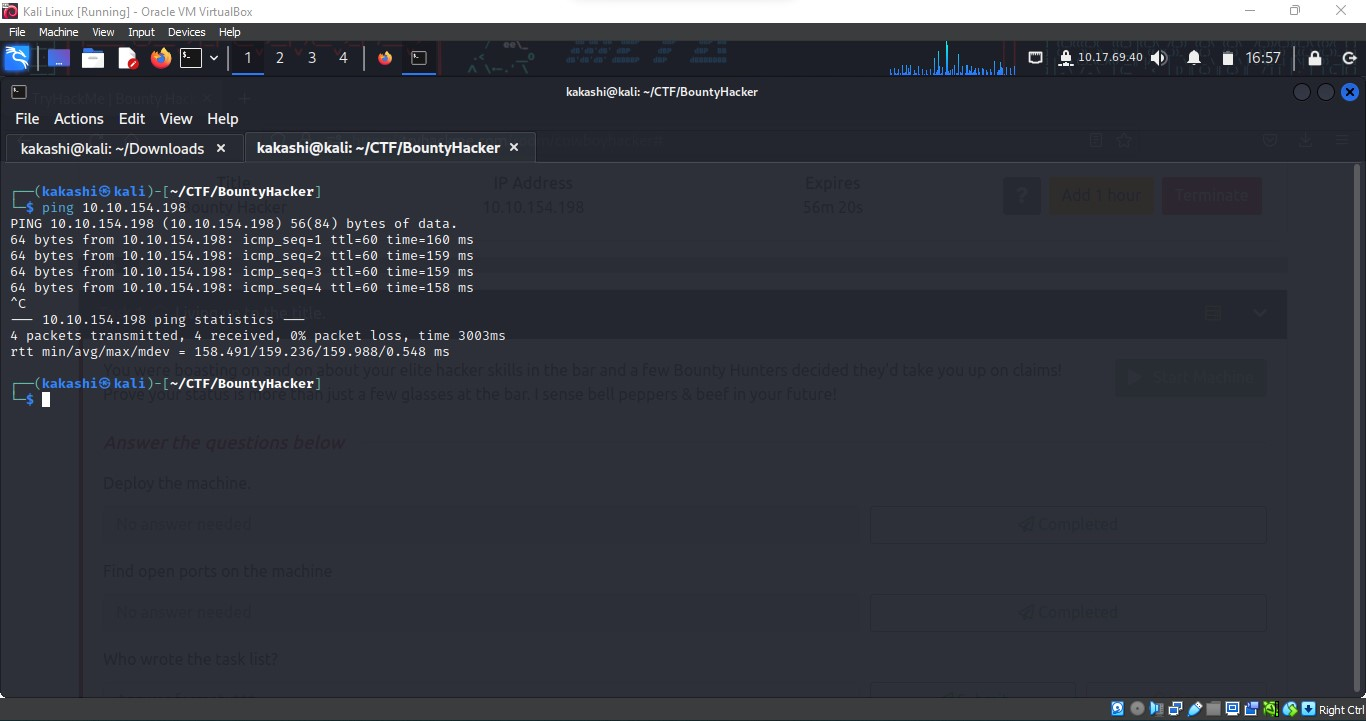
CTF Writeups

Try Hack Me

Bounty Hacker

Step 1: Deploy the Machine and check the Connectivity with the Target Machine using

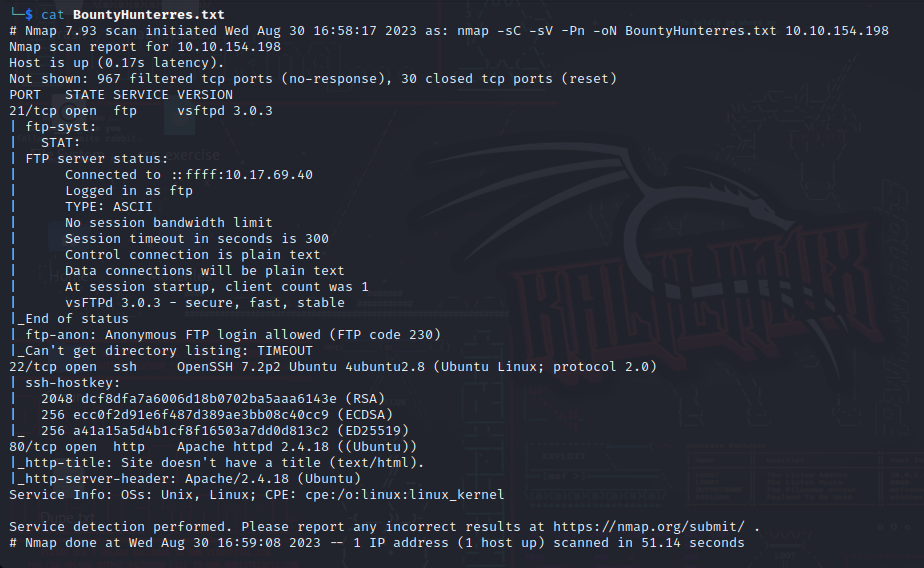
**Ping** command.



