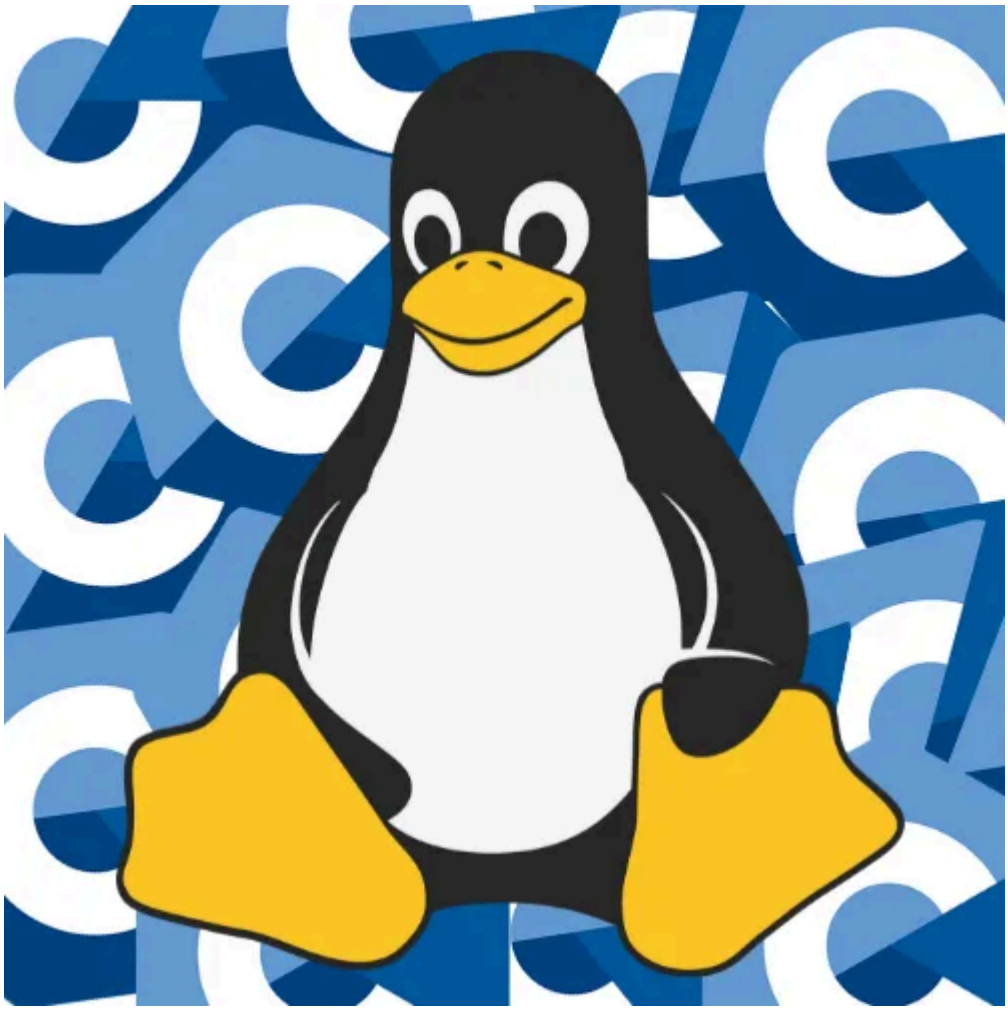
Linux Function Hooking

TryhackMe — Linux Function Hooking

Nehru G · Follow

2 min read · Jul 15, 2021



Task 1 Introduction

#1 :- I am ready to learn!

Answer :- No Needed Answer

Task 2 What are Shared Libraries?

#2 :- What is the name of the dynamic linker/loader on linux?

*Answer :- ld.so, ld-linux.so**

Task 3 Getting A Tad Bit Technical

#3.1:- What environment variable let's you load your own shared library before all others?

Answer :- LD_PRELOAD

#3.2:- Which file contains a whitespace-separated list of ELF shared objects to be loaded before running a program?

