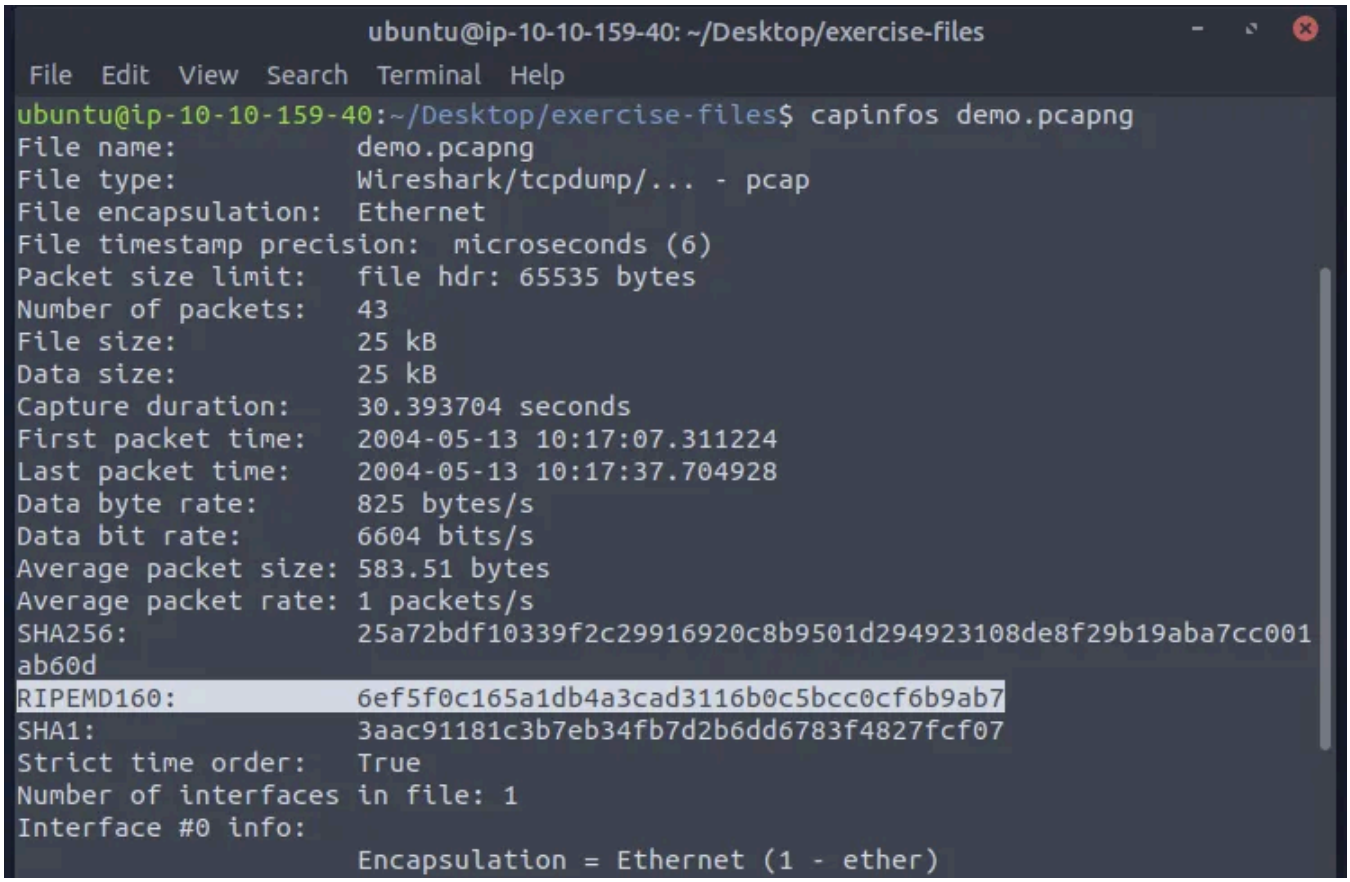
TShark: The Basics | TryHackMe | SOC Level 1

CyberTutes · Follow
4 min read · Aug 1, 2024

Question 1: Find the task files on the Desktop in the “exercise-files” folder.

Answer 1: No answer is needed

Question 2: View the details of the demo.pcapng file with “capinfos”.



