.

Easy 60 min

Task 1 Introduction

Task 2 Log Analysis Basics

Task 3 Investigation Theory

Task 4 Detection Engineering

Task 5 Automated vs. Manual Analysis

Task 6 Log Analysis Tools: Command Line

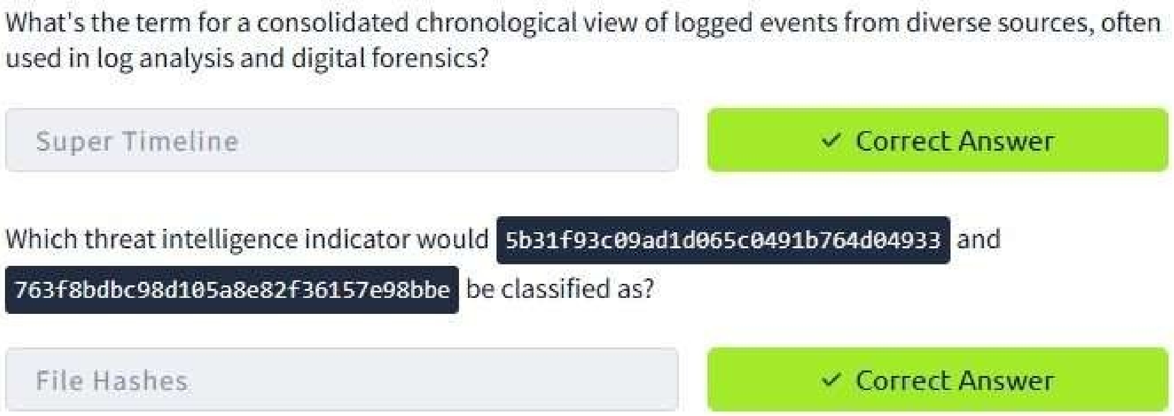
Task 7 Log Analysis Tools: Regular Expressions

Task 8 Log Analysis Tools: CyberChef

Task 9 Log Analysis Tools: Yara and Sigma

Task 10 Conclusion

TASK 3 : INVESTIGATION THEORY



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

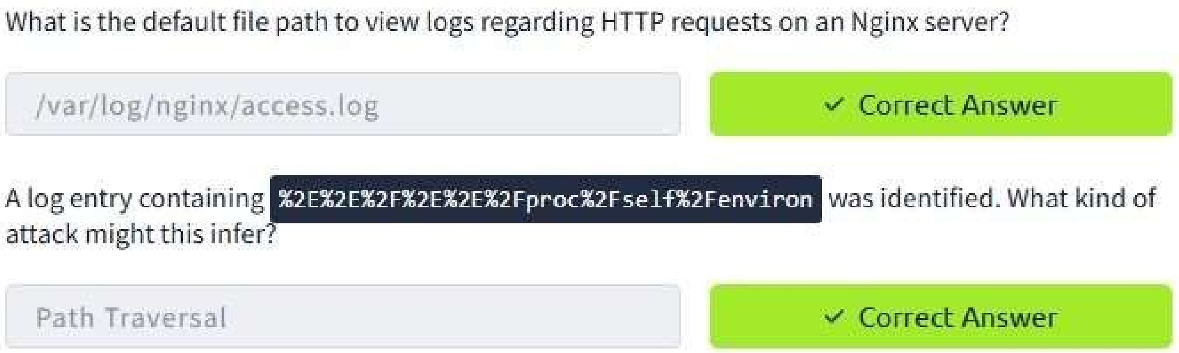
✓ Correct Answer

Which threat intelligence indicator would `5b31f93c09ad1d065c0491b764d04933` and `763f8bdbc98d105a8e82f36157e98bbe` be classified as?

