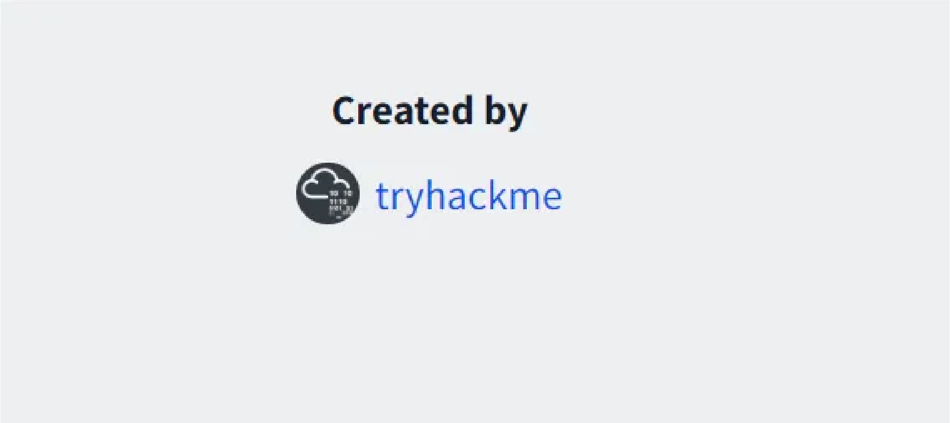
TShark Challenge II: Directory

0xMan1sh 🚀 · Follow
4 min read · Sep 1, 2024

Listen Share More

Put your TShark skills into practice and analyse some network traffic.

Kudos to the creator of this room



Created by

tryhackme

Introduction

This room presents you with a challenge to investigate some traffic data as a part of the SOC team. Let's start working with TShark to analyse the captured traffic. We recommend completing the TShark: The Basics and TShark: CLI Wireshark Features rooms first, which will teach you how to use the tool in depth.

> *Start the VM by pressing the green **Start Machine** button in this task. The machine will start in split view, so you don't need SSH or RDP. In case the machine does not appear, you can click the blue **Show Split View** button located at the top of this room.*

NOTE: Exercise files contain real examples. **DO NOT** interact with them outside of the given VM. Direct interaction with samples and their contents (files, domains, and IP addresses) outside the given VM can pose security threats to your machine.

Case: Directory Curiosity!

An alert has been triggered: "A user came across a poor file index, and their curiosity led to problems".

The case was assigned to you. Inspect the provided **directory-curiosity.pcap** located in `~/Desktop/exercise-files` and retrieve the artefacts to confirm that this alert is a true positive.

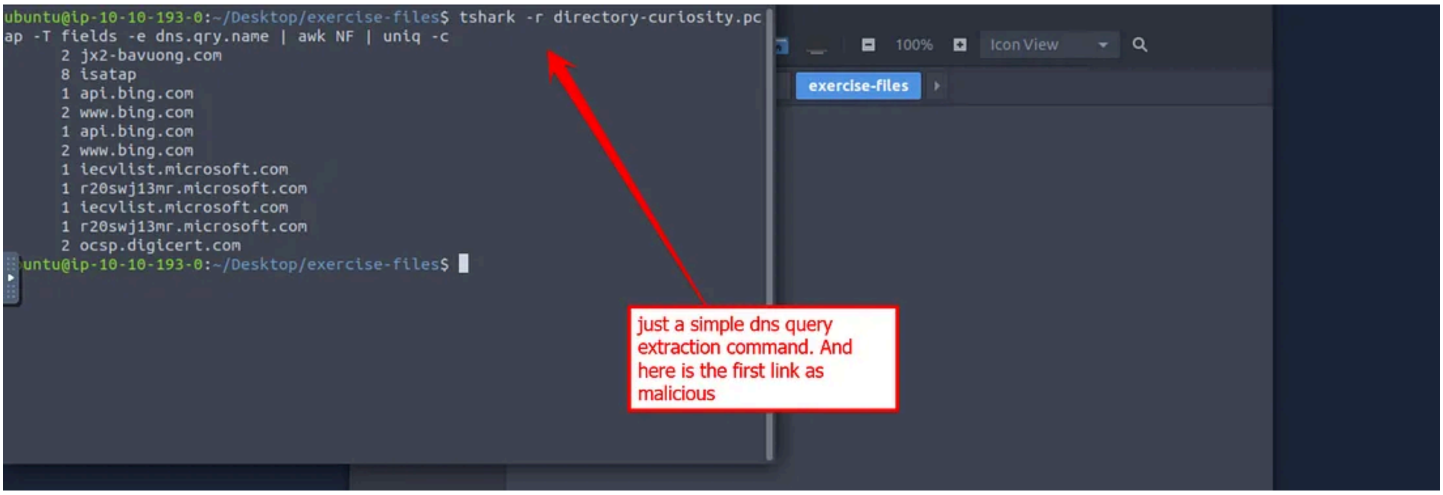
Your tools: TShark, VirusTotal.

Answer the questions below

Investigate the DNS queries.
Investigate the domains by using VirusTotal.
According to VirusTotal, there is a domain marked as malicious/suspicious.

What is the name of the malicious/suspicious domain?

*(Enter your answer in a **defanged** format.)*

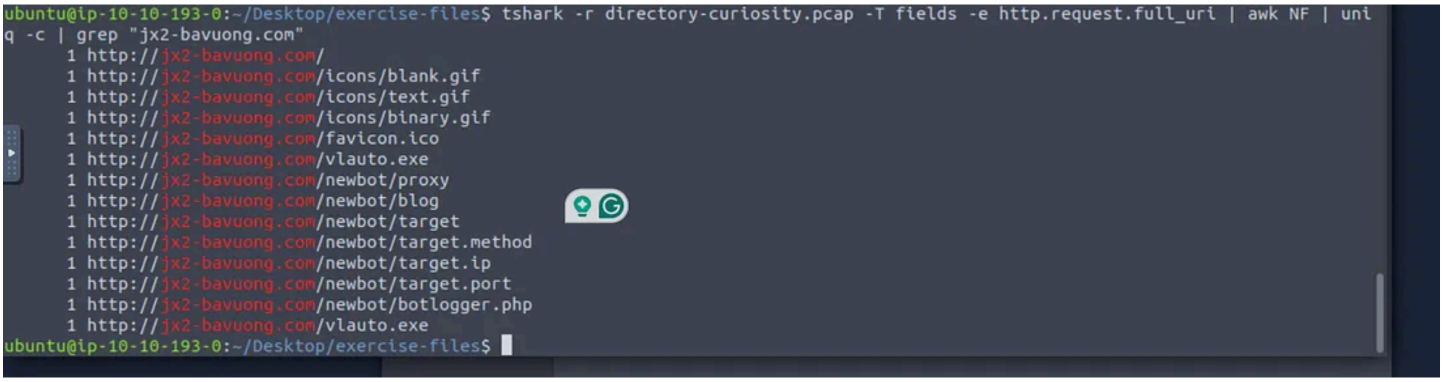


```
ubuntu@ip-10-10-193-0:~/Desktop/exercise-files$ tshark -r directory-curiosity.pc
ap -T fields -e dns.qry.name | awk NF | uniq -c
      2 jx2-bavuong.com
      8 isatap
      1 api.bing.com
      2 www.bing.com
      1 api.bing.com
      2 www.bing.com
      1 iecvlist.microsoft.com
      1 r20swj13mr.microsoft.com
      1 iecvlist.microsoft.com
      1 r20swj13mr.microsoft.com
      2 ocsp.digicert.com
ubuntu@ip-10-10-193-0:~/Desktop/exercise-files$
```

