EXPTNO:09 ROLLNO: 220701259

INTROTOLOG ANALYSIS

AIM:

Gain a foundational understanding of log analysis in cybersecurity by learning to investigate events using log data from various systems. This includes identifying anomaliesandsuspiciousbehaviorusingcommand-linetools,regularexpressions, and platforms like CyberChef.

PROCEDURE:

1. Beginwiththetheory oflogtypes,timelines,andthreat indicators.

2. UseLinuxCLItoolslike`cut`,`awk`,`grep`,and `uniq`forlogfiltering.

3. DecodeobfuscatedpayloadswithCyberChef(e.g.,Base64, MACs).

4. Useregexpatternstoextractspecificvaluesfrom logs.

5. UnderstandthefunctionofLogstashGrokfilters.

6. WriteandunderstanddetectionrulesusingYARAandSigmaYAMLformat.

TASK1–INTRODUCTION

-Introducesloganalysisanditsroleincybersecurityoperations.

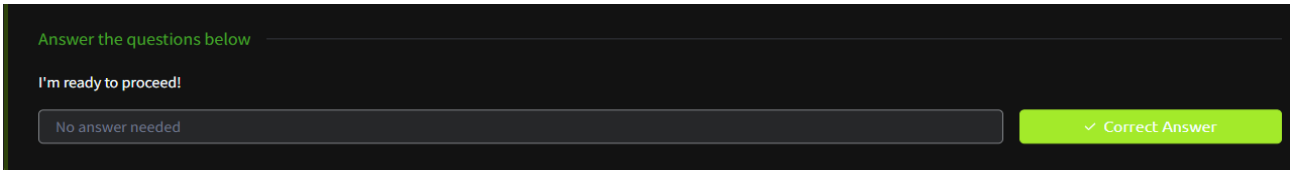
- Explainshowlogshelpdetectandinvestigatemaliciousactivity.

- Describesvariouslogtypeslikesystem,application,andsecuritylogs.

- Setsthefoundationforworkingwithforensictoolsandlogfiles.

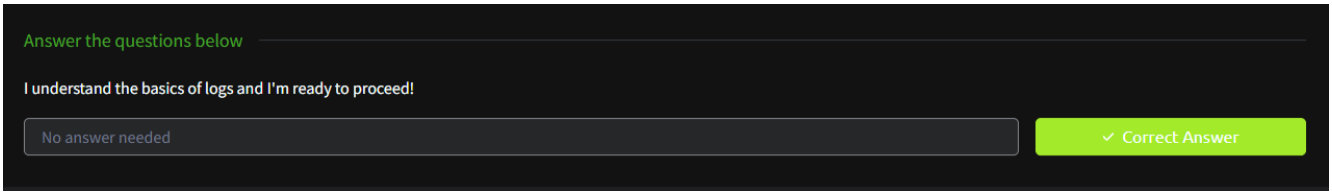
- Highlightshowlogtrailsareessentialinincidentresponse

