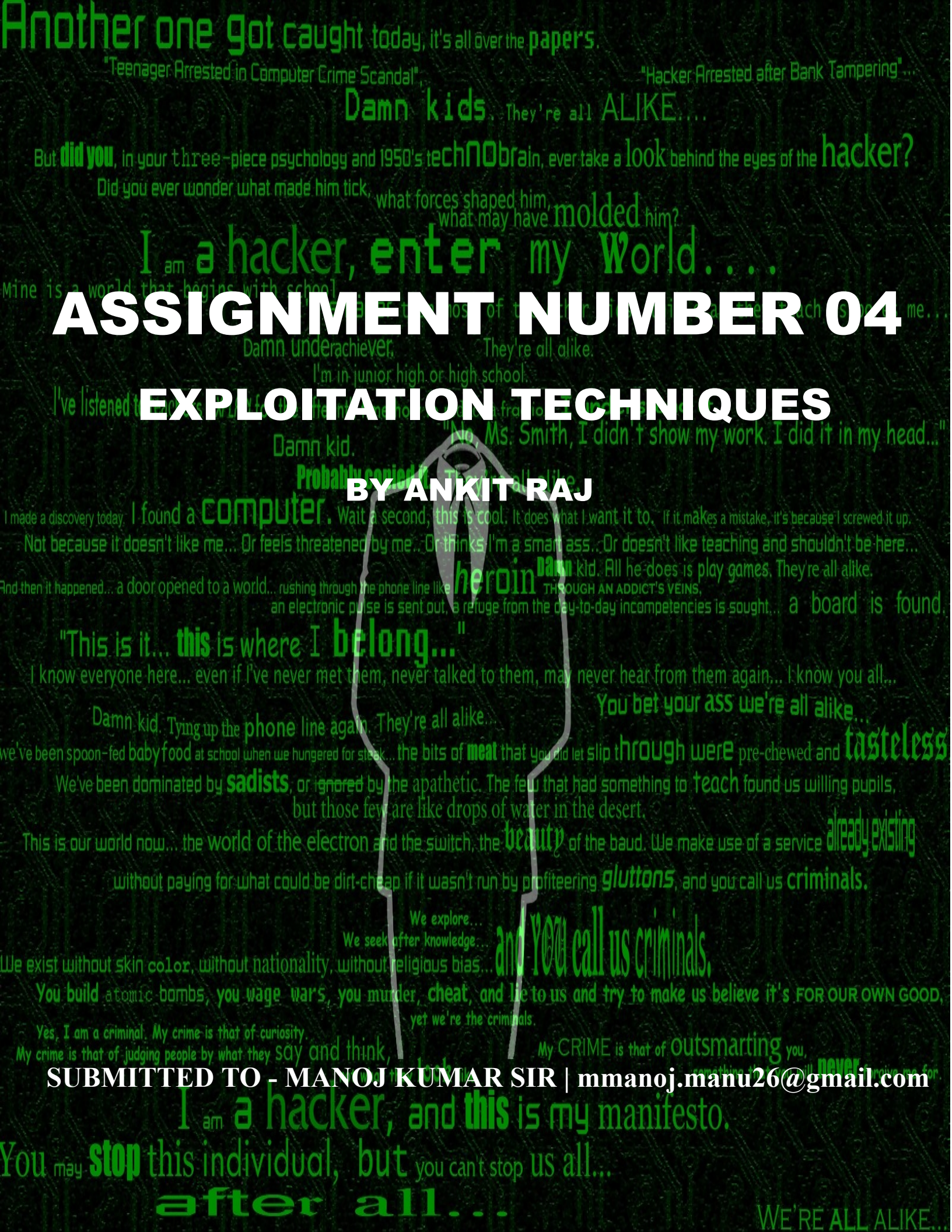


ASSIGNMENT NUMBER 04

EXPLOITATION TECHNIQUES

BY ANKIT RAJ

SUBMITTED TO - MANOJ KUMAR SIR | mmanoj.manu26@gmail.com

• TARGET - METASPOITABLE 2

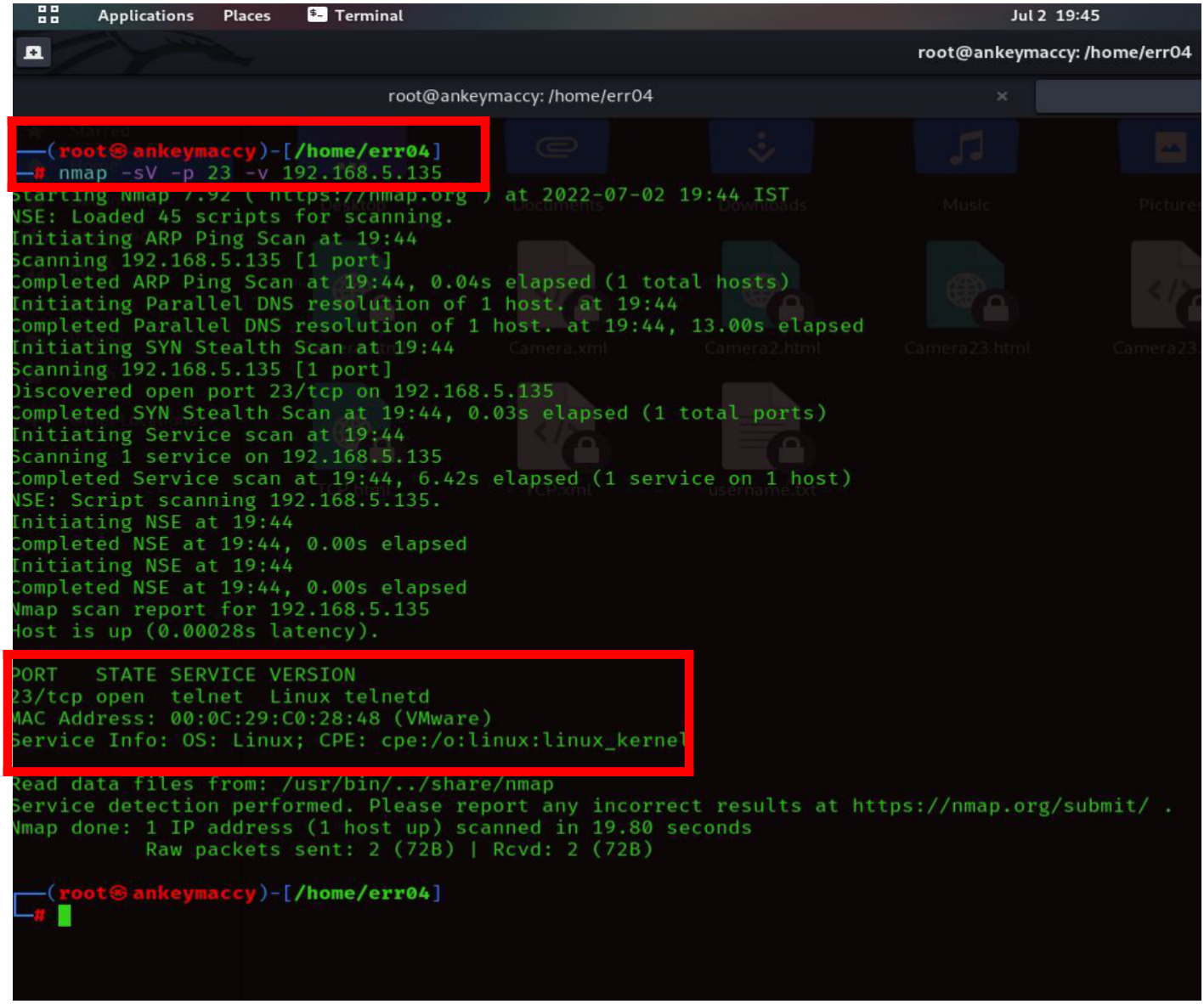
• TASKS TO DO AND OTHER INFO :-

1. TARGET'S IP - 192.168.5.135
2. EXISTENCE - LOCAL NETWORK
3. TASK - Hack Target using Port 23 using Metasploit Framework

• CONTENTS : -