just a simple dns query extraction command. And here is the first link as malicious

Correct Answer — **jx2-bavuong[.]com**

What is the total number of HTTP requests sent to the malicious domain?

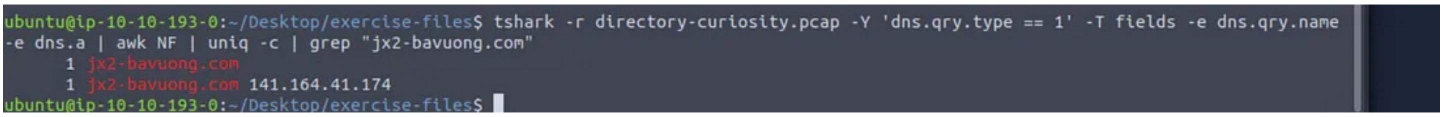


```
ubuntu@ip-10-10-193-0:~/Desktop/exercise-files$ tshark -r directory-curiosity.pcap -T fields -e http.request.full_uri | awk NF | uni
q -c | grep "jx2-bavuong.com"
      1 http://jx2-bavuong.com/
      1 http://jx2-bavuong.com/icons/blank.gif
      1 http://jx2-bavuong.com/icons/text.gif
      1 http://jx2-bavuong.com/icons/binary.gif
      1 http://jx2-bavuong.com/favicon.ico
      1 http://jx2-bavuong.com/vlauto.exe
      1 http://jx2-bavuong.com/newbot/proxy
      1 http://jx2-bavuong.com/newbot/blog
      1 http://jx2-bavuong.com/newbot/target
      1 http://jx2-bavuong.com/newbot/target.method
      1 http://jx2-bavuong.com/newbot/target.ip
      1 http://jx2-bavuong.com/newbot/target.port
      1 http://jx2-bavuong.com/newbot/botlogger.php
      1 http://jx2-bavuong.com/vlauto.exe
ubuntu@ip-10-10-193-0:~/Desktop/exercise-files$
```

Correct Answer — **14**

What is the IP address associated with the malicious domain?

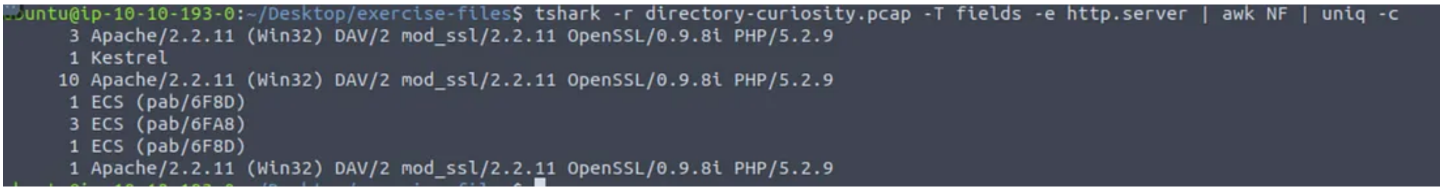
(Enter your answer in a ***defanged*** *format.)*



```
ubuntu@ip-10-10-193-0:~/Desktop/exercise-files$ tshark -r directory-curiosity.pcap -Y 'dns.qry.type == 1' -T fields -e dns.qry.name
-e dns.a | awk NF | uniq -c | grep "jx2-bavuong.com"
      1 jx2-bavuong.com
      1 jx2-bavuong.com 141.164.41.174
ubuntu@ip-10-10-193-0:~/Desktop/exercise-files$
```

Correct Answer-**141[.]164[.]41[.]174**

What is the server info of the suspicious domain?

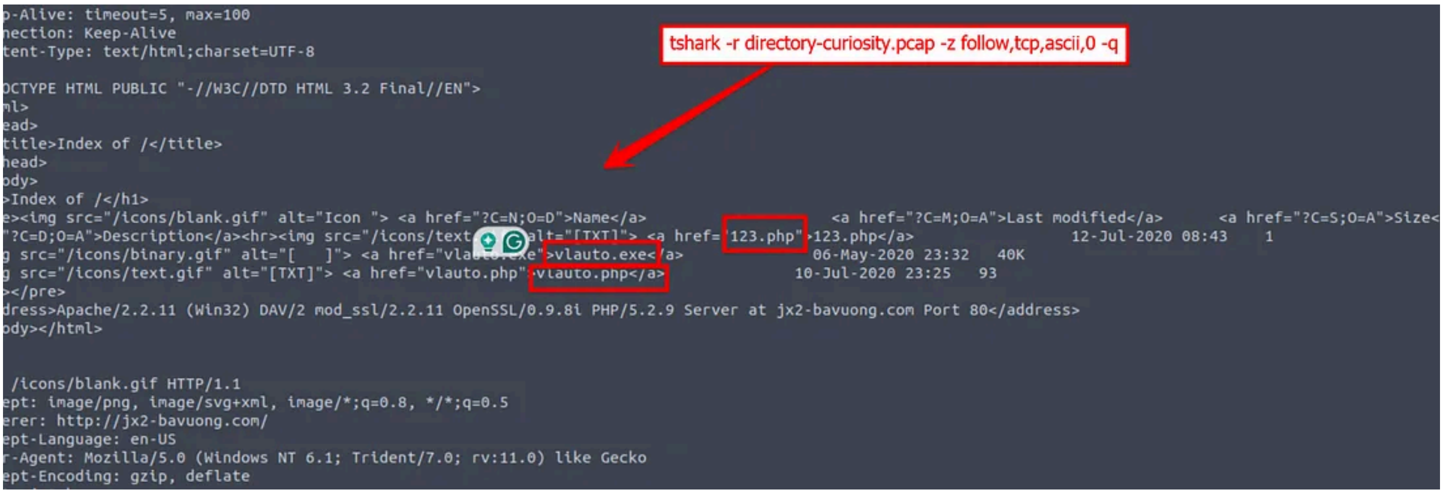


```
ubuntu@ip-10-10-193-0:~/Desktop/exercise-files$ tshark -r directory-curiosity.pcap -T fields -e http.server | awk NF | uniq -c
      3 Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i PHP/5.2.9
      1 Kestrel
     10 Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i PHP/5.2.9
      1 ECS (pab/6F8D)
      3 ECS (pab/6FA8)
      1 ECS (pab/6F8D)
      1 Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i PHP/5.2.9
```