Answer :- /etc/ld.so.preload

#3.3:- If both the environment variable and the the file are employed, the libraries specified by which would be loaded first?

Answer :- environment variable

Task 4 Putting On Our Coding Hats

#4.1 :- How many arguments does **write()** take?

Answer :- 3

#4.2 :- Which feature test macro must be defined in order to obtain the definitions of **RTLD_NEXT** from **<dlfcn.h>**?

Answer :- _GNU_SOURCE

Task 5 Let’s Gooooooooo

#5.1 :- When compiling our code to produce a Shared Object, which flag is used to create position independent code?

Answer :- -fPIC

#5.2 :- Can hooking libc functions affect the behavior of Python3? (Yay/Nay)

Answer :- yay

Task 6 Hiding Files From ls

#6.1 :- There are two mandatory fields of a **dirent** structure. One is **d_name**, and the other one is?

Answer :- d_ino

#6.2 :- I have read and understood how I can hide files using shared objects!

Answer :- No Needed Answer

Task 7 Conclusion

#7 :- Hooray! You made it to the end!

Answer :- No Needed Answer

Tryhackme Walkthrough | Tryhackme Writeup | Tryhackme

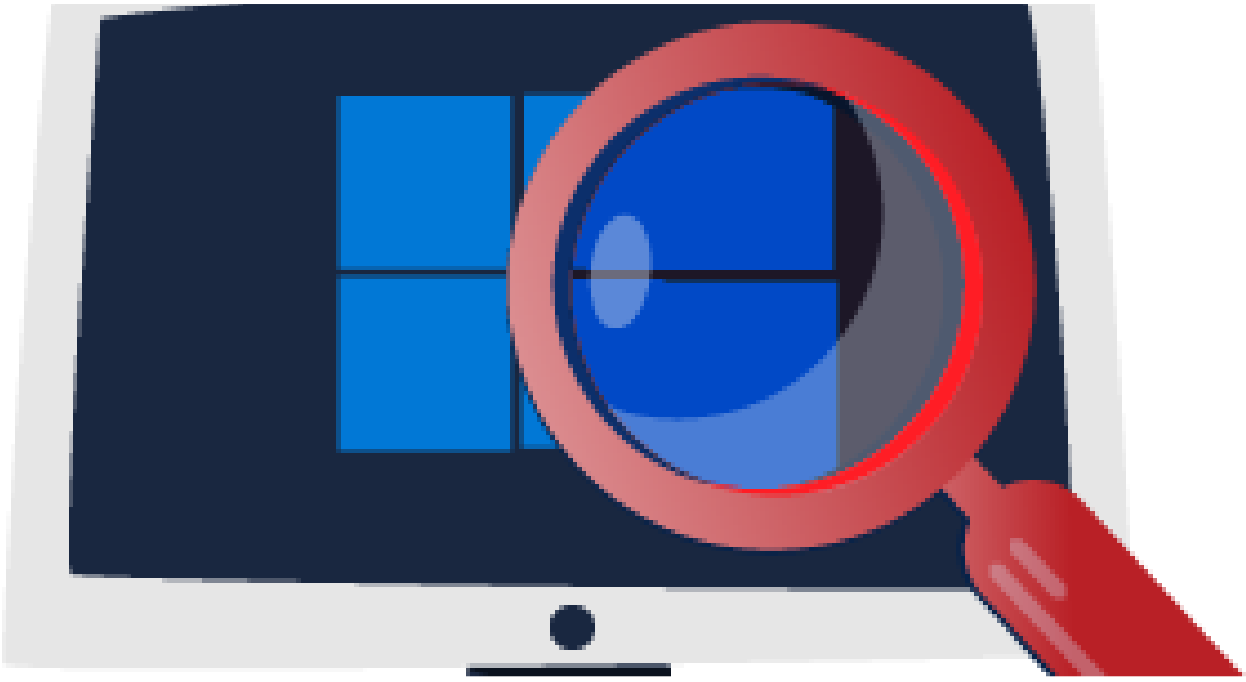
Follow

Written by Nehru G

191 Followers

Pentester

More from Nehru G



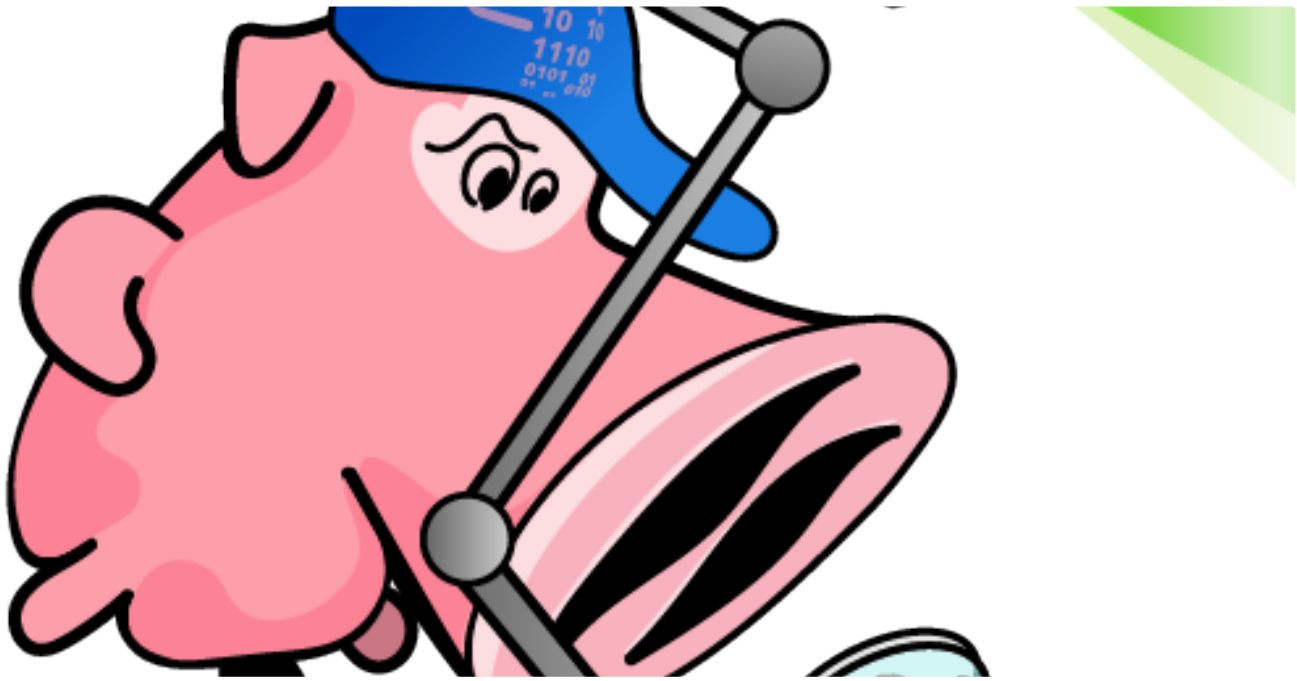
Nehru G

Windows Forensics 1 |TryHackMe

Task 1 -Introduction to Windows Forensics

23 min read · Aug 9, 2022

9



Nehru G

Snort -TryHackMe

Task 1-Introduction

