

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



TryHackMe NetworkMiner Write-Up



Toumo · [Follow](#)

7 min read · Jul 5, 2023



Listen



Share

... More



Image from tryhackme.com

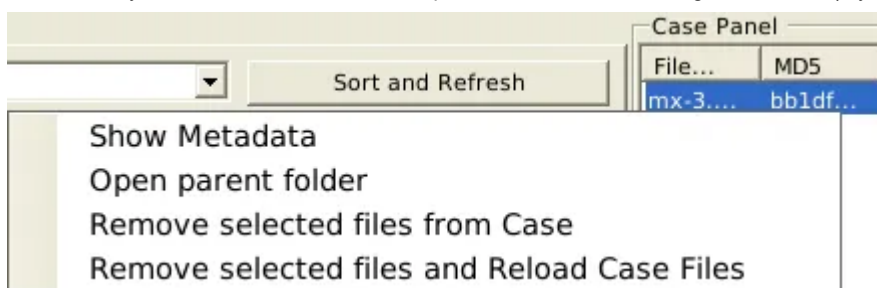
This time, we will be using a new tool called NetworkMiner. My assumption is that we're being exposed to many tools as we do not know what tool we may be using in the future. Not only that, there could be some tools that are more efficient for certain things than others. As always, I'll try my best to solve each question without external help, but if I do, I'll document it! As for the answers, I'll still write it but I'll stop after we are done with the Network Security and Traffic Analysis module. Let's get started!

Task 4 Tool Overview 1

1: Use **mx-3.pcap** What is the total number of frames?

I had to look at external sources for this one. I wasn't sure where frames were displayed. We have to check the metadata to get this information. I completely forgot that I read this section.

To get the metadata, go right click the file in the "Case Panel" section to the right. Select "Show Metadata." A new window should appear. Drag the columns a bit so you can see clearly what is being displayed.

A screenshot of the 'Metadata' window in the NetworkMiner application. The window has a blue title bar and a table with two columns: 'Name' and 'Value'. The table contains the following data:

Name	Value
Data Link	WTAP_ENCAP_ETHERNET
End	12/12/2021 20:14:17
Endianness	Little Endian
Filename	mx-3.pcap
Frames	460
MD5	bb1df7cb425b1e0c2c8317...
Parsing Time	00:00:00.1804060
Start	05/13/2004 10:17:07

Answer: 460

2: How many IP addresses use the same MAC address with host 145.253.2.203?

Look for the IP address under “Host” tab. Then expand the menu. Expand the “MAC” menu and count number of times it says “same MAC address.”

Answer: 2

3: How many packets were sent from host 65.208.228.223?

Look for the IP address under “Host.” Expand that menu and look for packets sent.

Answer: 72

4: What is the name of the webserver banner under host 65.208.228.223?

Go to the IP address under “Host” and expand the menu. This time, we are going to look at Host details. Expand that too and the server banner is there.

Answer: Apache

5: Use mx-4.pcap What is the extracted username?

Open mx-4.pcap using NetworkMiner. Head over to the “Credentials” tab. From there, right click the first packet, right click, and select “Copy Username.” Paste it onto the answer section.

Answer: #B\Administrator

6: What is the extracted password?

Do the same for the password now. As it's very long, I won't be posting the answer.

Task 5 Tool Overview 2

1: Use mx-7 pcap What is the name of the Linux distro mentioned in the file associated with frame 63075?

I loaded mx-7.pcap file and went to the “files” tab. From there, I scrolled to frame 63075, right clicked it, and opened file. There are three .txt files. I opened one of them and tried looking for any keywords that showed any Linux distributions, and there were!

