EXPTNO:08 ROLLNO:220701259

DEMONSTRATEINTRUSIONDETECTIONSYSTEM

AIM:

he aim of this experiment is to understand the working of Snort as an Intrusion Detection and Prevention System (IDS/IPS) by exploring its various operation modesincludingSniffer,Logger,NIDS/NIPS,andPCAPanalysis.Itinvolveslearning the rule structure used in Snort for traffic filtering and alert generation, investigating traffic logs

PROCEDURE:

1. Studythetheorybehind IDS/IPSsystemsandtheir types.

2. LaunchSnortindifferentmodesusingCLIparameters(Sniffer,Logger, IDS).

3. UsesamplePCAPsandlogstoanalyzenetworktraffic.

4. Writedetectionrulestofilterspecifictrafficbasedonheaders,flags,and content.

5. InvestigatealertsgeneratedbySnortandunderstandtheircomponents.

6. Testconfigurationfilesandcustomrulesetsforruleaccuracyand performance.

TASK1–INTRODUCTION

- Snortisanopen-sourceNIDS/NIPSmaintainedbyCisco Talos.

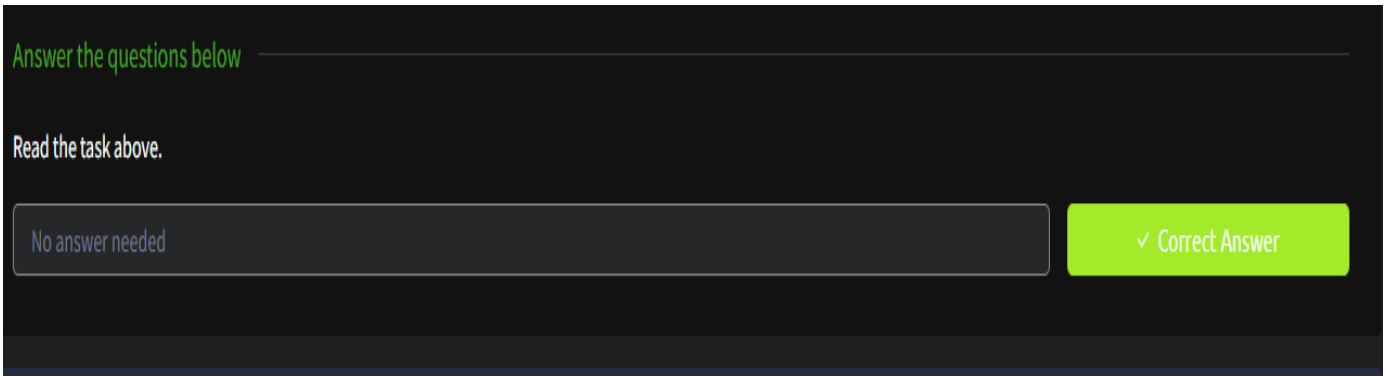
- Itdetectsmalicioustrafficusingrulesandgeneratesalerts.

- Offerslivetrafficinspection,packetlogging,andprotocolanalysis.

- CanoperateinSniffer,Logger,andIPSmodes.

- Cross-platformcompatibilitywithmodulararchitecture.

- Widelyusedinblue-teamandenterprisedefensesetups.



TASK2–INTERACTIVEMATERIALANDVM

- Runthecommand`./.easy.sh`inTask-Exercisesfolder.

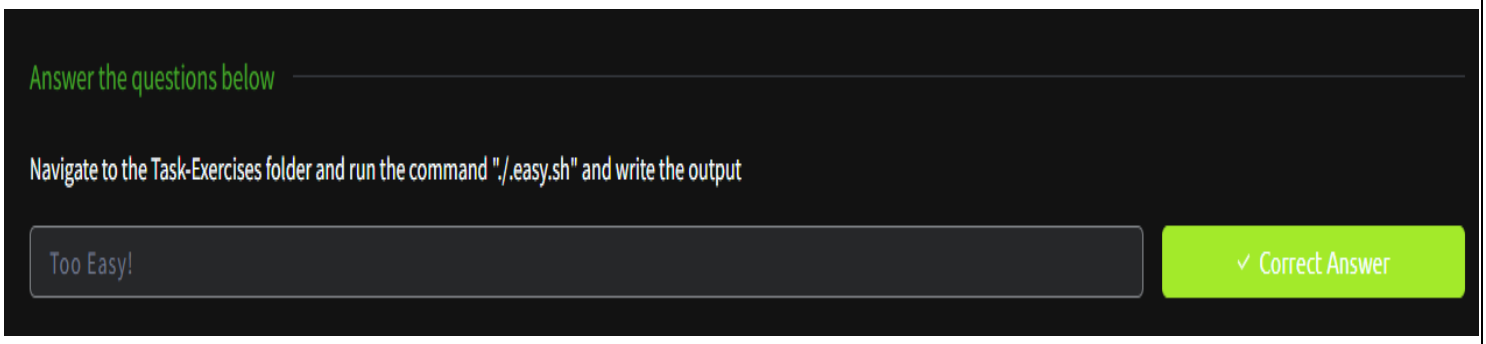
- ValidatesVMsetupandscriptexecutionpermissions.