Step 2: As usual for footprinting and Information Gathering, The First Step is to find open ports in the target machine.

sudo nmap -sC -sV -Pn -oN result.txt `target-ip`

-sC Script Scan it will check for vulnerability for a specific service for example in port 21 ftp will be running it will run script associated to ftp to check whether there is vulnerability or not, In this case ftp anonymous login vulnerability is found.

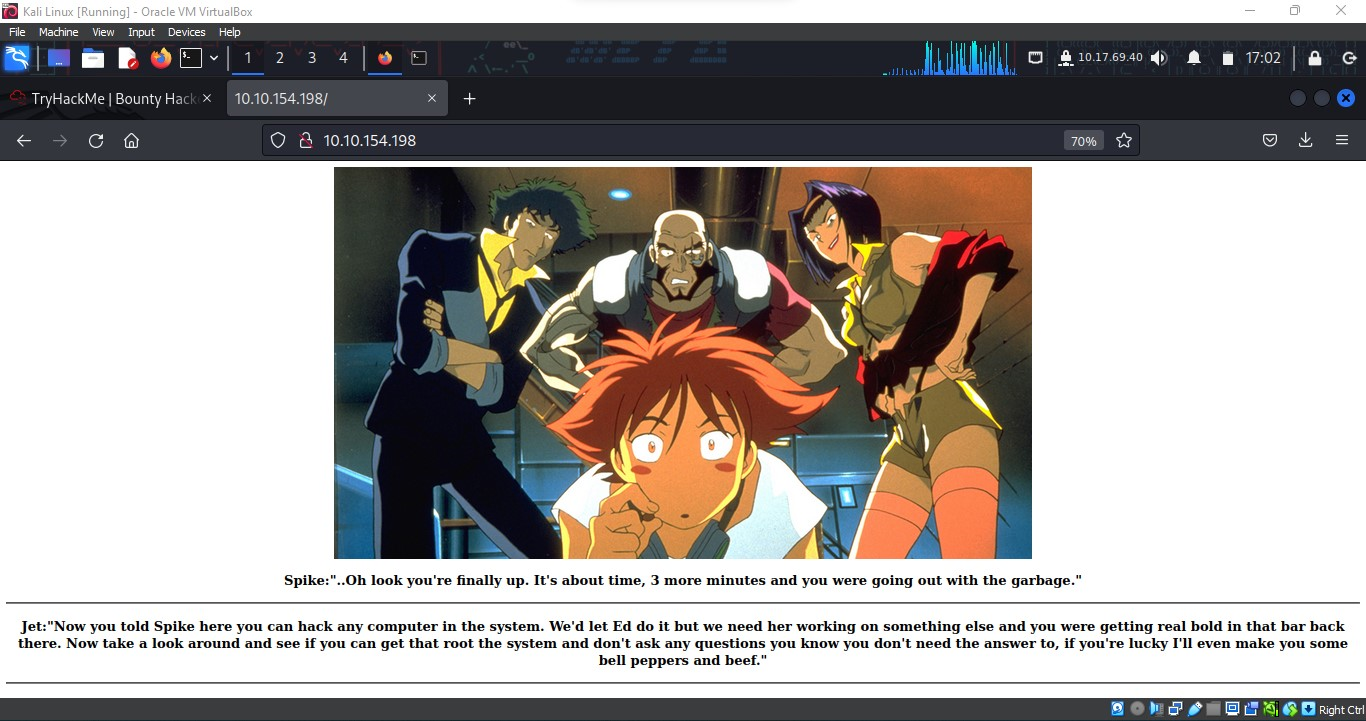


Step 3:

