IE4012

Offensive Hacking Tactical and Strategic

4th Year, 1st Semester

Report Submission

Submitted to

Sri Lanka Institute of Information Technology

In partial fulfillment of the requirements for the

Bachelor of Science Special Honors Degree in Information Technology

10.05.2020

About the Target

- There are two types of images in this, one for the Kali Linux and other is for the FTP server.
- In server side, you have to install the Immunity debugger for saw it.
- In immunity Debugger, we can attach the FTP server and check the exploitations. Images is in the figure 07.

About the Exploitation Code

- The Exploitation code is written in Python.
- It will be saw in Figure 04.
- Download Source is https://www.exploit-db.com/exploits/23243
- If you download the FTP server, you can add it to the immunity Debugger as I mention earlier.

1.Download the FTPserver exploitation.

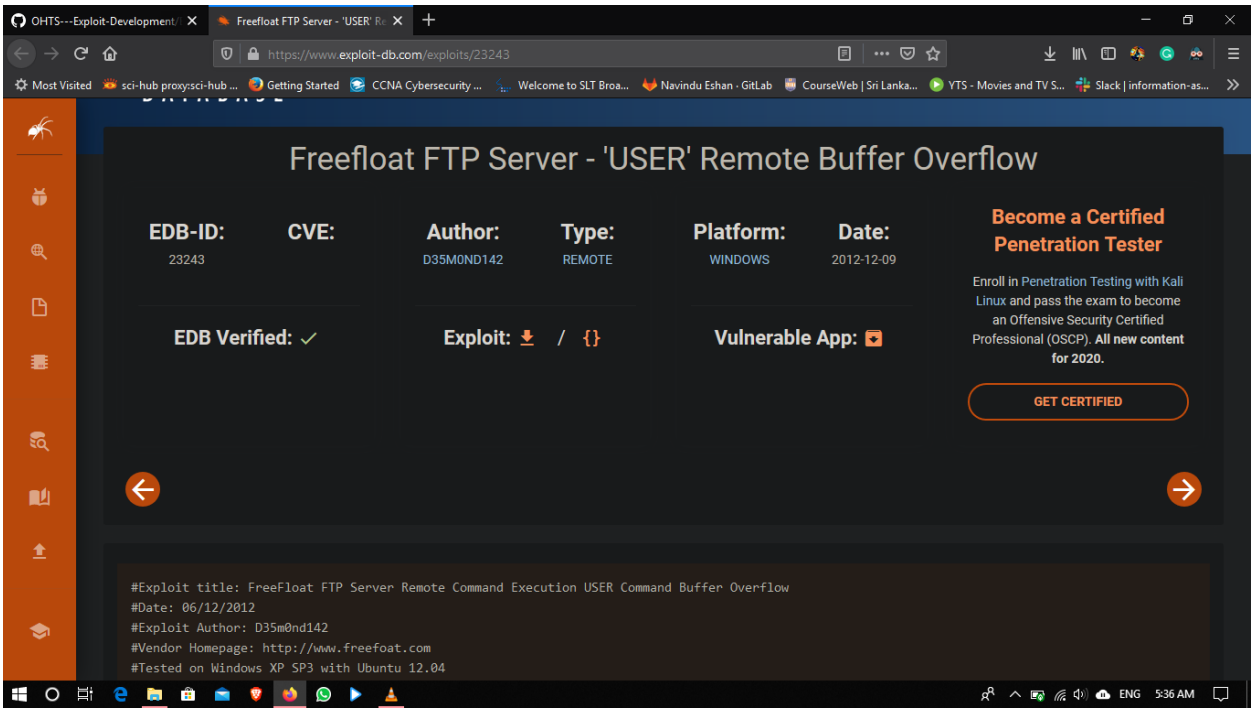

Figure 1

2.Download the Immunity Debugger ad install.