- Outputmessageverifiesreadiness:"TooEasy!"

- EnsuresuserenvironmentisconfiguredtostartSnortlabs.

- Nopacketanalysisinthistask—justinteractionvalidation.

- Setsthebaseforupcominghands-on tasks.



TASK3–INTRODUCTIONTOIDS/IPS

- CoversthedistinctionbetweenNIDS/HIDSandNIPS/HIPS.

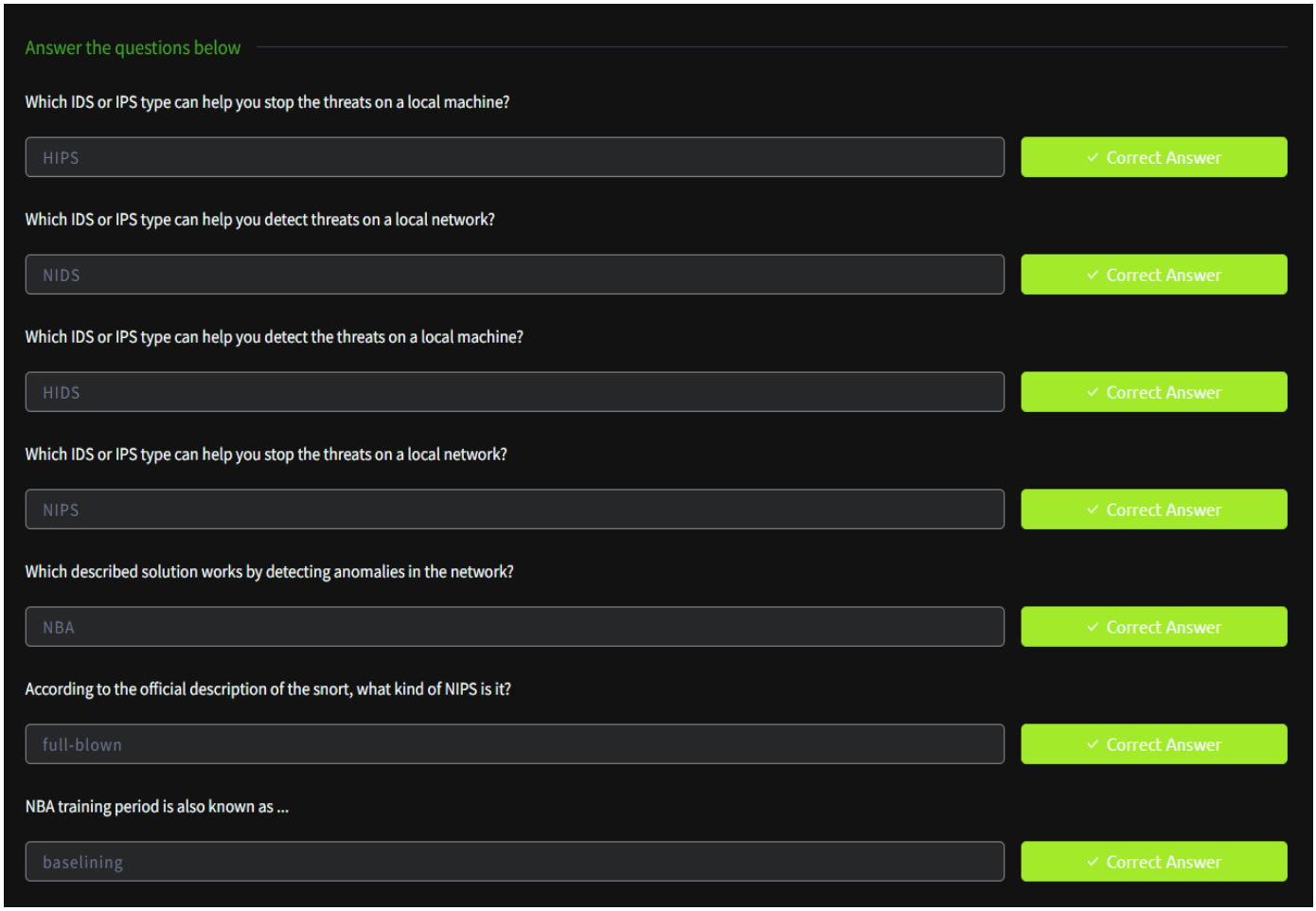
- Behavior-basedIPSsystems(NBA)requireatrainingperiod (baselining).