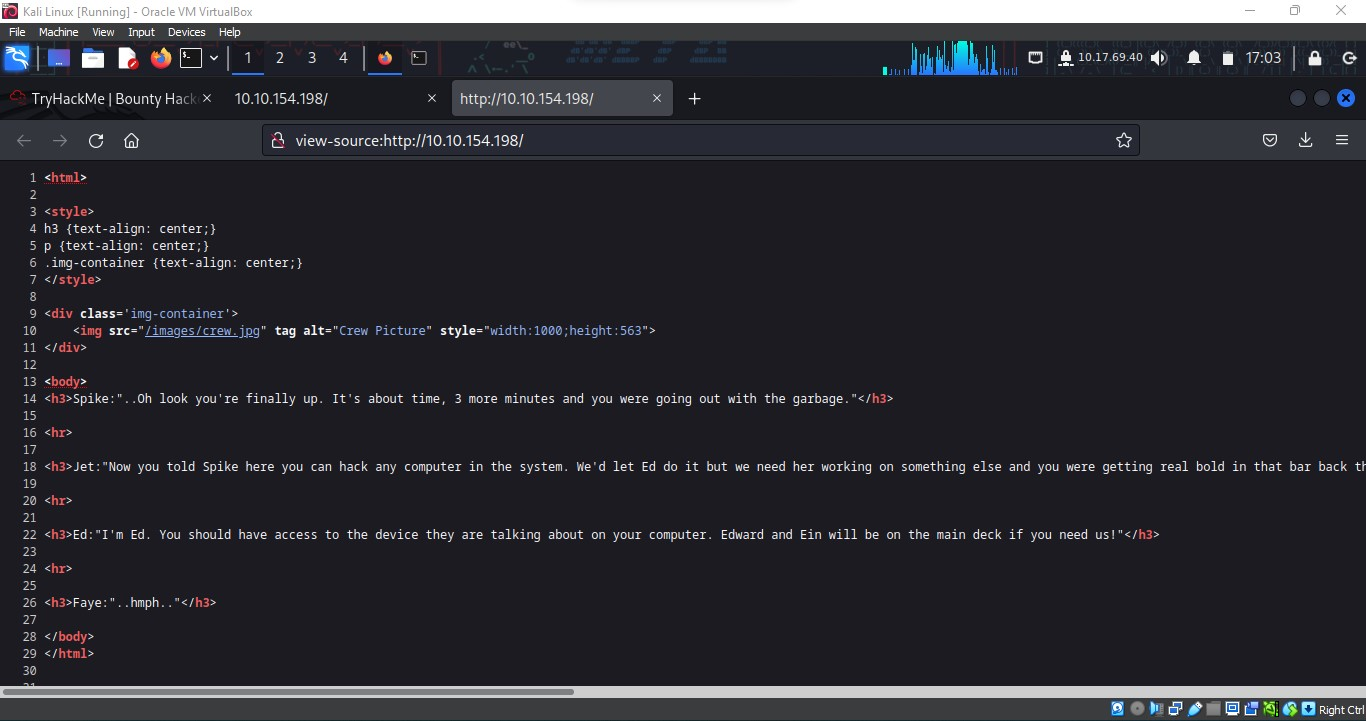
We found that port 21,22,80 are open.

For SSH we need username and password that is now available as of now.

Next we can inspect port 80 by typing the IP Address in the browser.



Inspecting the Page Source:



There is no sufficient information in Port 80, One thing i missed is the Directory Enumeration.

Then we left with Only one Option FTP.

Step 4:

FTP login with Username anonymous

Affer FTP Login we found 2 files locks.txt and task.txt

Download those 2 files to our local system and inspect it

To download a file from FTP server to our local system we can use **get** command.

get locks.txt

get task.txt

Step 5:

Task.txt file contains a message and a username (lin) that can be used for ssh login.

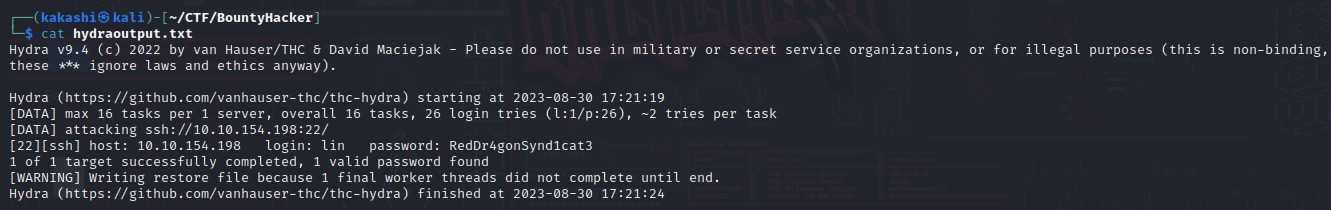
Locks.txt file contains a password list that we can use to bruteforce

lin username.