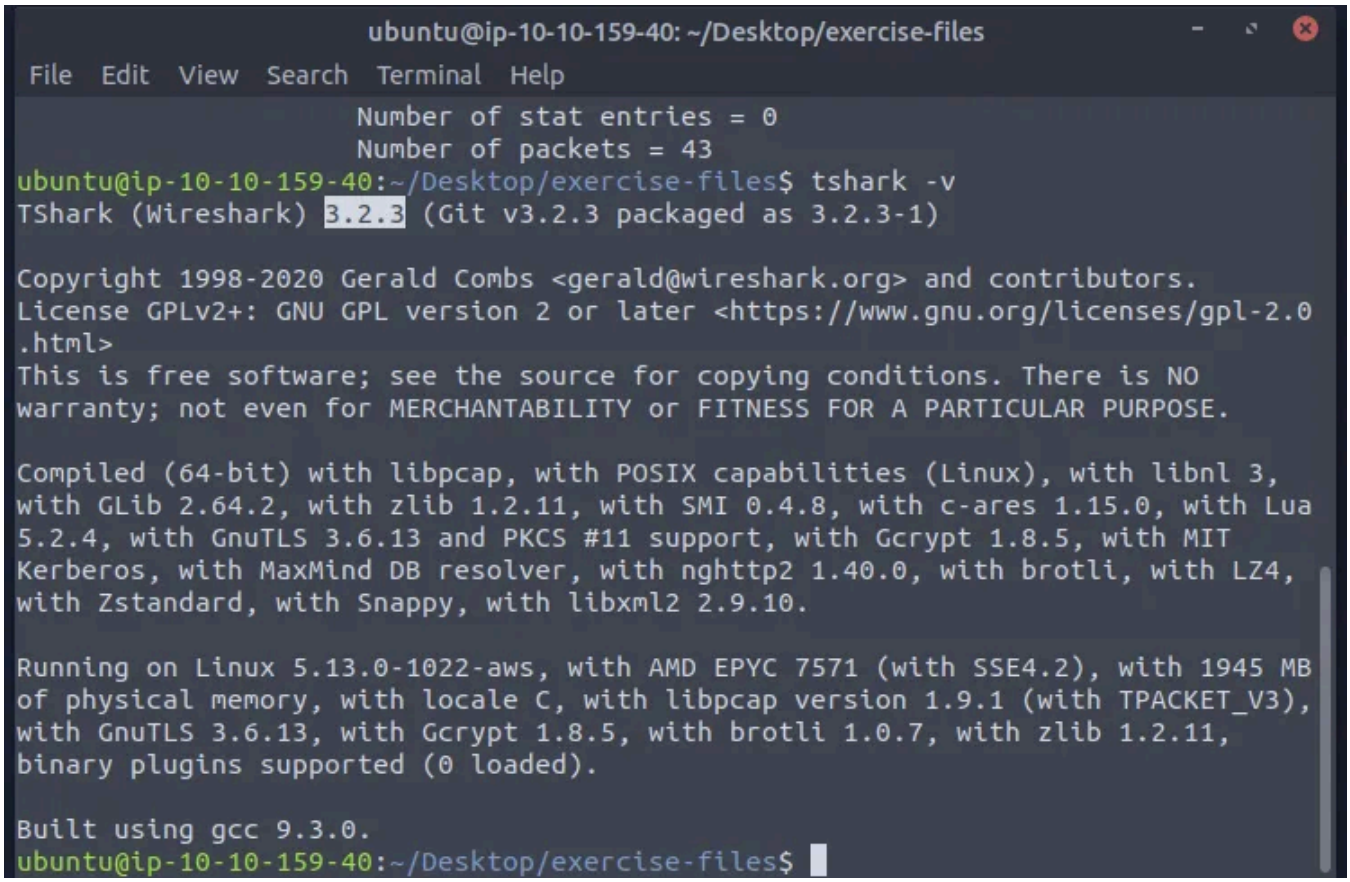
Command:

capinfos demo.pcapng

- What is the “RIPEMD160” value?

Answer 2: 6ef5f0c165a1db4a3cad3116b0c5bcc0cf6b9ab7

Question 3: What is the installed TShark version in the given VM?