File Tools Help

Hosts (100) Files (2852) Images (288) Messages Credentials (8) Sessions (5020) DNS (17180) Parameters (72526) Ke

Filter keyword:

Frame nr.	Filename	Extension	Size	Source host
62774	thawte Primary Root CA[323].cer	cer	1 060 B	217.72.201.130 [3c-bs.gmx.com]
62812	navigator-bs.gmx.com[153].cer	cer	1 221 B	212.227.111.53 [navigator-bs.gmx.com]
62812	thawte SSL CA - G2[153].cer	cer	1 206 B	212.227.111.53 [navigator-bs.gmx.com]
62812	thawte Primary Root CA[153].cer	cer	1 060 B	212.227.111.53 [navigator-bs.gmx.com]
62820	navigator-bs.gmx.com[154].cer	cer	1 221 B	212.227.111.53 [navigator-bs.gmx.com]
62820	thawte SSL CA - G2[154].cer	cer	1 206 B	212.227.111.53 [navigator-bs.gmx.com]
62820	thawte Primary Root CA[154].cer	cer	1 060 B	212.227.111.53 [navigator-bs.gmx.com]
62886	xhr.2790314313063[1].js	js	989 B	54.187.109.244 [tomshardware.co.uk] [www.t
62914	3c-bs.gmx.com[324].cer	cer	1 207 B	217.72.201.130 [3c-bs.gmx.com]
62914	thawte SSL CA - G2[324].cer	cer	1 206 B	217.72.201.130 [3c-bs.gmx.com]
62914	thawte Primary Root CA[324].cer	cer	1 060 B	217.72.201.130 [3c-bs.gmx.com]
62992	ads.bmp.428AF4A0.bmp	bmp	126 B	80.239.178.178 [a51.dscg10.akamai.net] [a49
62995	cnvideo.91CC0FF9[16].js	js	0 B	80.239.178.200 [a72.dscg10.akamai.net] [a70
63055	index.330B74CB.txt	txt	542 B	108.61.16.227 [mirrorlist.centos.org]
63065	index.5C8E6F3B.txt	txt	582 B	108.61.16.227 [mirrorlist.centos.org]
63075	index.EE08FE3A.txt	txt	588 B	108.61.16.227 [mirrorlist.centos.org]
63159	3c-bs.gmx.com[325].cer	cer	1 207 B	217.72.201.130 [3c-bs.gmx.com]
63159	thawte SSL CA - G2[325].cer	cer	1 206 B	217.72.201.130 [3c-bs.gmx.com]
63159	thawte Primary Root CA[325].cer	cer	1 060 B	217.72.201.130 [3c-bs.gmx.com]
63191	xhr.130812614025195.js	js	989 B	54.187.109.244 [tomshardware.co.uk] [www.t
63251	ads.bmp.4AAC7AE4.bmp	bmp	126 B	80.239.178.178 [a51.dscg10.akamai.net] [a49
63351	navigator-bs.gmx.com[155].cer	cer	1 221 B	212.227.111.53 [navigator-bs.gmx.com]
63351	thawte SSL CA - G2[155].cer	cer	1 206 B	212.227.111.53 [navigator-bs.gmx.com]
63351	thawte Primary Root CA[155].cer	cer	1 060 B	212.227.111.53 [navigator-bs.gmx.com]
63394	3c-bs.gmx.com[326].cer	cer	1 207 B	217.72.201.130 [3c-bs.gmx.com]
63394	thawte SSL CA - G2[326].cer	cer	1 206 B	217.72.201.130 [3c-bs.gmx.com]