1. Using Nmap To Scan Target's Port Info

⇒ STEP 1. In this step, we used nmap to find information about the services and its version running on the Port 23 of our target machine 192.168.5.135



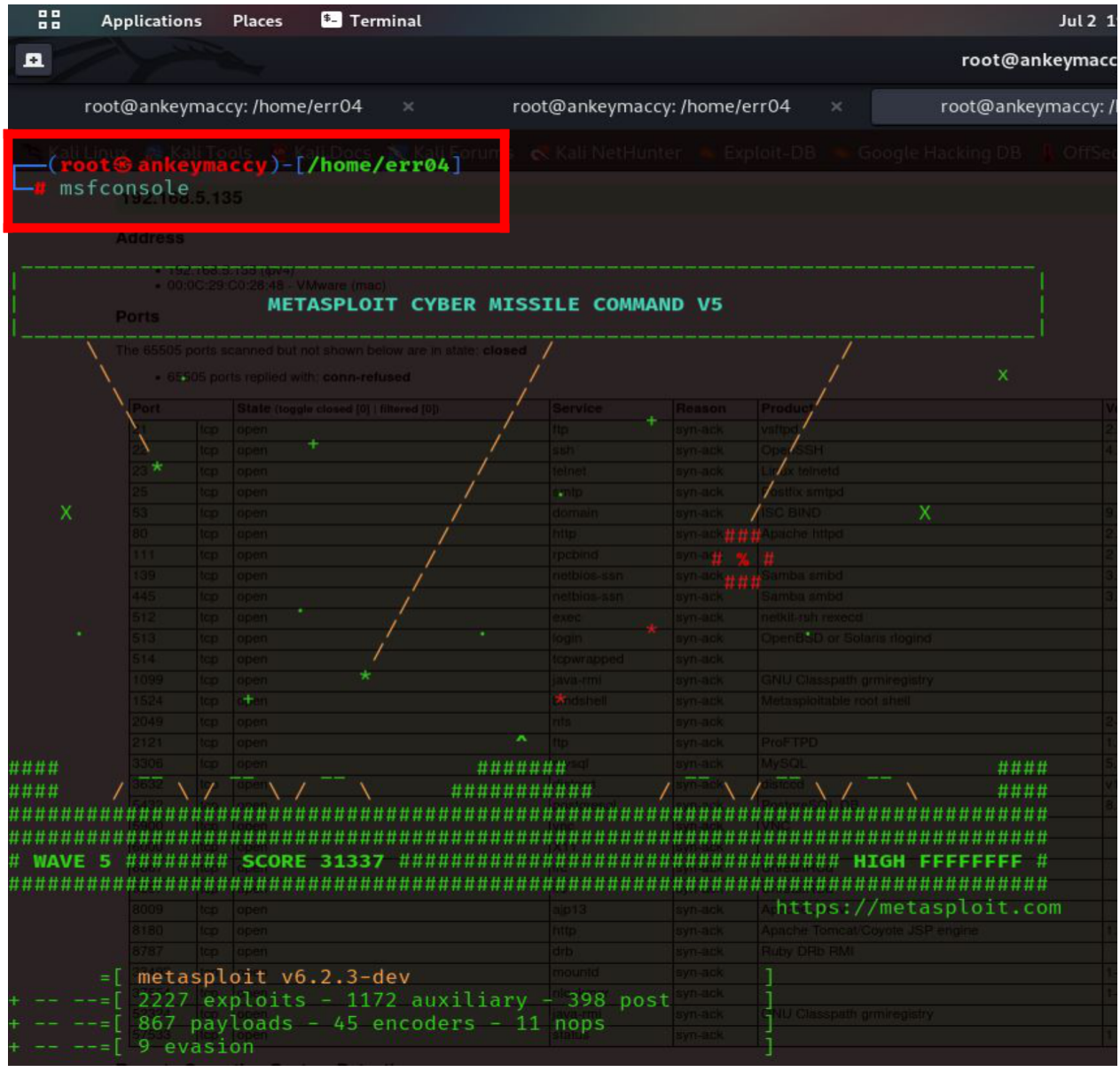
⇒ Details that we found about our target is shown above as well as written below:-

- PORT -23,
- SERVICE - telnet,
- VERSION - Linux telnetd,
- MAC - 00:0C:29:C0:28:48
- OS - Linux