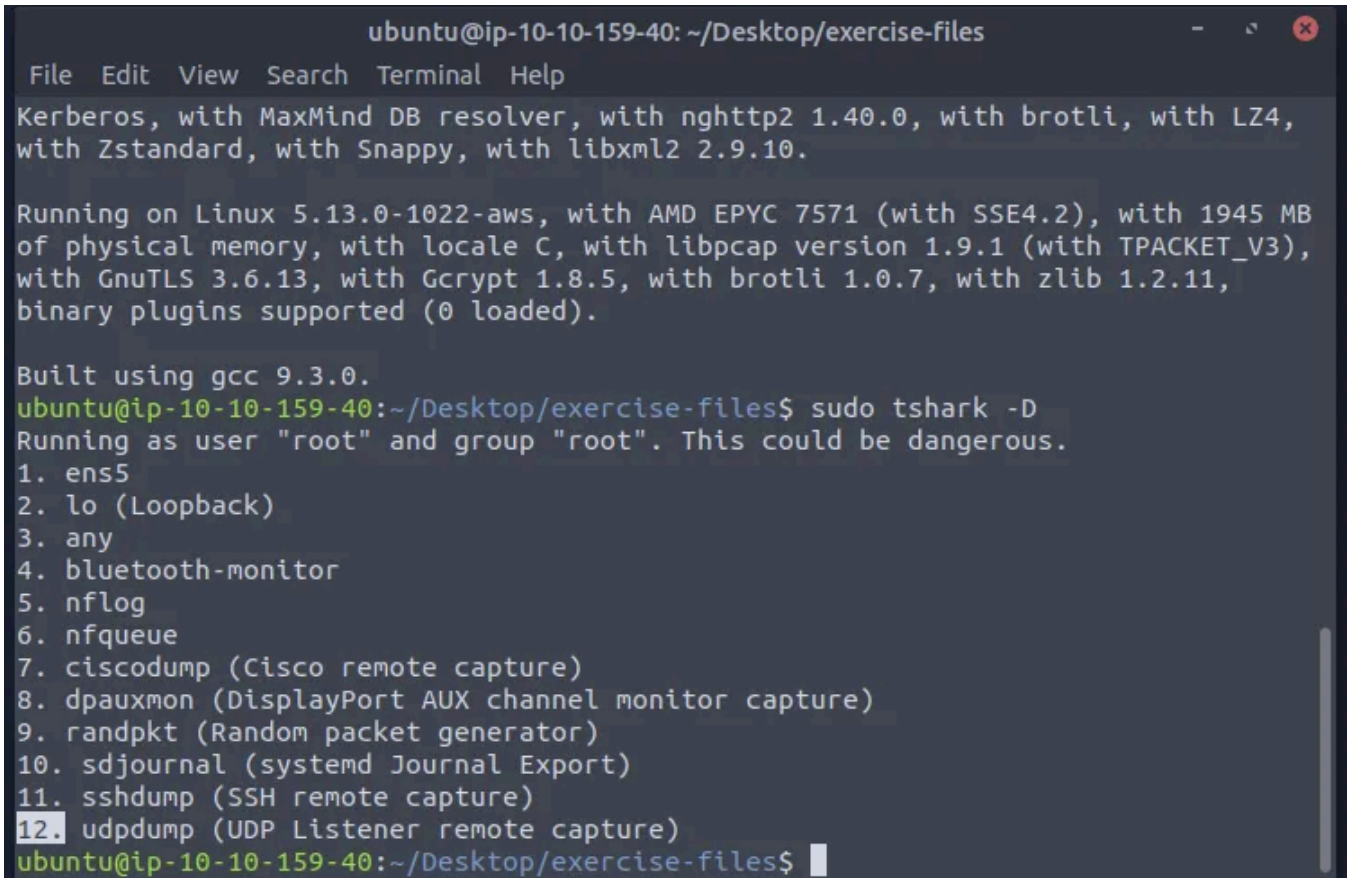


Command:

tshark -v

Answer 3: 3.2.3

Question 4: List the available interfaces with TShark.



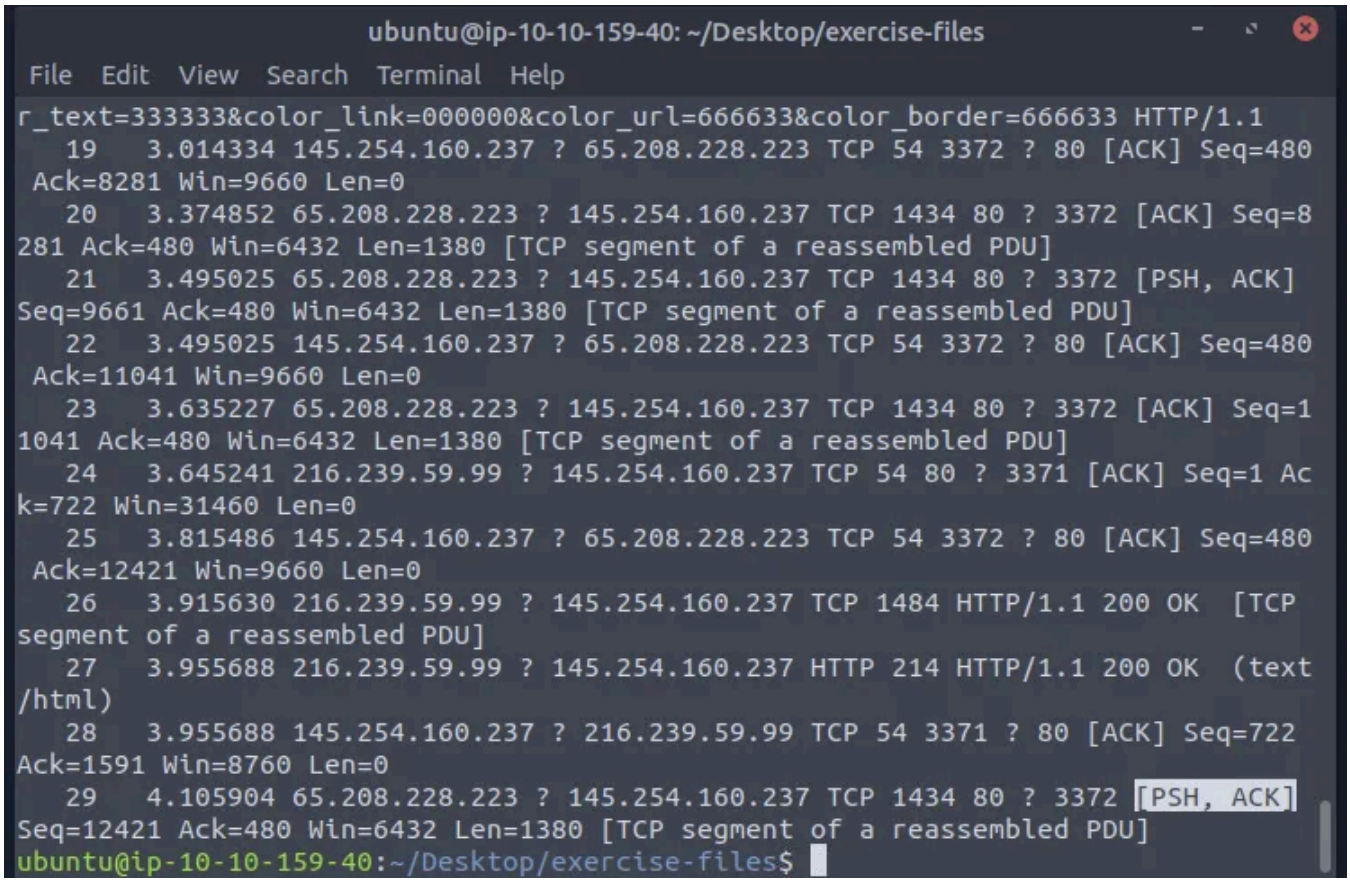
Command:

sudo tshark -D

- What is the number of available interfaces in the given VM?