Correct Answer — **Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i PHP/5.2.9**

Follow the "first TCP stream" in "ASCII".
Investigate the output carefully.

What is the number of listed files?



tshark -r directory-curiosity.pcap -z follow,tcp,ascii,0 -q

```
p-Alive: timeout=5, max=100
nection: Keep-Alive
tent-Type: text/html;charset=UTF-8

OCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
ml>
ead>
title>Index of /</title>
head>
ody>
>Index of /</h1>
e><img src="/icons/blank.gif" alt="Icon "> <a href="?C=N;O=D">Name</a>                    <a href="?C=M;O=A">Last modified</a>      <a href="?C=S;O=A">Size<
"?C=D;O=A">Description</a><hr><img src="/icons/text   alt="[TXT]"> <a href="123.php">123.php</a>                      12-Jul-2020 08:43    1
g src="/icons/binary.gif" alt="[   ]"> <a href="vlauto.exe">vlauto.exe</a>               06-May-2020 23:32   40K
g src="/icons/text.gif" alt="[TXT]"> <a href="vlauto.php">vlauto.php</a>              10-Jul-2020 23:25   93
></pre>
dress>Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i PHP/5.2.9 Server at jx2-bavuong.com Port 80</address>
ody></html>


 /icons/blank.gif HTTP/1.1
ept: image/png, image/svg+xml, image/*;q=0.8, */*;q=0.5
erer: http://jx2-bavuong.com/
ept-Language: en-US
r-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
ept-Encoding: gzip, deflate
```

Correct Answer — 3

What is the filename of the first file?

*(Enter your answer in a **defanged** format.)*

Correct Answer — **123[.]php**

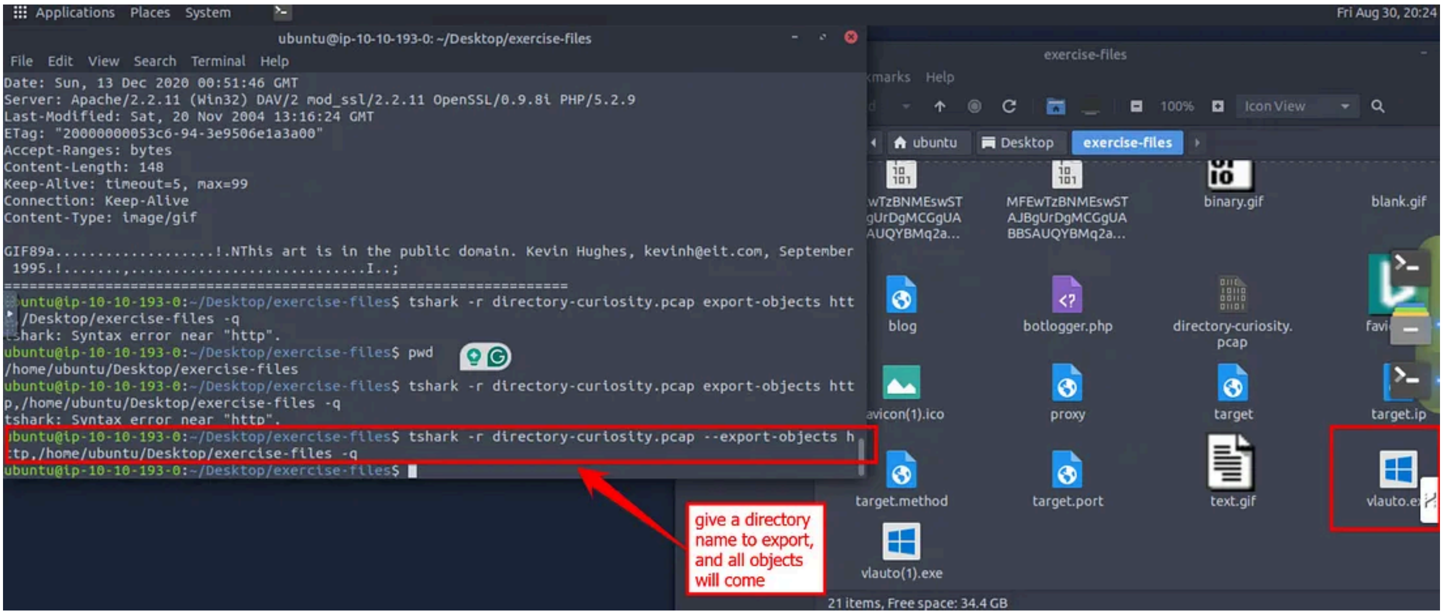
Export all HTTP traffic objects.

> *tshark -r directory-curiosity.pcap — export-objects http,/home/ubuntu/Desktop/exercise-files -q*

- **r directory-curiosity.pcap:** Reads the packet capture file named directory-curiosity.pcap.
- **— export-objects http,/home/ubuntu/Desktop/exercise-files:** Extracts and saves all HTTP objects (e.g., files like images, documents) from the packet capture. These objects are stored in the directory /home/ubuntu/Desktop/exercise-files.
- **-q:** Runs tshark in quiet mode, suppressing the usual packet summary output.

What is the name of the downloaded executable file?