2. Using msfconsole

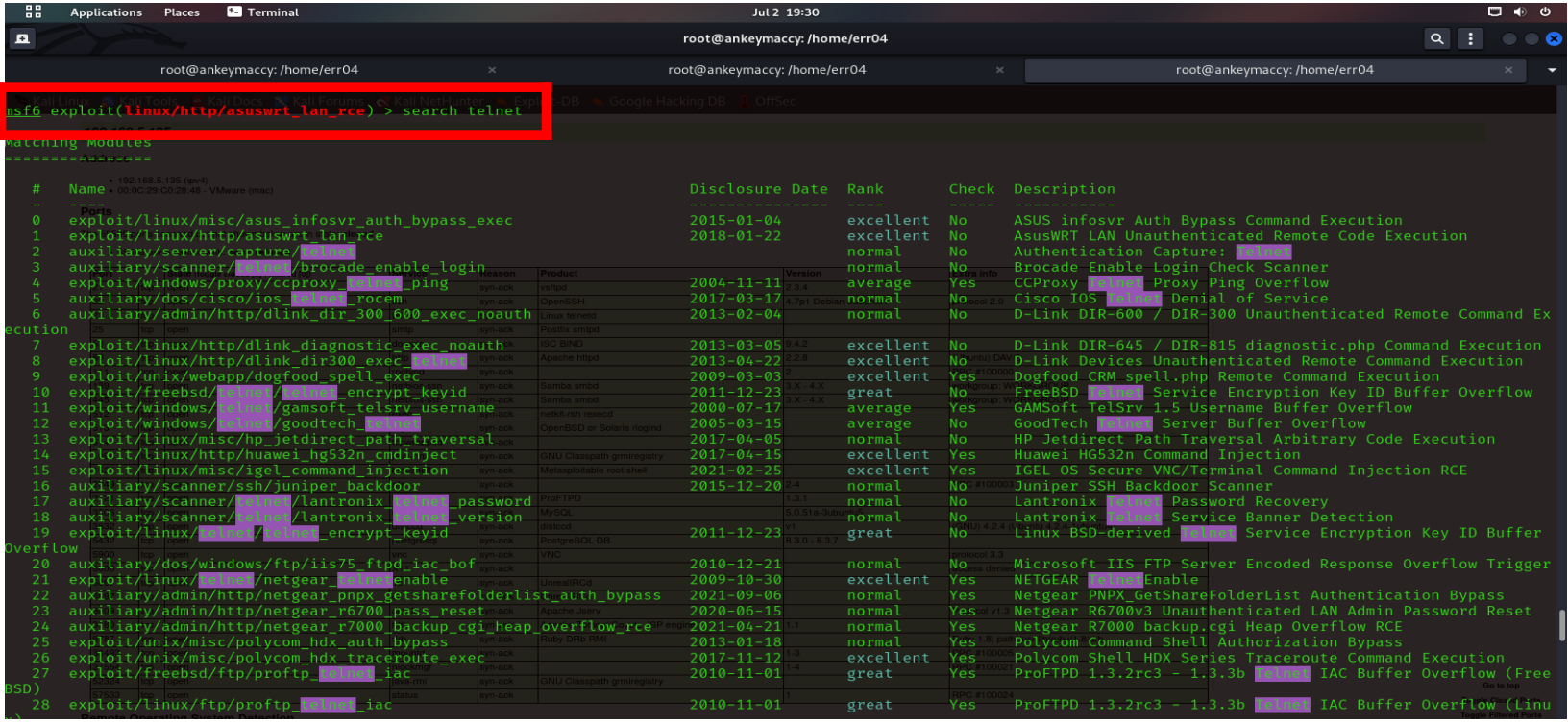
⇒ Step 1. Launching msfconsole in terminal

📝 Command Used:- msfconsole

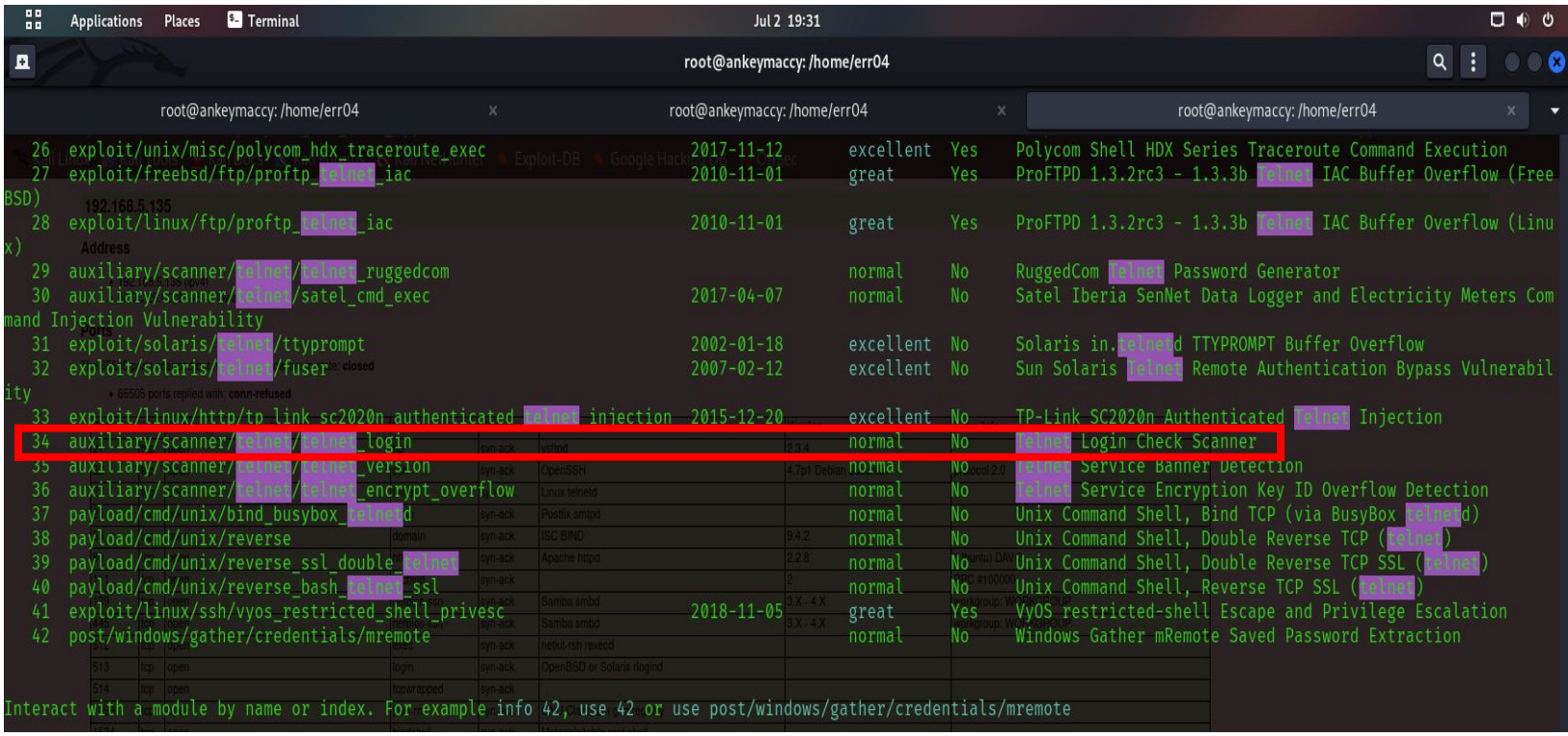


⇒ Step 2. Searching the required telnet exploit in msfconsole in order to get access in the target over port 23.

