EX NO: 14 Log Analysis for detection and response

AIM:

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

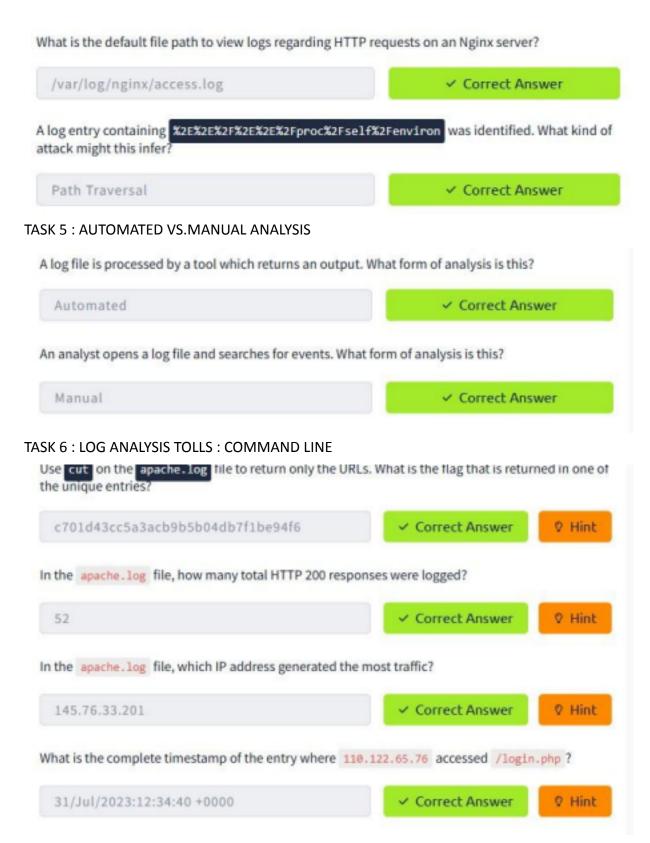


TASK 3: INVESTIGATION THEORY

What's the term for a consolidated chronological view of logged events from diverse sources, often used in log analysis and digital forensics?



TASK 4: DETECTION ENGINEERING



TASK 7: LOG ANALYSIS TOOLS: REGULAR EXPRESSIONS

How would you modify the original grep pattern above to match blog posts with an ID between 20-29? Correct Answer post=2[0-9] ♥ Hint What is the name of the filter plugin used in Logstash to parse unstructured log data? Correct Answer Grok TASK 8: LOG ANALYSIS TOOLS: CYBERCHEF 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



RESULT:

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