42 min read · Nov 24, 2022

14

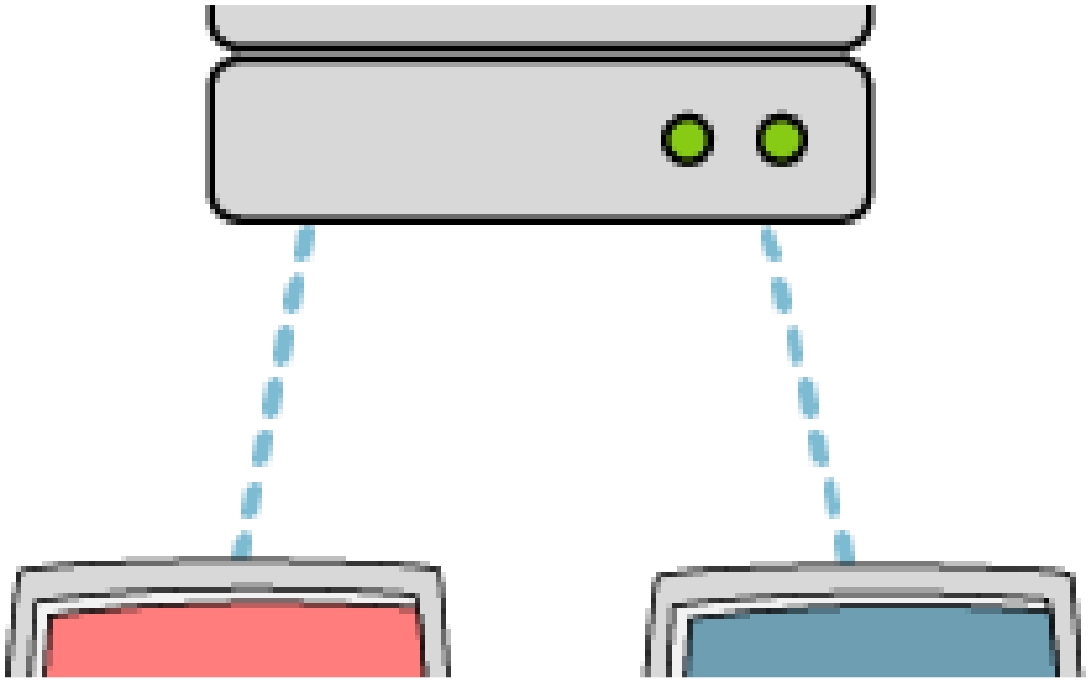
Nehru G

TryHackMe-Intro to Digital Forensics

Task 1 -Introduction To Digital Forensics

2 min read · Mar 21, 2022

13 2



Nehru G

Intro to C2 | TryHackMe

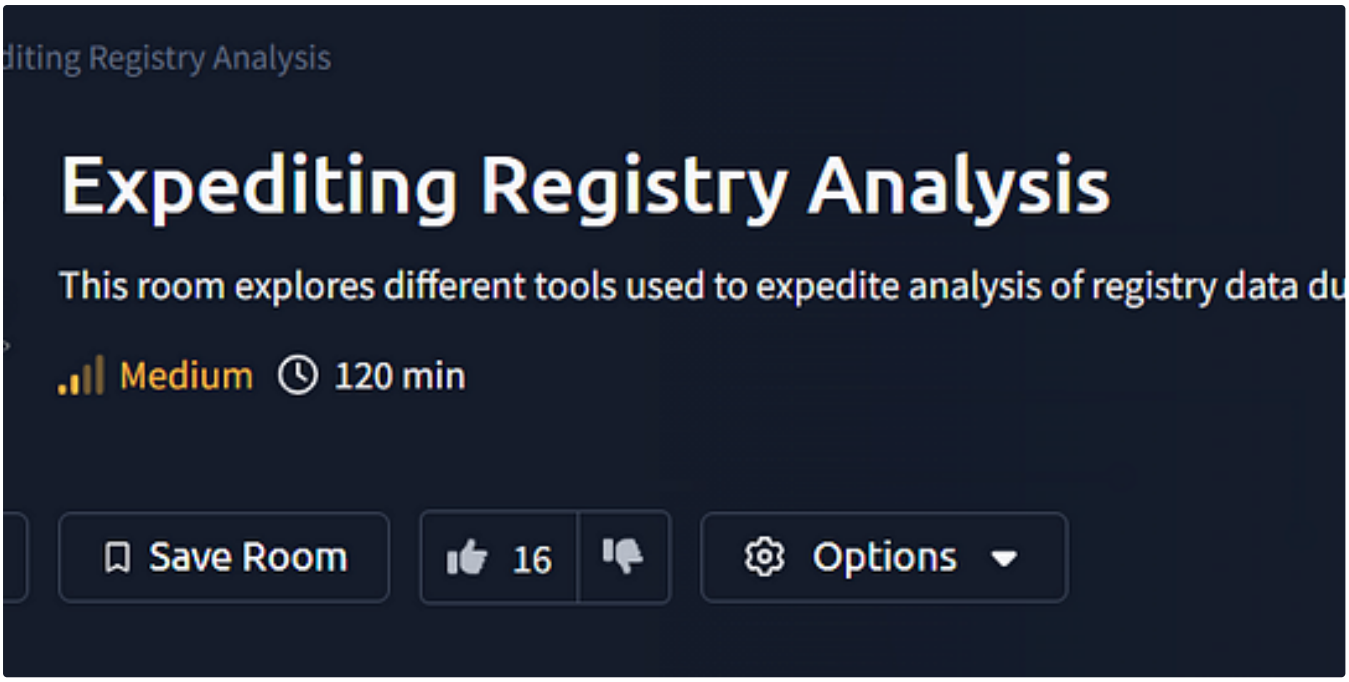
Task 1-Introduction

36 min read · Aug 11, 2022

6

See all from Nehru G

Recommended from Medium



Zainaaborumman

TryHackMe | Expediting Registry Analysis Writeup

Task 1: Introduction

5 min read · Apr 5, 2024

5

embossdotar

TryHackMe—Windows User Account Forensics—Writeup

Key points: Windows Account Types | Account Lifecycle Artefacts | Event Viewer | Security Account Manager | NTDS.dit | PowerShell |...

