

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



# TShark: The Basics | TryHackMe | SOC Level 1



CyberTutes · Follow

4 min read · Aug 1, 2024

Listen

Share

More



**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”.

```
ubuntu@ip-10-10-159-40:~/Desktop/exercise-files$ capinfos demo.pcapng
File name: demo.pcapng
File type: Wireshark/tcpdump/... - pcap
File encapsulation: Ethernet
File timestamp precision: microseconds (6)
Packet size limit: file hdr: 65535 bytes
Number of packets: 43
File size: 25 kB
Data size: 25 kB
Capture duration: 30.393704 seconds
First packet time: 2004-05-13 10:17:07.311224
Last packet time: 2004-05-13 10:17:37.704928
Data byte rate: 825 bytes/s
Data bit rate: 6604 bits/s
Average packet size: 583.51 bytes
Average packet rate: 1 packets/s
SHA256: 25a72bdf10339f2c29916920c8b9501d294923108de8f29b19aba7cc001
ab60d
RIPEMD160: 6ef5f0c165a1db4a3cad3116b0c5bcc0cf6b9ab7
SHA1: 3aac91181c3b7eb34fb7d2b6dd6783f4827fcf07
Strict time order: True
Number of interfaces in file: 1
Interface #0 info:
    Encapsulation = Ethernet (1 - ether)
```

**Command:****capinfos demo.pcapng**

- What is the “RIPEMD160” value?

**Answer 2:** 6ef5f0c165a1db4a3cad3116b0c5bcc0cf6b9ab7**Question 3:** What is the installed TShark version in the given VM?

The screenshot shows a terminal window titled "ubuntu@ip-10-10-159-40: ~/Desktop/exercise-files". The window contains the output of the command "tshark -v". The output includes copyright information from 1998-2020, license details (GPLv2+), and a detailed build configuration for a 64-bit Linux system. It mentions various libraries and protocols used in the build, such as libpcap, GLib, zlib, SMI, c-ares, Lua, GnuTLS, Gcrypt, brotli, LZ4, Zstandard, Snappy, libxml2, and MaxMind DB. The terminal also indicates it was built using gcc 9.3.0.

```
ubuntu@ip-10-10-159-40:~/Desktop/exercise-files
File Edit View Search Terminal Help
Number of stat entries = 0
Number of packets = 43
ubuntu@ip-10-10-159-40:~/Desktop/exercise-files$ tshark -v
TShark (Wireshark) 3.2.3 (Git v3.2.3 packaged as 3.2.3-1)

Copyright 1998-2020 Gerald Combs <gerald@wireshark.org> and contributors.
License GPLv2+: GNU GPL version 2 or later <https://www.gnu.org/licenses/gpl-2.0.html>
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Compiled (64-bit) with libpcap, with POSIX capabilities (Linux), with libnl 3,
with GLib 2.64.2, with zlib 1.2.11, with SMI 0.4.8, with c-ares 1.15.0, with Lua
5.2.4, with GnuTLS 3.6.13 and PKCS #11 support, with Gcrypt 1.8.5, with MIT
Kerberos, with MaxMind DB resolver, with nghttp2 1.40.0, with brotli, with LZ4,
with Zstandard, with Snappy, with libxml2 2.9.10.

Running on Linux 5.13.0-1022-aws, with AMD EPYC 7571 (with SSE4.2), with 1945 MB
of physical memory, with locale C, with libpcap version 1.9.1 (with TPACKET_V3),
with GnuTLS 3.6.13, with Gcrypt 1.8.5, with brotli 1.0.7, with zlib 1.2.11,
binary plugins supported (0 loaded).

Built using gcc 9.3.0.
ubuntu@ip-10-10-159-40:~/Desktop/exercise-files$
```