Open file

Open folder

Copy path to clipboard

File details

Auto-resize all columns

OSINT hash lookup isn't available in the free version

Sample submission isn't available in the free version

Answer: CentOS

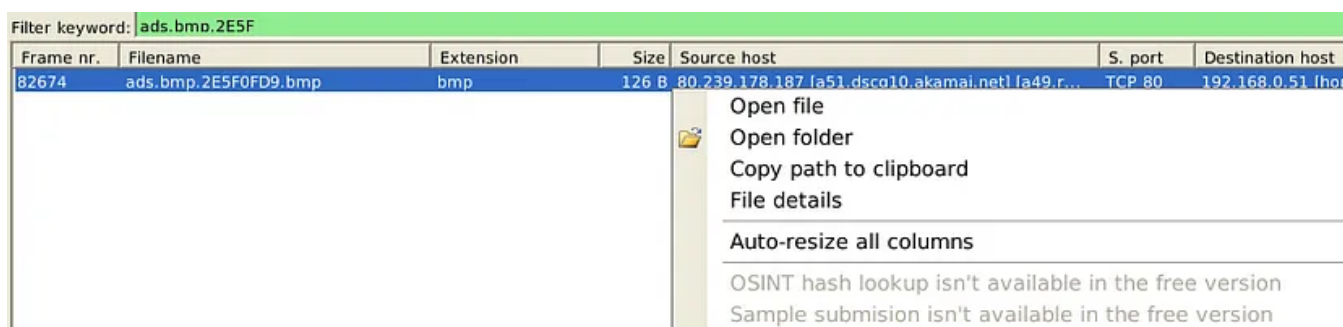
2: What is the header of the page associated with frame 75942?

This time, we will do the same thing but to frame 75942. After you open the file, open the index.html file. The answer is at the top.

Answer: Password-Ned AB

3: What is the source address of the image “ads.bmp.2E5F0FD9.bmp”?

We will be utilizing the search bar. Type the image name in the filter keyword section. Right click the file, and click on file details to see hash values, source address, and more.



The screenshot shows the NetworkMiner interface with a filter keyword of 'ads.bmp.2E5F'. A table lists search results, and a context menu is open over the first result.

Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host
82674	ads.bmp.2E5F0FD9.bmp	bmp	126 B	80.239.178.187 [a51.dsc010.akamai.net] [a49.r...	TCP 80	192.168.0.51 [hon

- Open file
- Open folder
- Copy path to clipboard
- File details
- Auto-resize all columns
- OSINT hash lookup isn't available in the free version
- Sample submission isn't available in the free version

Answer: 80.239.178.187

4: What is the frame number of the possible TLS anomaly?

Head over to the “Anomalies” tab. I entered the first frame out of two frames shown and it worked. I’m not sure if both answers would suffice however.

Answer: 36255

5: Use **mx-9 file** Look at the messages. Which platform sent a password reset email?

We will check out the “Messages” tab and look for anything that might seem like a password related message.

Answer: Facebook

6: What is the email address of Branson Matheson?

On the same screen, we will look for any emails from or to Branson Matheson.

Answer: branson@sandsite.org

Task 6 Version Differences

All the questions here are within the text.

1: Which version can detect duplicate MAC addresses?

Answer: 2.7

2: Which version can handle frames?

Answer: 1.6

3: Which version can provide more details on packet details?

Answer: 1.6

Task 7 Exercises

1: Use **case1.pcap** What is the OS name of the host 131.151.37.122?

I started with the “Hosts” tab and looked for the IP address. Expand that and look for “OS.” I tried out both answers before I looked at the asterisk hint.

Answer: Windows — Windows NT 4

2: Investigate the hosts 131.151.37.122 and 131.151.32.91.

How many data bytes were received from host 131.151.32.91 to host 131.151.37.122 through port 1065?

We are going to expand the “Incoming sessions” menu. There are two incoming sessions but only one that uses port 1065. We will expand the one that uses port 1065.

Answer: 192

3: Investigate the hosts 131.151.37.122 and 131.151.32.21.

How many data bytes were received from host 131.151.37.122 to host 131.151.32.21 through port 143?

We are going to look at the other session that used port 143. Expand that one to get the answer.

Answer: 20769

4: What is the sequence number of frame 9?

The reading did mention that the older version of NetworkMiner has more information regarding frames. I used the older version and opened case1.pcap. I then head over to the “Frames” tab, looked for Frame 9, then expanded the TCP section.

Answer: 2AD77400

5: What is the number of the detected “content types”?