Answer 4: 12

Question 5: Read the “demo.pcapng” file with TShark.



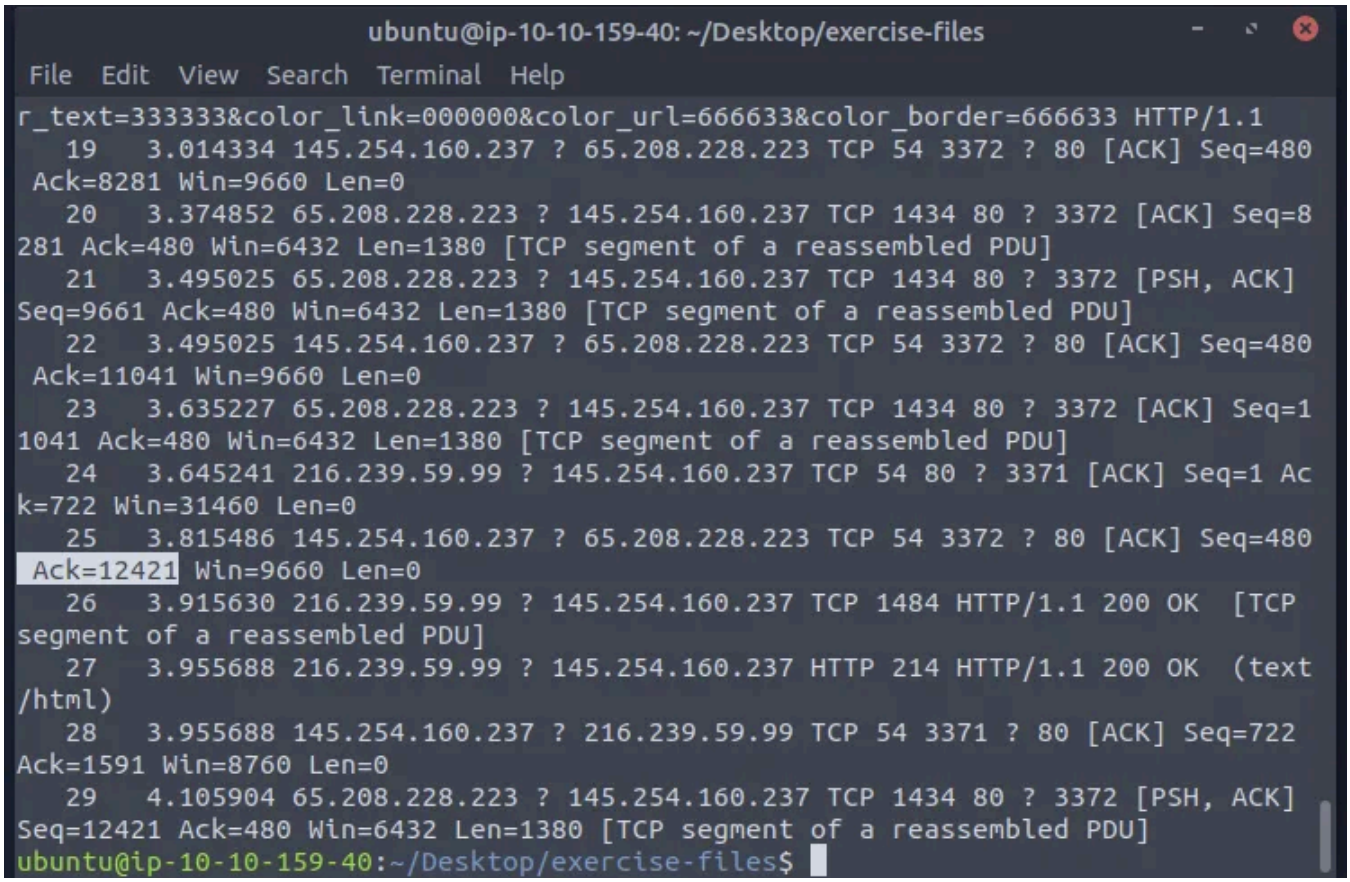
Command:

tshark -r demo.pcapng

- What are the assigned TCP flags in the 29th packet?

Answer 5: PSH, ACK

Question 6: What is the “Ack” value of the 25th packet?