- IPSsystemscanactivelydroporblockmaliciouspackets.

- Explainssignature-based,behavior-based,andpolicy-baseddetection.

- MatchesSnortmodestoappropriateprotectionscopes(HIDS,NIDS,HIPS, NIPS).

- ClarifiesthatSnortisafull-blown IPSwithmulti-mode functionality.5yyy



TASK4–FIRSTINTERACTIONWITHSNORT

- Use`snort-V`tocheckSnortversionand build.

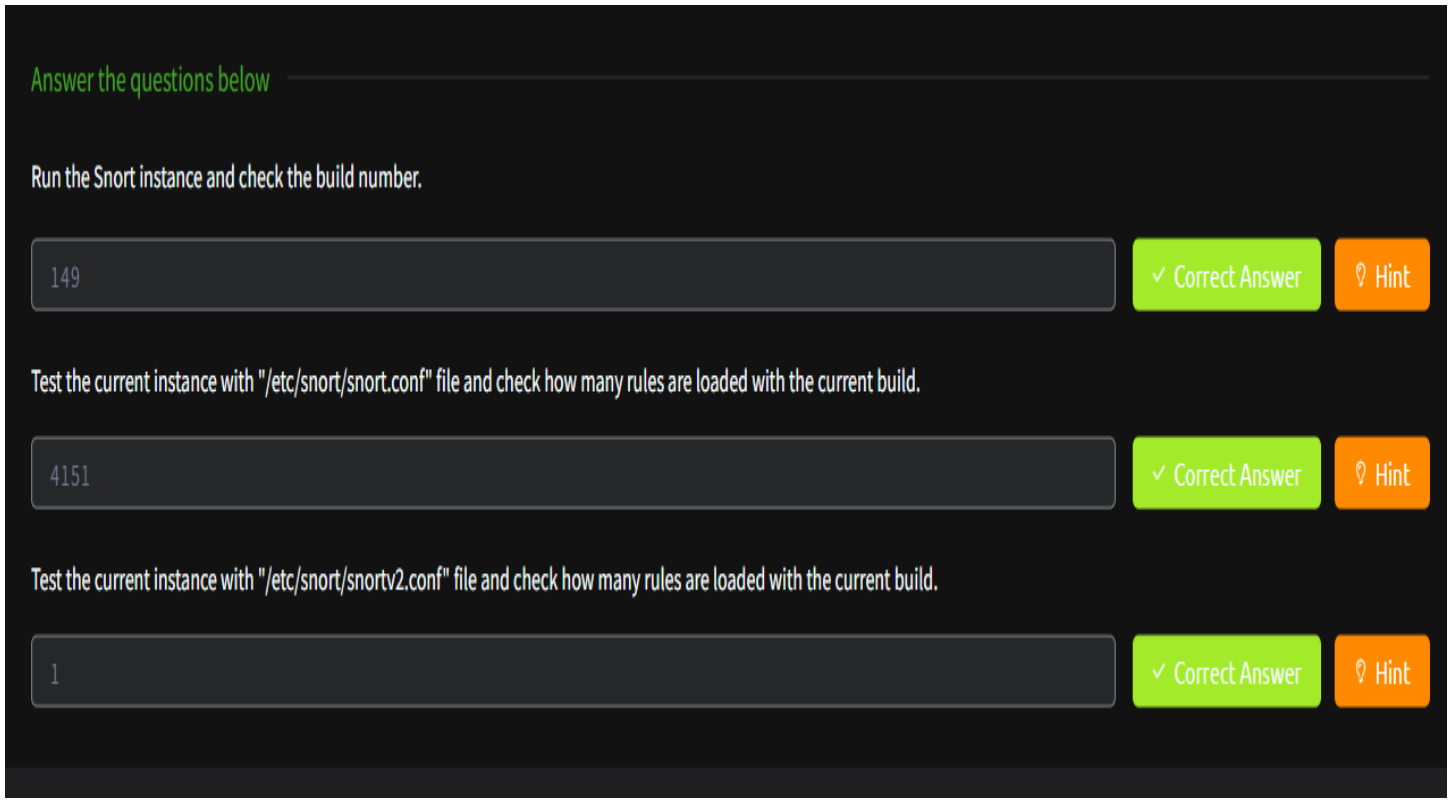
- Runself-testusing`snort-T-c<config>`toverifyconfig validity.

