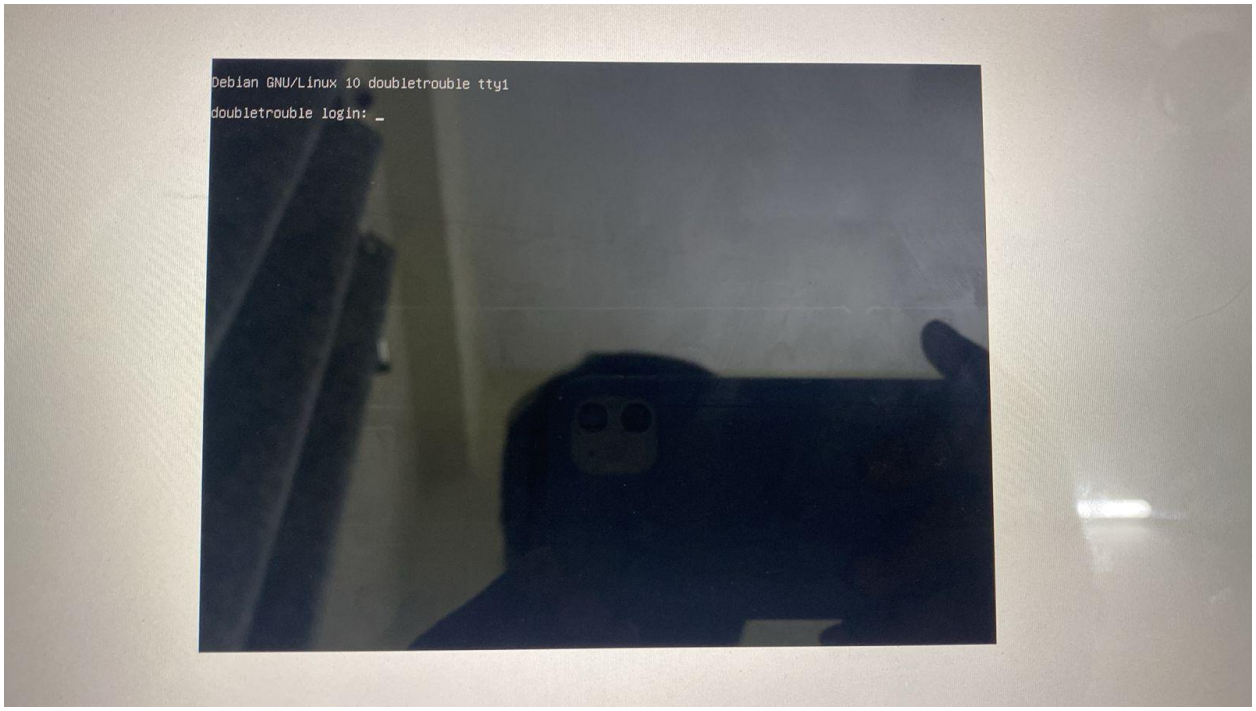
CTF = CATCH THE FLAG
DOUBLETROUBLE machine

exploiting the doubletrouble machine

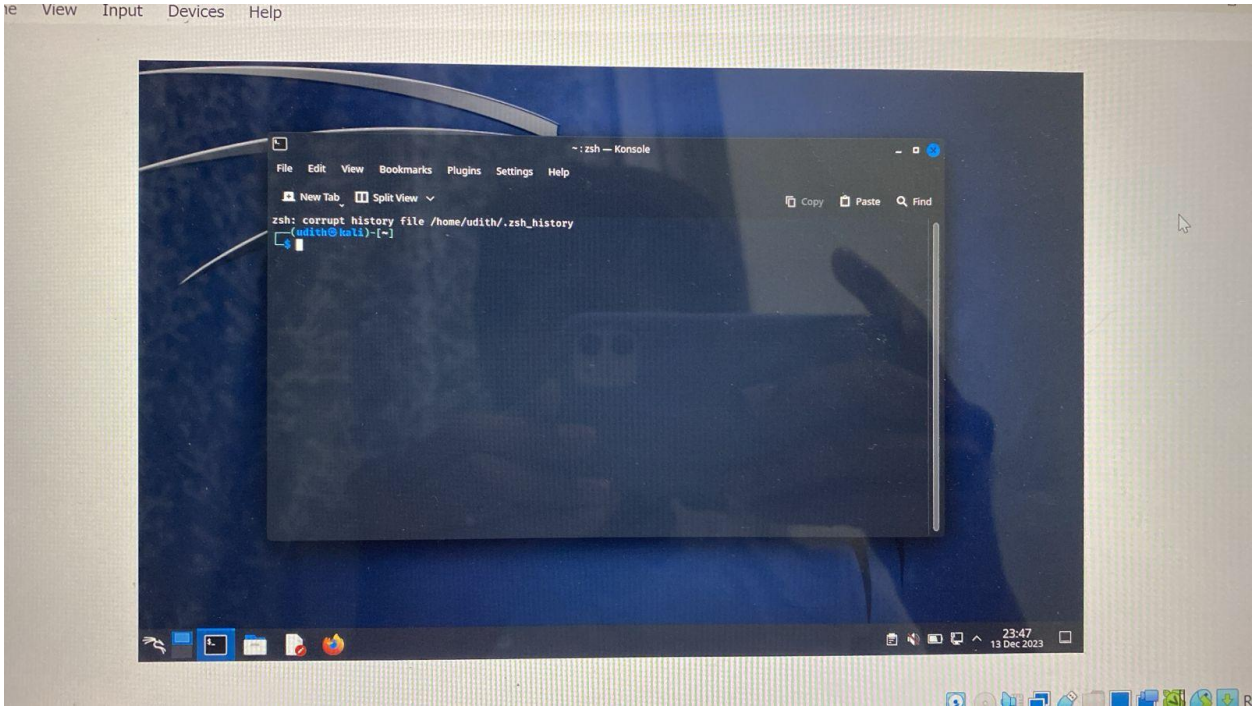
steps
1:Getting the target machine IP address by using Netdiscover
2:Getting open port details by using the Nmap tool
3:Identifying vulnerabilities in running web applications
4:Enumerating applications with Drib utility
5:Cracking password with StegCracker

Download the Doubletrouble machine from the vulnhub.com and import in the virtual machine and the set the network to NAT and also check that the attacker machine also in NAT