Step 6:

Using **hydra** tool to bruteforce password.

hydra -l lin -P /directory/locks.txt



We found the credentials for ssh login:

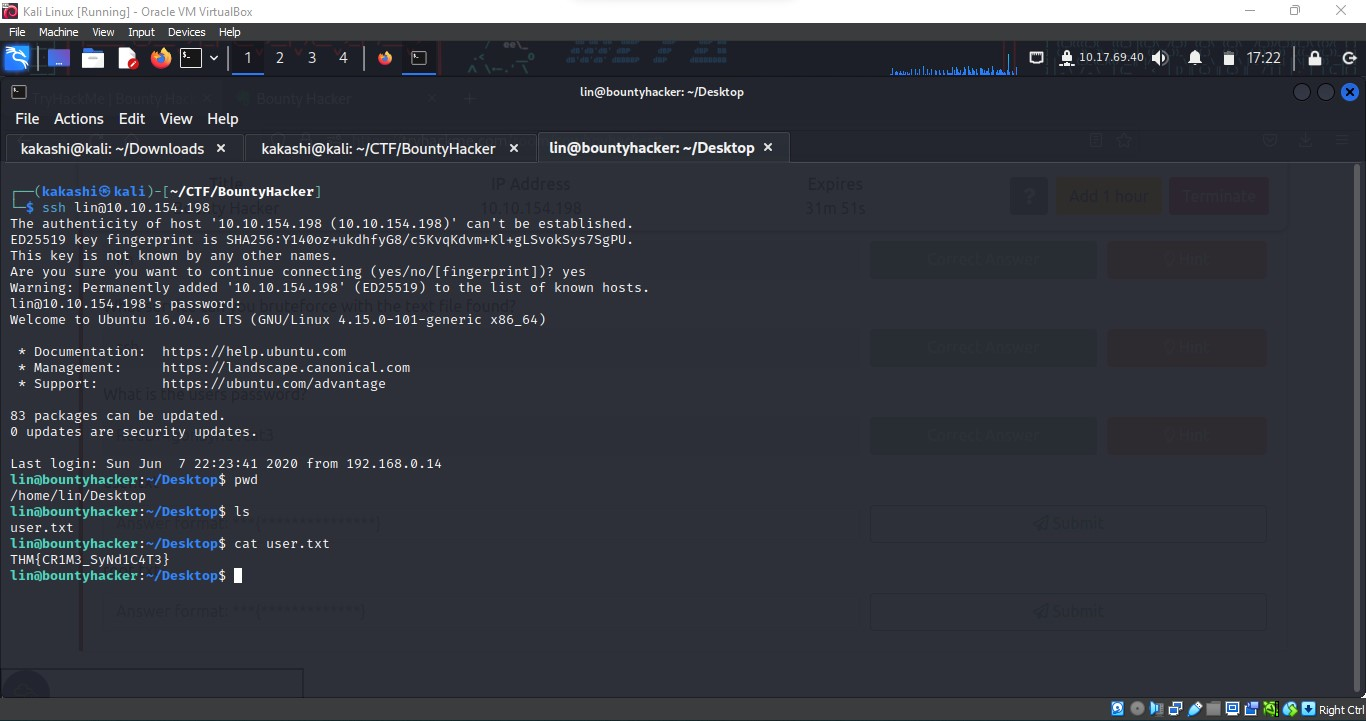
Lin : RedDr4gonSynd1cat3

Step 7:

SSH Login with the Obtained Credentials

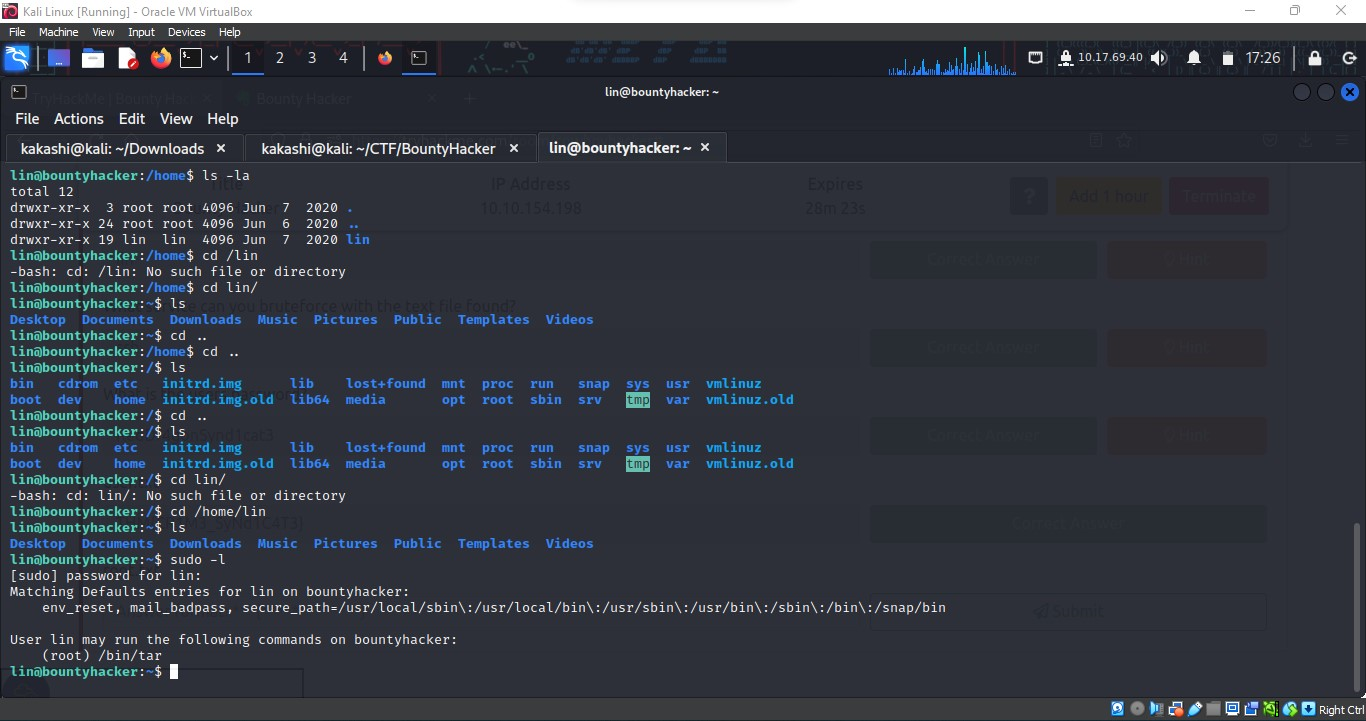


While Inspecting the files in the Directory we found user.txt flag



The Remaining thing is to find root.txt flag, For that we need to do Previlege Escalation to root account.