📝 Command Used : - search telnet



⇒ Step 3. Now, Select the correct Module. We are going to Bruteforce our target so we've chosen module number 34 i.e., auxillary/scanner/telnet/telnet_login.

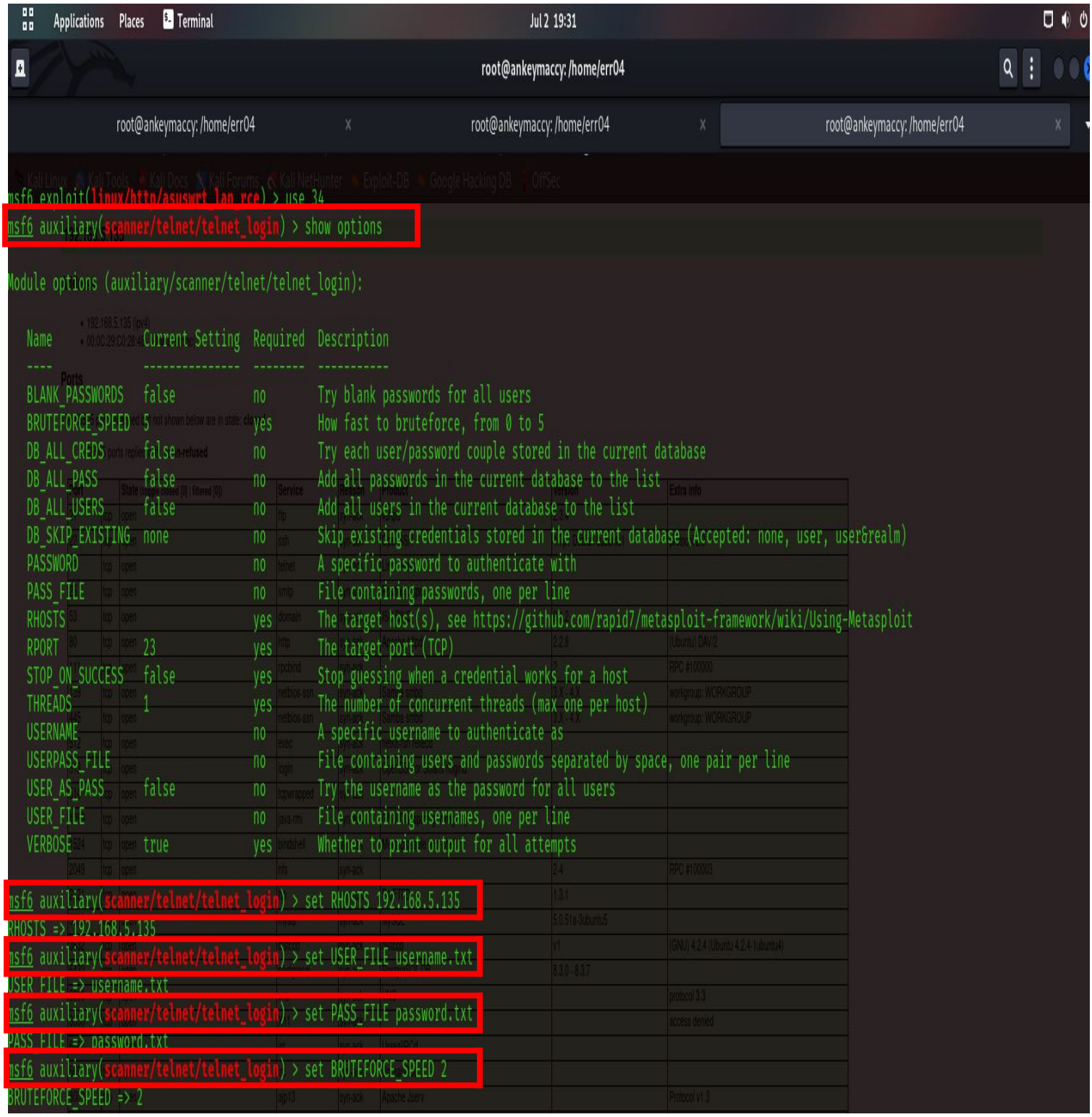


📝 Command Used : - use 34

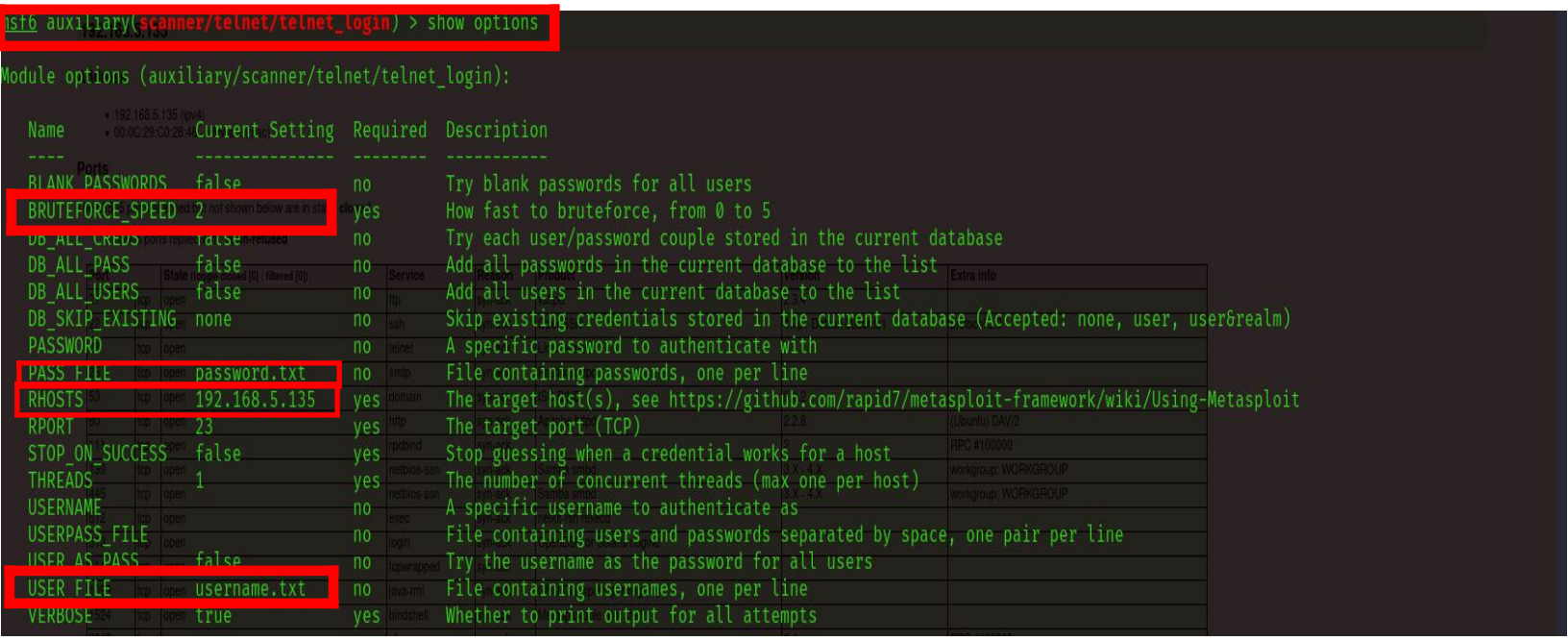
```
msf6 exploit(linux/http/asuswrt_lan_rce) > use 34
```

