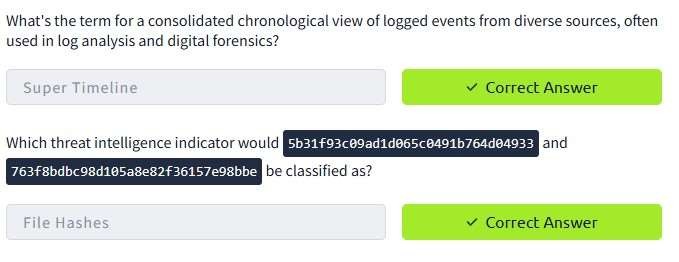
EX NO : 14 Log Analysis for detection and response 231901005

AIM:

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



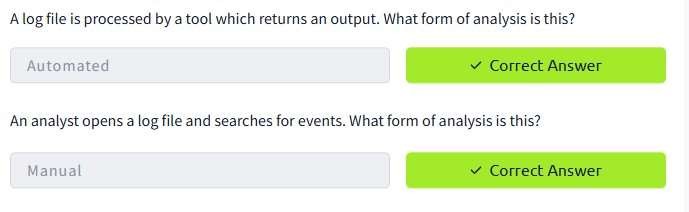
TASK 3 : INVESTIGATION THEORY



TASK 4 : DETECTION ENGINEERING



TASK 5 : AUTOMATED VS.MANUAL ANALYSIS



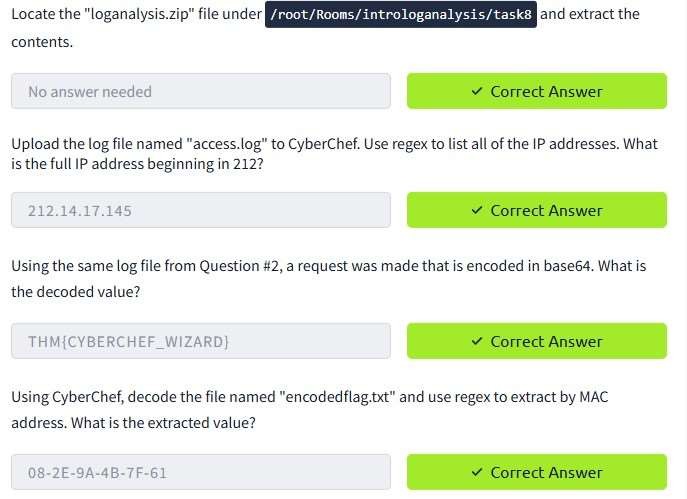
TASK 6 : LOG ANALYSIS TOLLS : COMMAND LINE



TASK 7 : LOG ANALYSIS TOOLS : REGULAR EXPRESSIONS



TASK 8 : LOG ANALYSIS TOOLS : CYBERCHEF



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.