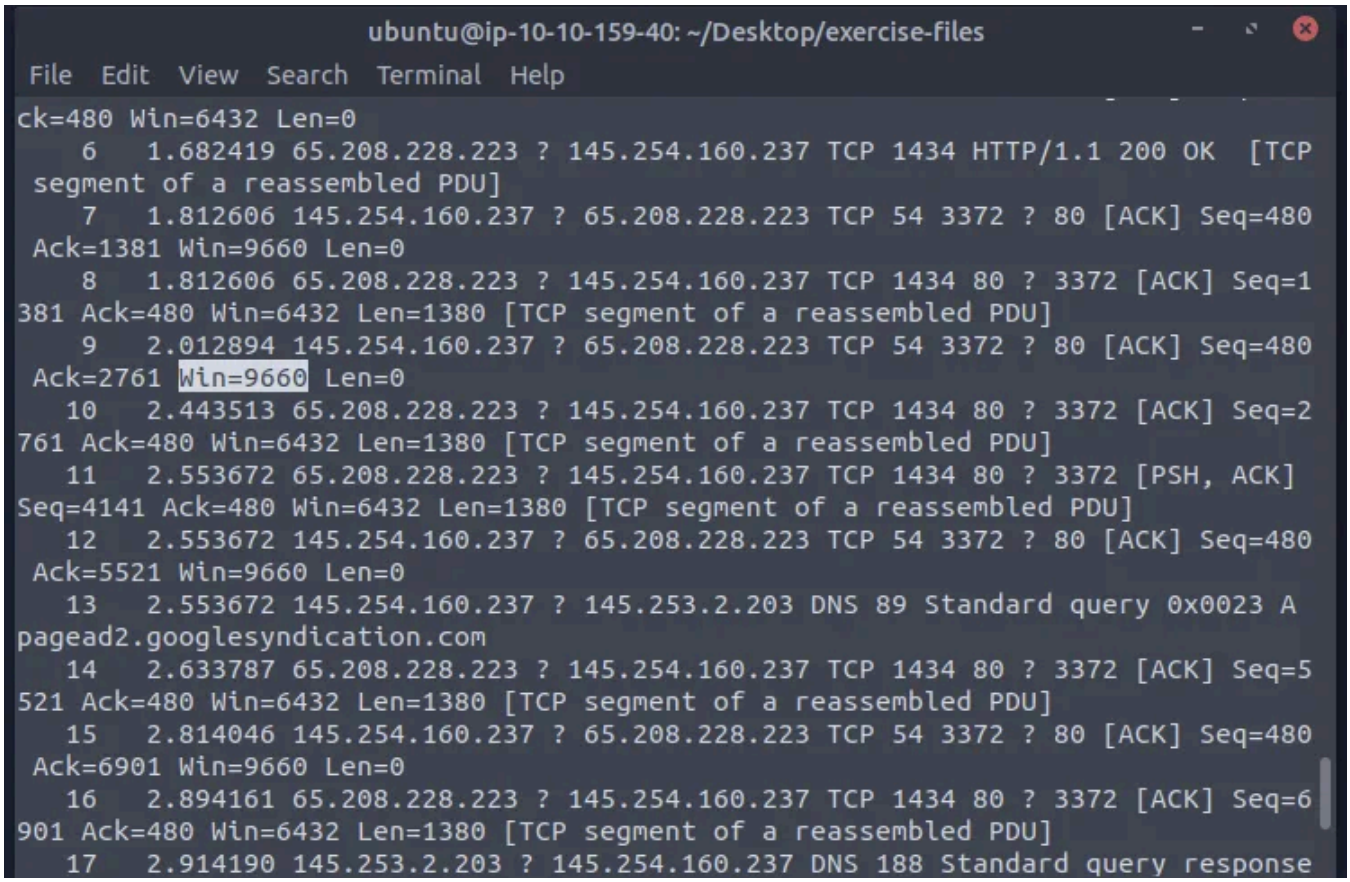


Command:

tshark -r demo.pcapng -T fields -e tcp.ack -Y frame.number==25

Answer 6: 12421

Question 7: What is the “Window size value” of the 9th packet?



Command:

tshark -r demo.pcapng -T fields -e tcp.window_size -Y frame.number==9

Answer 7: 9660

Question 8: Which parameter can help analysts to create a continuous capture dump?

	Ring buffer control options. Define capture conditions for multiple runs/loops. **(INFINITE LOOP)**.

-b	• **Duration:** Sniff the traffic for X seconds, create a new file and write output to it.
	  • `tshark -w test.pcap -b duration:1`
	• **Filesize:** Define the maximum capture file size. Create a new file and write output to it after reaching filesize X (KB).
	  • `tshark -w test.pcap -b filesize:10`
	• **Files:** Define the maximum number of output files. Rewrite the first/oldest file after creating X files.
	  • `tshark -w test.pcap -b filesize:10 -b files:3`

Answer 8: -b

Question 9: Can we combine autostop and ring buffer parameters with TShark? y/n

pcap file and apply the capture condition parameters. The idea is to save the capture files in specific sizes during live capturing. If you need to extract sorts of packets from a specific capture file, you will need to use discussed in the previous task.

Hint: TShark supports combining autostop (`-a`) parameters with ring buffer control parameters (`-b`). parameters according to your needs. Use the infinite loop options carefully; remember, you must use parameter to stop the infinite loop.

Answer 9: y

Question 10: Which parameter is used to set “Capture Filters”?