*(Enter your answer in a **defanged** format.)*



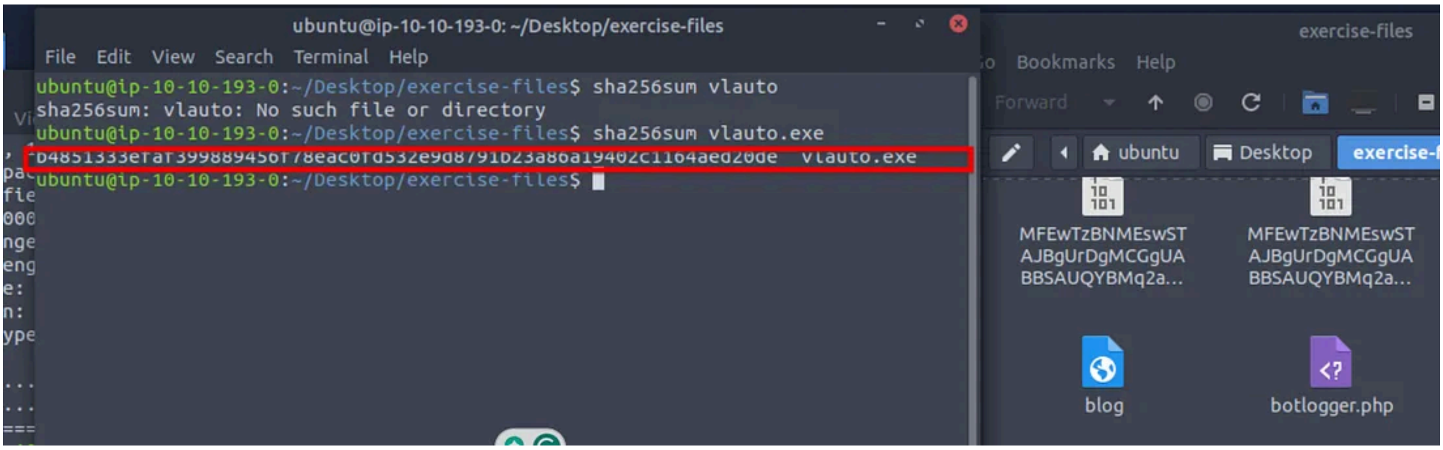
```
Date: Sun, 13 Dec 2020 00:51:46 GMT
Server: Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i PHP/5.2.9
Last-Modified: Sat, 20 Nov 2004 13:16:24 GMT
ETag: "20000000053c6-94-3e9506e1a3a00"
Accept-Ranges: bytes
Content-Length: 148
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: image/gif

GIF89a..................!.NThis art is in the public domain. Kevin Hughes, kevinh@eit.com, September
 1995.!.......,..............................I..;
====================================================================
untu@ip-10-10-193-0:~/Desktop/exercise-files$ tshark -r directory-curiosity.pcap export-objects htt
/Desktop/exercise-files -q
shark: Syntax error near "http".
ubuntu@ip-10-10-193-0:~/Desktop/exercise-files$ pwd
/home/ubuntu/Desktop/exercise-files
ubuntu@ip-10-10-193-0:~/Desktop/exercise-files$ tshark -r directory-curiosity.pcap export-objects htt
p,/home/ubuntu/Desktop/exercise-files -q
tshark: Syntax error near "http".
ubuntu@ip-10-10-193-0:~/Desktop/exercise-files$ tshark -r directory-curiosity.pcap --export-objects h
ttp,/home/ubuntu/Desktop/exercise-files -q
ubuntu@ip-10-10-193-0:~/Desktop/exercise-files$
```

give a directory name to export, and all objects will come

Correct Answer — **vlauto[.]exe**

What is the SHA256 value of the malicious file?



```
ubuntu@ip-10-10-193-0:~/Desktop/exercise-files$ sha256sum vlauto
sha256sum: vlauto: No such file or directory
ubuntu@ip-10-10-193-0:~/Desktop/exercise-files$ sha256sum vlauto.exe
b4851333efaf399889456f78eac0fd532e9d8791b23a86a19402c1164aed20de  vlauto.exe
ubuntu@ip-10-10-193-0:~/Desktop/exercise-files$
```

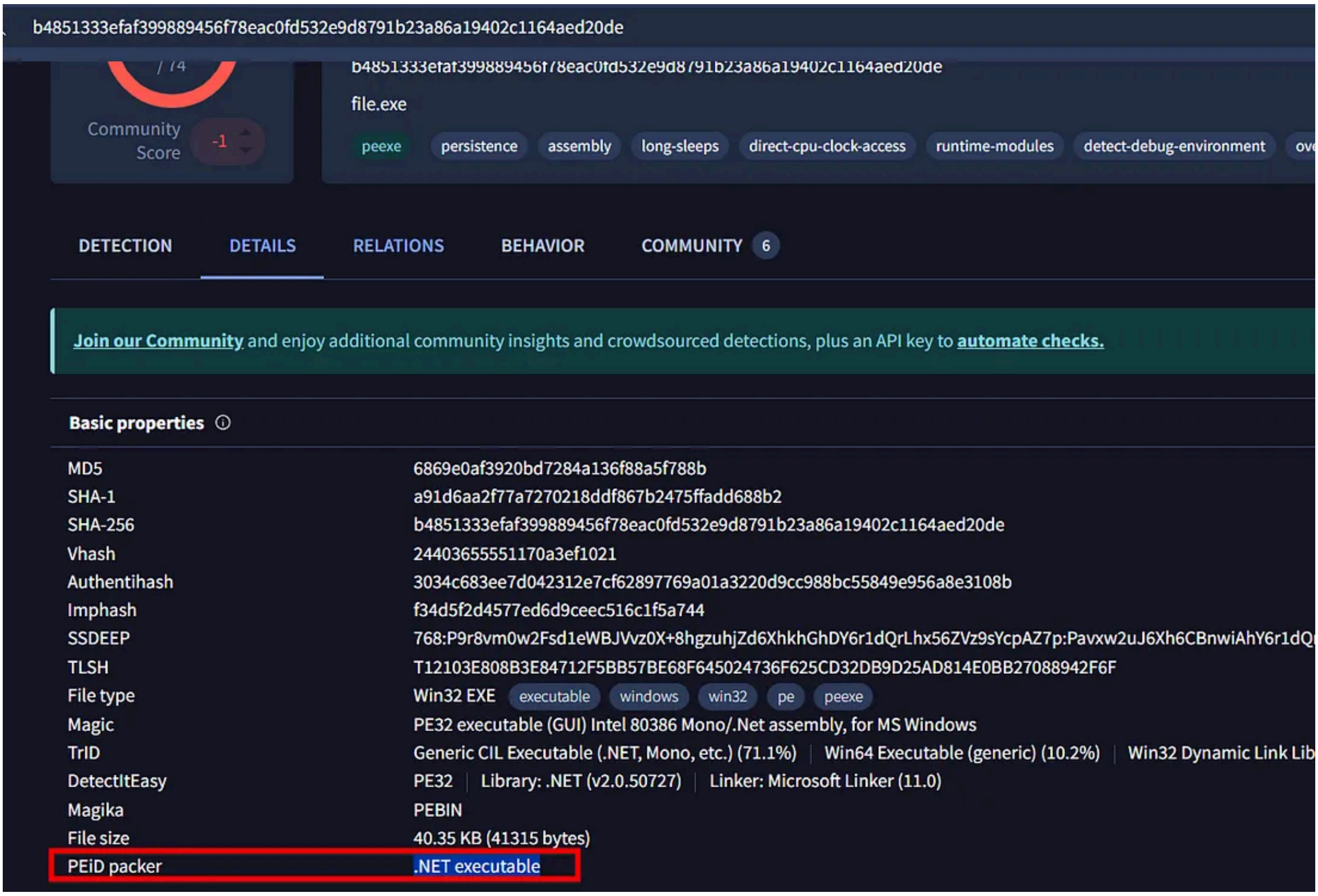
ubuntu@ip-10-10-193-0: ~/Desktop/exercise-files
File
Edit
View
Search
Terminal
Help
exercise-files
Bookmarks
Help
Forward
ubuntu
Desktop
exercise-f
MFEwTzBNMEswST AJBgUrDgMCGgUA BBSAUQYBMq2a...
MFEwTzBNMEswST AJBgUrDgMCGgUA BBSAUQYBMq2a...
blog
botlogger.php