**Command:****tshark -v****Answer 3:** 3.2.3**Question 4:** List the available interfaces with TShark.

The screenshot shows a terminal window titled "ubuntu@ip-10-10-159-40: ~/Desktop/exercise-files". The window contains the following text:

```
Kerberos, with MaxMind DB resolver, with nghttp2 1.40.0, with brotli, with LZ4,  
with Zstandard, with Snappy, with libxml2 2.9.10.  
  
Running on Linux 5.13.0-1022-aws, with AMD EPYC 7571 (with SSE4.2), with 1945 MB  
of physical memory, with locale C, with libpcap version 1.9.1 (with TPACKET_V3),  
with GnuTLS 3.6.13, with Gcrypt 1.8.5, with brotli 1.0.7, with zlib 1.2.11,  
binary plugins supported (0 loaded).  
  
Built using gcc 9.3.0.  
ubuntu@ip-10-10-159-40:~/Desktop/exercise-files$ sudo tshark -D  
Running as user "root" and group "root". This could be dangerous.  
1. ens5  
2. lo (Loopback)  
3. any  
4. bluetooth-monitor  
5. nflog  
6. nfqueue  
7. ciscodump (Cisco remote capture)  
8. dpauxmon (DisplayPort AUX channel monitor capture)  
9. randpkt (Random packet generator)  
10. sdjournal (systemd Journal Export)  
11. sshdump (SSH remote capture)  
12. udptdump (UDP Listener remote capture)
```

**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.

The screenshot shows a terminal window titled "ubuntu@ip-10-10-159-40: ~/Desktop/exercise-files". The window displays a list of network packets. The first few lines of the output are:

```
r_text=333333&color_link=000000&color_url=666633&color_border=666633 HTTP/1.1
19 3.014334 145.254.160.237 ? 65.208.228.223 TCP 54 3372 ? 80 [ACK] Seq=480
Ack=8281 Win=9660 Len=0
20 3.374852 65.208.228.223 ? 145.254.160.237 TCP 1434 80 ? 3372 [ACK] Seq=8
281 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
21 3.495025 65.208.228.223 ? 145.254.160.237 TCP 1434 80 ? 3372 [PSH, ACK]
Seq=9661 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
22 3.495025 145.254.160.237 ? 65.208.228.223 TCP 54 3372 ? 80 [ACK] Seq=480
Ack=11041 Win=9660 Len=0
23 3.635227 65.208.228.223 ? 145.254.160.237 TCP 1434 80 ? 3372 [ACK] Seq=1
1041 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
24 3.645241 216.239.59.99 ? 145.254.160.237 TCP 54 80 ? 3371 [ACK] Seq=1 Ac
k=722 Win=31460 Len=0
25 3.815486 145.254.160.237 ? 65.208.228.223 TCP 54 3372 ? 80 [ACK] Seq=480
Ack=12421 Win=9660 Len=0
26 3.915630 216.239.59.99 ? 145.254.160.237 TCP 1484 HTTP/1.1 200 OK [TCP
segment of a reassembled PDU]
27 3.955688 216.239.59.99 ? 145.254.160.237 HTTP 214 HTTP/1.1 200 OK (text
/html)
28 3.955688 145.254.160.237 ? 216.239.59.99 TCP 54 3371 ? 80 [ACK] Seq=722
Ack=1591 Win=8760 Len=0
29 4.105904 65.208.228.223 ? 145.254.160.237 TCP 1434 80 ? 3372 [PSH, ACK]
Seq=12421 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
```

At the bottom of the terminal window, the prompt "ubuntu@ip-10-10-159-40: ~/Desktop/exercise-files\$ " is visible.