Parameter	Purpose
-f	Capture filters. Same as BPF syntax and **Wireshark's capture filters.**
-Y	Display filters. Same as **Wireshark's display filters.**

eck out the **Wireshark: Packet Operations** room (Task 4 & 5) if you want to review the principles of packet fil

Answer 10: -f

Question 11: Which parameter is used to set “Display Filters”?

Answer 11: -Y

Run the commands from the above Terminator terminals on the target machine and answer the questions.

Question 12: What is the number of packets with SYN bytes?

```
de:ef ? Broadcast    ARP 42 Who has 10.10.10.10? Tell 10.10.245.51
erver-32_0d:3d:86:b5:2f ? 02:8c:ba:b3:de:ef ARP 42 10.10.10.10 is at 02:2d:3d:86
 ? 10.10.10.10  TCP 74 39506 ? 80 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM
 ? 10.10.245.51 TCP 74 80 ? 39506 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=896
 ? 10.10.10.10  TCP 66 39506 ? 80 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=347217
 ? 10.10.10.10  HTTP 141 GET / HTTP/1.1
 ? 10.10.245.51 TCP 66 80 ? 39506 [ACK] Seq=1 Ack=76 Win=62592 Len=0 TSval=16895
 ? 10.10.245.51 TCP 252 HTTP/1.1 200 OK  [TCP segment of a reassembled PDU]
 ? 10.10.10.10  TCP 66 39506 ? 80 [ACK] Seq=76 Ack=187 Win=62720 Len=0 TSval=347
 ? 10.10.245.51 HTTP 1286 HTTP/1.1 200 OK  (text/html)
```

Command:

tshark -r demo.pcapng -Y “tcp.flags.syn == 1” | wc -l

Answer 12: 2

Question 13: What is the number of packets sent to the IP address “10.10.10.10”?

Command:

tshark -r demo.pcapng -Y “ip.dst == 10.10.10.10” | wc -l

Answer 13: 7

Question 14: What is the number of packets with ACK bytes?

Command:

tshark -r demo.pcapng -Y “tcp.flags.ack == 1” | wc -l

Answer 14: 8

Use the “demo.pcapng” file to answer the questions.

Question 15: What is the number of packets with a “65.208.228.223” IP address?

Command:

tshark -r demo.pcapng -Y “ip.addr == 65.208.228.223” | wc -l

Answer 15: 34

Question 16: What is the number of packets with a “TCP port 3371”?

Command:

tshark -r demo.pcapng -Y “tcp.port == 3371” | wc -l

Answer 16: 7

Question 17: What is the number of packets with a “145.254.160.237” IP address as a source address?

Command:

tshark -r demo.pcapng -Y “ip.src == 145.254.160.237” | wc -l

Answer 17: 20

Rerun the previous query and look at the output.

Question 18: What is the packet number of the “Duplicate” packet?

Command:

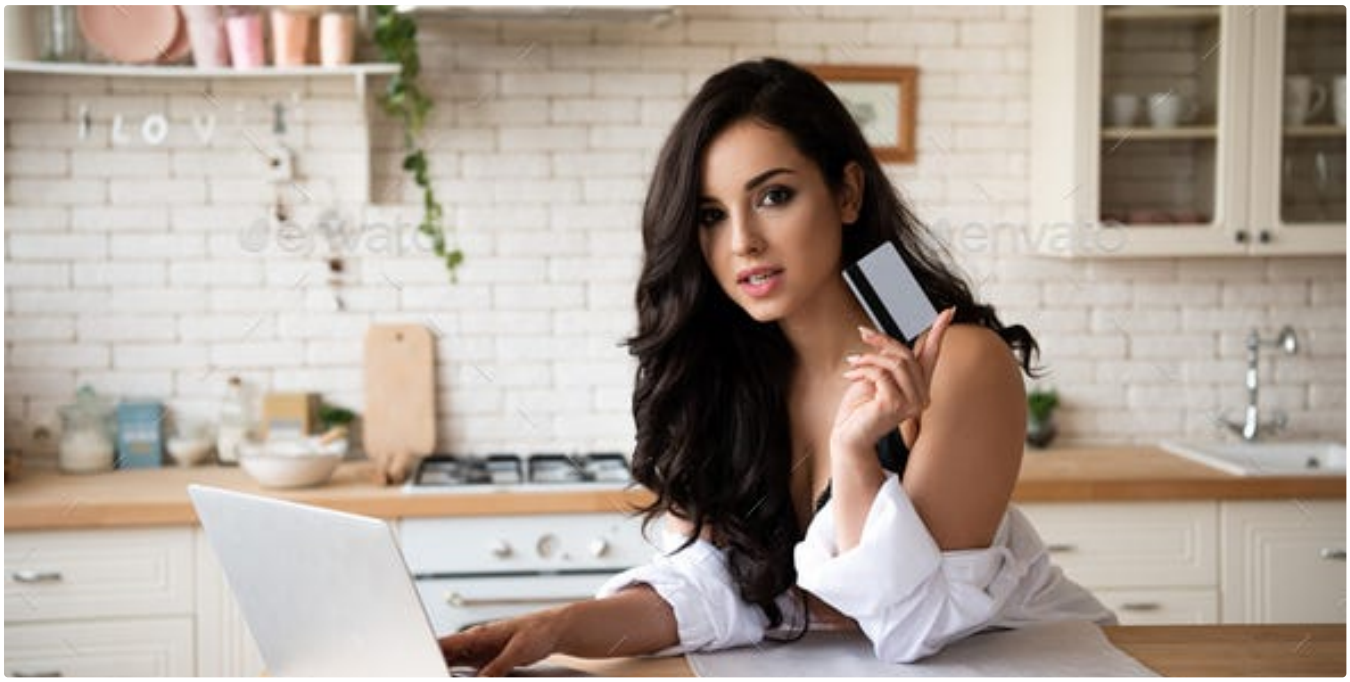
tshark -r demo.pcapng -Y ‘ip.src == 145.254.160.237 and udp.analysis.duplicate’ -T fields -e frame.number

Answer 18: 37

Thank You!