sha256 file_name **(just type in the terminal)**

Correct Answer — **b4851333efaf399889456f78eac0fd532e9d8791b23a86a19402c1164aed20de**

Search the SHA256 value of the file on VirtusTotal.

What is the "PEiD packer" value?



b4851333efaf399889456f78eac0fd532e9d8791b23a86a19402c1164aed20de

b4851333efaf399889456f78eac0fd532e9d8791b23a86a19402c1164aed20de

file.exe

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

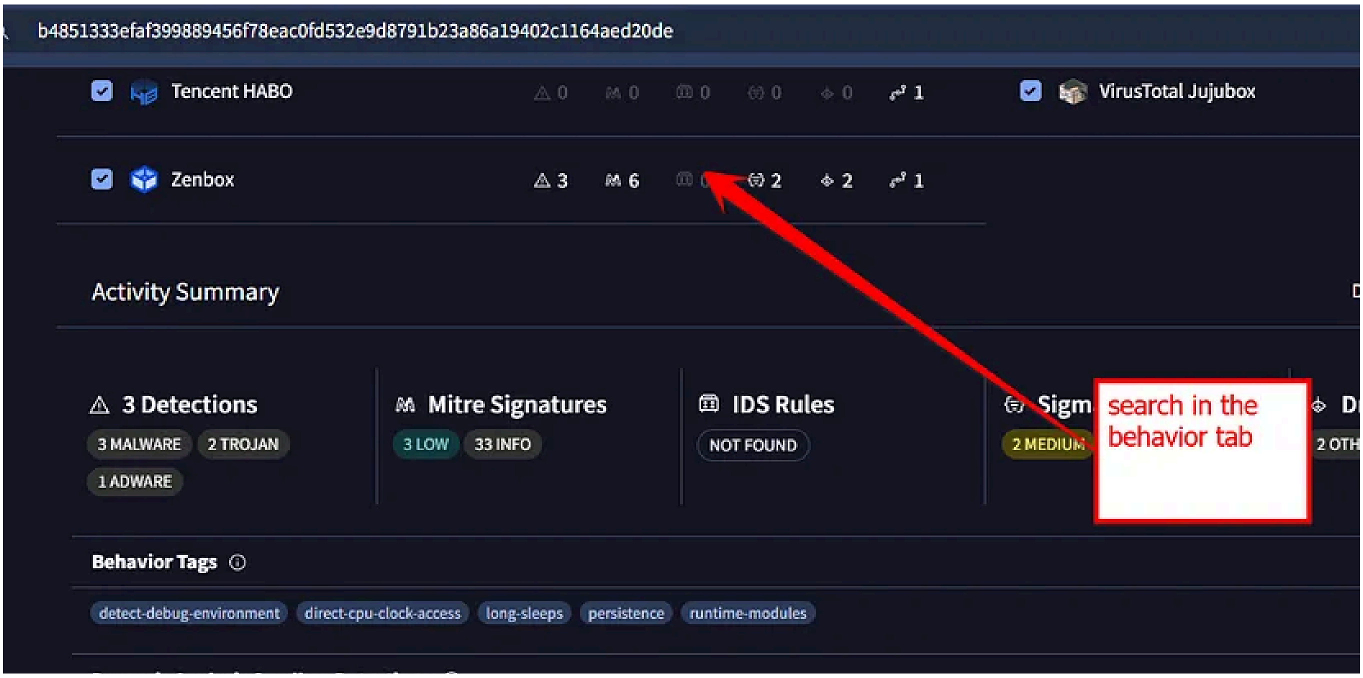
Basic properties ⓘ

MD5	6869e0af3920bd7284a136f88a5f788b
SHA-1	a91d6aa2f77a7270218ddf867b2475ffadd688b2
SHA-256	b4851333efaf399889456f78eac0fd532e9d8791b23a86a19402c1164aed20de
Vhash	24403655551170a3ef1021
Authentihash	3034c683ee7d042312e7cf62897769a01a3220d9cc988bc55849e956a8e3108b
Imphash	f34d5f2d4577ed6d9ceec516c1f5a744
SSDEEP	768:P9r8vm0w2Fsd1eWBJVvz0X+8hgzuhjZd6XhkhGhDY6r1dQrLhx56ZVz9sYcpAZ7p:Pavxw2uJ6Xh6CBnwiAhY6r1dQ
TLSH	T12103E808B3E84712F5BB57BE68F645024736F625CD32DB9D25AD814E0BB27088942F6F
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
TrID	Generic CIL Executable (.NET, Mono, etc.) (71.1%) | Win64 Executable (generic) (10.2%) | Win32 Dynamic Link Lib
DetectItEasy	PE32 | Library: .NET (v2.0.50727) | Linker: Microsoft Linker (11.0)
Magika	PEBIN
File size	40.35 KB (41315 bytes)
PEiD packer	.NET executable

Correct Answer — **.NET executable**

Search the SHA256 value of the file on VirtusTotal.