After the importing start the virtual machine

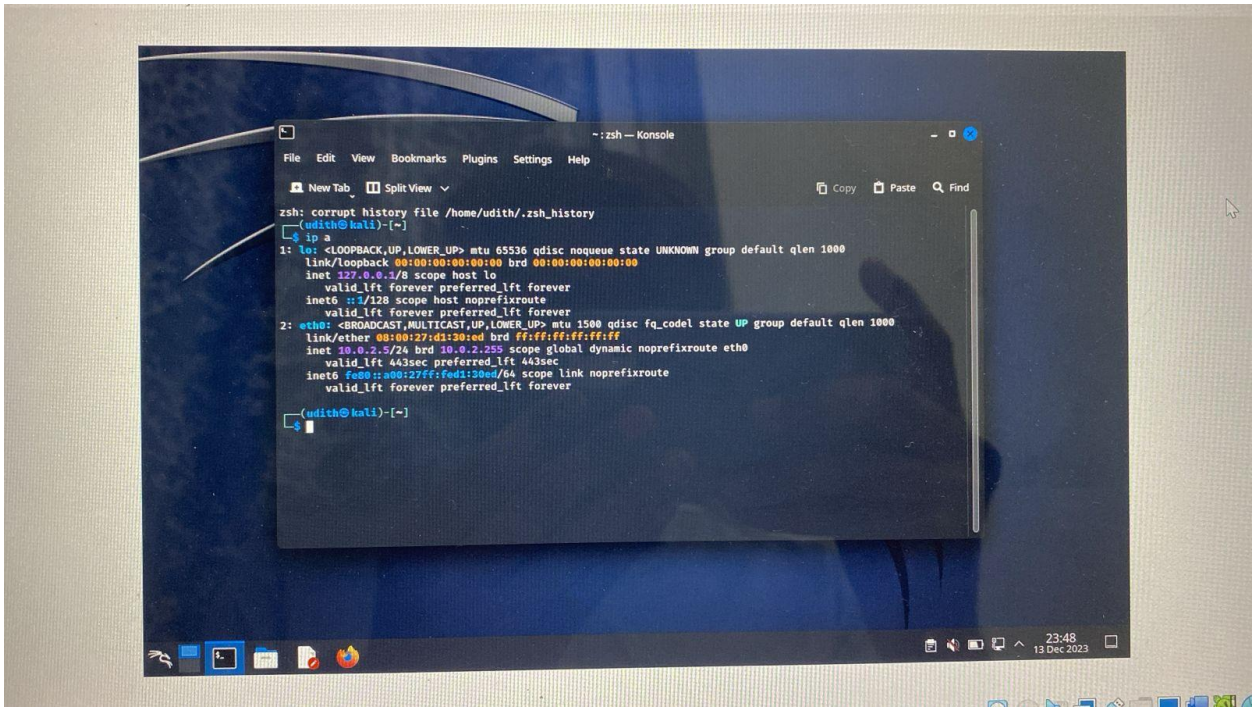


open the terminal in kali

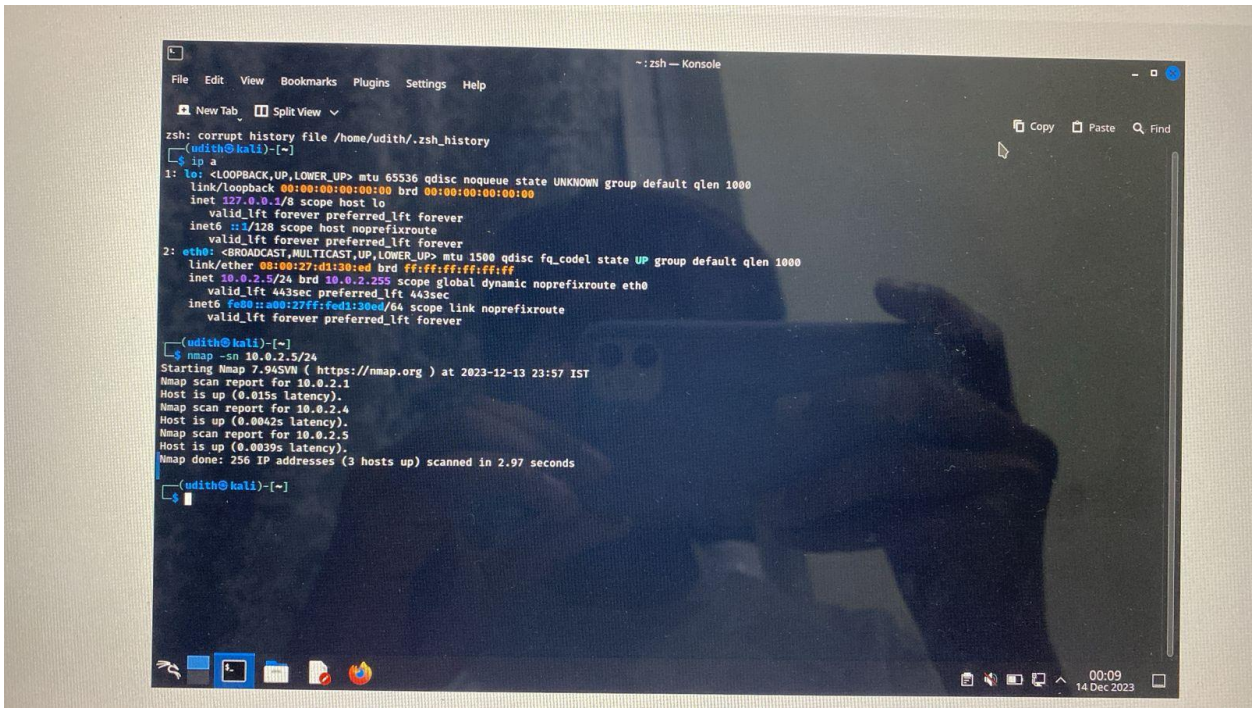


Step 1
GETTING THE TARGET MACHINE IP ADDRESS BY USING NETDISCOVER

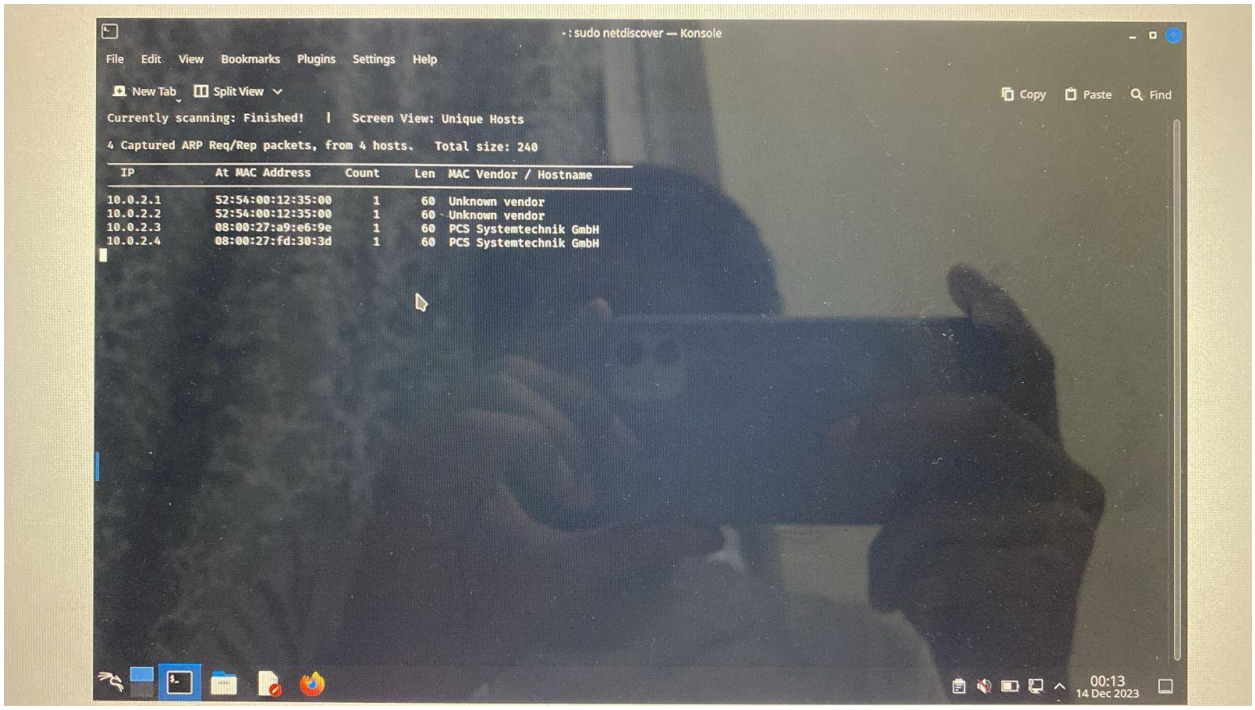
Firstly we need to get the attacker IP address
Execute common “ip a”



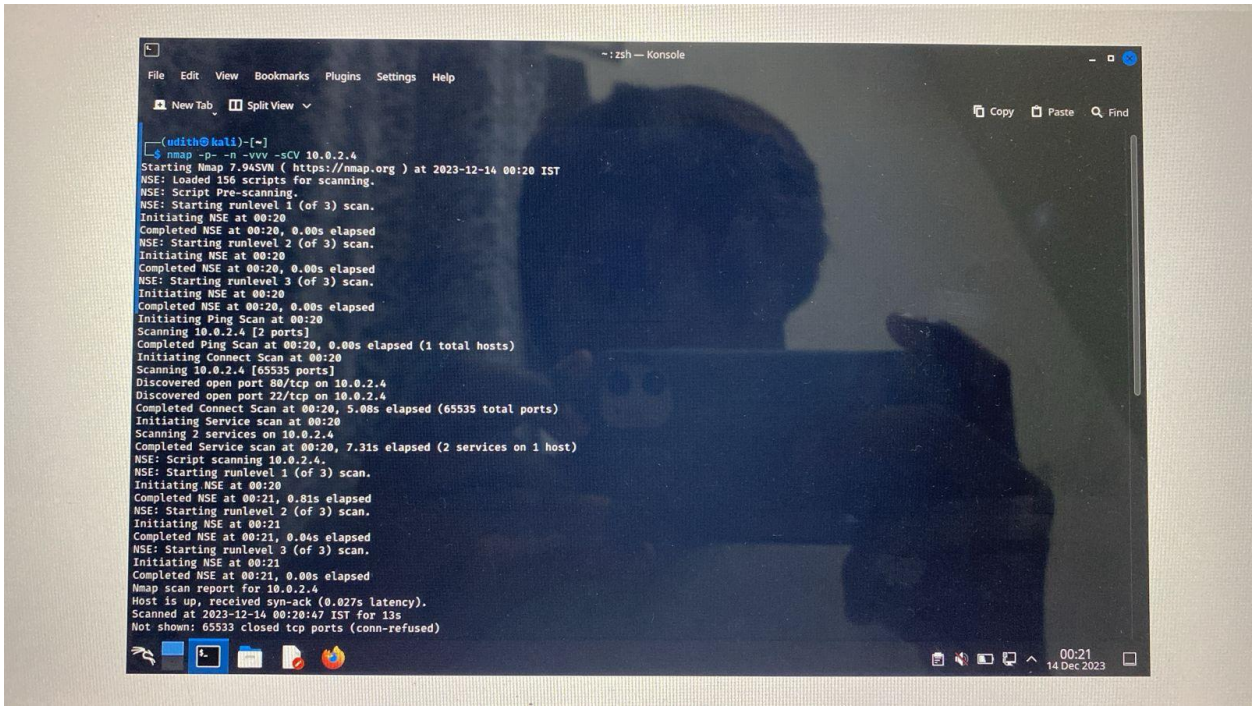
The machine is in the eth0 interface and the IP address is 10.0.2.5
Next move is to find the target machine IP address by using the nmap and netdiscover we can get target machine IP address
Execute the command
“nmap -sn 10.0.2.5”
Where -sn is the ping scan flag
The result is