**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?

The screenshot shows a terminal window titled "ubuntu@ip-10-10-159-40: ~/Desktop/exercise-files". The window displays a network capture of a TCP session. The session consists of several ACK and PSH, ACK frames. The 9th packet is highlighted in green, indicating it is the answer to the question. The packet details are as follows:

- Packet 9: r\_text=333333&color\_link=000000&color\_url=666633&color\_border=666633 HTTP/1.1
- Sequence Number: Seq=480
- Acknowledgment Number: Ack=8281
- Window Size: Win=9660
- Length: Len=0

Subsequent packets (10-29) show the continuation of the session with various ACK and PSH, ACK frames. The last packet (29) is also highlighted in green.

```
r_text=333333&color_link=000000&color_url=666633&color_border=666633 HTTP/1.1
 19  3.014334 145.254.160.237 ? 65.208.228.223 TCP 54 3372 ? 80 [ACK] Seq=480
Ack=8281 Win=9660 Len=0
 20  3.374852 65.208.228.223 ? 145.254.160.237 TCP 1434 80 ? 3372 [ACK] Seq=8
281 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
 21  3.495025 65.208.228.223 ? 145.254.160.237 TCP 1434 80 ? 3372 [PSH, ACK]
Seq=9661 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
 22  3.495025 145.254.160.237 ? 65.208.228.223 TCP 54 3372 ? 80 [ACK] Seq=480
Ack=11041 Win=9660 Len=0
 23  3.635227 65.208.228.223 ? 145.254.160.237 TCP 1434 80 ? 3372 [ACK] Seq=1
1041 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
 24  3.645241 216.239.59.99 ? 145.254.160.237 TCP 54 80 ? 3371 [ACK] Seq=1 Ac
k=722 Win=31460 Len=0
 25  3.815486 145.254.160.237 ? 65.208.228.223 TCP 54 3372 ? 80 [ACK] Seq=480
Ack=12421 Win=9660 Len=0
 26  3.915630 216.239.59.99 ? 145.254.160.237 TCP 1484 HTTP/1.1 200 OK [TCP
segment of a reassembled PDU]
 27  3.955688 216.239.59.99 ? 145.254.160.237 HTTP 214 HTTP/1.1 200 OK (text
/html)
 28  3.955688 145.254.160.237 ? 216.239.59.99 TCP 54 3371 ? 80 [ACK] Seq=722
Ack=1591 Win=8760 Len=0
 29  4.105904 65.208.228.223 ? 145.254.160.237 TCP 1434 80 ? 3372 [PSH, ACK]
Seq=12421 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
```

ubuntu@ip-10-10-159-40:~/Desktop/exercise-files\$

**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?

```

ubuntu@ip-10-10-159-40: ~/Desktop/exercise-files
File Edit View Search Terminal Help
ck=480 Win=6432 Len=0
 6  1.682419 65.208.228.223 ? 145.254.160.237 TCP 1434 HTTP/1.1 200 OK [TCP
segment of a reassembled PDU]
 7  1.812606 145.254.160.237 ? 65.208.228.223 TCP 54 3372 ? 80 [ACK] Seq=480
Ack=1381 Win=9660 Len=0
 8  1.812606 65.208.228.223 ? 145.254.160.237 TCP 1434 80 ? 3372 [ACK] Seq=1
381 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
 9  2.012894 145.254.160.237 ? 65.208.228.223 TCP 54 3372 ? 80 [ACK] Seq=480
Ack=2761 Win=9660 Len=0
 10  2.443513 65.208.228.223 ? 145.254.160.237 TCP 1434 80 ? 3372 [ACK] Seq=2
761 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
 11  2.553672 65.208.228.223 ? 145.254.160.237 TCP 1434 80 ? 3372 [PSH, ACK]
Seq=4141 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
 12  2.553672 145.254.160.237 ? 65.208.228.223 TCP 54 3372 ? 80 [ACK] Seq=480
Ack=5521 Win=9660 Len=0
 13  2.553672 145.254.160.237 ? 145.253.2.203 DNS 89 Standard query 0x0023 A
pagead2.googlesyndication.com
 14  2.633787 65.208.228.223 ? 145.254.160.237 TCP 1434 80 ? 3372 [ACK] Seq=5
521 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
 15  2.814046 145.254.160.237 ? 65.208.228.223 TCP 54 3372 ? 80 [ACK] Seq=480
Ack=6901 Win=9660 Len=0
 16  2.894161 65.208.228.223 ? 145.254.160.237 TCP 1434 80 ? 3372 [ACK] Seq=6
901 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
 17  2.914190 145.253.2.203 ? 145.254.160.237 DNS 188 Standard query response

```

### 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
<code>-f</code>	Capture filters. Same as BPF syntax and <b>Wireshark's capture filters</b> .
<code>-Y</code>	Display filters. Same as <b>Wireshark's display filters</b> .