What does the “Lastline Sandbox” flag this as?



b4851333efaf399889456f78eac0fd532e9d8791b23a86a19402c1164aed20de

☑ Tencent HABO ⚠ 0 0 0 0 0 1 ☑ VirusTotal Jujubox

☑ Zenbox ⚠ 3 6 0 2 2 1

Activity Summary

⚠ 3 Detections: 3 MALWARE, 2 TROJAN, 1 ADWARE

Mitre Signatures: 3 LOW, 33 INFO

IDS Rules: NOT FOUND

Sigm… 2 MEDIUM

2 OTH…

Behavior Tags ⓘ

detect-debug-environment direct-cpu-clock-access long-sleeps persistence runtime-modules

MITRE ATT&CK Tactics and Techniques

+ Execution TA0002

Correct Answer — MALWARE TROJAN

Thank you for reading! 👽

I hope this write-up has provided valuable insights. 🐉

If you found it helpful, don’t forget to share it with others and leave your thoughts in the comments.

Connect with me on LinkedIn and support me on Medium.

> My LinkedIn — *https://www.linkedin.com/in/manishknayak/*

Until next time, keep learning, pawn well and stay secure!!!!!!!!!!!!! 👹

Hacking Cybersecurity Tryhackme Writeup Hackthebox Wirteup

Follow

Written by 0xMan1sh 🚀

21 Followers · 2 Following

Just a meow away to pawn it 😉

Responses (1)

What are your thoughts?

Respond

Sunny Singh Verma [SuNnY]
4 months ago

One of my fav topics .. nice writeup

Reply

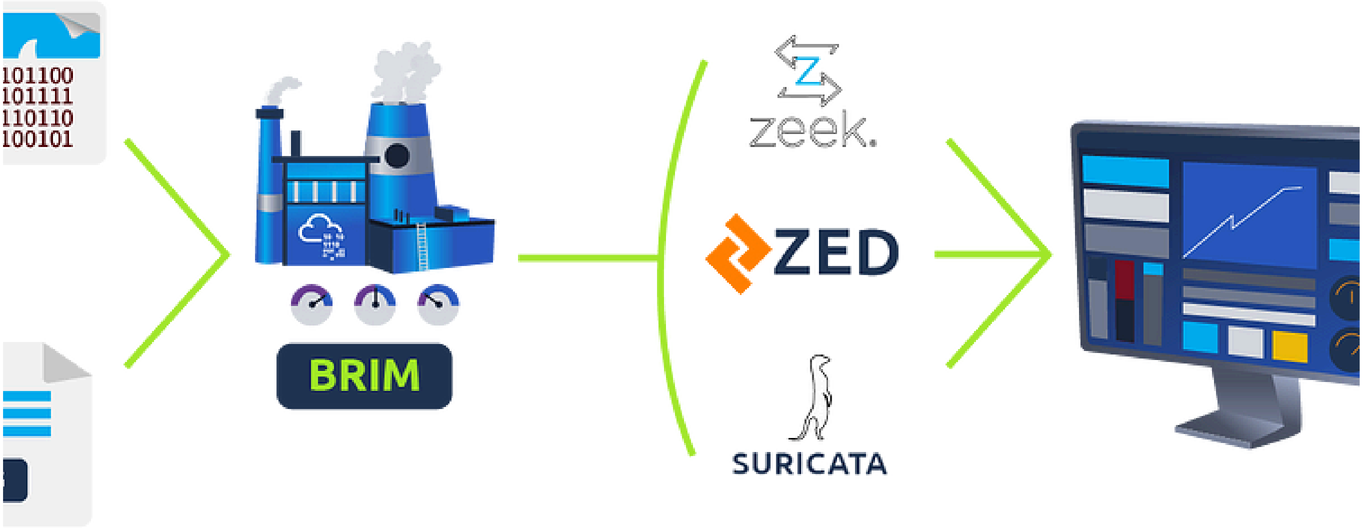
More from 0xMan1sh 🚀

0xMan1sh 🚀

Unattended Writeup TryHackMe || Medium Level || Detailed Walkthrough 🔥

Use your Windows forensics knowledge to investigate an incident.

Dec 17, 2024 👏 50 💬 1



0xMan1sh 🚀

Brim

Network security analysis is a critical skill in cybersecurity, enabling us to detect, investigate, and mitigate threats effectively. The...