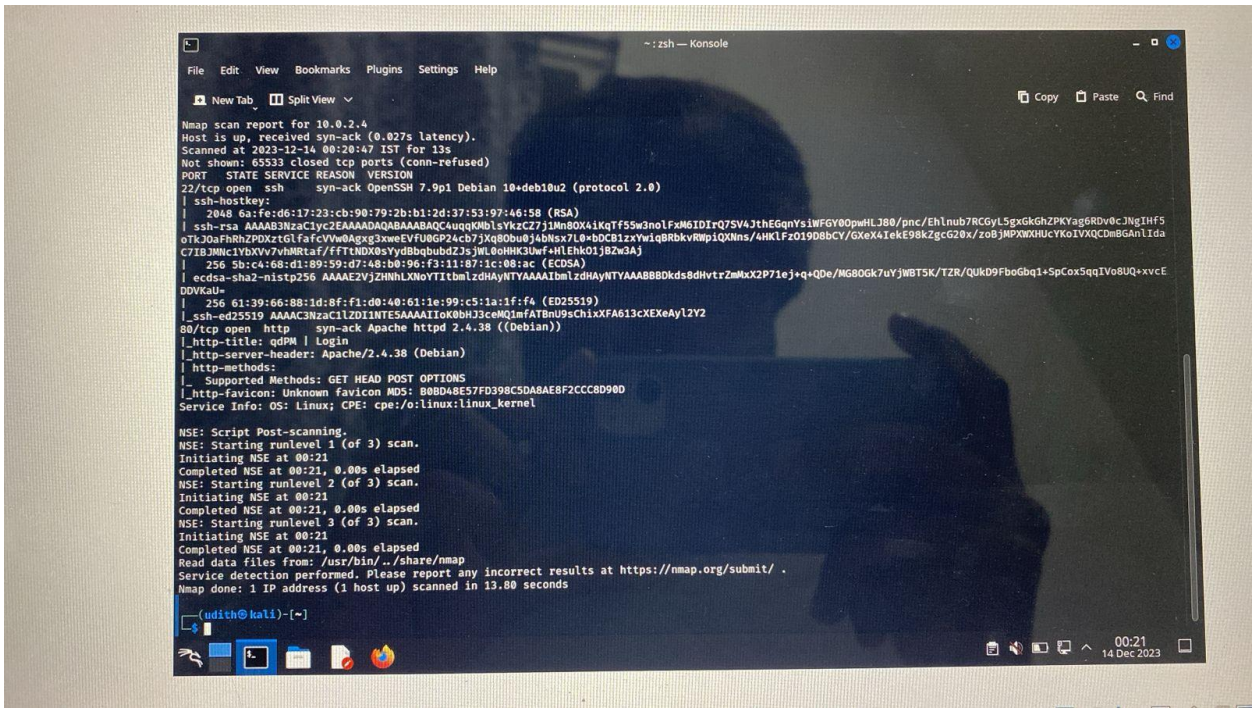


And the another method in is the NETDISCOVER
Execute command “sudo netdiscover -i eth0 -r 10.0.2.5/24”
Flag -i is the interface flag
-r the attacker ip address
After the execution it will ask the password enter the kali password
We get the target machine ip address



The target machine ip address is 10.0.2.4
After getting the target machine ip address the next step is
Step 2: GETTING THE OPEN PORT DETAILS BY USING THE NMAP TOOL
Getting the open port details on the machine
Execute the command
“nmap -p- -n -vvv -sCV 10.0.2.4”
Where flag -p- is for scan all ports
-n for do not resolve for dns(domain name system)
-vvv for verbosity it is used to get the open ports quickly
-sCV for default scripts and v for the version detection scan
The result is





By this nmap port scan we can know that there are 2 open ports one is 80 which is a http port and second is 22 port which is ssh port which is a security port

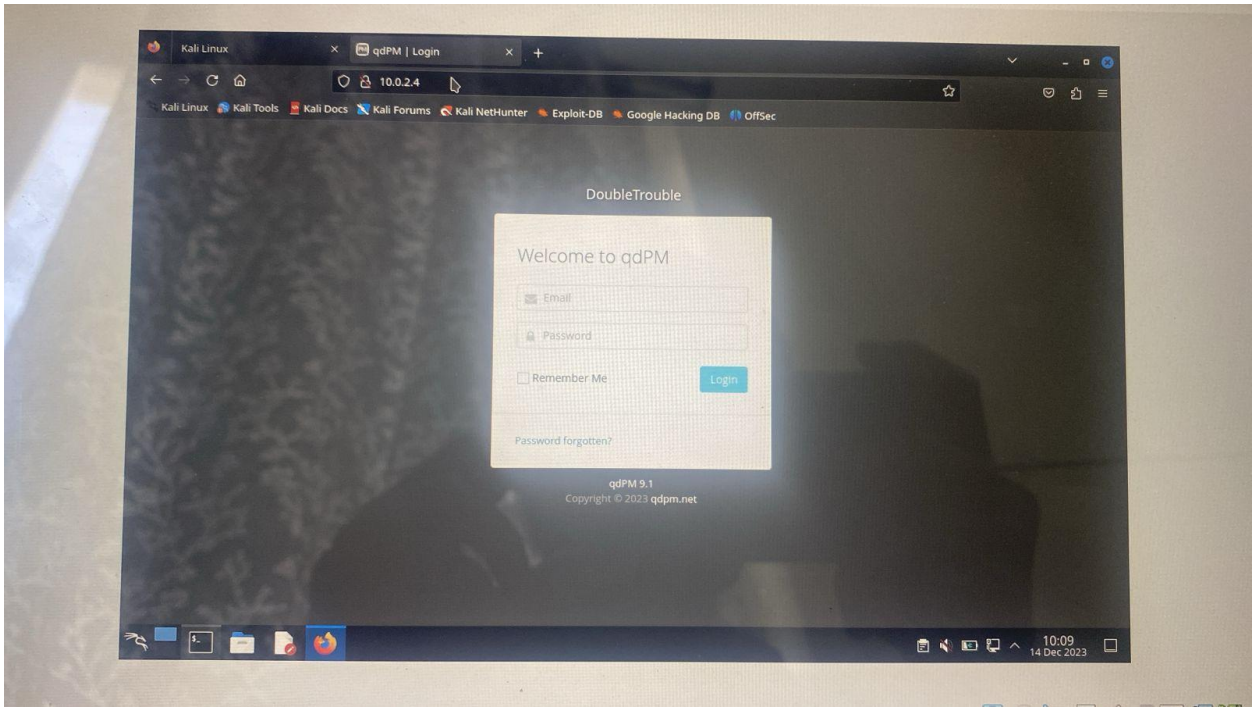
Next step is

Step 3:IDENTIFYING VULNERABILITIES IN RUNNING WEB PAGE

Where the port 80 is the http port so open browser in the kali and search about the ip address

When i search the http://10.0.2.4/ i get a welcome to qdpm login page

And it has the vulnerability that it is showing error in the username when we enter the wrong user