Tryhackme | Tryhackme Walkthrough | Tryhackme Writeup | Cybertutes | Wireshark

More from CyberTutes



CyberTutes

Cybersecurity for Remote Work: A Guide for Ethical Hackers

Greetings, future ethical hackers! If you've mastered the world of cybersecurity and are eager to embrace the remote work lifestyle, you're...

Sep 24, 2023

CyberTutes

AI Magic: Unleashing Cyber Superheroes and the Treasure Hunt of Tomorrow!

Get ready for a digital adventure! Imagine a world where your online stuff needs a superhero to stay safe. That hero is called Artificial...

Aug 27, 2023 1

CyberTutes

Unmasking the Cyber Ninja Moves: Zero-Day Vulnerabilities and Exploits Explained

Hey there, cyber explorers! 🦹 Imagine you're in a secret game of digital hide and seek, and you found a super sneaky way to get into a...

Aug 13, 2023 5

CyberTutes

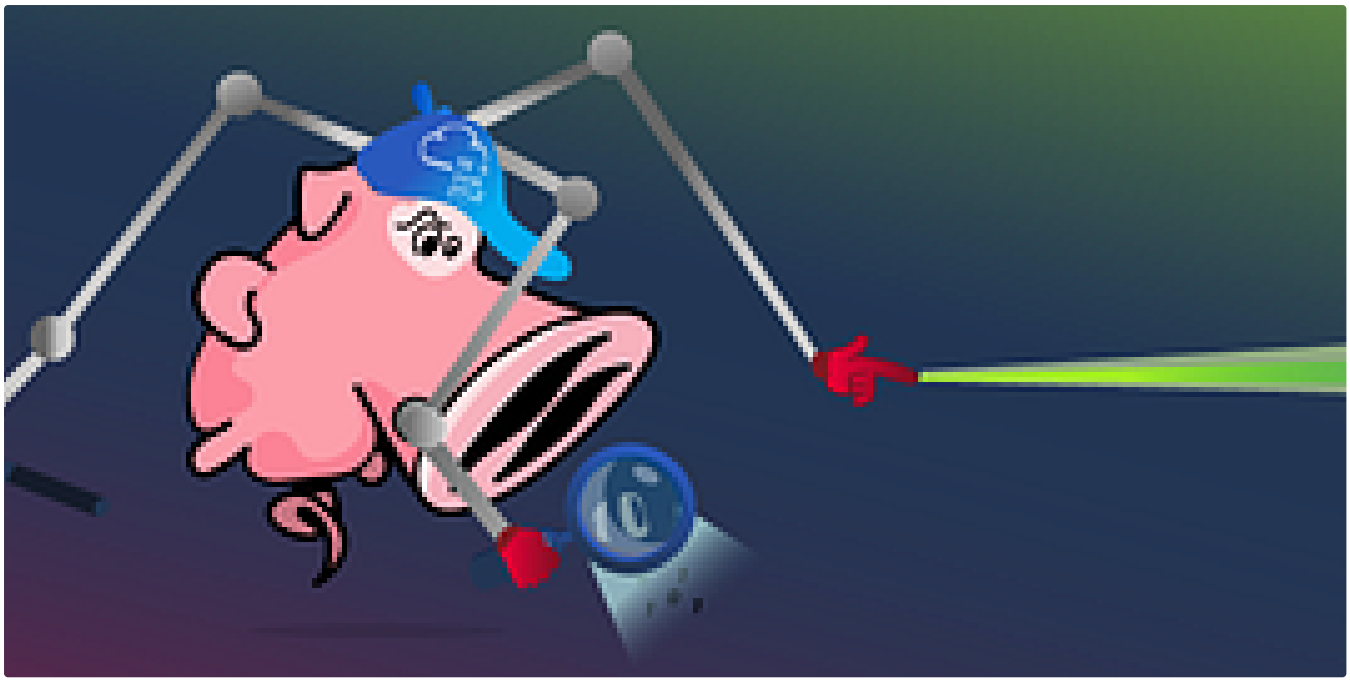
Staying Safe Online: Understanding Cyber Threats Around Us!

Hey there, young cyber enthusiasts! Today, we're going to explore the amazing world of Cyber Threat Landscape. It's like a digital jungle...