File Hashes

✓ Correct Answer

TASK 4 : DETECTION ENGINEERING



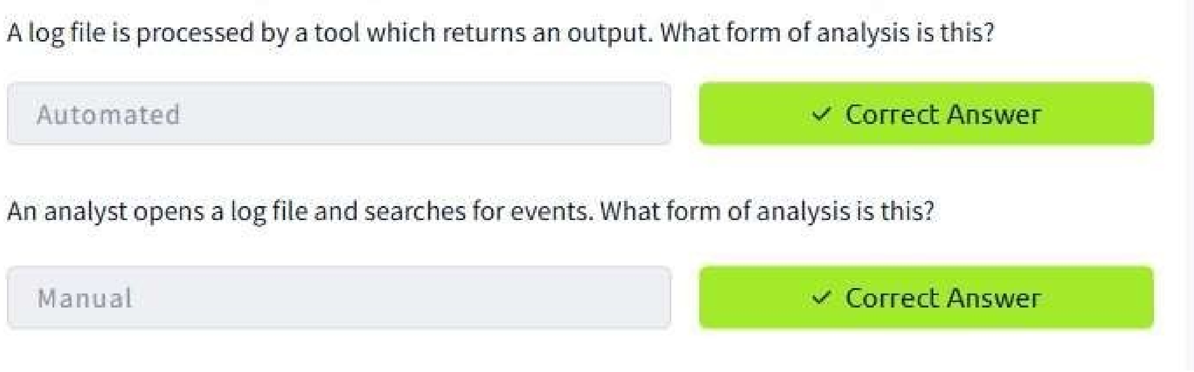
What is the default file path to view logs regarding HTTP requests on an Nginx server?

/var/log/nginx/access.log

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

Path Traversal

TASK 5 : AUTOMATED VS.MANUAL ANALYSIS



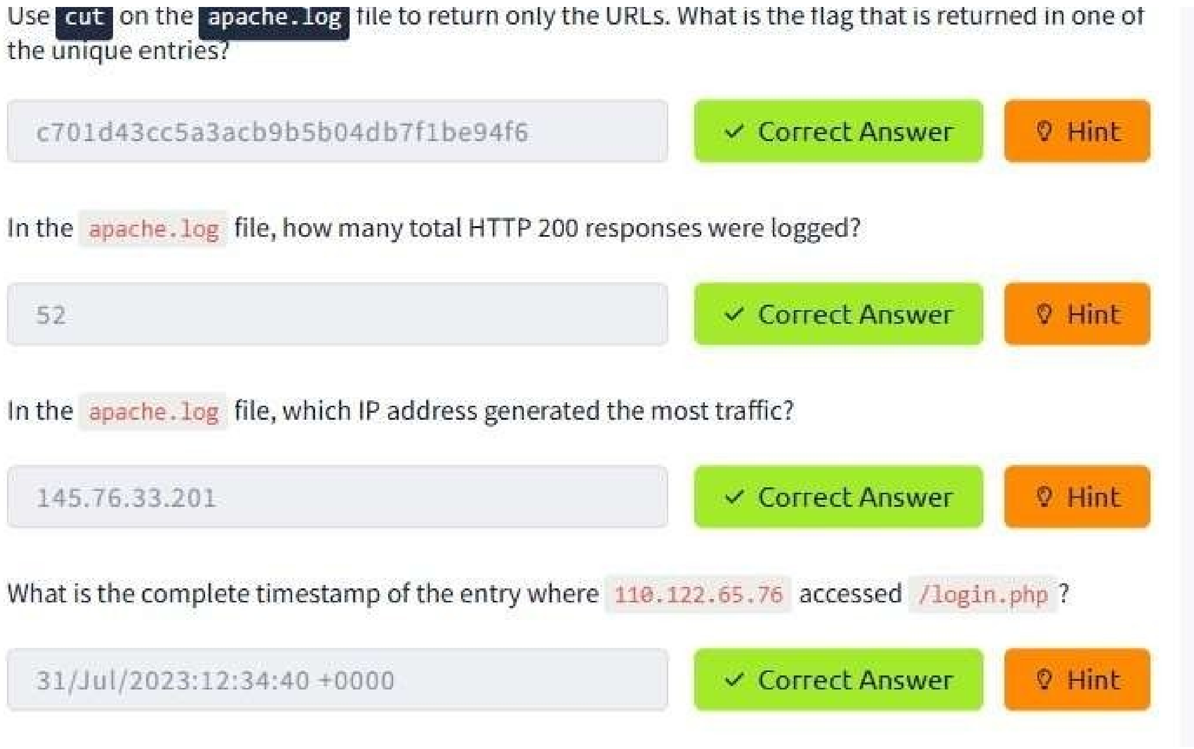
A log file is processed by a tool which returns an output. What form of analysis is this?

