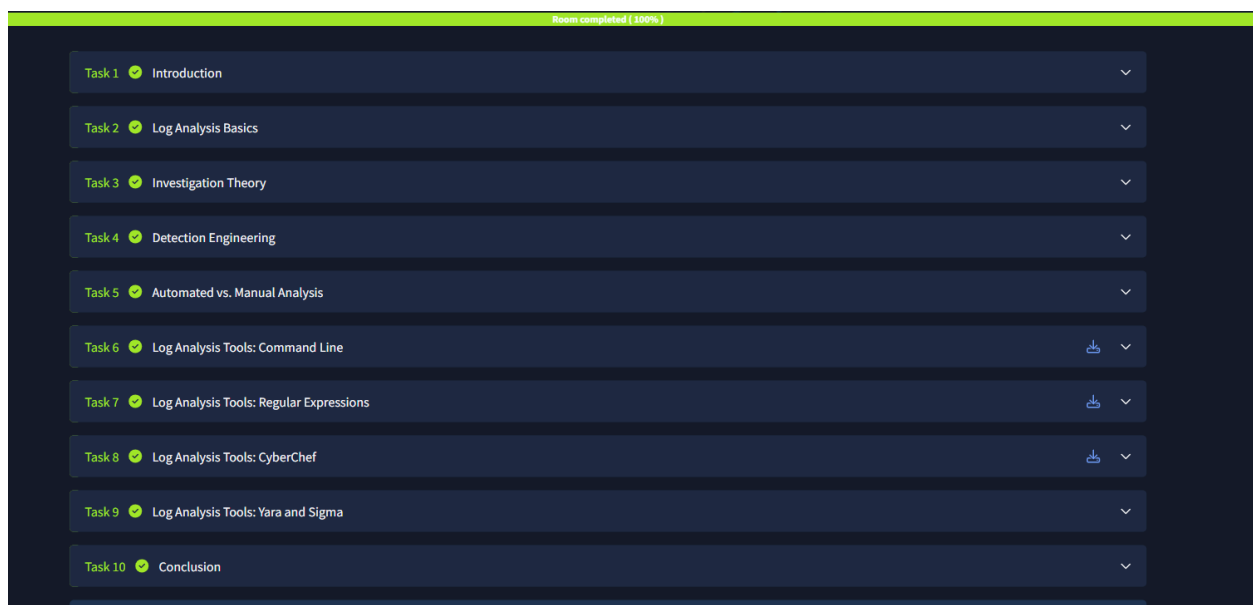
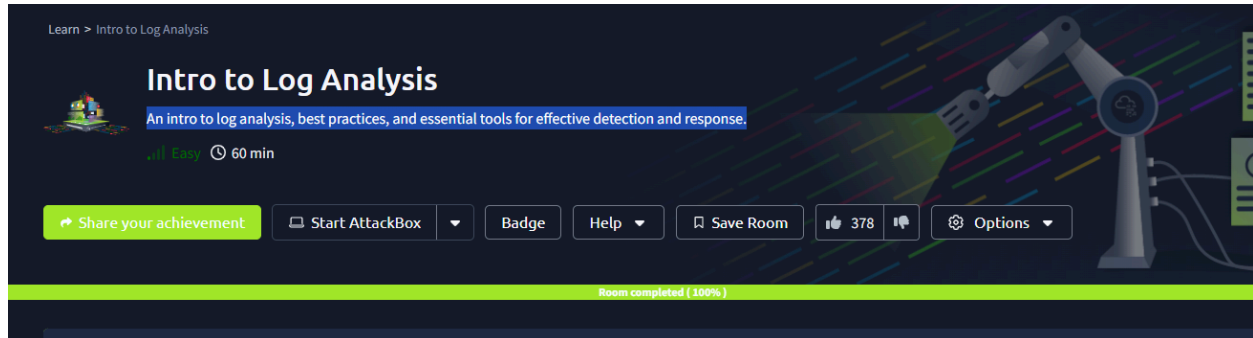


EXERCISE 14

LOG ANALYSIS FOR DETECTION AND RESPONSE

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



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?

✓ Correct Answer Hint

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

✓ Correct Answer Hint

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

✓ Correct Answer Hint

What is the complete timestamp of the entry where `119.122.65.76` accessed `/login.php`?

✓ Correct Answer Hint

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

✓ Correct Answer

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?

✓ Correct Answer

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

✓ Correct Answer

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

✓ Correct Answer

Answer the questions below

What languages does Sigma use?

✓ Correct Answer

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

✓ Correct Answer

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

✓ Correct Answer

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