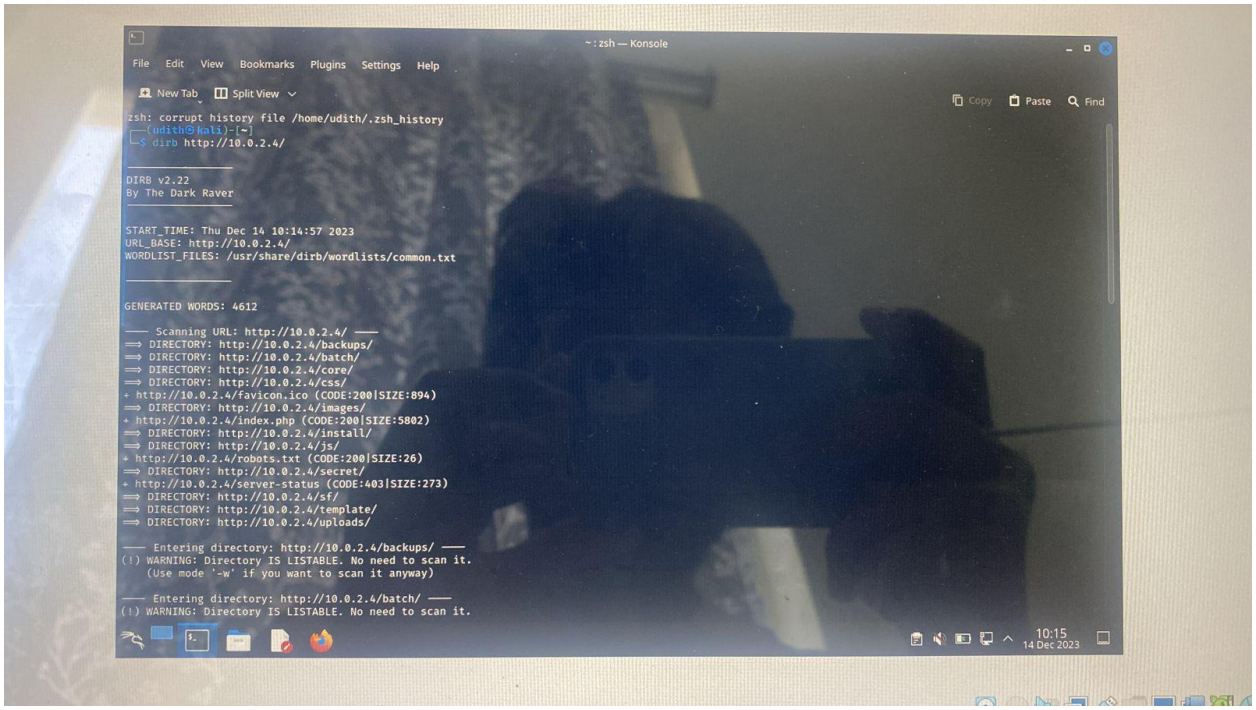


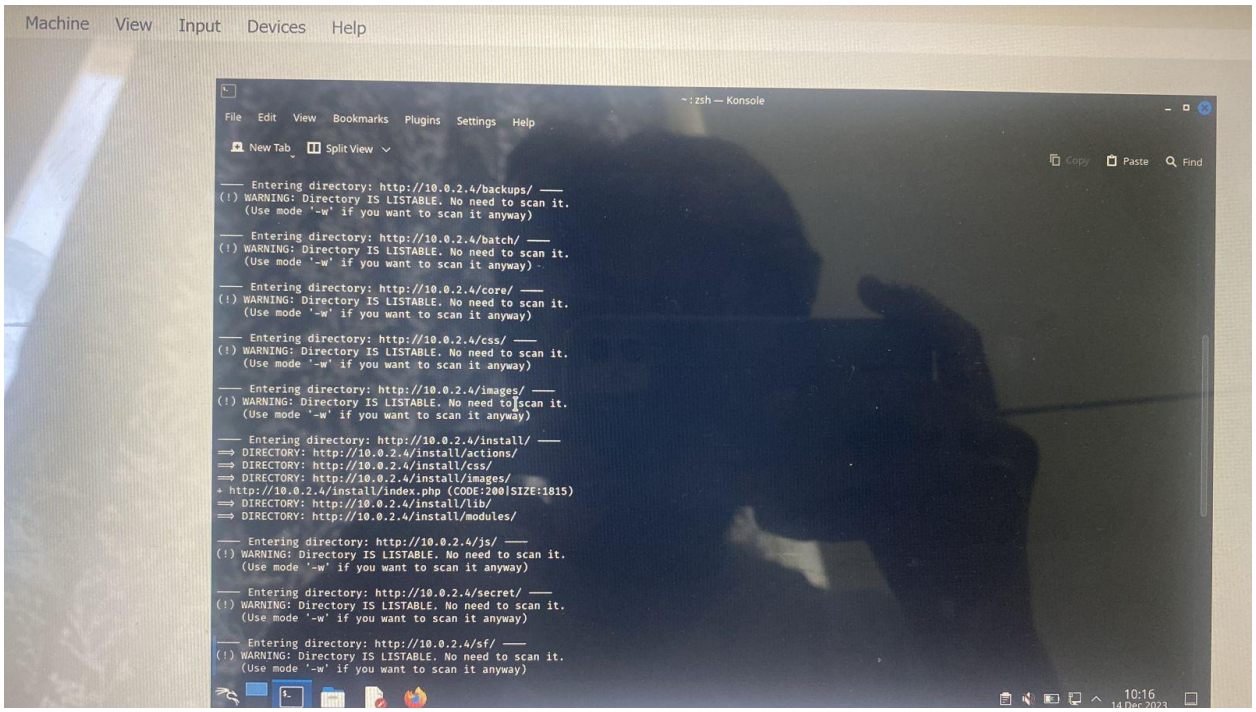
And the next step is

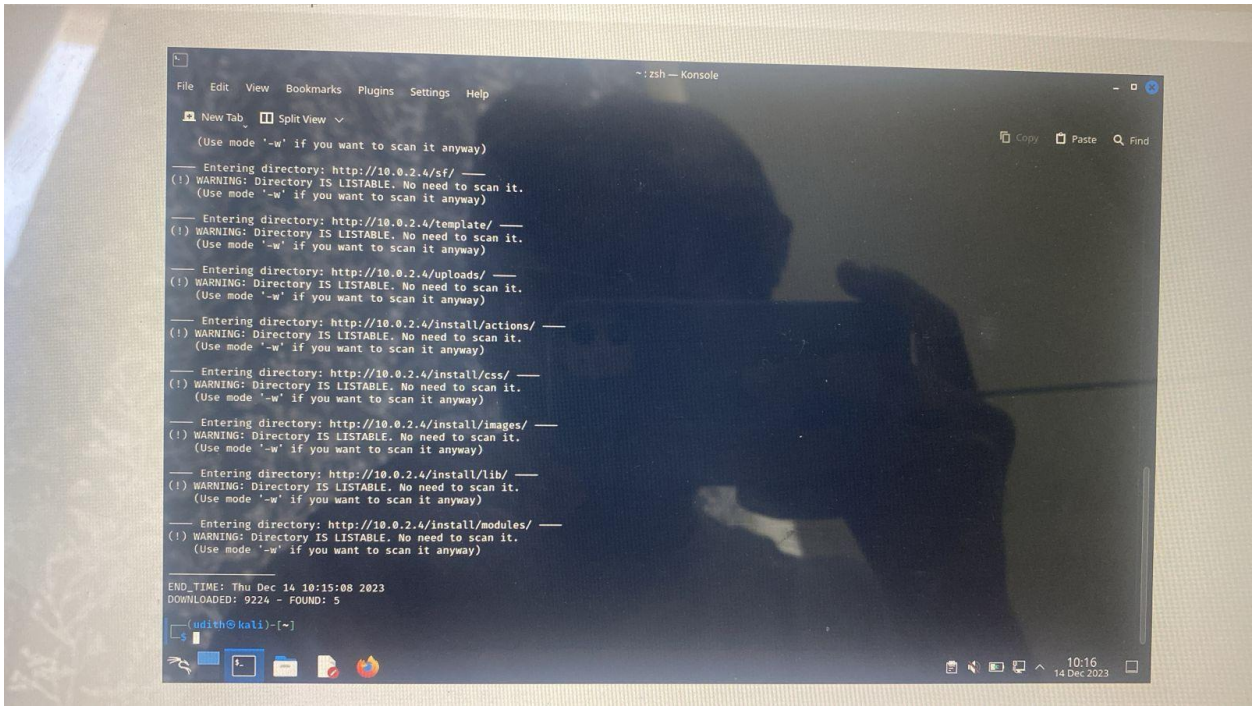
Step 4:ENUMERATING APPLICATION WITH DIRB UTILITY

It is directory brute force method which helps to get the find hidden or unprotected directories and files on web server

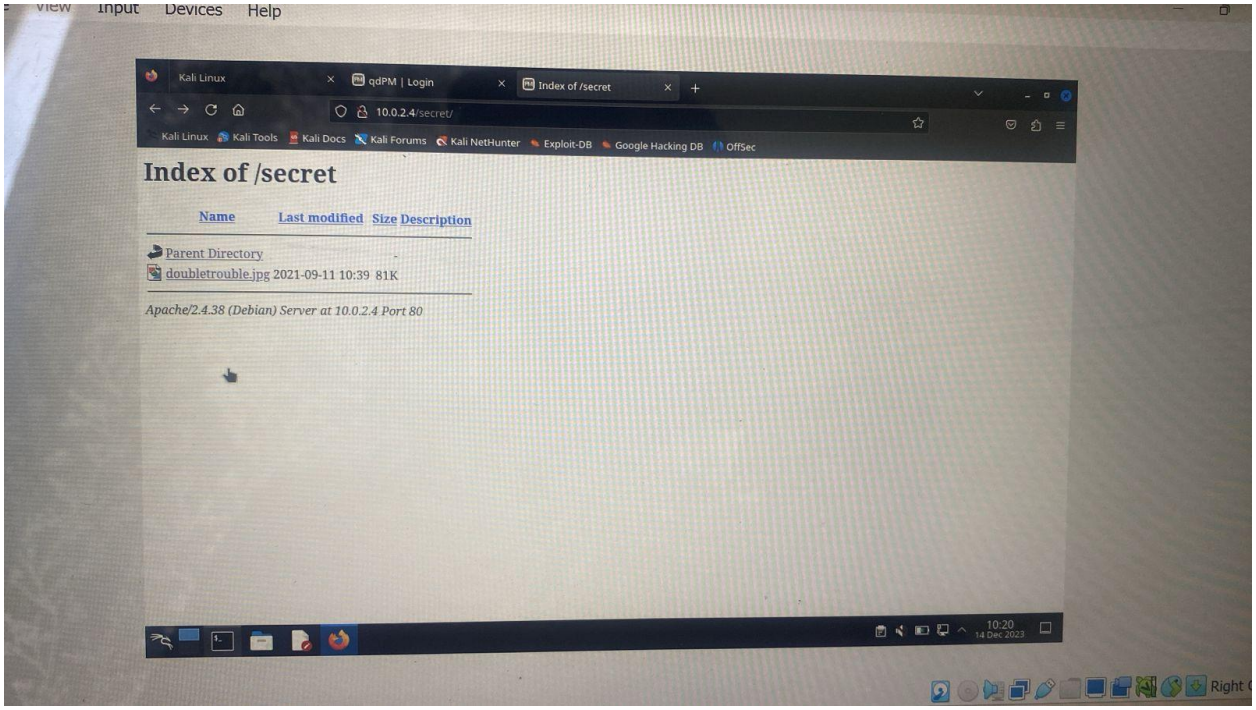
Execute the command “dirb http://10.0.2.4/”

