# CYBERSECURITY TASK

CTF in tryhackme website

## ✓ *Aim:-*

To tryout a basic and simple CTF in tryhackme as well as give the respective report

## ✓ *Room Information*

- Room name:- Lo-Fi
- Category :- Linux
- Difficulty :- Easy
- Link :- https://tryhackme.com/room/lofi

## ✓ *Summary*

Basically in this CTF it was mainly directed to simply find a flag by exploring through the rootsystem of the website.Here , I have used the inbuild attackbox of the tryhackme servere where the operations was performed.The CTF will only completed if we eneter the correct flag to the directed area in the tryhack me website.

## ✓ *Step by Step Exploration*

### 1.Machine starting and entering the attackbox

At the outset of the task in order to begin the CTF we need to start the machine only by this we will be given the IP address to explore through.After starting the machine and getting the IP address I have Started the Attackbaox which is a virtual machine box of tryhackme itself. By enabling the attackbox I have done the exploration batway by entering the IP address in it's Mozilla Setup.

## 2. Tasks in the bridge to find flag

After entering the IP address I have checked through the various parameters in the website to get that almost pathway to the CTF. Furthermore, By clicking the key word called ‘relax’ on the specification part I have obtained a change in the URL section of the bar. From here when I checked at the guidelines of CTF it is mentioned as the flag may be present in the rootsystem and you can go through the concept of LFI path traversal and File inclusion to get the flag.

## 3. Going through the serch process

After searching and going through a lot in this LFI anfd file inclusions, I got to know a specific kind of url in the LFI website whose format is similar to the kind of existing in my website when clicked on relax.

It’s format was :-

http://example.com/index.php?file=../../../../../etc/passwd

This literally exphasis Local File Inclusion (LFI) is a web vulnerability where an attacker tricks a website into loading files from the server by tampering with URL parameters like file=. By using directory traversal (e.g., ../../), they can access sensitive files such as /etc/passwd on Linux systems. This helps attackers gather system info, view source code, or even execute malicious scripts in some cases. LFI is commonly seen in CTFs and real-world hacking scenarios to gain deeper access into a server.

## 4. Changing the url’s

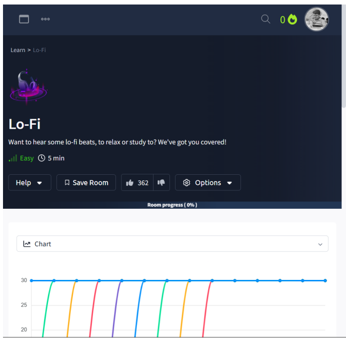
By establishing this format in URL we have obstained root storage mode in a paragraph manner.So by trying out various txt formar in the ‘ etc/passwd ‘ section I got a knowledge we can crack the flag.

## 5. Cracking the flag

Finally by entering the txt format keyword ‘flag.txt’ I have successfully cracked the flag and got the output.

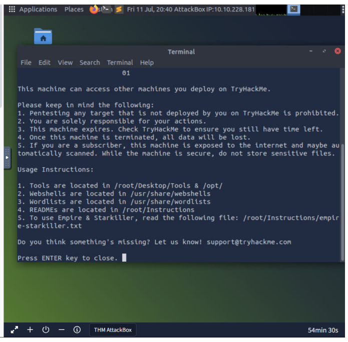
Obviously, I have refered certain other platforms also to know how to crack this flag and understand ctf manner working.

## ✓ *Images Of my works*

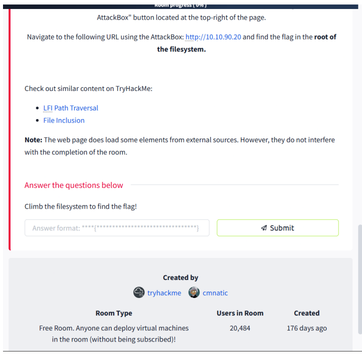

Learn > Lo-Fi

Lo-Fi

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



```
                      01

This machine can access other machines you deploy on TryHackMe.

Please keep in mind the following:
1. Pentesting any target that is not deployed by you on TryHackMe is prohibited.
2. You are solely responsible for your actions.
3. This machine expires. Check TryHackMe to ensure you still have time left.
4. Once this machine is terminated, all data will be lost.
5. If you are a subscriber, this machine is exposed to the internet and maybe au
tomatically scanned. While the machine is secure, do not store sensitive files.

Usage Instructions:

1. Tools are located in /root/Desktop/Tools & /opt/
2. Webshells are located in /usr/share/webshells
3. Wordlists are located in /usr/share/wordlists
4. READMEs are located in /root/Instructions
5. To use Empire & Starkiller, read the following file: /root/Instructions/empir
e-starkiller.txt

Do you think something's missing? Let us know! support@tryhackme.com

Press ENTER key to close.
```


AttackBox" button located at the top-right of the page.

Navigate to the following URL using the AttackBox: http://10.10.90.20 and find the flag in the **root of the filesystem.**

Check out similar content on TryHackMe:

- LFI Path Traversal
- File Inclusion

**Note:** The web page does load some elements from external sources. However, they do not interfere with the completion of the room.

Answer the questions below

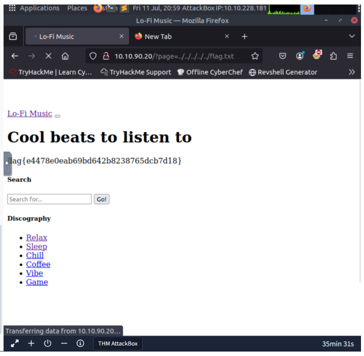
Climb the filesystem to find the flag!

Answer format: ****{********************************}

Created by

tryhackme cmnatic

| Room Type | Users in Room | Created |
|---|---|---|
| Free Room. Anyone can deploy virtual machines in the room (without being subscribed)! | 20,484 | 176 days ago |



10.10.90.20/?page=../../../../../flag.txt

Lo-Fi Music

### Cool beats to listen to

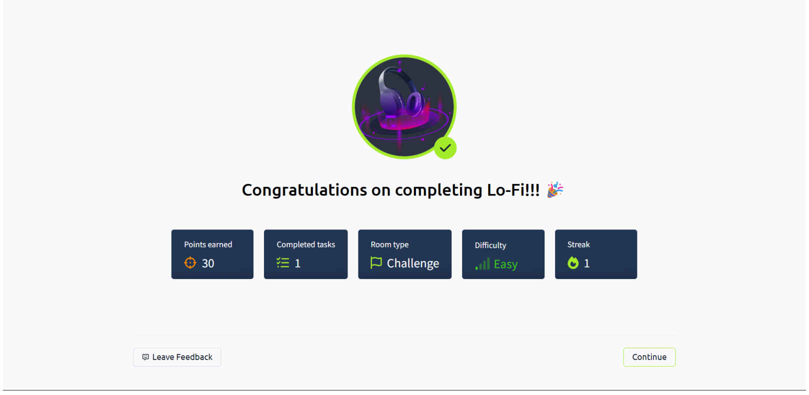
lag{e4478e0eab69bd642b8238765dcb7d18}

**Search**

Search for... Go!

**Discography**

- Relax
- Sleep
- Chill
- Coffee
- Vibe
- Game


Congratulations on completing Lo-Fi!!! 🎉

| Points earned | Completed tasks | Room type | Difficulty | Streak |
|---|---|---|---|---|
| 30 | 1 | Challenge | Easy | 1 |