- Encouragesamindsetofcuriosityandpatternrecognition



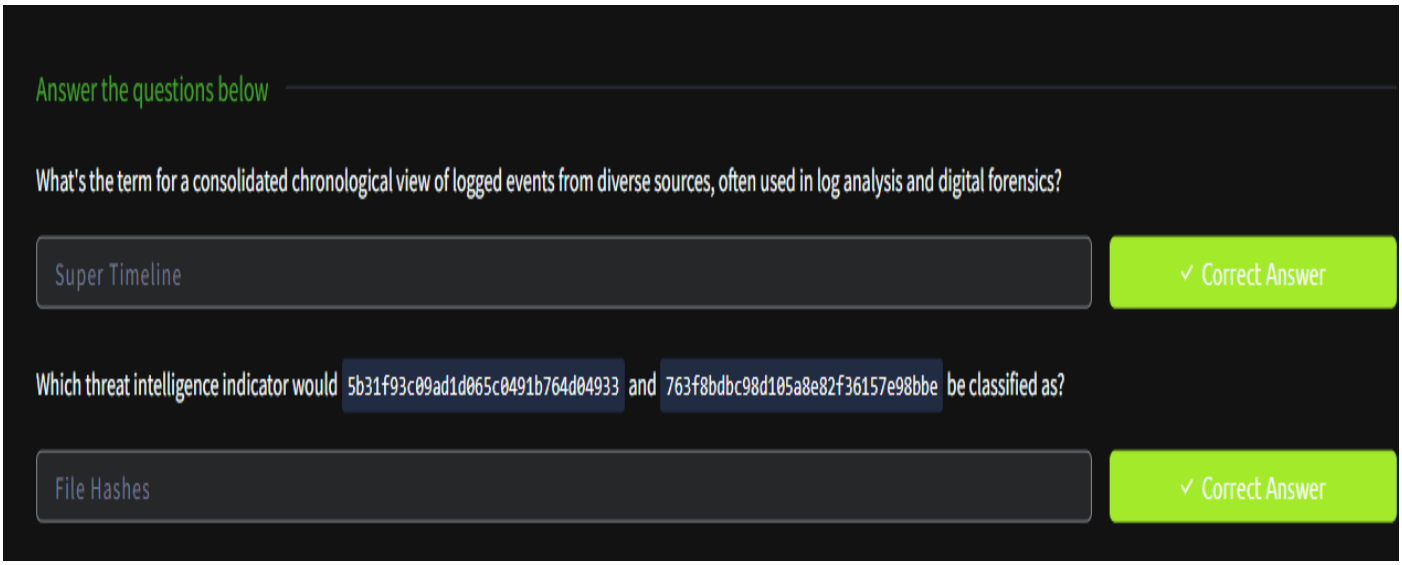
TASK2–TYPESOFLOGS

- Coversvarioustypesoflogsusedinanalysis,suchasApache,DNS,Syslog.
- Explainsthestructureandpurposeofeachlogtype.
- Helpsidentifywhichlogsareusefulforwhich kindofthreator anomaly.
- Emphasizesreadingtimestamps,IPs,andmethod/statusfields.
- Reinforceslogrelevanceinreal-world investigations.
- Formsthebasisforchoosingtherightlogduringtriage.



TASK3–INVESTIGATIONTHEORY

- Introducestheconceptoftimelinesandeventcorrelation.
- Definesa"SuperTimeline"forcross-systemanalysis.
- Discussesthreatindicatorslikefilehashes (MD5).
- Coversvisualizingeventsandidentifyingintrusionpatterns.
- Questionshelpreinforceunderstandingofanalysistheory.
- Equipsuserstothinksystematicallyduringlogreview.

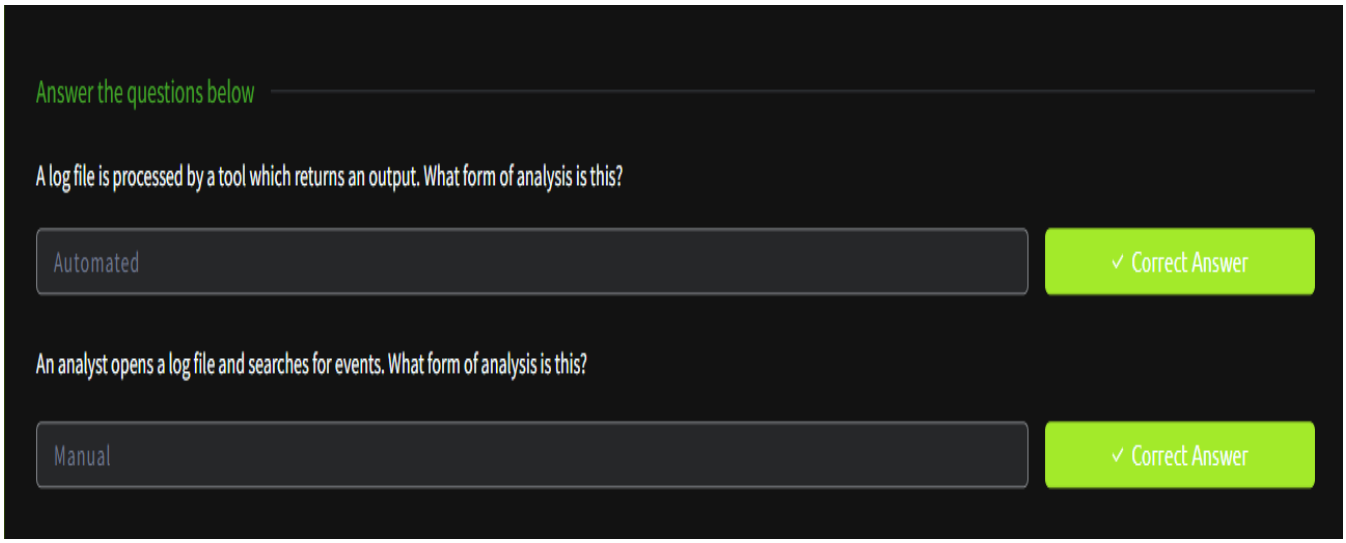


TASK4–DETECTIONENGINEERING

- Focusesonidentifyingsuspiciousbehaviorin logs.
- Highlightsdefaultloglocations,like`/var/log/nginx/access.log`.
- Teachesdetectionofencodedattackslikepath traversal.
- Showshowtodecode`%2E%2E/`and otherencodedthreats.
- Buildsawarenessofsignature-basedlogindicators.
- Practicalexamplesprepareusersforrealdetection tasks.