⇒ Step 4. We will now see the options of module 34 and will set required values in the options field of module 34.

- Command Used:- show options to view options.
- Command Used:- set RHOSTS 192.168.5.135 to set target's IP.
- Command Used:- set USER_FILE username.txt to set wordlist file.
- Command Used:- set BRUTEFORCE_SPEED 2 to set bruteforcing speed.



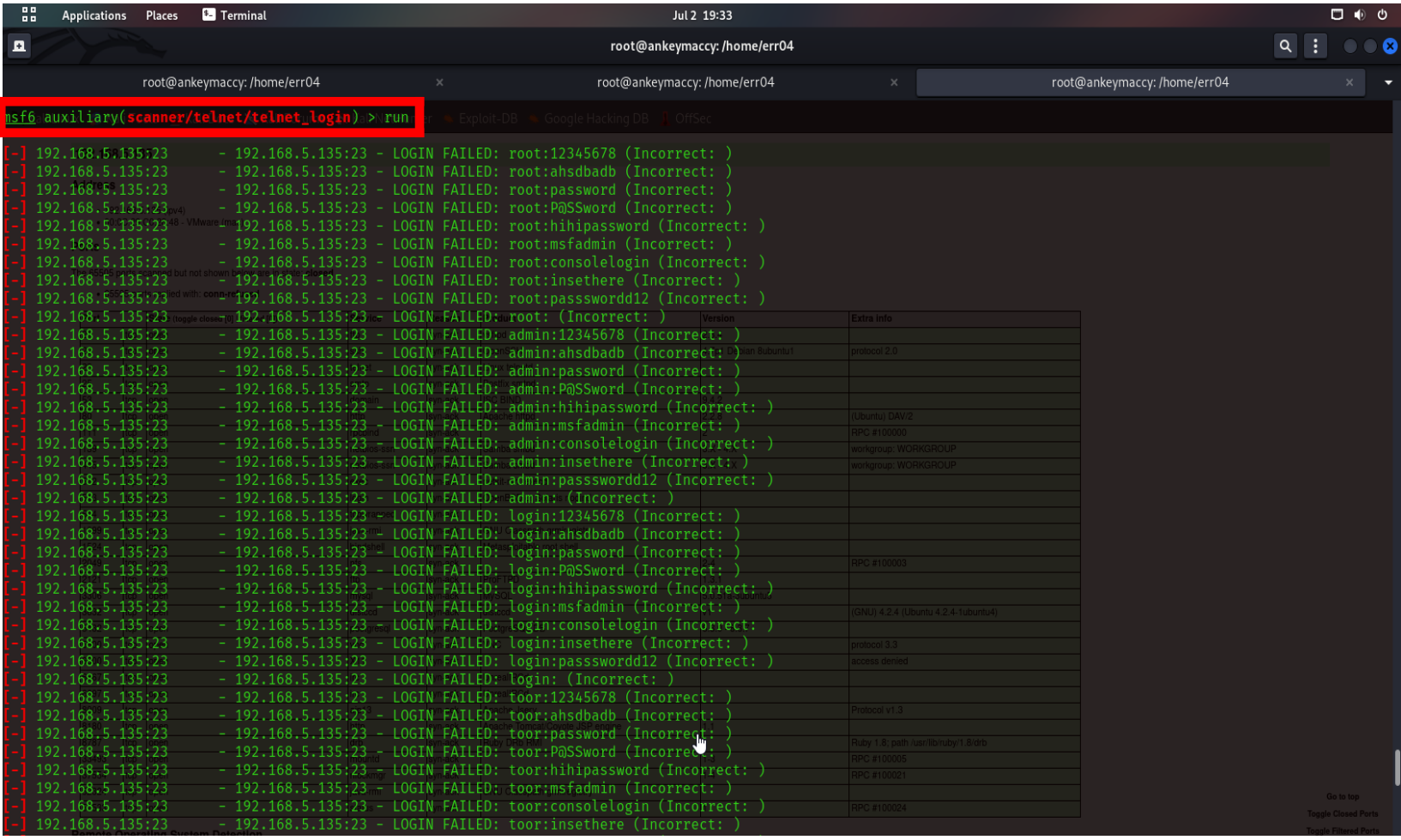
⇒ Step 5. After setting all the values, Let's cross check for the options we set. Again using show options command.



