

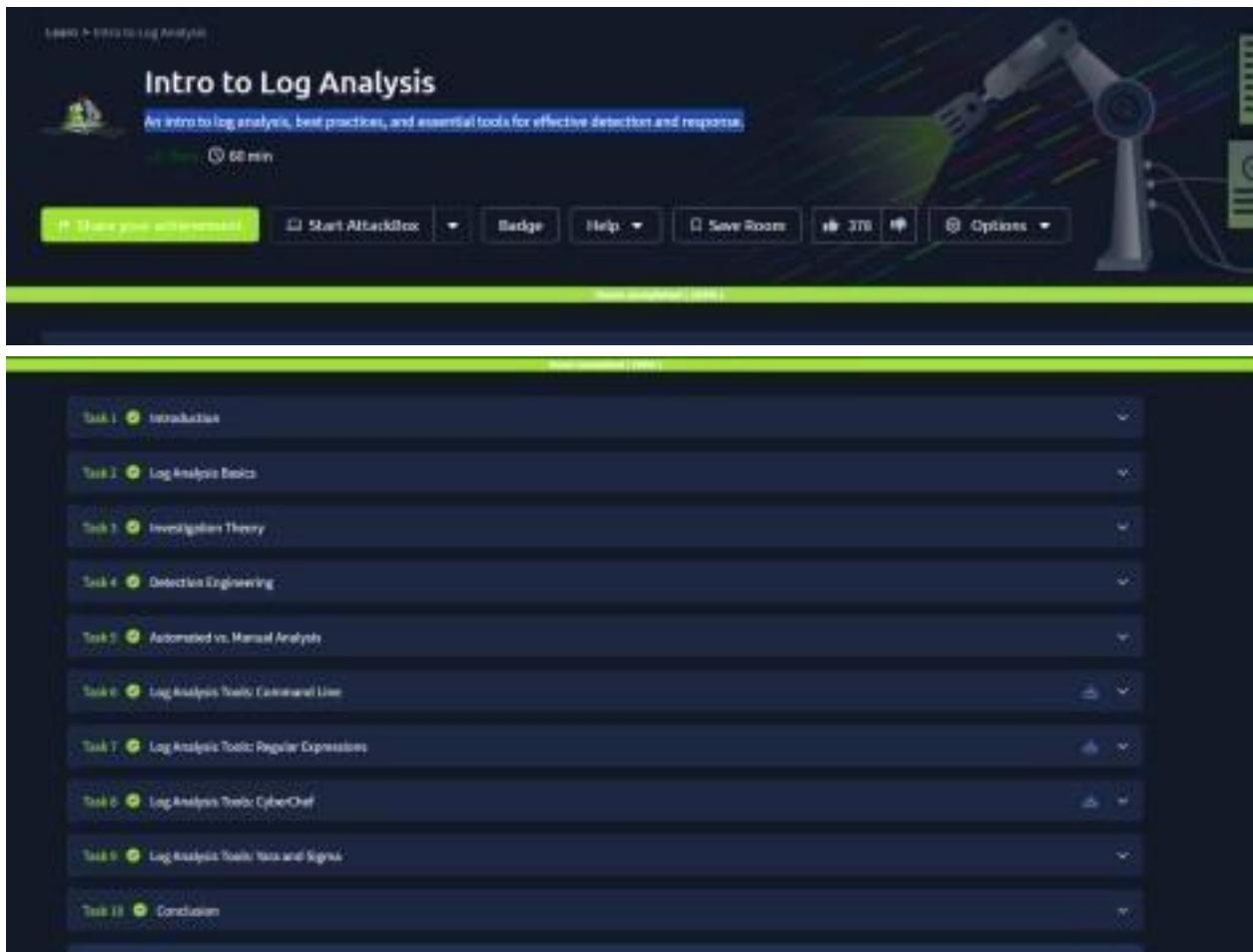
EXP-NO:14 LOG ANALYSIS FOR DETECTION AND RESPONSE

DATE :28-4-25

231901016

Jose Mugilan D

Aim: To understand log analysis, implement best practices, and use essential tools for efficient threat detection and incident response.



Use `cat` on the `apache_log` file to return only the URLs. What is the flag that is returned in one of the unique entries?

`200` ✓ Correct Answer 5 / 10 pts

In the `apache_log` file, how many total HTTP 200 responses were logged?

`10` ✓ Correct Answer 5 / 10 pts

In the `apache_log` file, which IP address generated the most traffic?

`192.168.1.100` ✓ Correct Answer 5 / 10 pts

What is the complete timestamp of the entry where `10.10.10.10` accessed `/index.php`?

`2020-10-10 10:10:10` ✓ Correct Answer 5 / 10 pts

Locate the "loganalysis.zip" file under `/root/.ssh/ctfloganalysis/tasks` and extract its contents.

=> Correct Answer

Upload the log file named "access.log" in CyberChef. Use regex to list all of the IP addresses. What is the full IP address beginning in 212?

=> Correct Answer

Using the same log file from Question 42, a request was made that is encoded in base64. What is the decoded value?

=> Correct Answer

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

=> Correct Answer

Answers the questions below

What languages does Sigma use?

YAML

Correct Answer

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

title

Correct Answer

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

meta

Correct Answer

Result: Gained insights into analyzing logs effectively, applying best practices, and leveraging tools to detect and respond to security events.