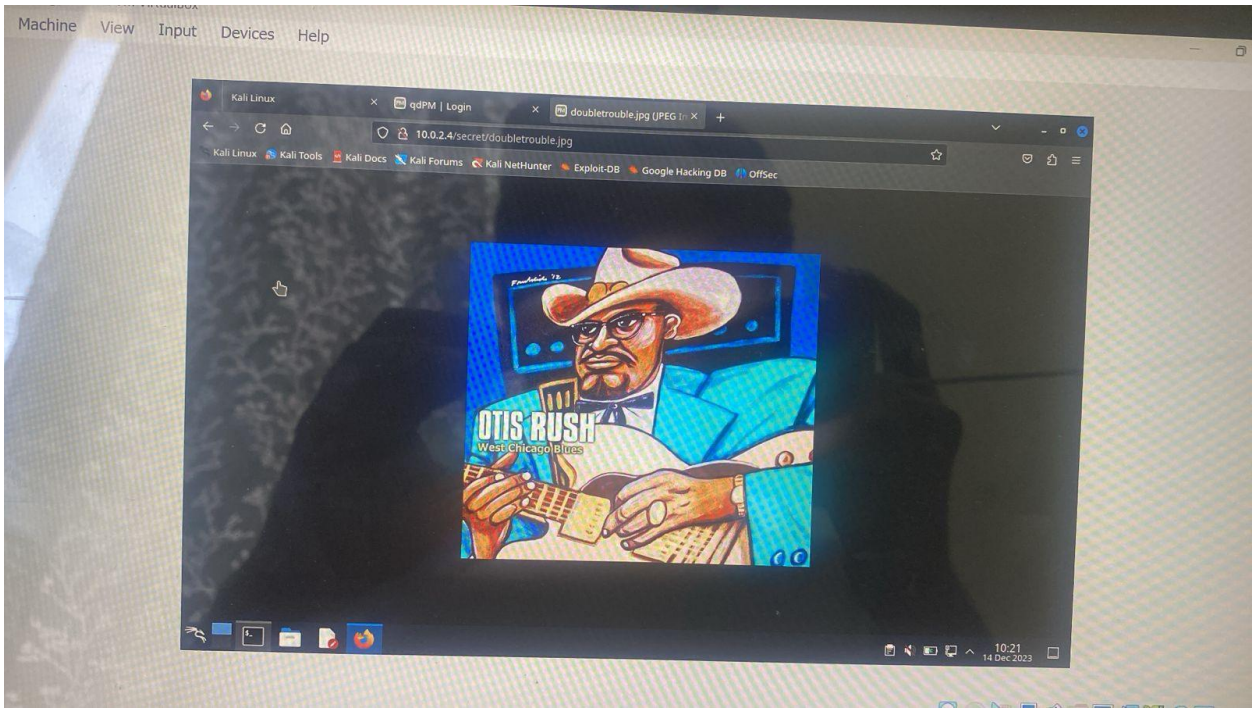

~ : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
zsh: corrupt history file /home/udith/.zsh_history
┌──(udith㉿kali)-[~]
└─$ dirb http://10.0.2.4/
DIRB v2.22
By The Dark Raver
START_TIME: Thu Dec 14 10:14:57 2023
URL_BASE: http://10.0.2.4/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
GENERATED WORDS: 4612
---- Scanning URL: http://10.0.2.4/ ----
==> DIRECTORY: http://10.0.2.4/backups/
==> DIRECTORY: http://10.0.2.4/batch/
==> DIRECTORY: http://10.0.2.4/core/
==> DIRECTORY: http://10.0.2.4/css/
+ http://10.0.2.4/favicon.ico (CODE:200|SIZE:894)
==> DIRECTORY: http://10.0.2.4/images/
+ http://10.0.2.4/index.php (CODE:200|SIZE:5802)
==> DIRECTORY: http://10.0.2.4/install/
==> DIRECTORY: http://10.0.2.4/js/
+ http://10.0.2.4/robots.txt (CODE:200|SIZE:26)
==> DIRECTORY: http://10.0.2.4/secret/
+ http://10.0.2.4/server-status (CODE:403|SIZE:273)
==> DIRECTORY: http://10.0.2.4/sf/
==> DIRECTORY: http://10.0.2.4/template/
==> DIRECTORY: http://10.0.2.4/uploads/
---- Entering directory: http://10.0.2.4/backups/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://10.0.2.4/batch/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
10:15
14 Dec 2023


Machine View Input Devices Help
~ : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
---- Entering directory: http://10.0.2.4/backups/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://10.0.2.4/batch/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://10.0.2.4/core/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://10.0.2.4/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://10.0.2.4/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://10.0.2.4/install/ ----
==> DIRECTORY: http://10.0.2.4/install/actions/
==> DIRECTORY: http://10.0.2.4/install/css/
==> DIRECTORY: http://10.0.2.4/install/images/
+ http://10.0.2.4/install/index.php (CODE:200|SIZE:1815)
==> DIRECTORY: http://10.0.2.4/install/lib/
==> DIRECTORY: http://10.0.2.4/install/modules/
---- Entering directory: http://10.0.2.4/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://10.0.2.4/secret/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://10.0.2.4/sf/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
10:16
14 Dec 2023

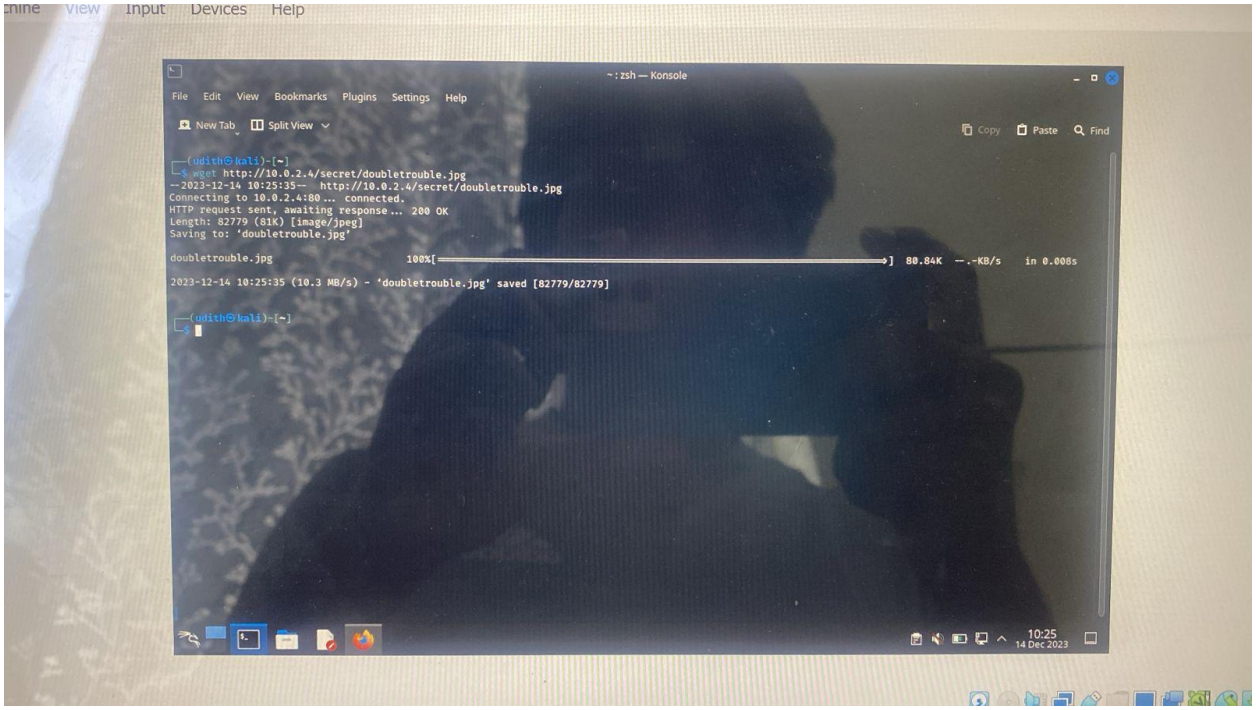


After getting the hidden or unprotected directories
We explore the website and directories in the browser and find the important information which will help to login
There is a website interesting directory that http://10.0.2.4/secret/
Open this directory in the browser
In this directory we found a interesting image which is named with the machine name called doubletrouble.jpg

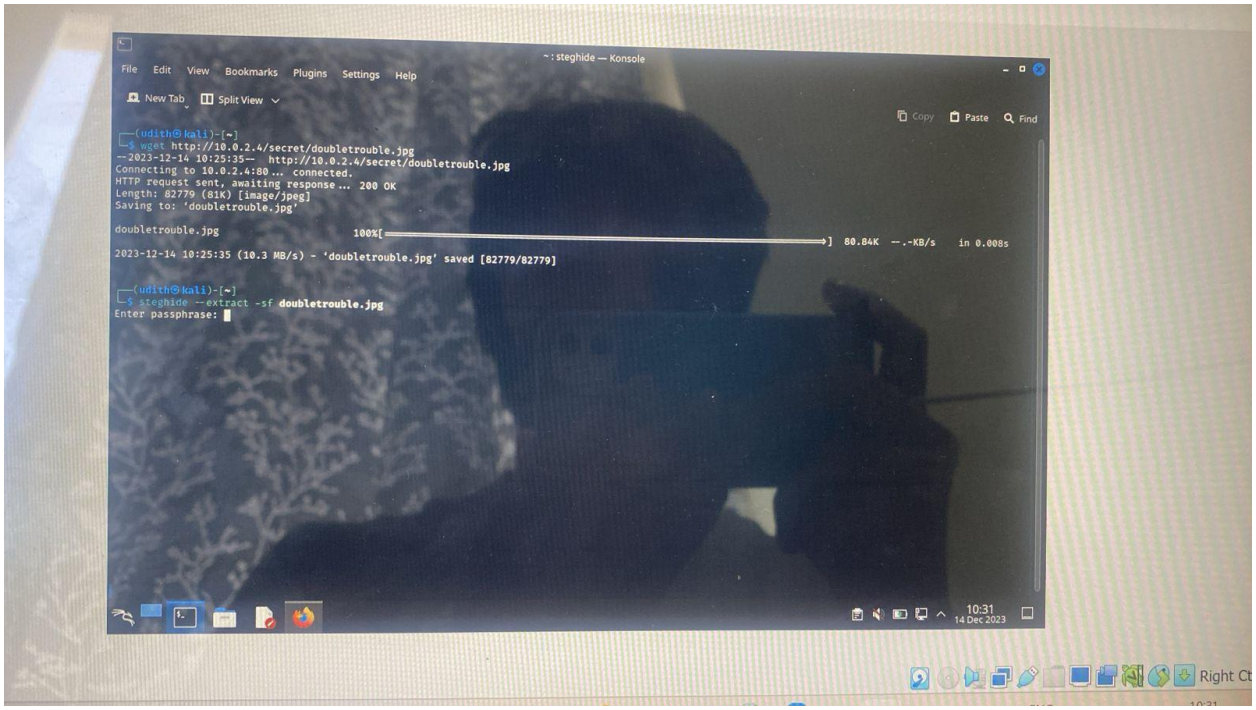




Download the jpg in the kali by executing the “wget http://10.0.2.4/secret/doubletrouble.jpg”