- Loaddefaultandalternativeconfigstocomparerule counts.

- `-T`testsconfigurationfilesforsyntaxandruleloading.

- Answers:Buildnumber=149,Rules loaded (default)=4151,(v2)= 1.

- Validatessetupbeforerealtrafficanalysis begins.



TASK5–OPERATIONMODE1:SNIFFERMODE

- Enablesreal-timepacketinspection(liketcpdump).

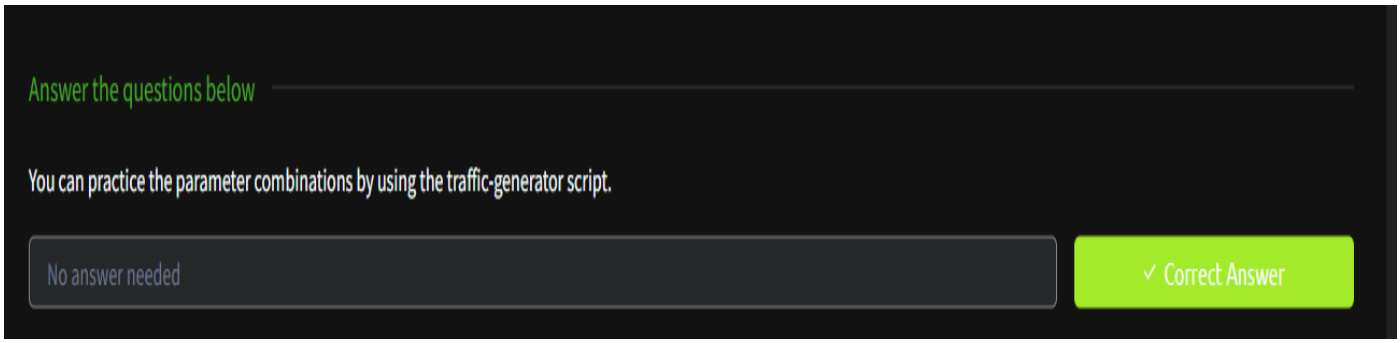
- Useflagslike`-v`,`-d`,`-e`,and`-X`forverbosityandheaders.

- `-i`specifiestheinterfacetosniff.

- Allowscombiningflagsfordetailedanalysis:`-v-d-e`.

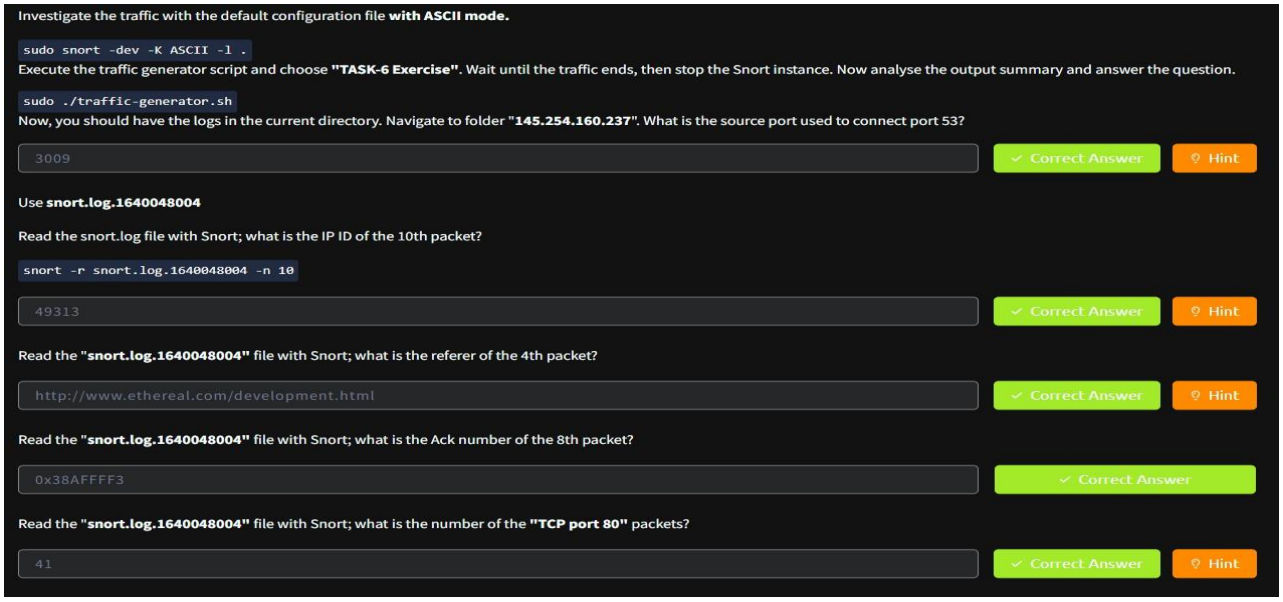
- Usefulforviewinglivetrafficpayloadsandheaders.

