LOG ANALYSIS FOR DETECTION AND RESPONSE

EXP.NO: 9 DATE:25-03-2025

AIM:

The primary aim of the Log Analysis for Detection and Response is to equip learners with the knowledge and practical skills required to analyze system and network logs effectively. This is to identify potential security incidents, respond to threats, and enhance the overall security posture of an organization.

OBJECTIVE:

- 1. Introduction to Logs: A log is a stream of time-sequenced messages that record occurring events. Log analysis is the process of making sense of the events captured in the logs to paint a clear picture of what has happened across the infrastructure.
- 2. Importance of Logs:

System Troubleshooting: Analyzing system errors and warning logs helps IT teams understand and quickly respond to system failures, minimizing downtime, and improving overall system reliability.

Cyber Security Incidents: In the security context, logs are crucial in detecting and responding to security incidents. Firewall logs, intrusion detection system (IDS) logs, and system authentication logs, for example, contain vital information about potential threats and suspicious activities. Performing log analysis helps SOC teams and Security Analysts identify and quickly respond to unauthorized access attempts, malware, data breaches, and other malicious activities.

Threat Hunting: On the proactive side, cyber security teams can use collected logs to actively search for advanced threats that may have evaded traditional security measures. Security Analysts and Threat Hunters can analyze logs to look for unusual patterns, anomalies, and indicators of compromise (IOCs) that might indicate the presence of a threat actor.

Compliance: Organizations must often maintain detailed records of their system's activities for regulatory and compliance purposes. Regular log analysis ensures that organizations can provide accurate reports and demonstrate compliance with regulations such as GDPR, HIPAA, or PCI DSS.

3. Different Types of Logs

TASK 1: INVESTIGATION THEORY

Understand the concepts of timelines, data visualisation and threat intelligence.

TASK 2: DETECTION ENGINEERING

This task encompasses common log file locations on Linux systems, common patterns for identifying suspicious behaviour, and common attack signatures.

TASK 3: AUTOMATED VS. MANUAL ANALYSIS

This short task explains the pros and cons of automated and manual analysis. Manual analysis is the process of examining data and artifacts without using automation tools, whereas automated analysis involves tools.

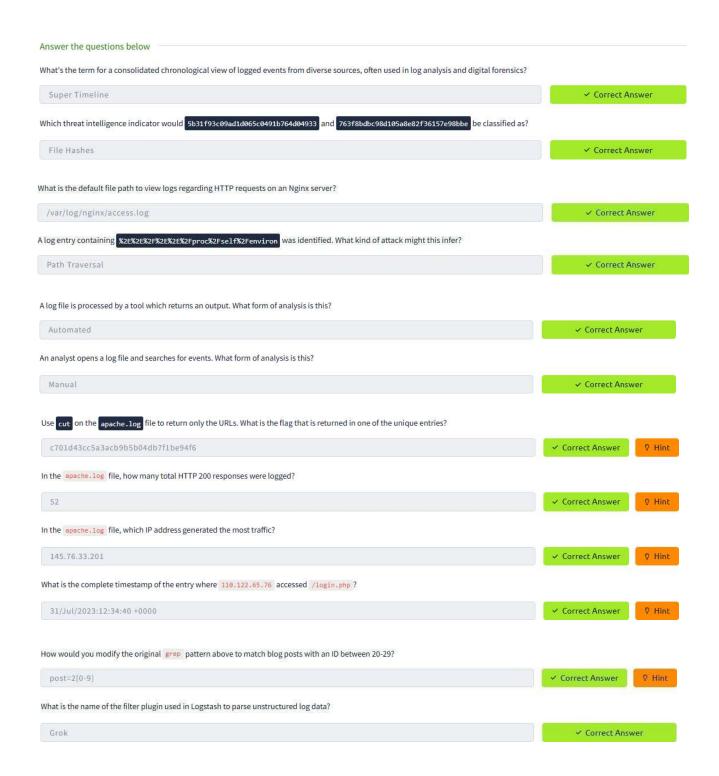
PADMAPRIYA S 220701193

TASK 4: LOG ANALYSIS TOOLS USING LINUX COMMAND LINE

TASK 5: LOG ANALYSIS USING REGULAR EXPRESSIONS

TASK 6: LOG ANALYSIS USING CYBERCHEF

TASK 7: LOG ANALYSIS TOOLS: YARA AND SIGMA



PADMAPRIYA S 220701193

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
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

RESULT:

After completing this, got a solid foundation in log analysis, a critical skill in cybersecurity for identifying, investigating, and responding to security threats efficiently.

PADMAPRIYA S 220701193