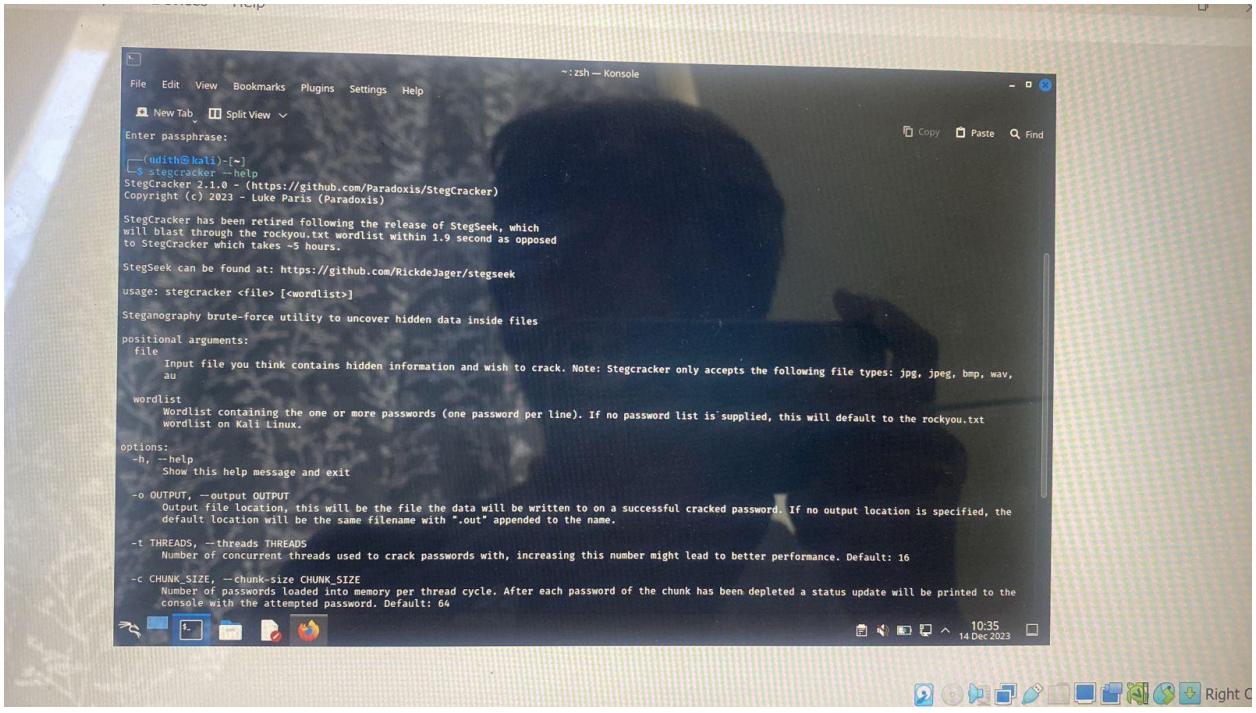


Downloaded in the kali
And the next step is to
For extracting the information from the file we use
Execute command “steghide –extract -sf doubletrouble.jpg”
Steghide is a steganography program that is able to hide data in various kinds of image- and audio-files.
After executing the command
It is asking passphrase

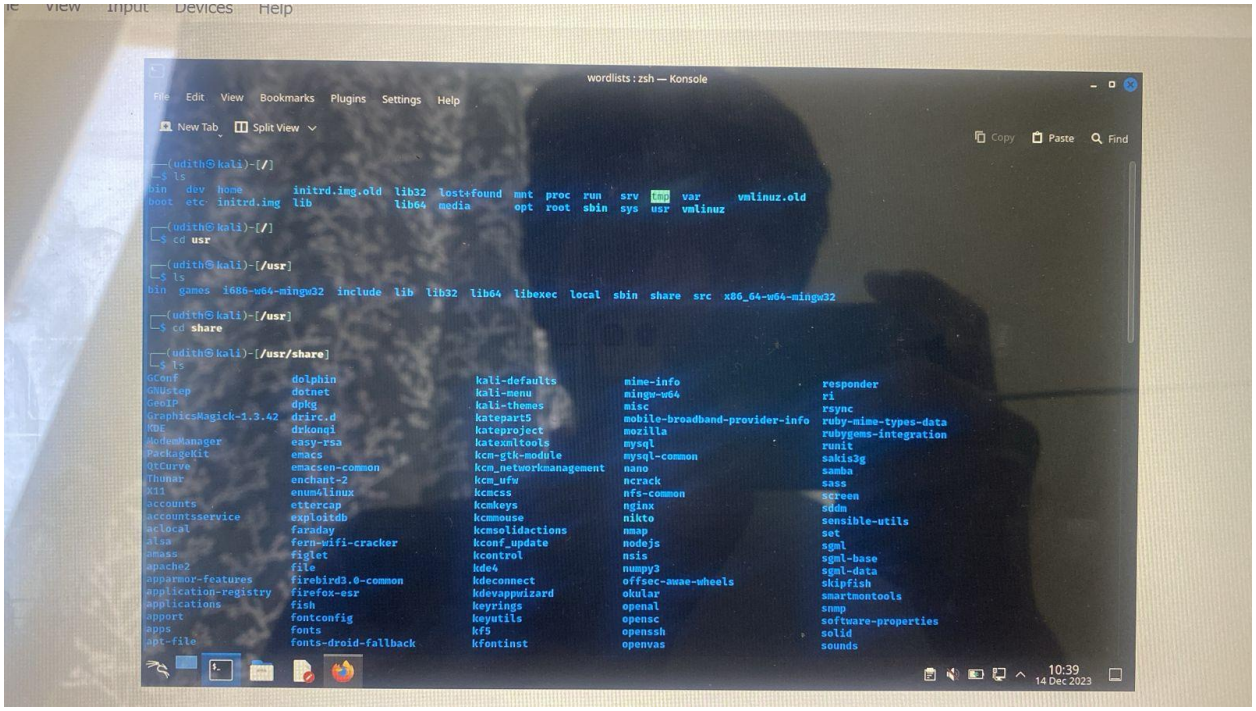


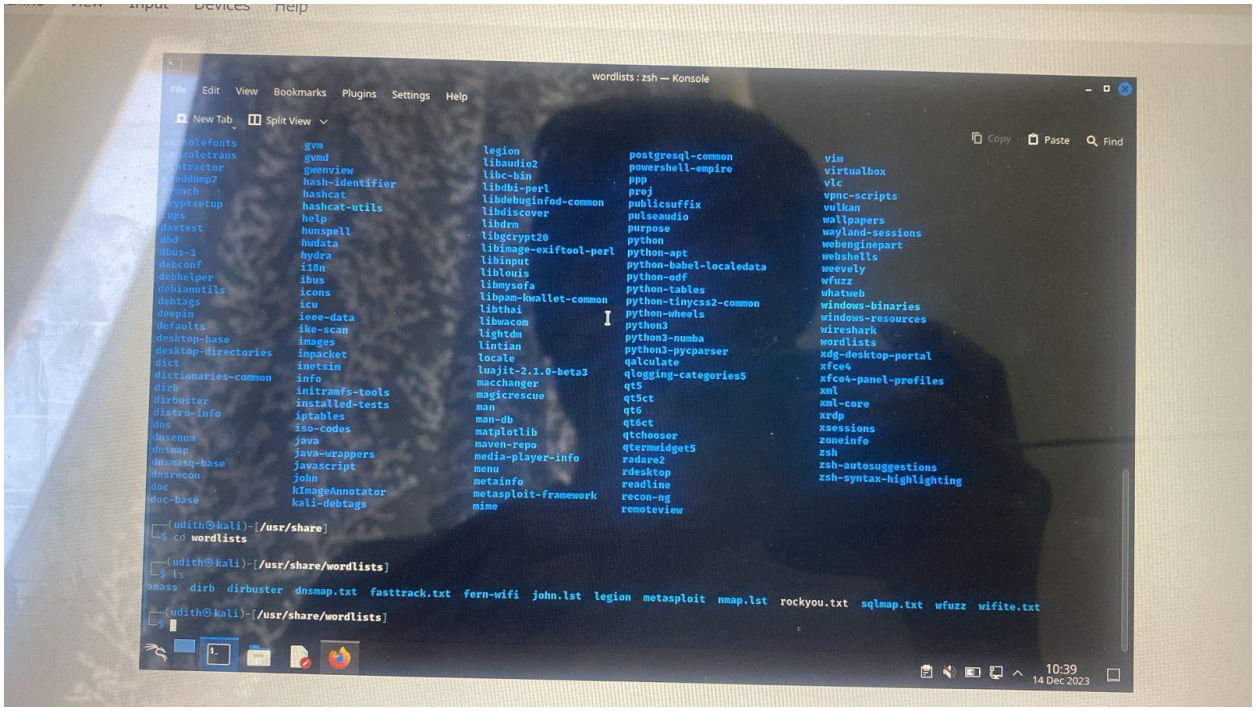
The next step is to crack the passphrase
We use stegcracker tool to get the passphrase

stegcracker is steganography brute-force utility to uncover hidden data inside files
Install the stegcracker by using the command “stegcrackeer –help”
After installing it will show like this