I went back to the newer version and looked at the “Parameters” tab. From there, I clicked on the “Parameter name” column so it will arrange itself in alphabetical order. Then I counted each unique “Parameter value” that matched with “content types.”

Answer: 2

**6: Use case2.pcap
Investigate the files.**

What is the USB product’s brand name?

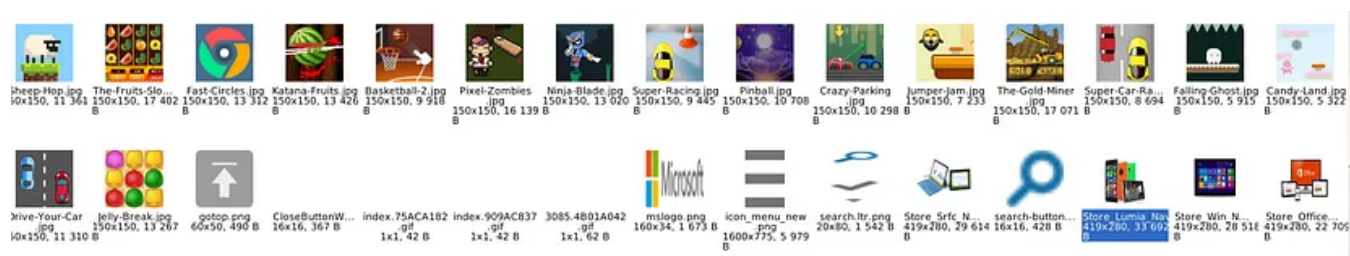
I used the filter and typed in USB. It didn’t really help me out a lot. I went to “Images” tab instead to see if there is anything interesting there. I saw a picture of a USB. I opened the image and typed in “AX88772 Demo board USB.” It led me to a website and that was the answer! I checked the hint afterwards and said no external research is necessary. Oh well, I suppose there are always multiple ways to solve these questions.

Answer: ASIX

7: What is the name of the phone model?

This one was tough for me. I had to look at how other people did it. I don’t know a lot of phone models outside of Samsung, Apple, and Google’s products.

First, we will go to “Images” and scroll down past the Simpson and Game icons. We should see the highlight picture, a picture of a phone model called Lumia.



This isn't enough information for our question though. We need the model number too. To do that, we will now go to the “Files” tab and type in “Lumia” in the filter. Two results should come up, one of which will give us the answer!

Answer: Lumia 535

8: What is the source IP of the fish image?

I typed in “fish” in the “Files” tab to see if I can find the image. One result came up. I right clicked it and clicked on File details and found the source IP.

Hosts (472) | Files (2190) | Images (612) | Messages | Credentials (312) | Sessions (2828) | DNS (8940) | Parameters (

Filter keyword: fish

Frame nr.	Filename	Extension	Size	Source host
31934	Crazy-Fishing.jpg	jpg	11 113 B	50.22.95.9 [yiv.com] [w...

Crazy-Fishing.jpg - File Details

Destination	
LastWriteTime	03/06/2015 14:12:26
MD5	be2030b8015e362fc2e155035946c538
Name	Crazv-Fishing.jpg
Path	/home/ubuntu/Desktop/NetworkMiner 2-7-2/Assem
SHA1	d5046c96e664dc46e3a090cec0769318fc8b60dc
SHA256	0718acd9aed28bfbcce6b371dfbdf928212113ccea6
Size	11113
Source	50.22.95.9 [viv.com] [www.viv.com]

Answer: 50.22.95.9

9: What is the password of the “homer.pwned.se@gmx.com”?

I went to the “Credentials” tab and clicked on the “Usernames” tab to arrange it in alphabetical order. Once that is done, look for the email address we need and then the password field.

Answer: spring2015

10: What is the DNS Query of frame 62001?

Head on over the the “DNS” tab. Look for the frame number we need, which is 62001. When we find the frame, look for the DNS Query.