Automated

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

Manual

TASK 6 : LOG ANALYSIS TOLLS : COMMAND LINE



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

In the `apache.log` file, how many total HTTP 200 responses were logged?

52

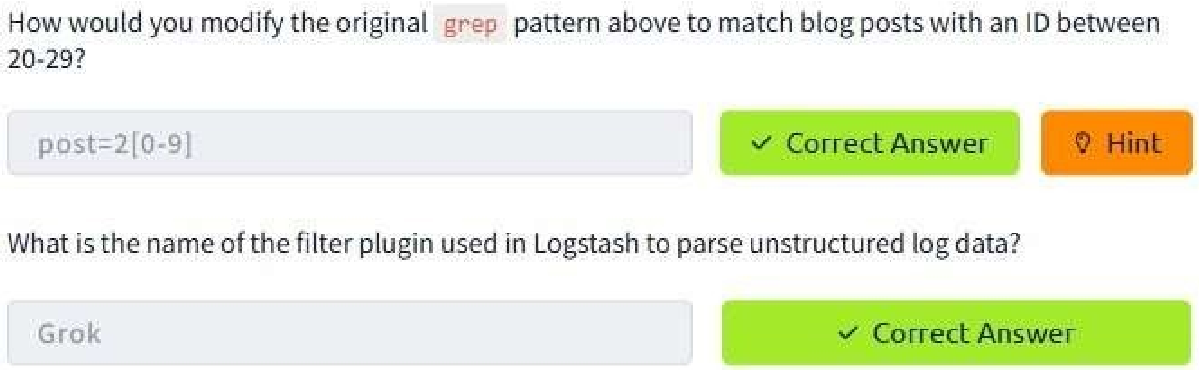
In the `apache.log` file, which IP address generated the most traffic?

145.76.33.201

What is the complete timestamp of the entry where `110.122.65.76` accessed `/login.php` ?

31/Jul/2023:12:34:40 +0000

TASK 7 : LOG ANALYSIS TOOLS : REGULAR EXPRESSIONS



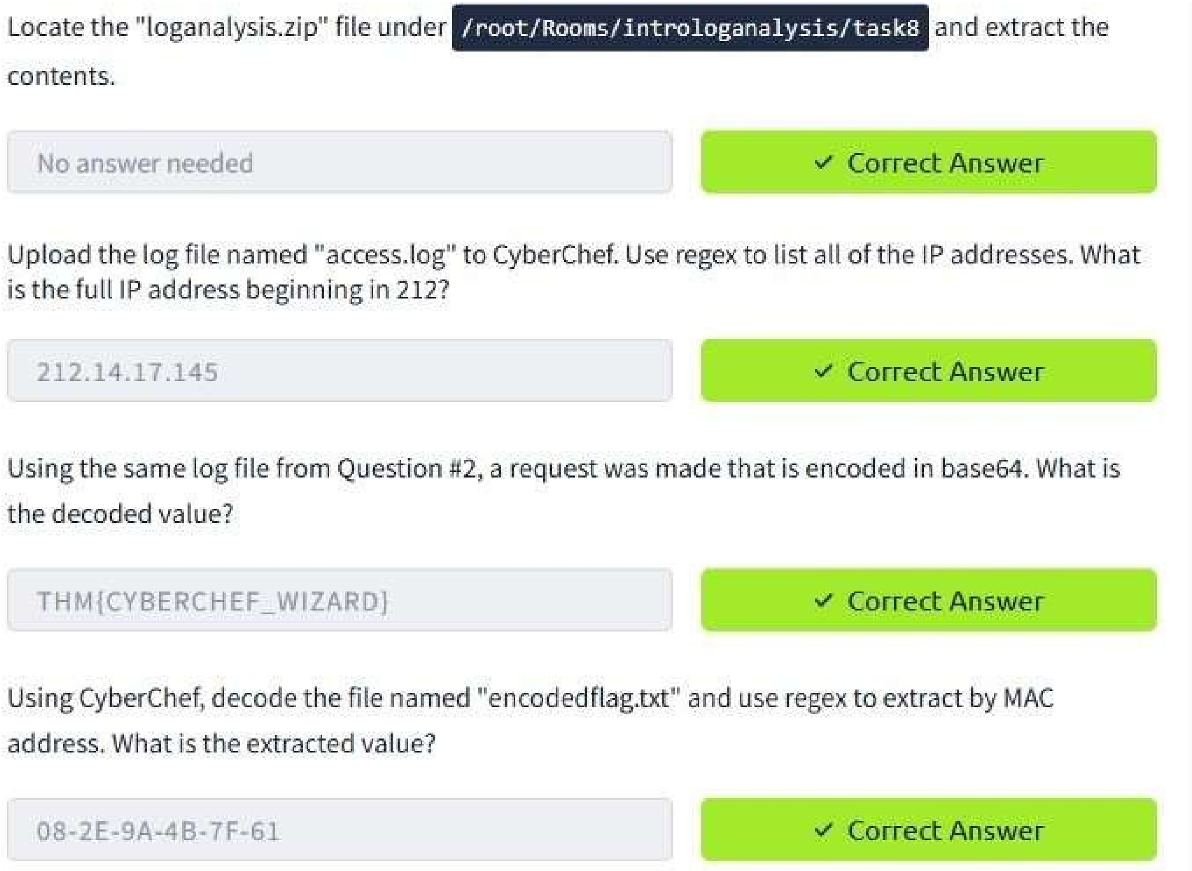
How would you modify the original `grep` pattern above to match blog posts with an ID between 20-29?