To check Current User permission type **sudo -l**

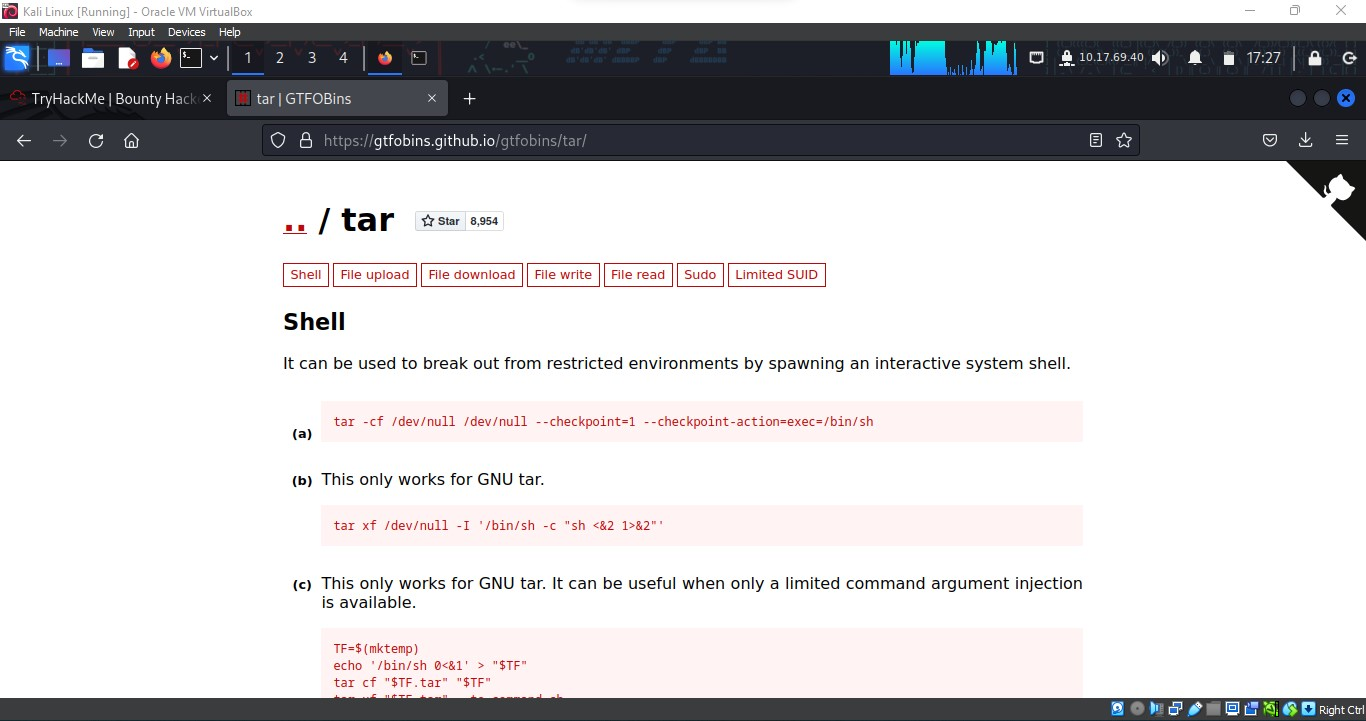


We found that the current user lin can use root privileges for the **tar** command.

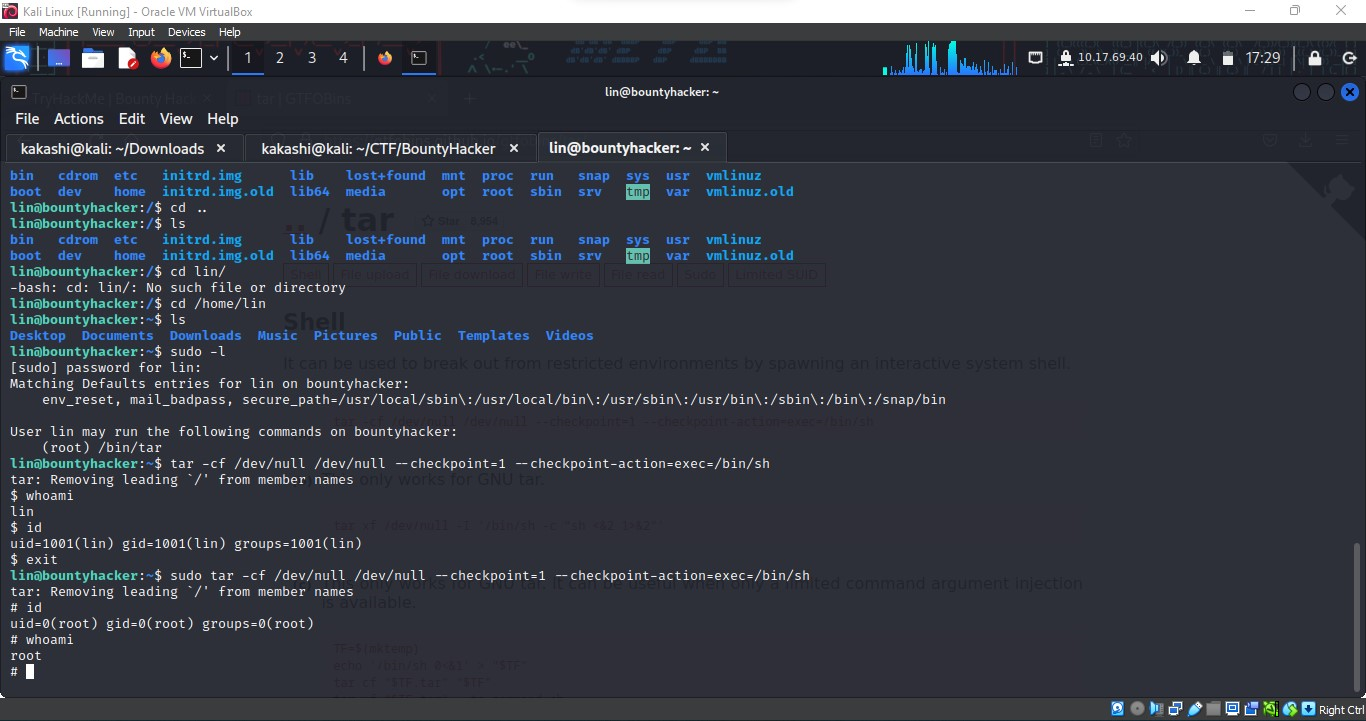
We need to exploit the above vulnerability to gain root shell.