- Noalertingorlogging —justpacket visibility.



TASK6–OPERATIONMODE2:PACKETLOGGERMODE

- LogspacketsinASCIIortcpdumpformatto disk.
- `-l`specifiesthelogdirectory,defaultis`/var/log/snort`.
- Use`-r`toreadloggedfilesand`-n`tolimitpackets.
- Analyzelogsforsourceports,IPIDs,ACKnumbers,andreferers.
- UsefilterslikeBPF toisolatepackets(e.g.,`tcpport 80`).
- Enablesofflinepacketanalysisfrompreviouslycaptured sessions.



TASK7–OPERATIONMODE3:IDS/IPS

- Requiresrulefilesandconfiguration(`-c<snort.conf>`).

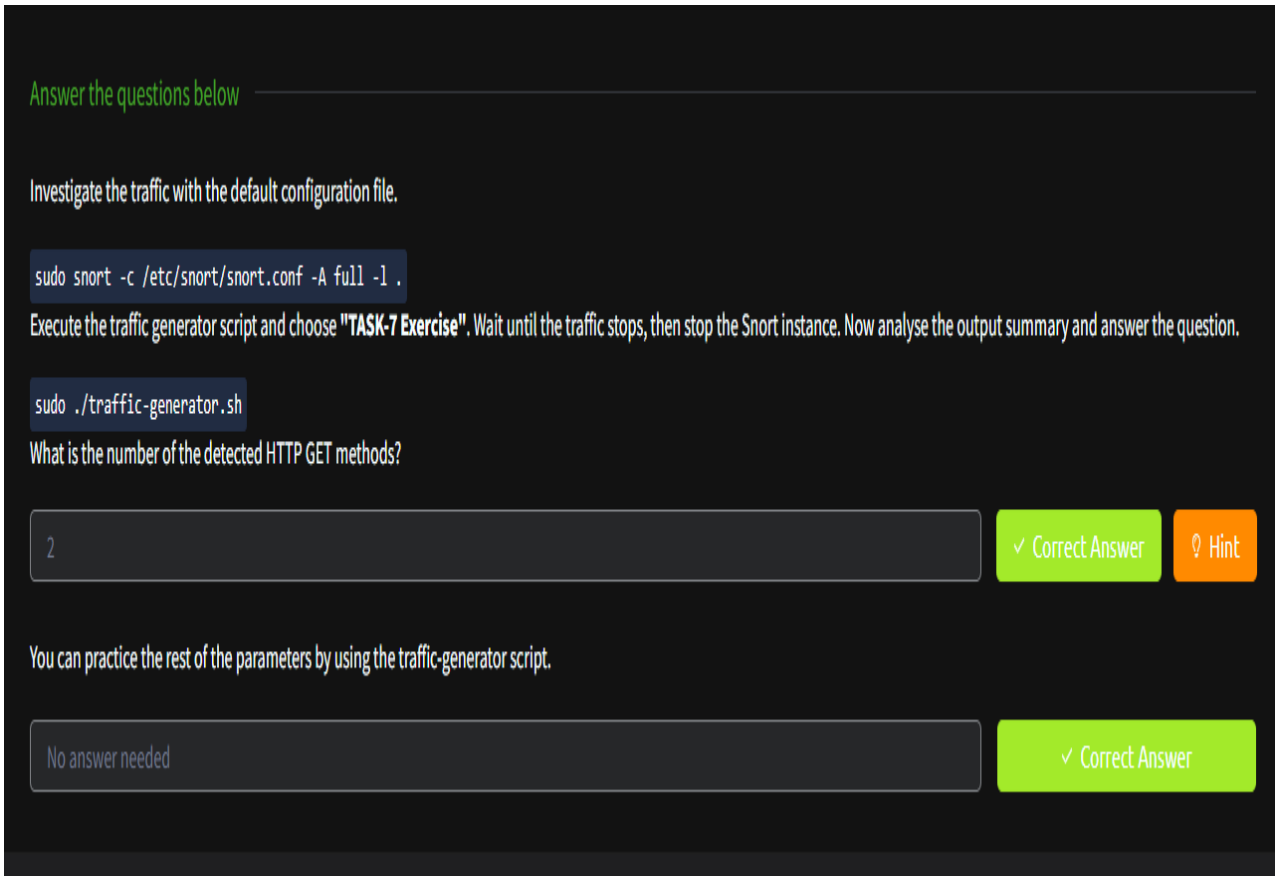
- Runwithmodeslike`-Afull`,`-Aconsole`,`-Afast`foralert types.