3. Initiating Attack

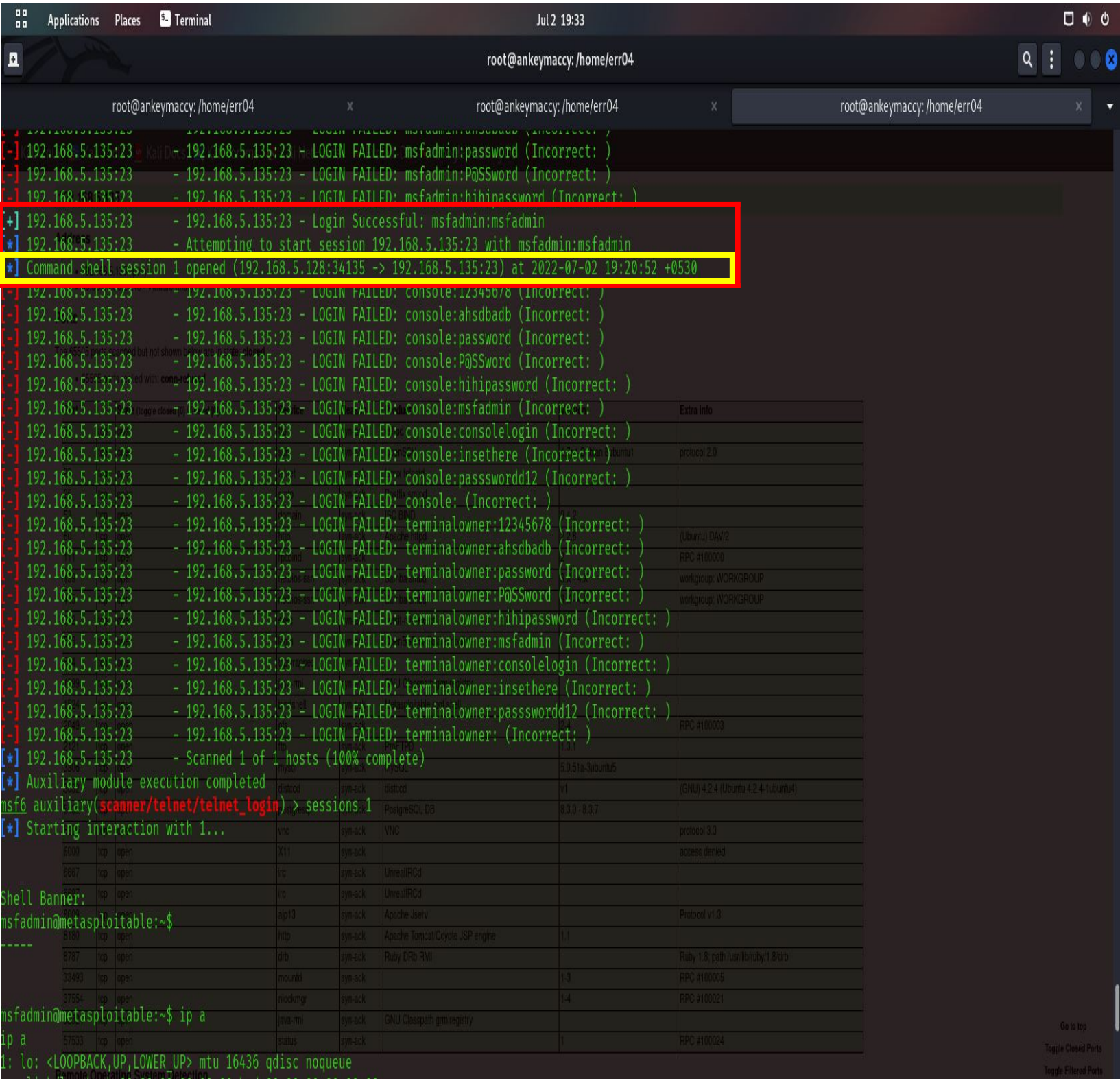
⇒ Step 1. After, Crosschecking every values and parameter initiate the attack.

📝 Command Used : - run



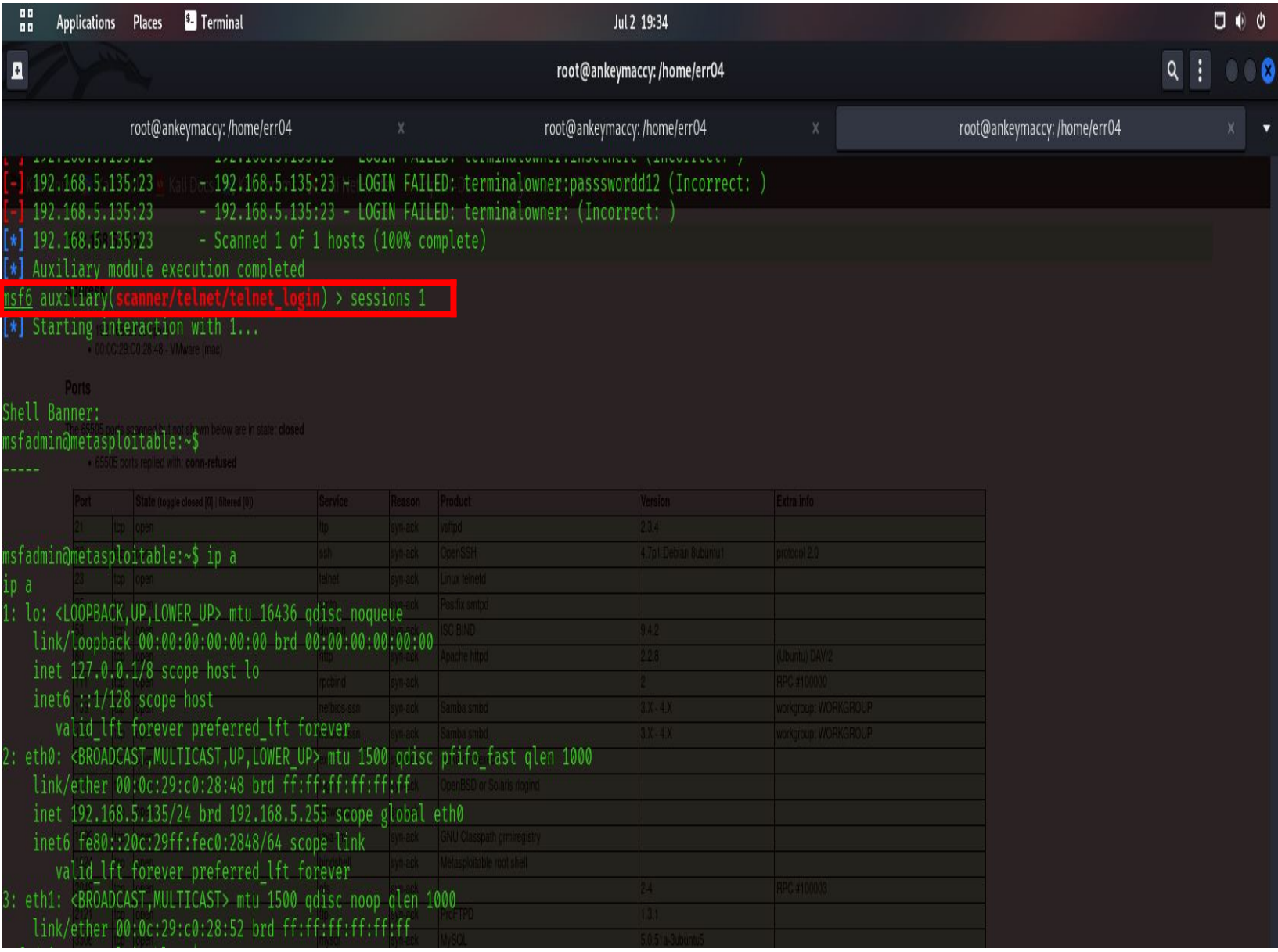
⇒ Step 2. Bruteforcing we be started suddenly after this, and we will see the same in the terminal.