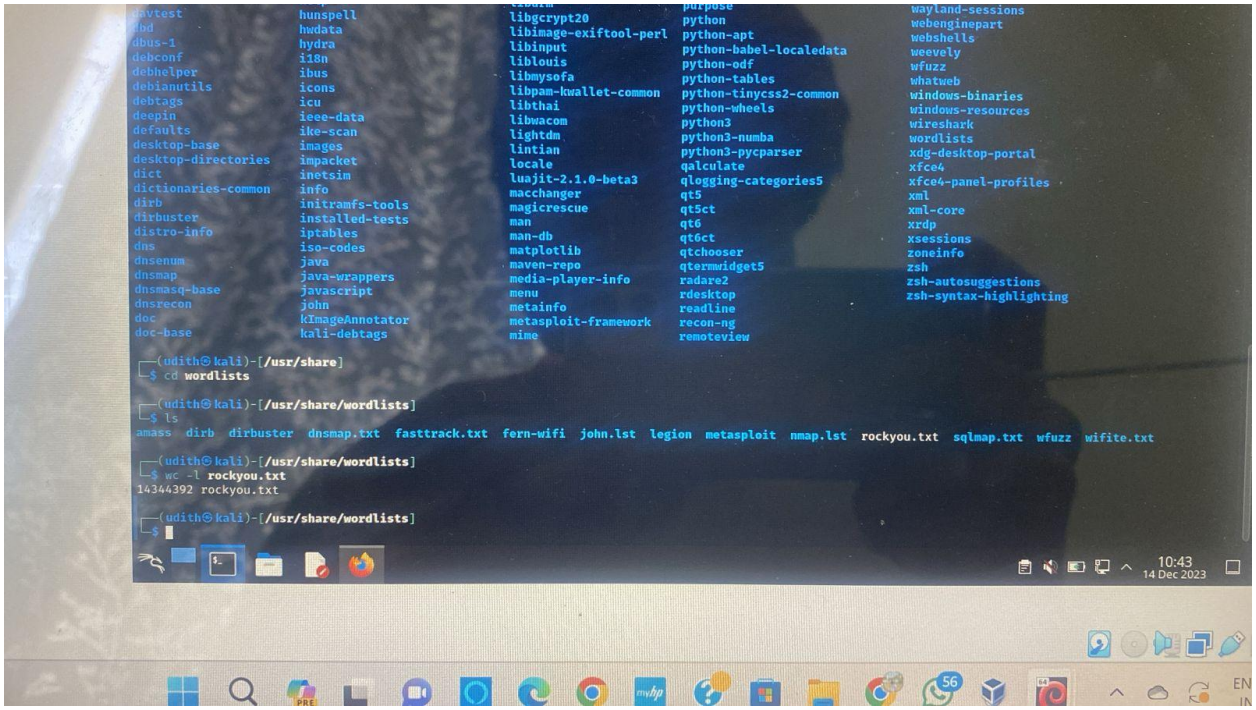


The next step is
STEP 5:cracking the password with stegcracker
Find the default wordlists in the kali
By exploring the files in the kali

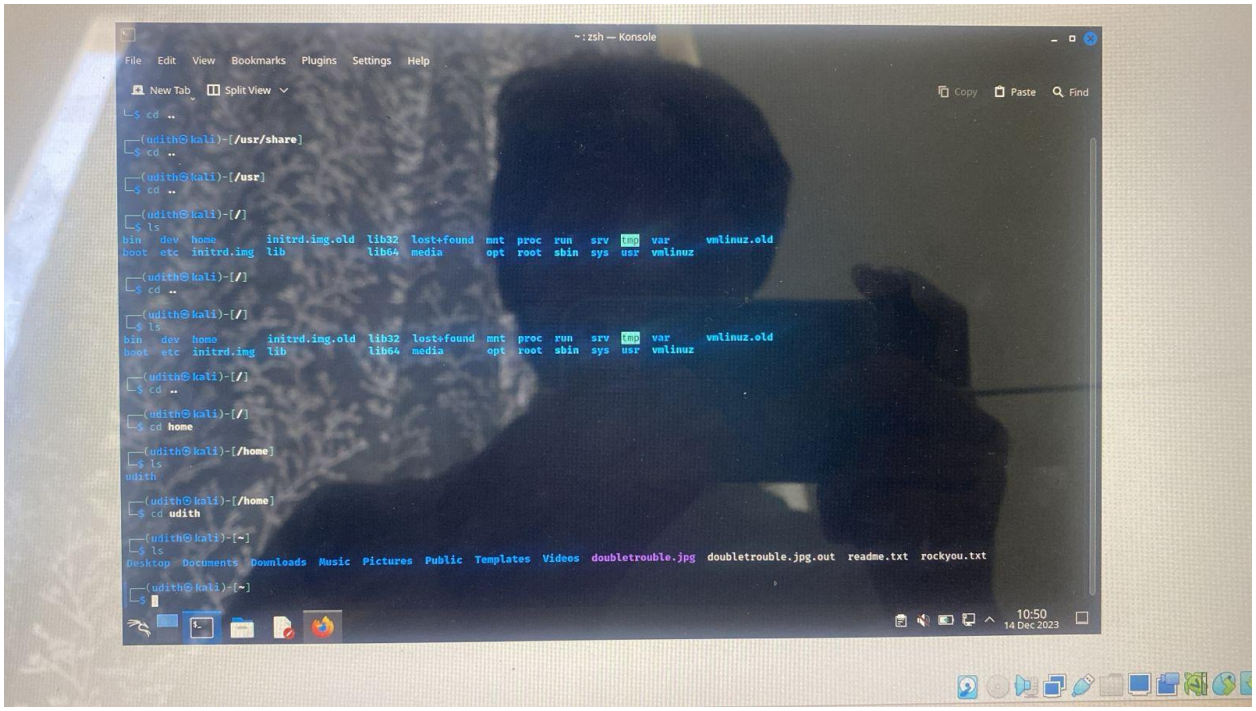




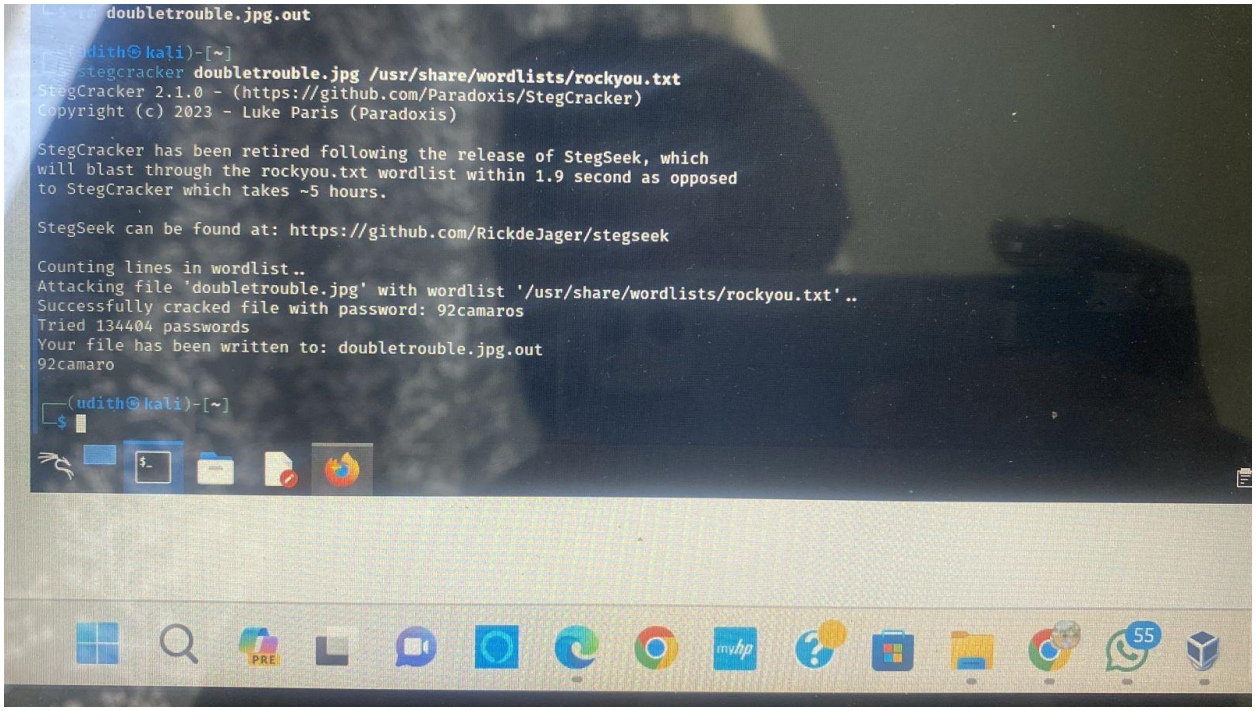
We find a default wordlist which is rockyou.txt
Check the words in the file by executing “wc -l rockyou.txt”