- `-D`runsSnortinbackground,`-X`enablesHEX output.

- Examplerule:`alerticmpanyany<>anyany(msg:"ICMPPacketFound";sid: 100001; rev:1;)`

- IPSmode:`-Q--daqafpacket -ieth0:eth1`enablesinlineprevention.

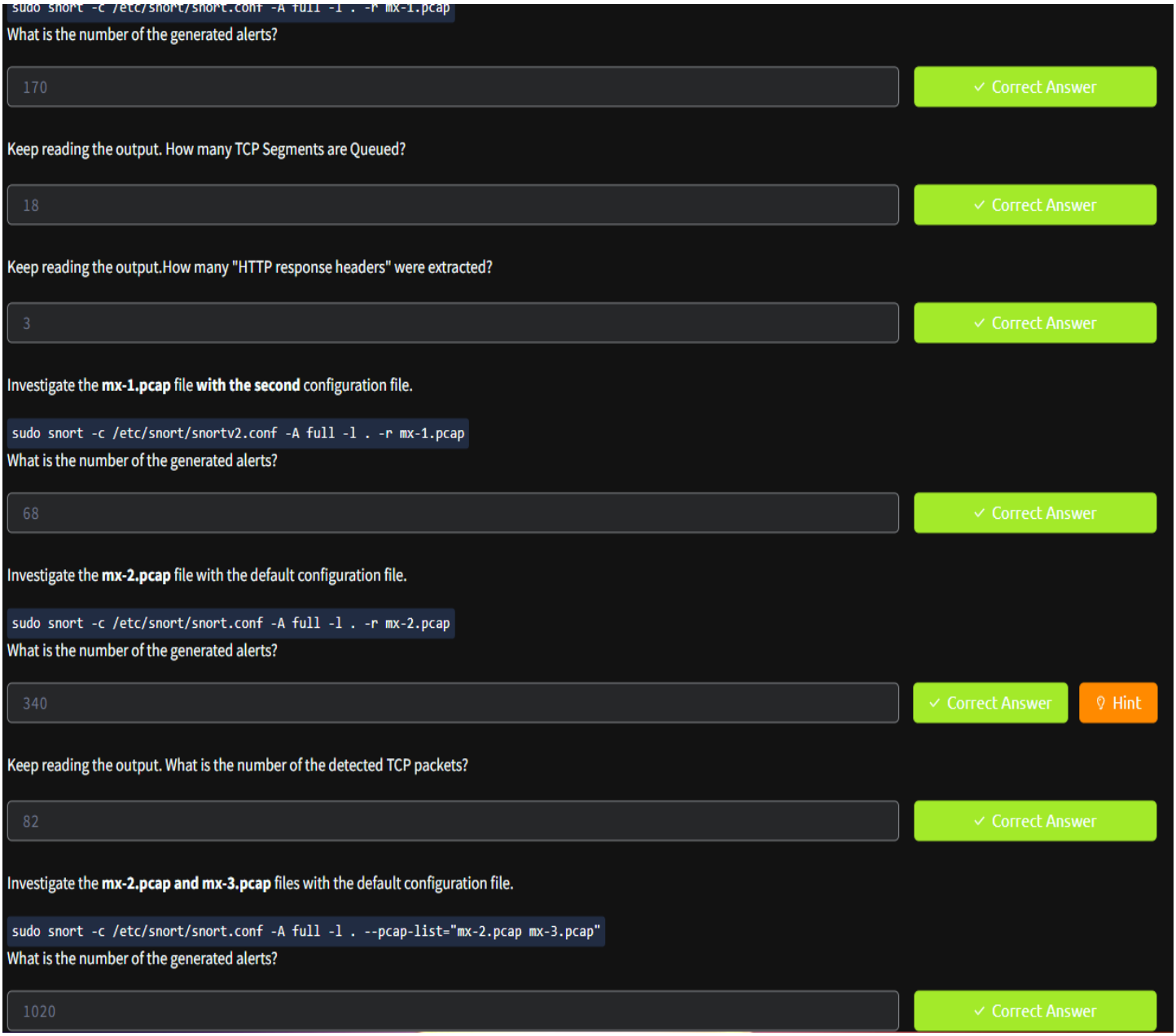
- Example:HTTPGETmethodcount=2fromgenerated traffic.



