



Intro to Log Analysis

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

Easy ⌚ 60 min

Share your achievement

Start AttackBox

Badge

Help

Save Room

400

Options

Task 2 ✓ Log Analysis Basics

Task 3 ✓ Investigation Theory

Answer the questions below

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 `763f8dbdc98d105a8e2f36157e98bbe` be classified as?

File Hashes

✓ Correct Answer

Task 4 ✓ Detection Engineering

Answer the questions below

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

`/var/log/nginx/access.log`

✓ Correct Answer

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

Path Traversal

✓ Correct Answer

Task 5 ✓ Automated vs. Manual Analysis

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

Task 6 ✓ Log Analysis Tools: Command Line

Answer the questions below

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

✓ Correct Answer

🔍 Hint

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

52

✓ Correct Answer

🔍 Hint

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

145.76.33.201

✓ Correct Answer

🔍 Hint

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

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

✓ Correct Answer

🔍 Hint

Task 7 Log Analysis Tools: Regular Expressions



Answer the questions below

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

post=2[0-9]

✓ Correct Answer

🔍 Hint

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

Grok

✓ Correct Answer

Task 8 Log Analysis Tools: CyberChef



Answer the questions below

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

No answer needed

✓ 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?

212.14.17.145

✓ Correct Answer

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}

✓ Correct Answer

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

✓ Correct Answer

Task 9 Log Analysis Tools: Yara and Sigma



Answer 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?

rule

✓ Correct Answer

Task 10 Conclusion