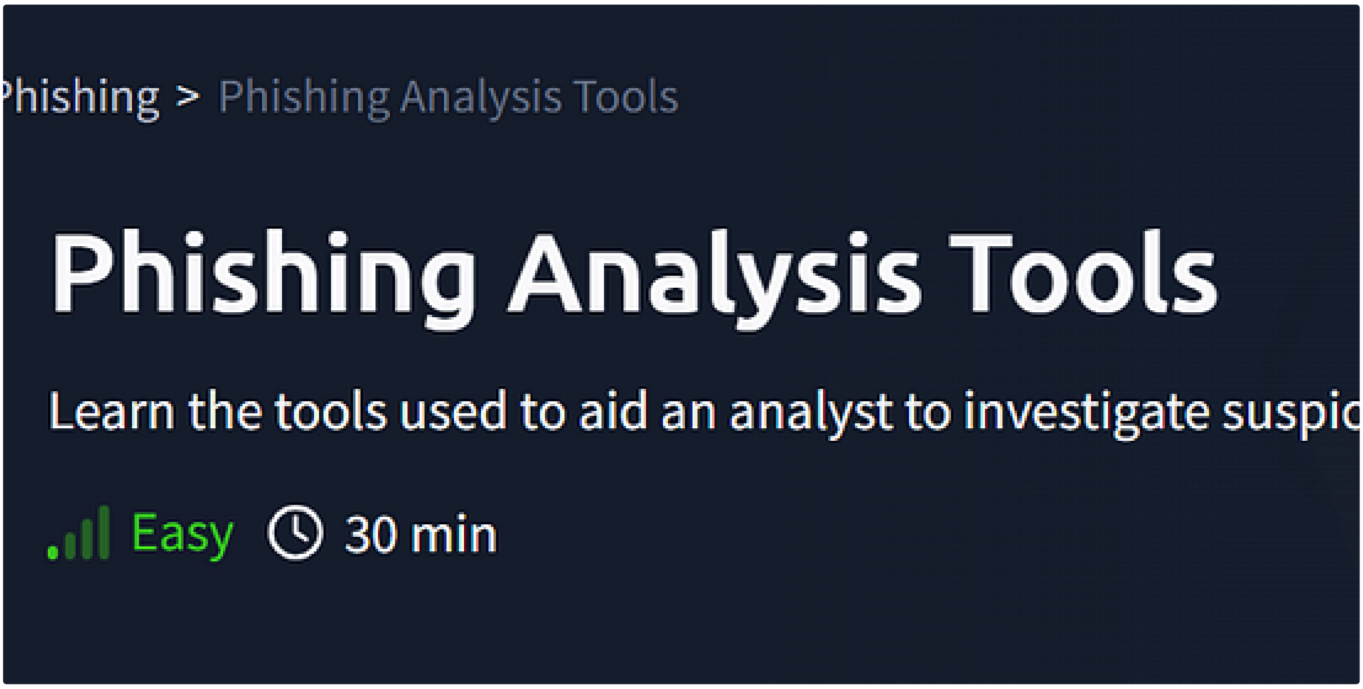
Jul 18, 2024

0xMan1sh 🚀

CTI Trooper

Room Link—https://tryhackme.com/r/room/trooper

Aug 7, 2024



Phishing > Phishing Analysis Tools

Phishing Analysis Tools

Learn the tools used to aid an analyst to investigate suspic

Easy 30 min

0xMan1sh 🚀

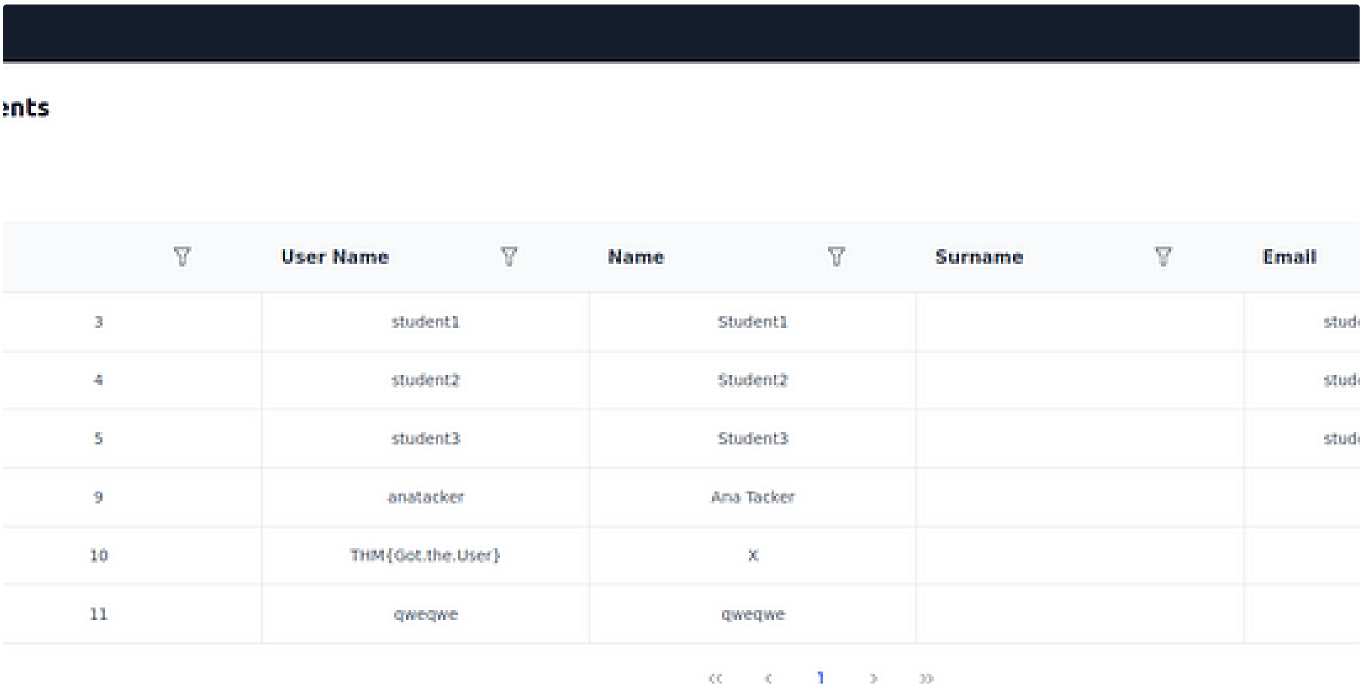
Phishing Analysis Tools

Remember , in Phishing Room 1 we covered how to manually sift through the email raw source code to extract information. In Phishing Room 2...

Jul 9, 2024 👏 3

See all from 0xMan1sh 🚀

Recommended from Medium



ents

	User Name	Name	Surname	Email
3	student1	Student1		stud
4	student2	Student2		stud
5	student3	Student3		stud
9	anatacker	Ana Tacker		
10	THM{Got.the.User}	X		
11	qweqwe	qweqwe		

embossdotar

TryHackMe—Session Management—Writeup

Key points: Session Management | Authentication | Authorisation | Session Management Lifecycle | Exploit of vulnerable session management…

✦ Aug 7, 2024 👏 27

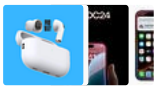
In InfoSec Write-ups by Satyam Pathania

SOC Analyst Roadmap for 2025: Your Step-by-Step Self-Study Guide

{Updated}—This is an updated article with new resources and few more steps breakdowns

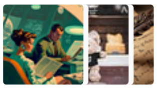
✦ Dec 26, 2024 👏 229 💬 6

Lists



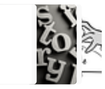
Tech & Tools

22 stories · 380 saves



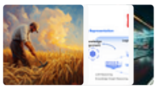
Medium's Huge List of Publications Accepting Submissions