TASK8–OPERATIONMODE4:PCAPINVESTIGATION

- Use`-r<file.pcap>`toreadPCAPfiles.

- SupportssingleandmultiplePCAPsusing`--pcap-list`and`--pcap-show`.



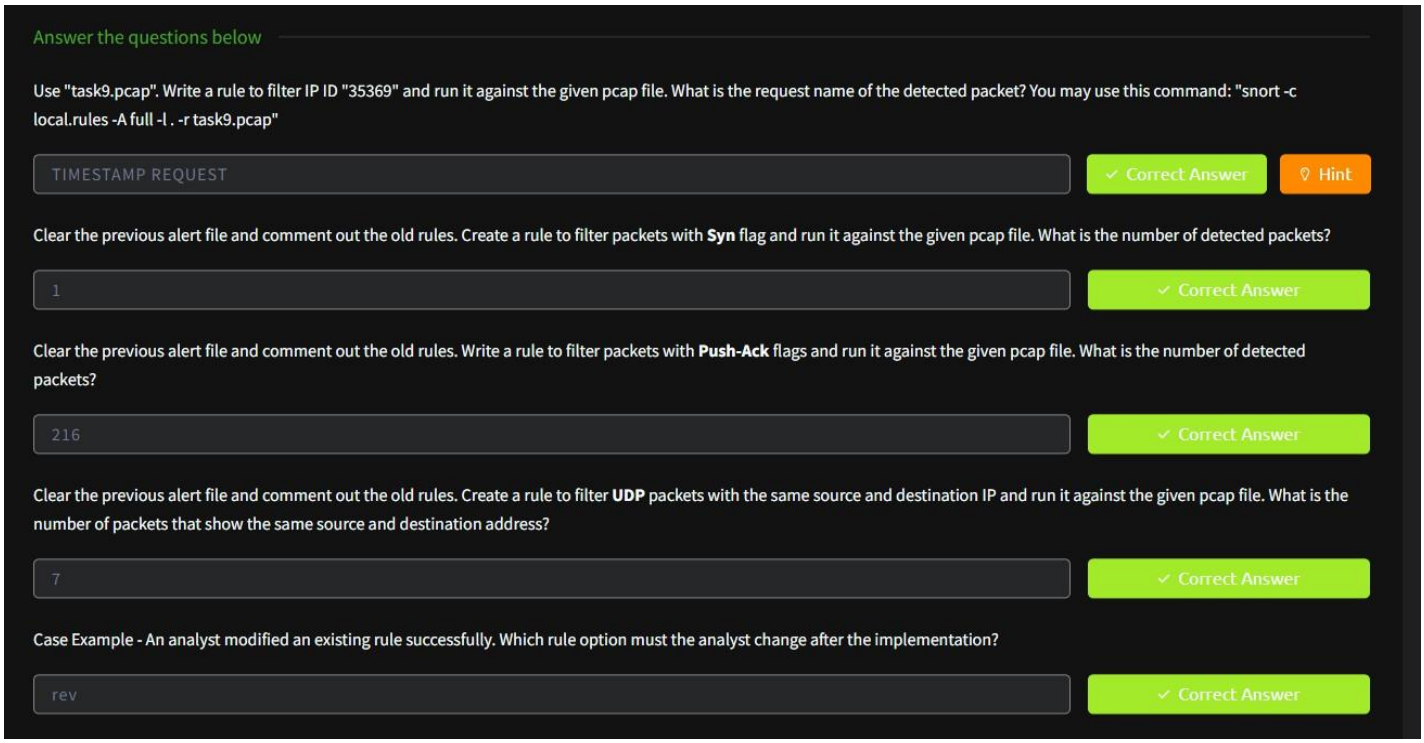
- Investigate`mx-1.pcap`,`mx-2.pcap`,and`mx-3.pcap`foralertstatistics.