⇒ Step 3. Once the bruteforcing is successful, we will see Login successful message in the terminal.
And, a command shell will be spwaned for us.



⇒ Step 4. Now, We are ready to start the remote shell using sessions command. So, Let's spawn the remote shell.

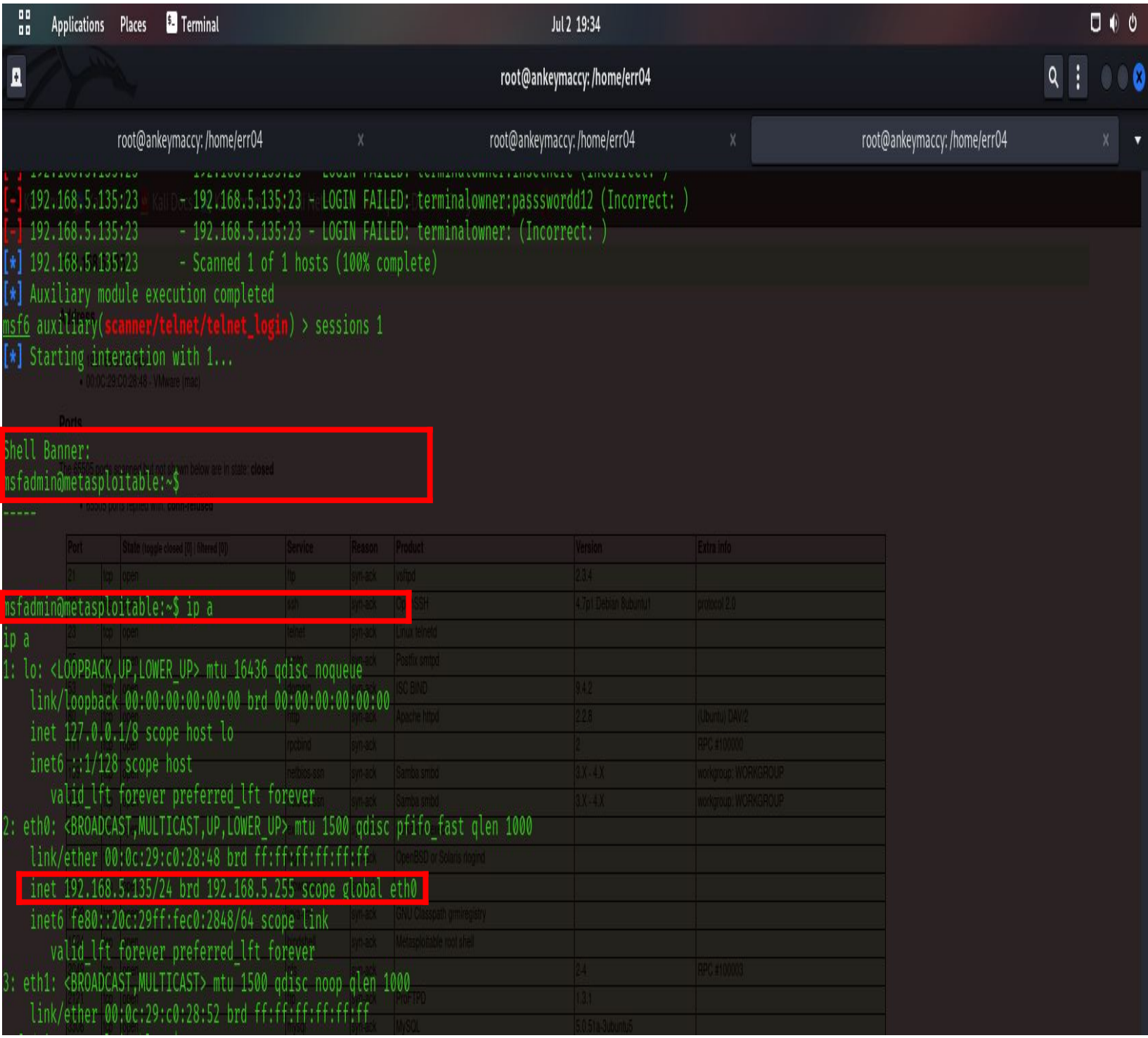
📝 Command Used : - sessions 1



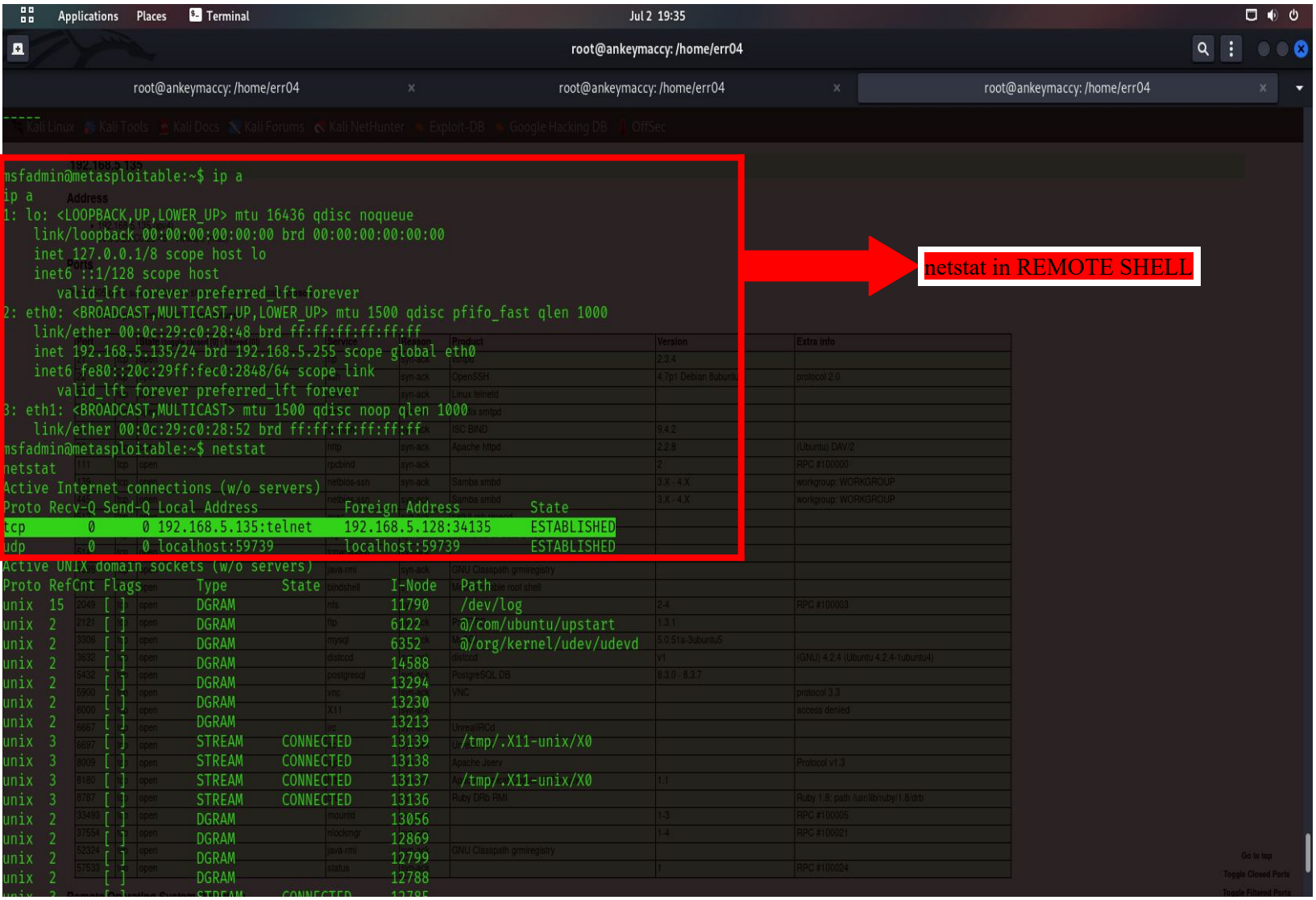
