NAME: RITHIKA BASKAR ROLL NO: 231901042

Intro to Log Analysis

EX-NO:14

AIM:

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

PROCEDURE:

- 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

Task 1 Introduction:



Task 2 Log Analysis Basics:



Task 3 Investigation Theory:



Task 4 Detection Engineering:

NAME: RITHIKA BASKAR ROLL NO: 231901042



Task 5 Automated vs. Manual Analysis:



Task 6 Log Analysis Tools: Command Line:

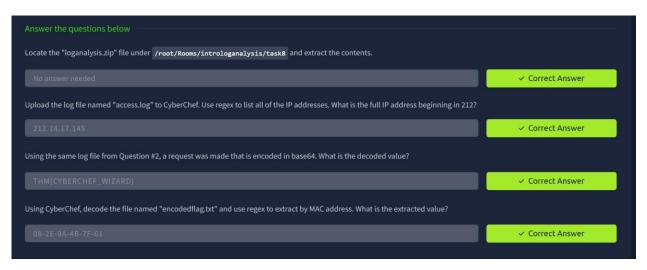


Task 7 Log Analysis Tools: Regular Expressions:



Task 8 Log Analysis Tools: CyberChef:

NAME: RITHIKA BASKAR ROLL NO: 231901042



Task 9 Log Analysis Tools: Yara and Sigma:



Task 10 Conclusion:



RESULT:

Thus the Intro To Log Analysis is completed using tryhackme platform.