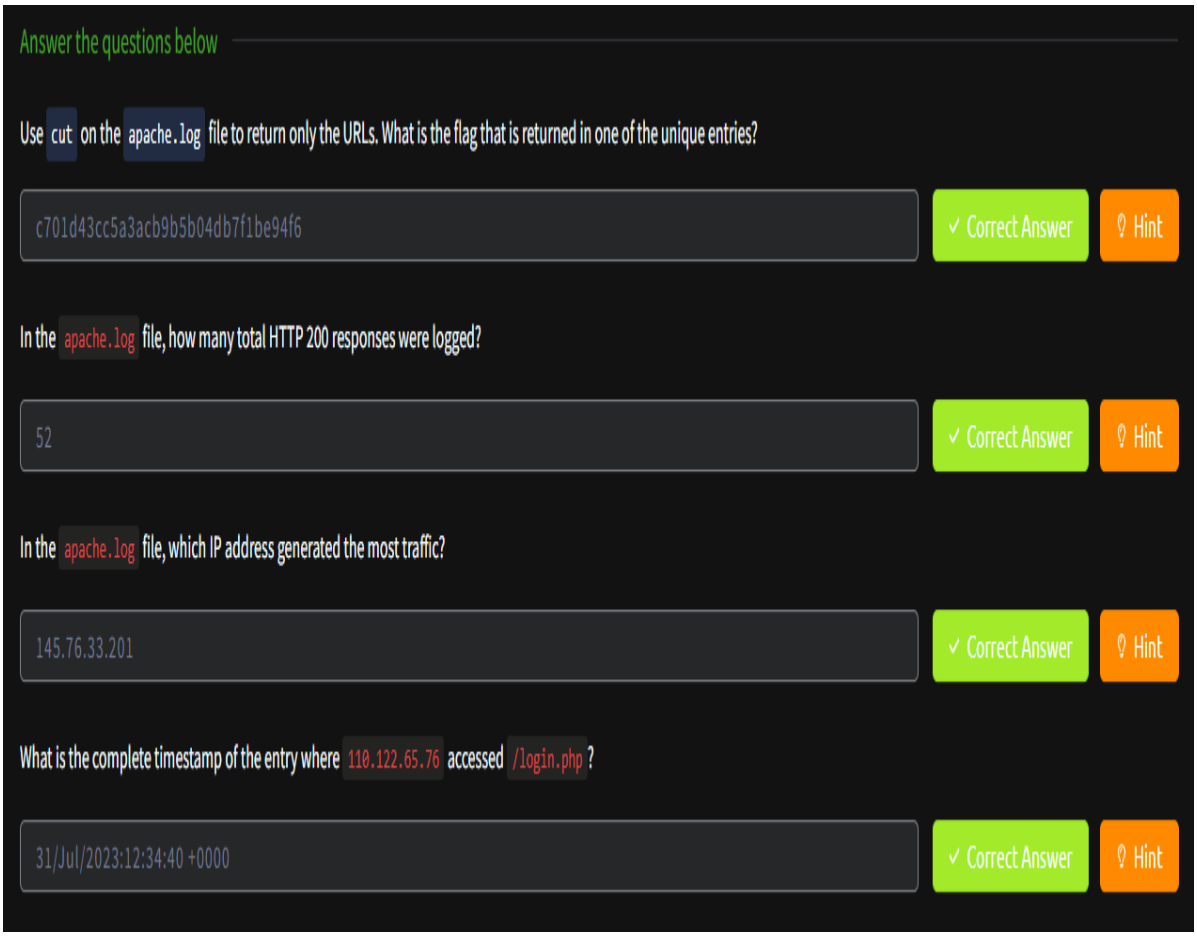
TASK5–AUTOMATEDVS.MANUALANALYSIS

- Comparesautomatedlogparsingwithmanualinvestigation.
- Showswhentousetoolsvs.human-ledjudgment.
- Demonstratesstrengthsandlimitsofbothapproaches.
- Promoteshybridusageofautomateddetectionandhumaninsight.
- Reinforceshowautomationsavestime,buthumanscatchcontext.
- SimpleQ&Amakestheconceptclearandapplicable.