⇒ Step 5. We are logged into the Target Computer.

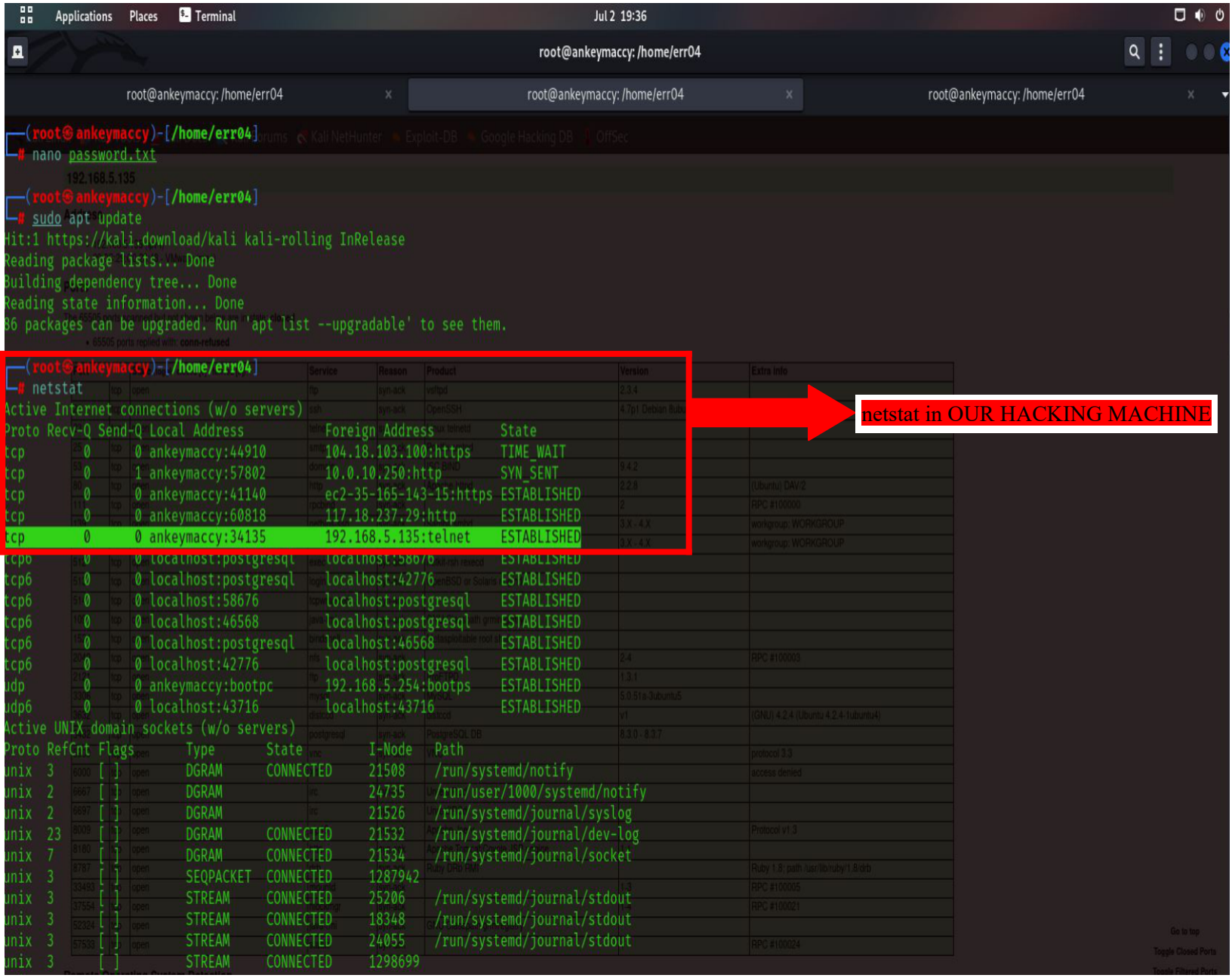
4. Proof

⇒ Step 1. In the shell we can check the ip of it to make sure we are logged in the remote shell.



⇒ Step 2. As another proof we can also check the connection via netstat into both machines i.e., in our remote shell as well as in our hacking machine.





---END-OF-REPORT--