377 stories · 4347 saves



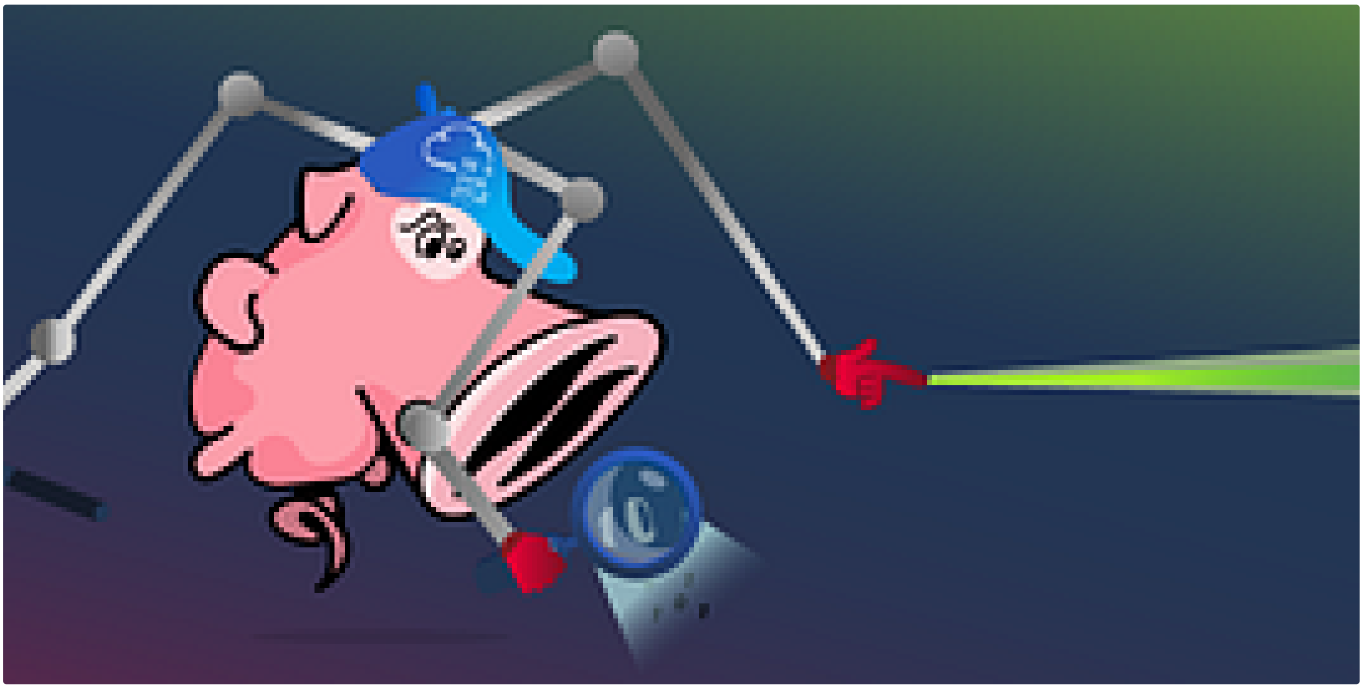
Staff picks

796 stories · 1560 saves



Natural Language Processing

1884 stories · 1530 saves

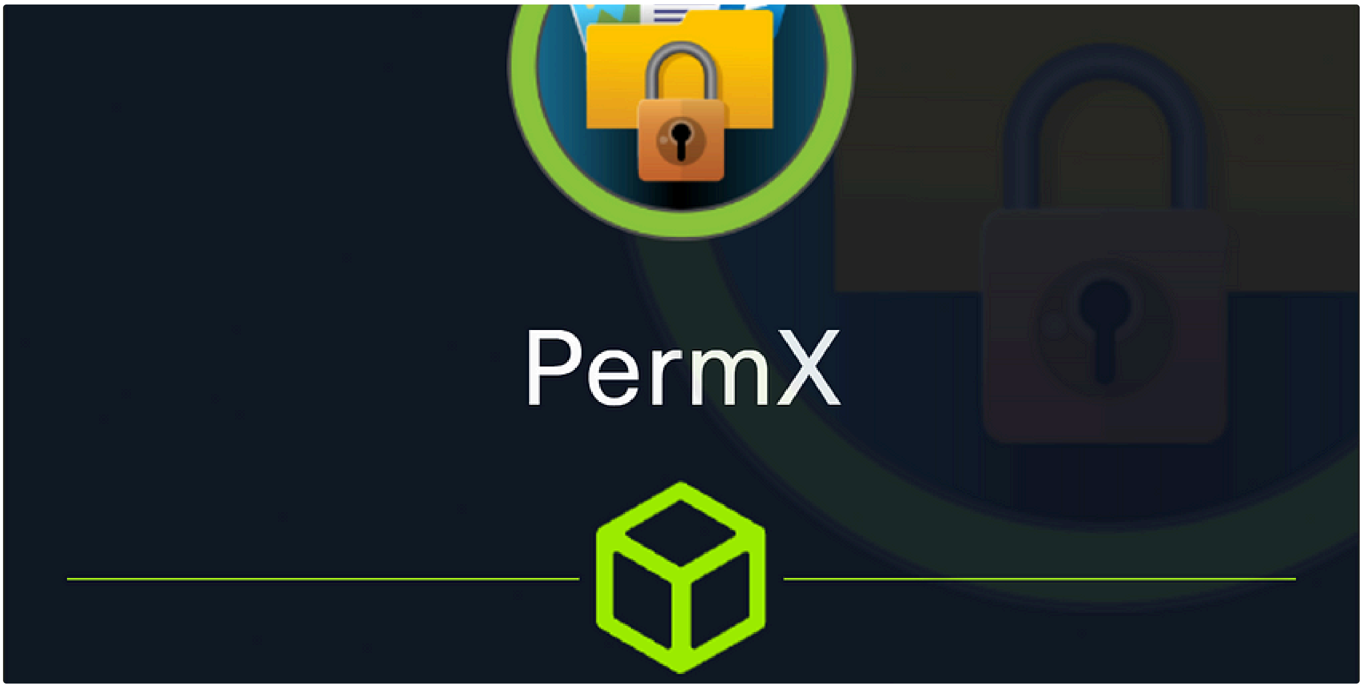


In T3CH by Axoloth

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



Error

PermX(Easy) Writeup User Flag—HackTheBox CTF

Lets start with NMAP scan. This showed how there is 2 ports open on both 80 and 22. From there it is simple you must ….

Jul 28, 2024

```
v3.2.1

[!] Live Forensicator

[!] Examines the host for suspicious activities and grabs required data for further forens
[!] By Ebuka John Onyejegbu.
[!] https://github.com/Johnng007/Live-Forensicator
[!] https://john.ng
```

Riley Pickles

BTLO Walkthrough | Digital Forensics |Detailed Guide Step by Step

Swift

Sep 29, 2024 4

Chicken0248

[LetsDefend Write-up] IcedID Malware Family

Challenge Files (pass: infected): /root/Desktop/ChallengeFile/challenge-files.zip

Dec 22, 2024

See more recommendations