2 min read · Apr 12, 2024

46

Lists

Staff Picks

629 stories · 916 saves

Stories to Help You Level-Up at Work

19 stories · 573 saves

Self-Improvement 101

20 stories · 1660 saves

Productivity 101

20 stories · 1531 saves

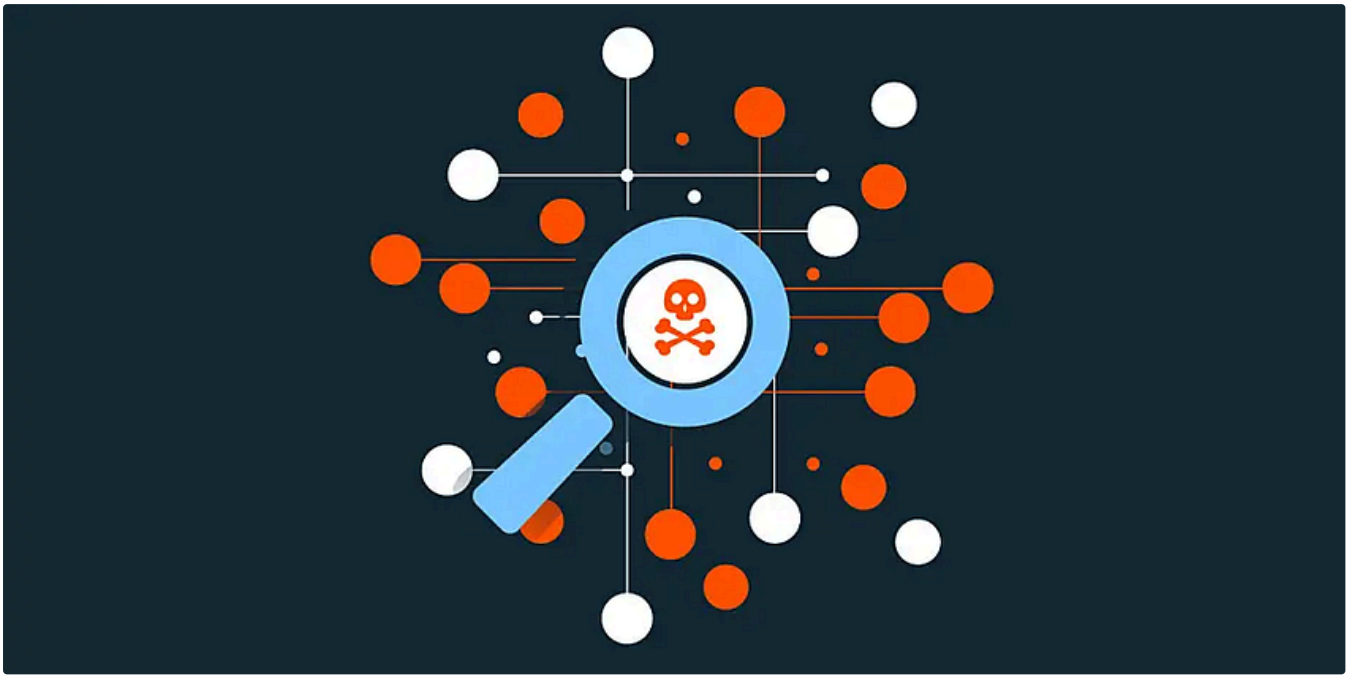
Cindy (Shunxian) Ou

TryHackMe: Windows Forensics 1—Detailed Write-Up

Windows is one of the most widely used operating systems, so it's likely that a significant portion of digital evidence in cybercrime...

8 min read · Nov 1, 2023

6



Retr0

TryHackMe |MAL: Researching Walkthrough|By Retr0

