

Vishwanath M 231901062

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.

Learn > Intro to Log Analysis

Intro to Log Analysis

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

Skill Level: Easy ⌚ 60 min

Share your achievement Start AIBackBox Badge Help Save Rooms 378 Options

Now completed (100%)

- 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

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?

✓ 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 `198.322.85.76` accessed `/?logix.php?`

✓ Correct Answer
🔔 Hint

Locate the "loganalysis.zip" file under `/root/.moons/jetrolanalysts/tasks` 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.