TASK6–LOGANALYSISTOOLS:COMMANDLINE

- UsesCLItoolslike`cut`,`awk`,`sort`,`uniq`,and`wc`.
- ExtractsURLs,IPs,andcountsresponsecodesinApache logs.
- HelpsidentifymostactiveIPsoranomaliesin logs.
- Tasksincludetimestampextraction,patternfiltering.
- Encourageshands-onpracticeandefficientloghandling.
- ReinforcesLinuxCLIasaprimaryskillfor analysts.



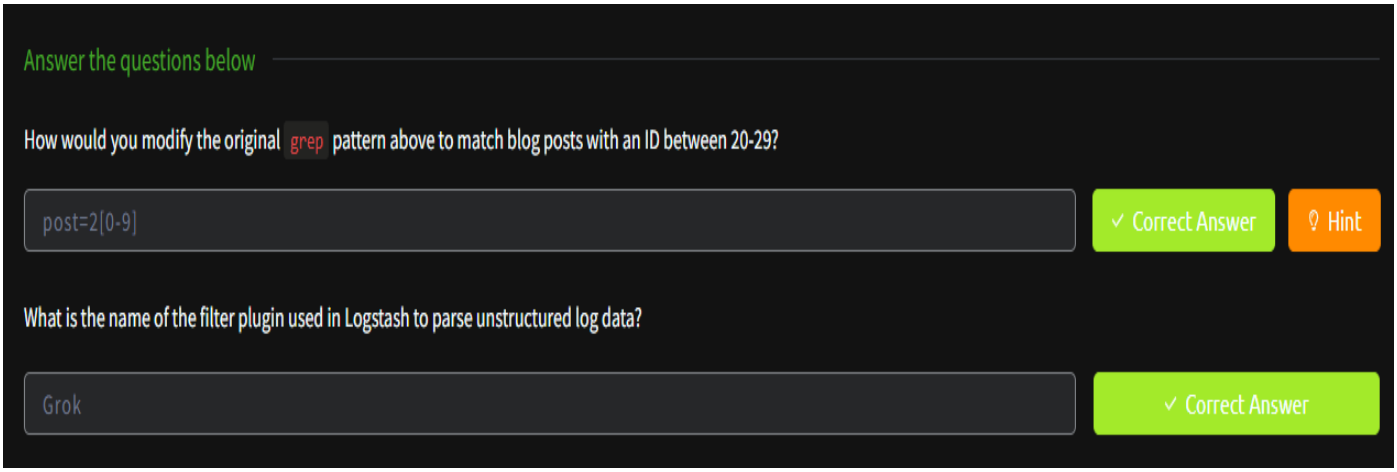
TASK7–LOGANALYSISTOOLS:REGULAREXPRESSIONS

- Introducesregexforlogpatternextractionandfiltering.

- Teachesmatchingranges(e.g.,post=2[2–6])andwildcards.

- Showshowregexsimplifieslocatingkeydataentries.

- ExplainstheGrokpluginforparsingunstructuredlogs.



- FormsthebaseforautomationinSIEMlogparsing.

- Buildsmusclememoryinlogfilteringprecision.

TASK8–LOGANALYSISTOOLS:CYBERCHEF

- DemonstratesuseofCyberChefforIP/MACextractionanddecoding.

- ShowsregexmatchingforIPv4andBase64decoding.

- Usesfilterstorefinelargedatasetsintoactionabledata.

- Tasksincludedecodingembeddedflagsandextractingpatterns.

- Reinforcesvisual/logicalchainingoftransformations.

- Makesadvancedparsingaccessibleforbeginners.

TASK9–LOGANALYSISTOOLS:YARAANDSIGMA

- IntroducesdetectionrulewritingwithYARA(malware)andSigma(logs).
- Explainssyntaxlike`rule`(YARA)and`title`(SigmaYAML).
- DemonstrateshowSigmahelpsstandardizedetectionacrossplatforms.
- Teachesrulereadabilityandstructureinthreatdetection.
- Buildsabridgebetweenmanualdetectionandautomatedalerts.
- Finalizestheroombyintegratingrulesintopracticaluse.

RESULT:

Successfullyunderstood the principles of loganalysis, practiced logfilteringand decoding,andappliedddetectionrulewritingusingindustrytools,layingastrong foundation for real-world security operations.