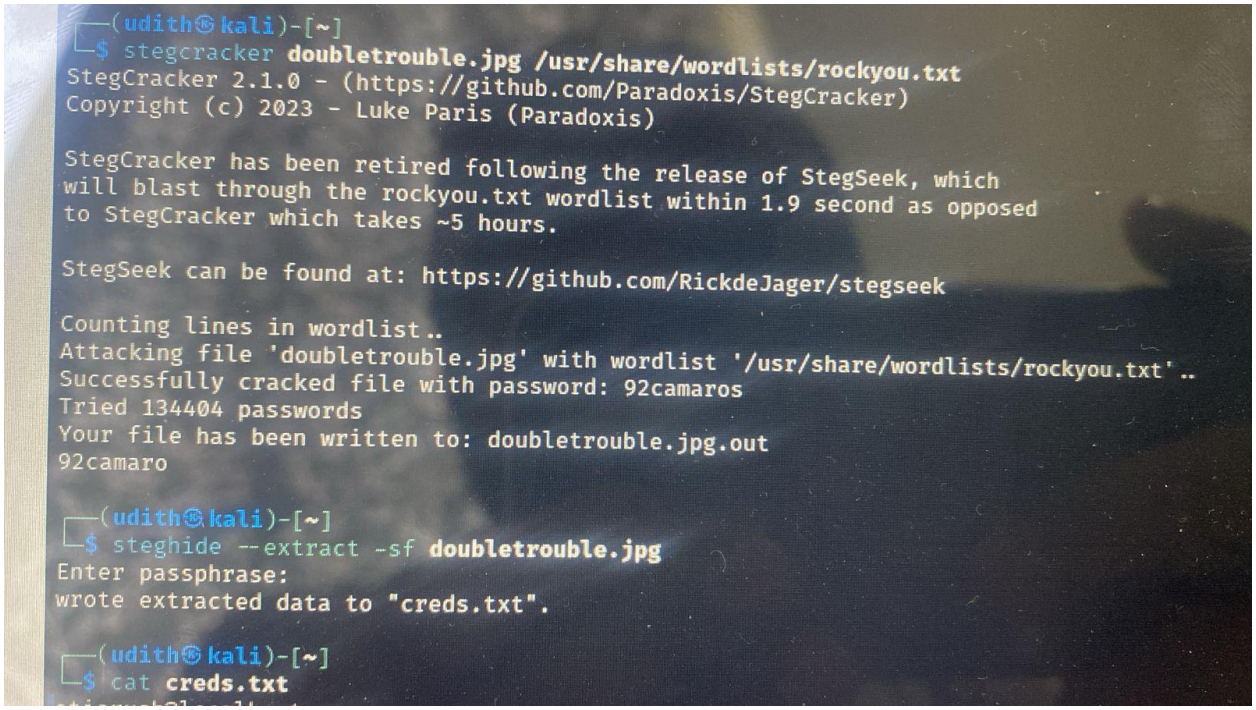
There are 14344392 words
To crack the passphrase we use stegcracker to crack
Go to the directory of the doubletrouble.jpg and



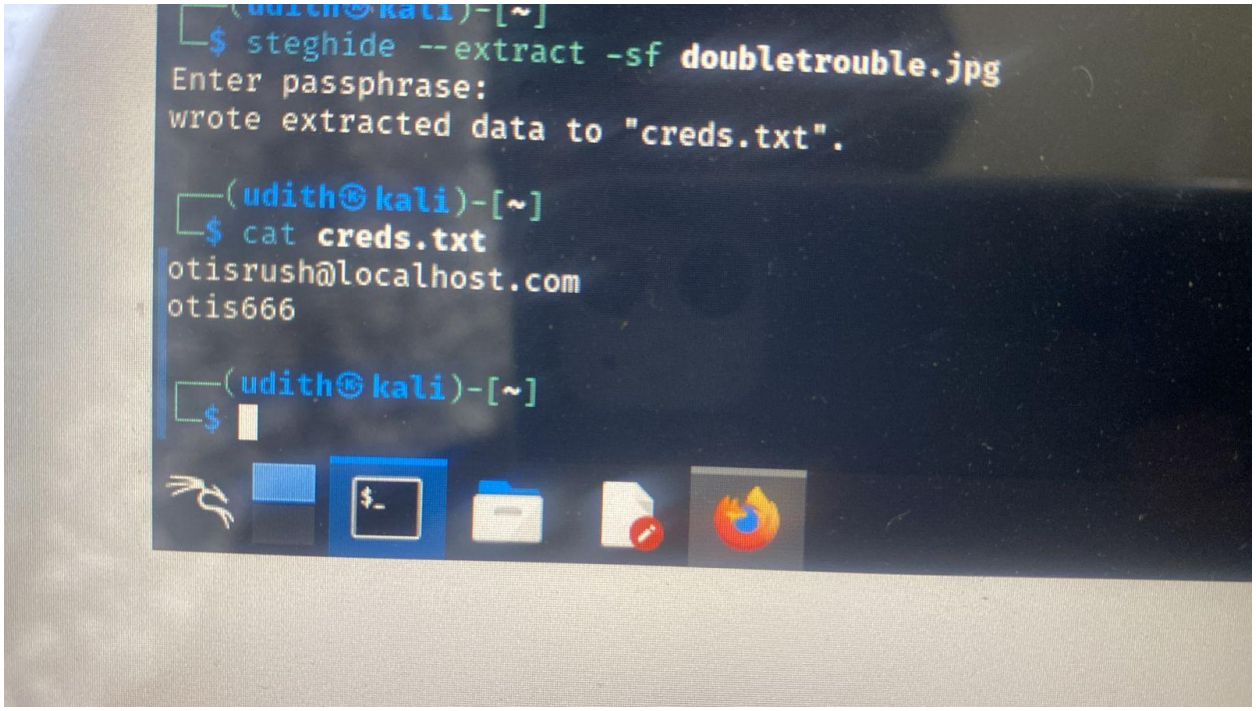
After reaching to the doubletrouble.jpg directory
Execute the command “stegcracker doubletrouble.jpg /usr/share/wordlists/rockyou.txt”
To crack the passphrase



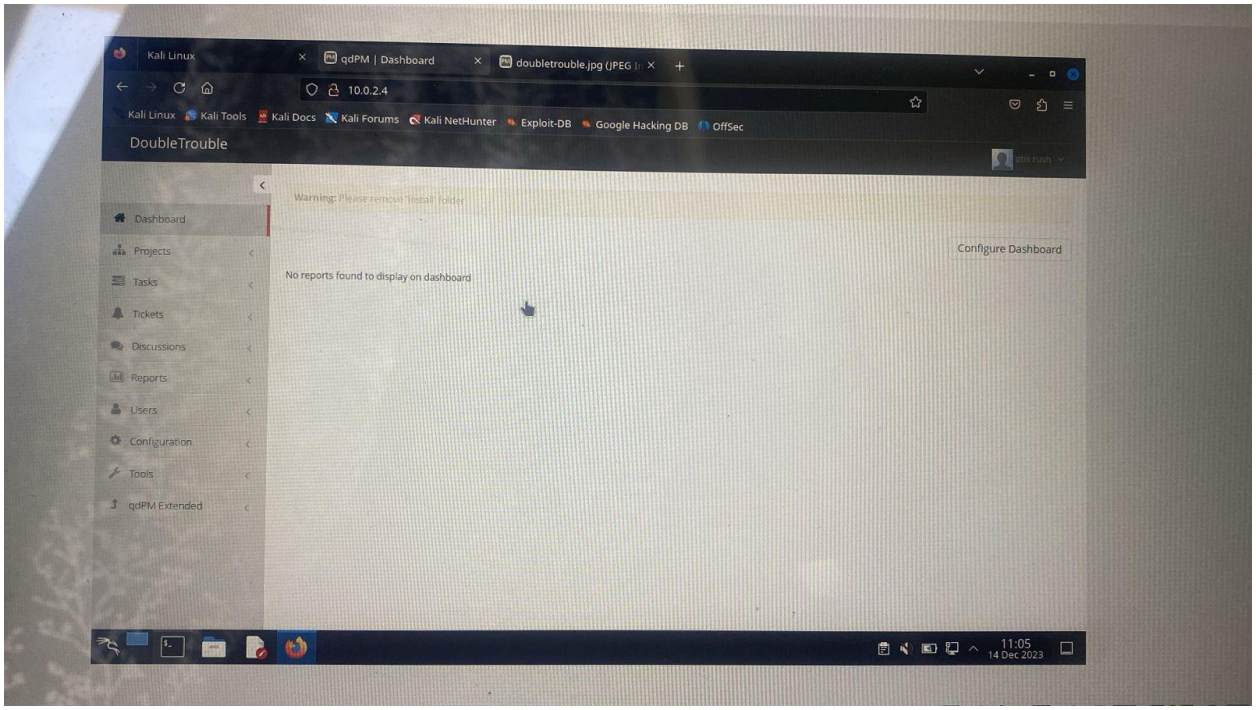
after the cracking we get the passphrase as 92camaro
Now extract the data from the image by again executing the command “steghide –extract -sf doubletrouble.jpg”
It will ask the passphrase
Enter the passphrase



It save the extracted file ass creds.txt
Open the file by “cat creds.txt”



After reading the creds.txt file we get the credentials for the qdpm login
Enter the credentials in the login



By this step wee logged in to the qdpm
The credentials are
User gmail:otisrush@localhost.com
Password:otis666
By this we enter the machine and we can reshell the program and get the connectivity also
THIS ARE THE STEPS FOR CTF OF DOUBLETROUBLE MACHINE