To exploit a vulnerability in a command we can refer **GTFOBIN** website.

GTFobin is a website that lists various Unix-like operating system commands that can be used to escalate privileges or bypass security restrictions. It provides examples and explanations on how to use these commands to gain unauthorized access or perform other malicious activities.



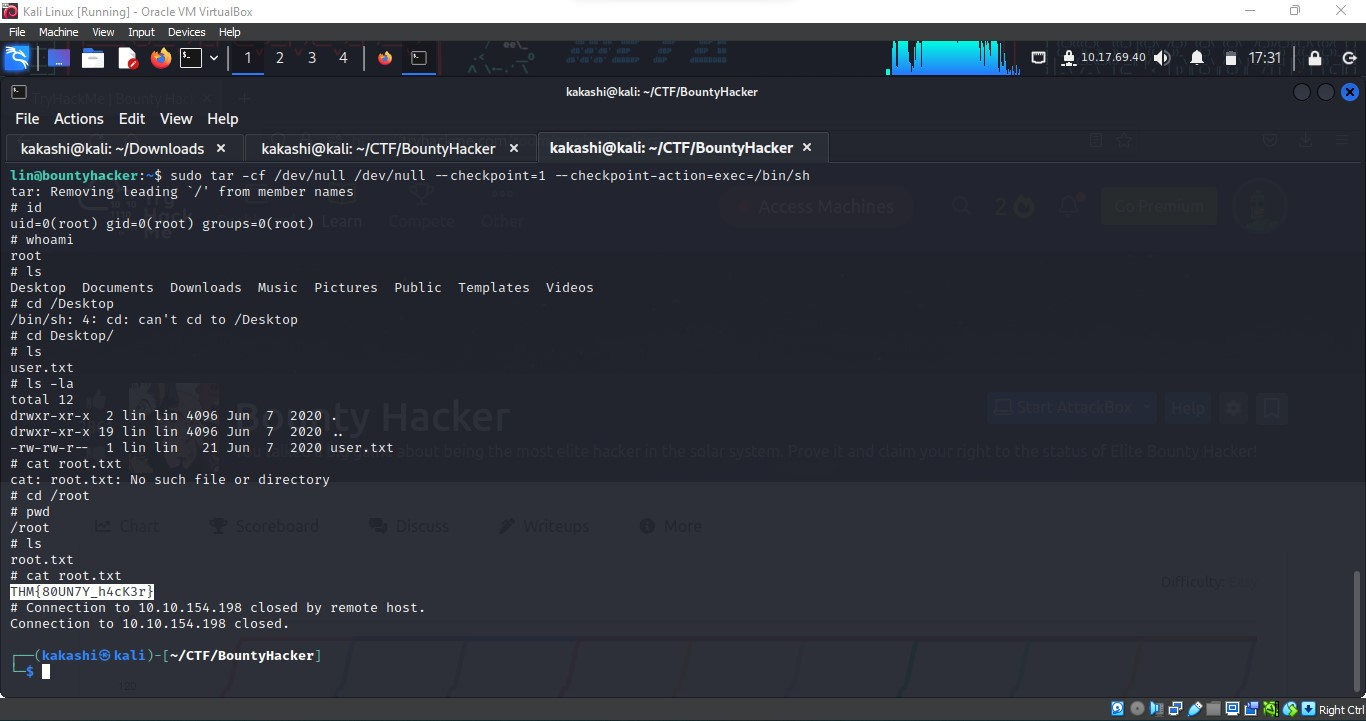
By entering the above mentioned sudo command for tar we can get root shell



We entered the root shell, our final goal is to find the root.txt flag. That can be found in the root directory that can be accessed by the following command

**cd root**

**cat root.txt**



We found both the flag.