Answer: pop.gmx.com

Thoughts

Another tool to add to my arsenal for network analysis. It seems like NetworkMiner compliments Wireshark. NetworkMiner gives a rough rundown of what happened in our network while Wireshark gives us a deeper analysis by inspecting each individual packet. I’m having lots of fun learning these network tools but I’m sure in the real world, it’ll be a lot more difficult.

Cybersecurity

Tryhackme

Network Security

Pcap

Digital Forensics



Follow

Written by Toumo

152 Followers · 1 Following

Responses (1)



What are your thoughts?

Respond



Wade Brumbaugh

9 months ago

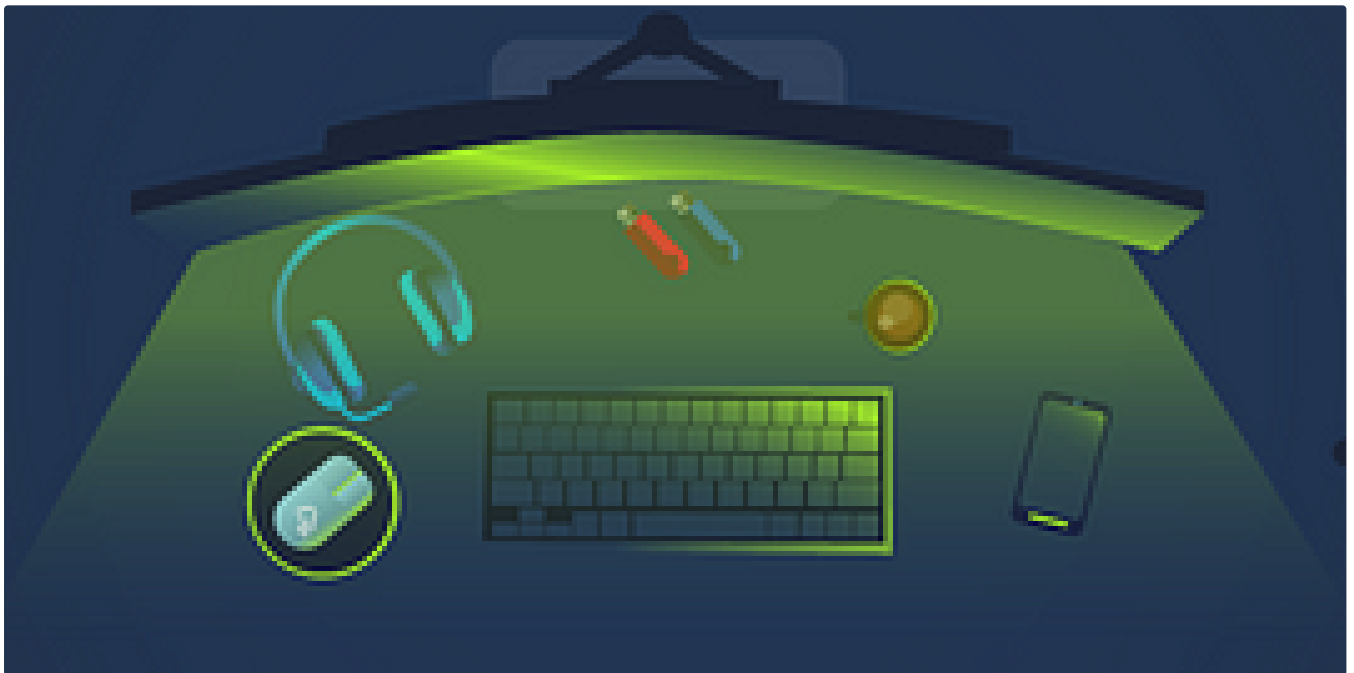


Thank you for the write up. I've wasted an hour of my life trying to find that phone model thinking that there was a phone connected to the network.



Reply

More from Toumo



Toumo

TryHackMe Velociraptor Write-Up

We'll be learning about Velociraptor now. Another tool that I never heard of but I wonder how this will be different compared to the rest...