- AnalyzeTCPsegments,HTTPheaders,andalertvolumes.

- Snortdetectsalertsbasedonappliedrulesets.

- Enableshistoricaltrafficanalysisviapacketreplay.

TASK9–SNORTRULE STRUCTURE



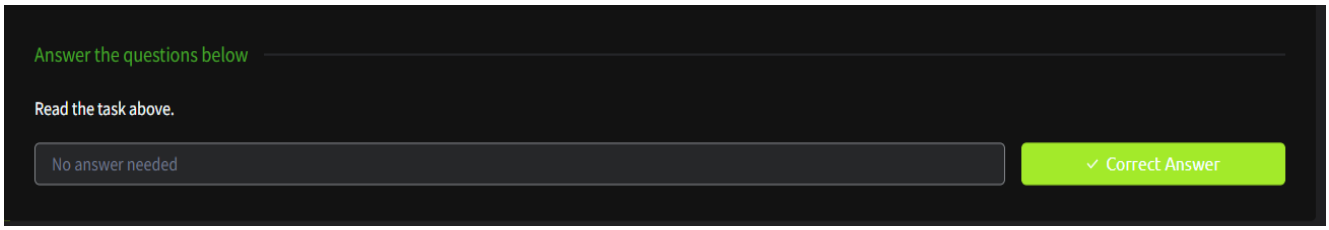
- Rulesinclude:action,protocol,source/destinationIP&port, options.
- Use`msg`,`sid`,`rev`,`reference`ingeneralruleoptions.
- Use`content`,`nocase`,`fast_pattern`inpayloadrules.
- Use`flags`,`id`,`sameip`,`dsize` innon-payload rules.
- Practicerulewritingusing`task9.pcap`and`local.rules`.
- DetectTCPflags,identicalIPs,andpayloadpatternsviacustomrules.

TASK10–SNORT2OPERATIONLOGIC:POINTSTOREMEMBER

- Components:PacketDecoder,Pre-processors,DetectionEngine,Logging,Plugins.
- DAQmodules(afpacket,pcap,nfq)controltrafficacquisition.
- Configurationfile:`snort.conf`,customrules:`local.rules`.
- Rulesets:Community, Registered,and Subscriber.

- Configurationinvolvesenablingvariables,outputplugins,andcustomrulesets.

- Avoiddeletingworkingrules—commentandtest incrementally.



TASK11–CONCLUSION

- Snortprovidesmulti-modethreatdetectionandpreventioncapabilities.

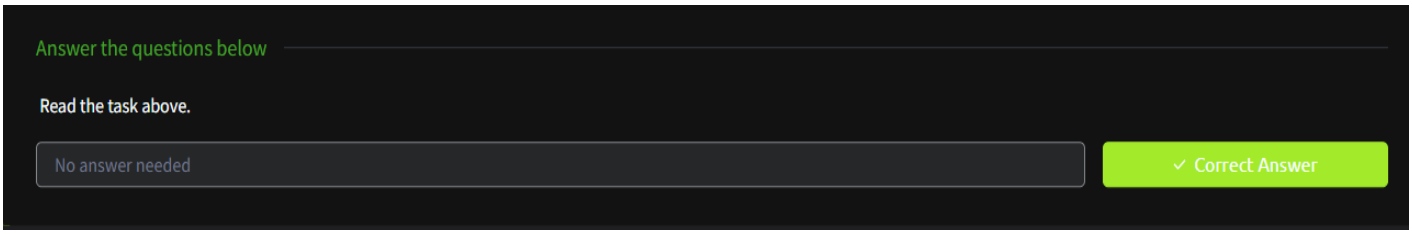
- Learningrulesyntaxisessentialforcreatingcustomdetections.

- Testrulesinlabbeforedeployinginproduction.

- Incrementallyenhancerulestoavoidsyntaxorlogicerrors.

- Maintainbackupsofconfigurationandrulefiles.

- RefertotheSnortChallengeandofficialcheatsheetforcontinuedpractice.



RESULT:

Successfully understood the working of Snort in Sniffer, Logger, IDS, and PCAP modes.Gainedhands-onexperienceinwriting,applying,andtestingdetectionrules using custom traffic and PCAP data. This equips learners with skills necessary for intrusion detection engineering in real-world environments.