Aug 6, 2023 1

See all from CyberTutes

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

rutbar

TryHackMe—Search Skills | Cyber Security 101 (THM)

Evaluation of Search Results

Oct 26, 2024 1

Lists

Staff picks

796 stories · 1560 saves

Stories to Help You Level-Up at Work

19 stories · 912 saves

Self-Improvement 101

20 stories · 3195 saves

Productivity 101

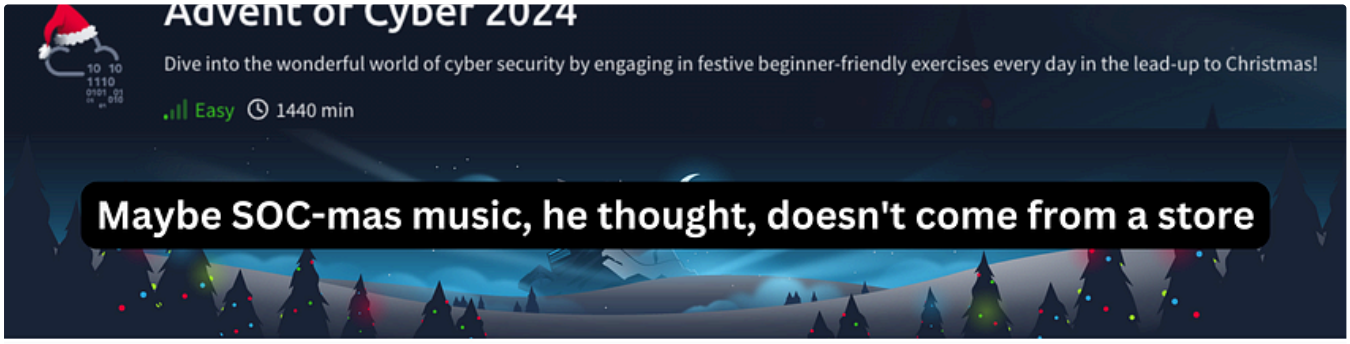
20 stories · 2707 saves

In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

Nov 5, 2024 60



In System Weakness by Karthikeyan Nagaraj

Advent of Cyber 2024 [Day 1] Writeup with Answers | TryHackMe Walkthrough

Maybe SOC-mas music, he thought, doesn't come from a store?

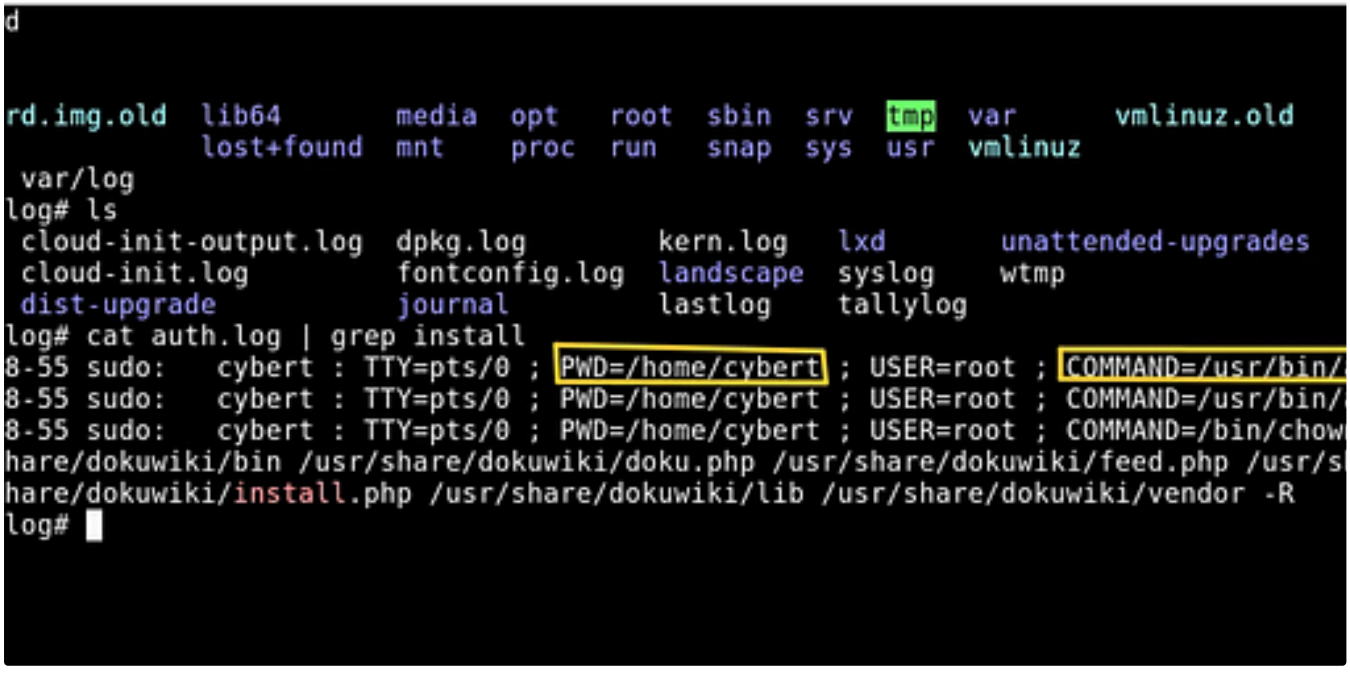
Dec 1, 2024 906 1

In T3CH by Axoloth

TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

Nov 28, 2024 50



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

See more recommendations