Aug 9, 2023



20



1





T Toumo

TryHackMe Sysmon Write-Up

We will be doing the Sysmon room this time. I don't know about Sysmon too much except that it's usually running in the background and helps...

Jul 31, 2023 🖱 6



T Toumo

TryHackMe TheHive Project Write-Up

I don't know why, but the idea of having multiple people working on a case simultaneously sounds pretty cool. It's like working on Google...

Aug 9, 2023 🖱 11



Toumo

TryHackMe Osquery: The Basics Write-Up

We finally finished Sysmon last time. Only a couple more logging related rooms before we move on to the SIEM room!

Aug 2, 2023 🖱 4 💬 2

[See all from Toumo](#)[Open in app](#) ➤**Medium**

Search





 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



```
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

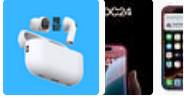
This is a great CTF on TryHackMe that can be accessed through this link here:

<https://tryhackme.com/room/disgruntled>

Oct 22, 2024

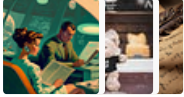


Lists



Tech & Tools

22 stories · 380 saves



Medium's Huge List of Publications Accepting Submissions

377 stories · 4345 saves



Staff picks

796 stories · 1561 saves



Natural Language Processing

1884 stories · 1530 saves



In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations



Nov 5, 2024



60



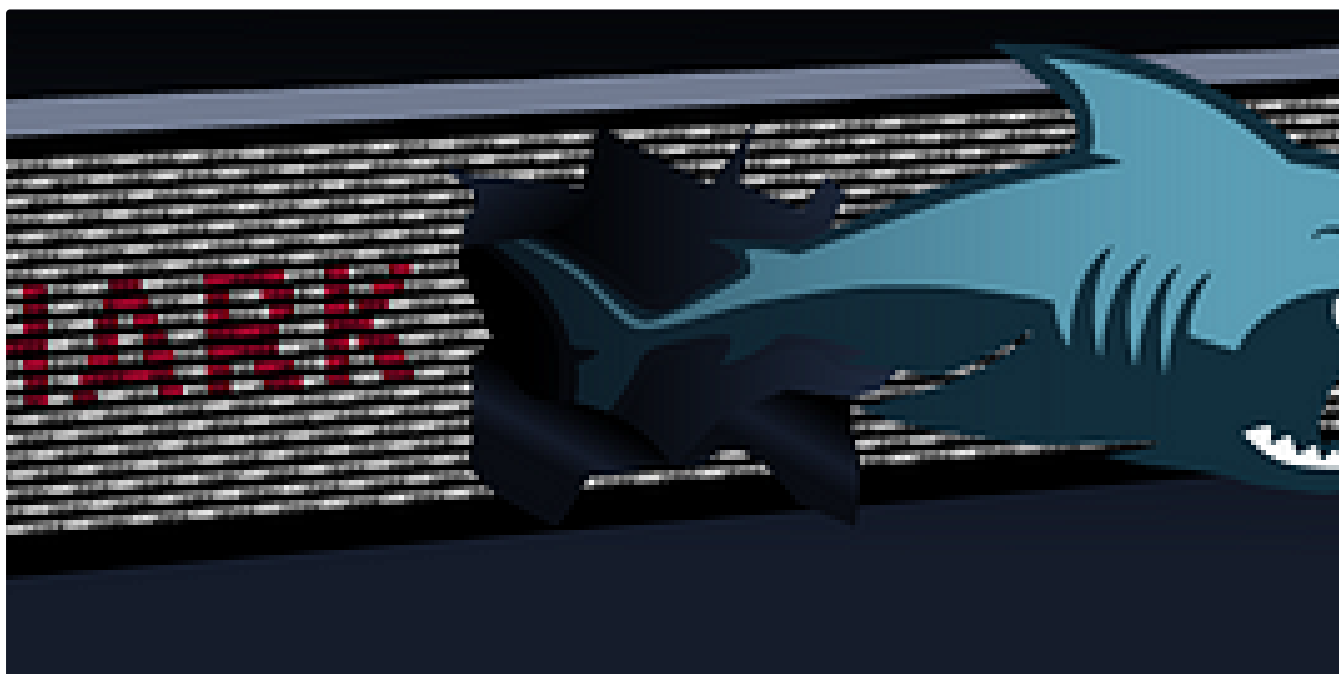


 In T3CH by Axoloth

TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

★ Nov 28, 2024 🖱 50



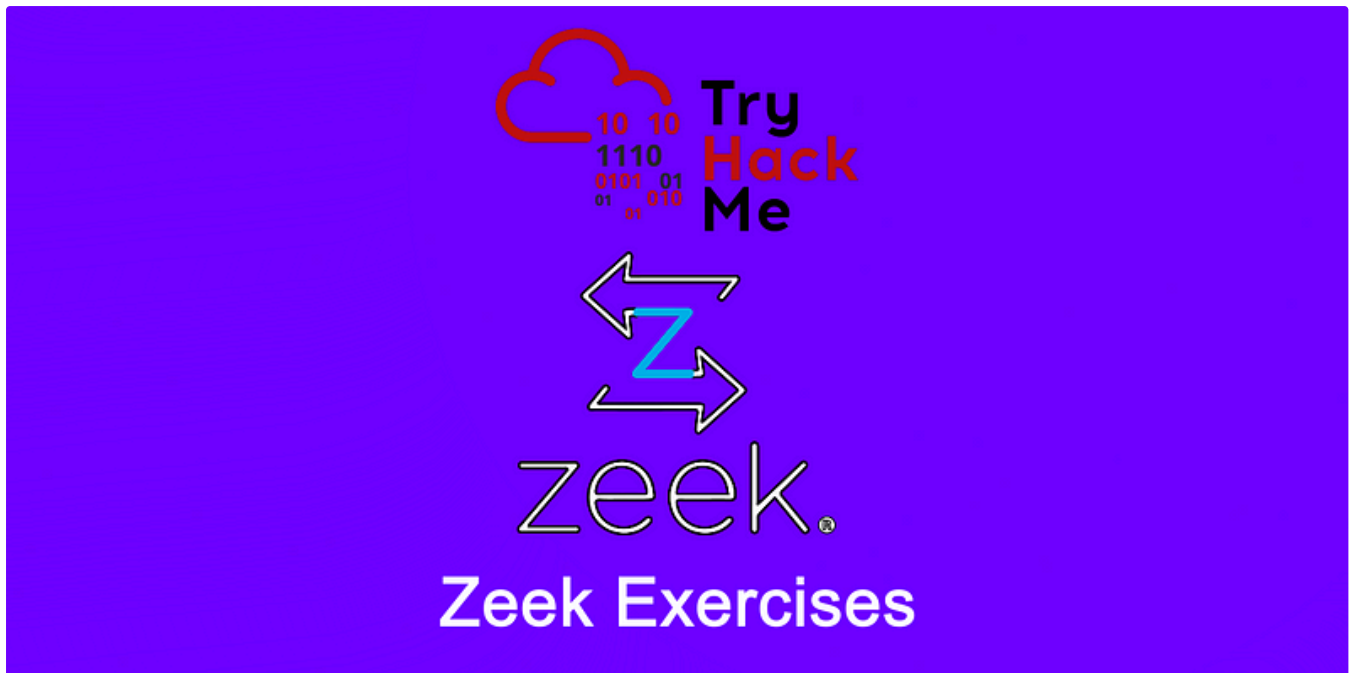
 MAGESH

TShark: The Basics—Tryhackme

Learn the basics of TShark and take your protocol and PCAP analysis skills a step further.

Sep 3, 2024





Carson Shaffer

TryHackMe | Zeek Exercises Writeup

TryHackMe's Zeek Exercises room is a medium-level room that requires using Zeek and other command-line tools to investigate network...

Aug 25, 2024



See more recommendations