post=2[0-9]

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

Grok

TASK 8 : LOG ANALYSIS TOOLS : CYBERCHEF



Locate the "loganalysis.zip" file under `/root/Rooms/introloganalysis/task8` and extract the contents.

No answer needed

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

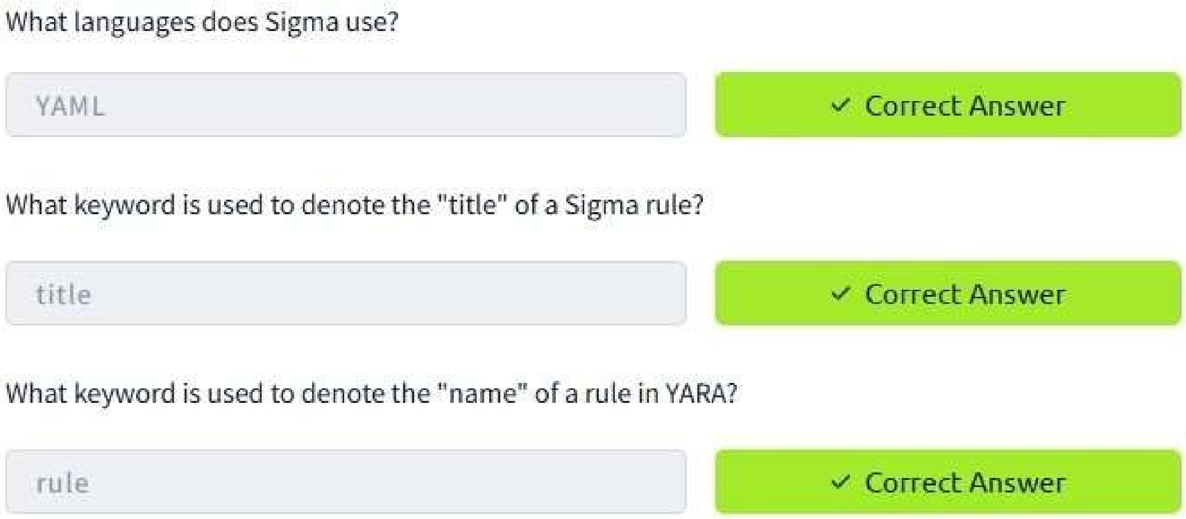
Using the same log file from Question #2, a request was made that is encoded in base64. What is the decoded value?

THM{CYBERCHEF_WIZARD}

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

TASK 9 ; LOG ANALYSIS TOOLS : YARA AND SIGMA



What languages does Sigma use?

YAML

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

title

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

rule

RESULT :

An intro to log analysis, best practices and essential tools for effective detection and response learned and successfully executed.