#Intro

6 min read · Oct 31, 2023

9

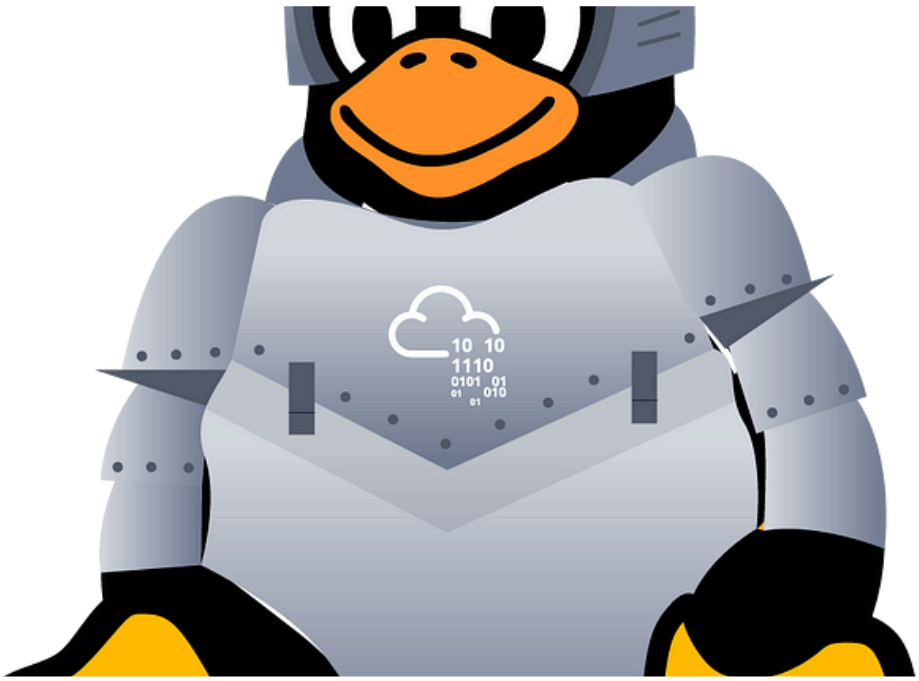
empise

TryHackMe—Tempest Writeup

This room aims to introduce the process of analysing endpoint and network logs from a compromised asset. Given the artefacts, we will aim...

12 min read · Jan 30, 2024

1



lshsome

TryHackMe- Bulletproof Penguin

Bulletproof plugin is an easy room which deals with hardening security on the common services that runs on a Linux machine. This room...

6 min read · Oct 29, 2023

16

See more recommendations