Check 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=8961
? 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=347217
? 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](#)[Follow](#)

## Written by CyberTutes

14 Followers · 2 Following

[Open in app ↗](#)

# Medium

[Search](#)

## No responses yet



What are your thoughts?

[Respond](#)

## 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



...





## 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



...



## 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...

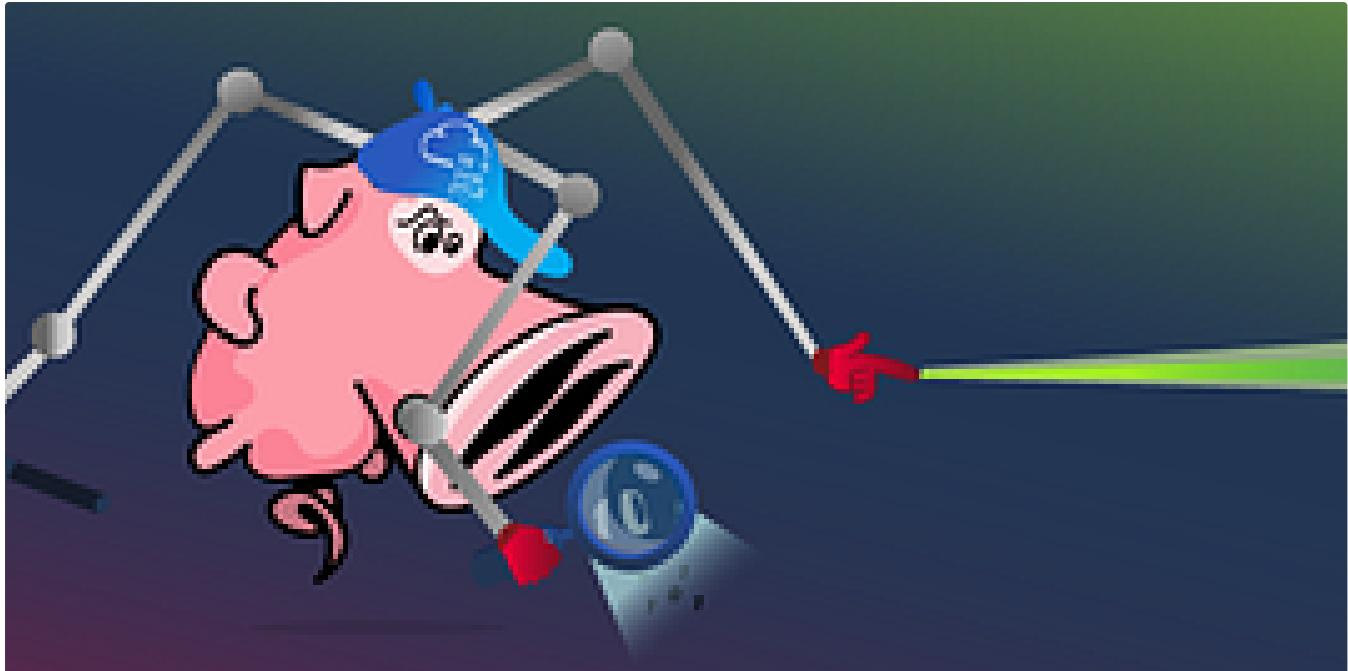
Aug 6, 2023 1



...

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



**Advent of Cyber 2024**



Dive into the wonderful world of cyber security by engaging in festive beginner-friendly exercises every day in the lead-up to Christmas!

Easy 1440 min

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



**Day 1  
Answers**

[cyberw1ng.medium.com](https://cyberw1ng.medium.com)

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



```
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



...

See more recommendations