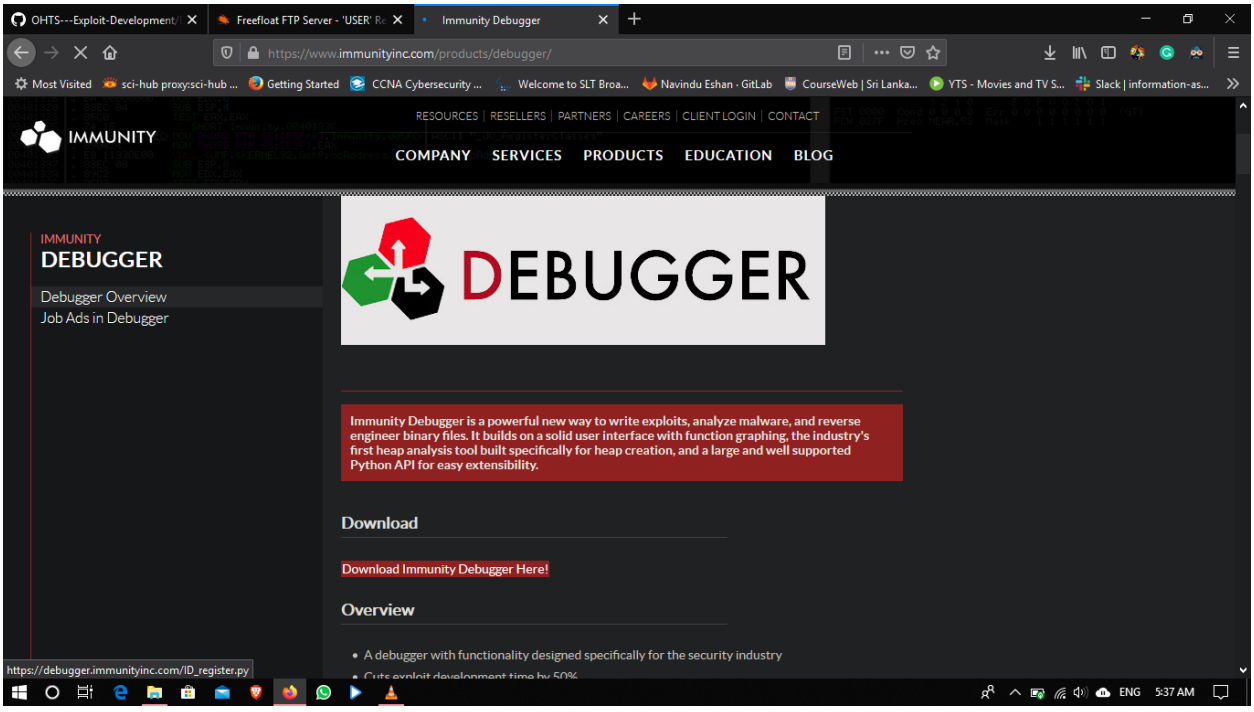

Figure 2

3.Nano exploit.py

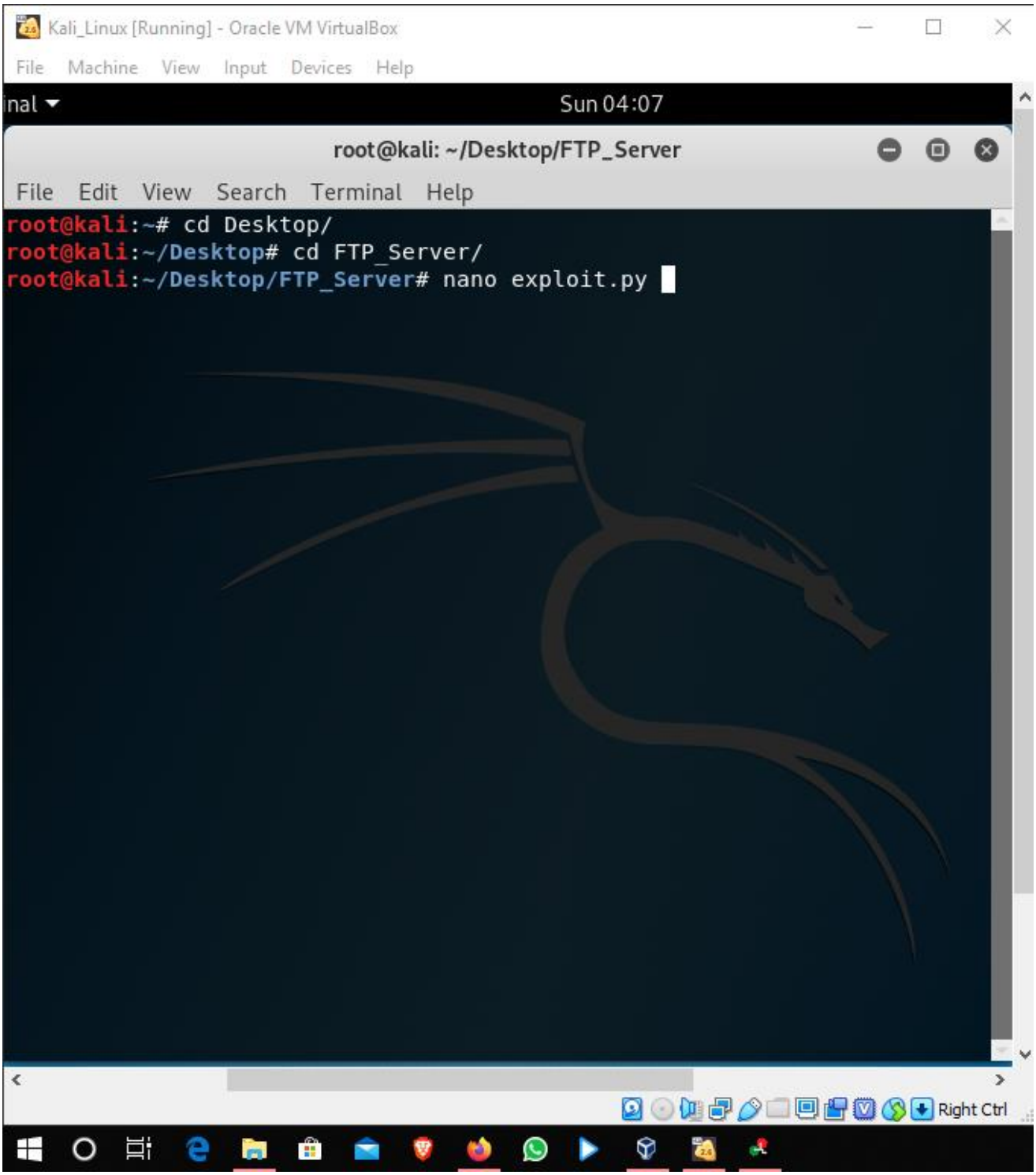

Figure 3

4. Inside the exploit.py

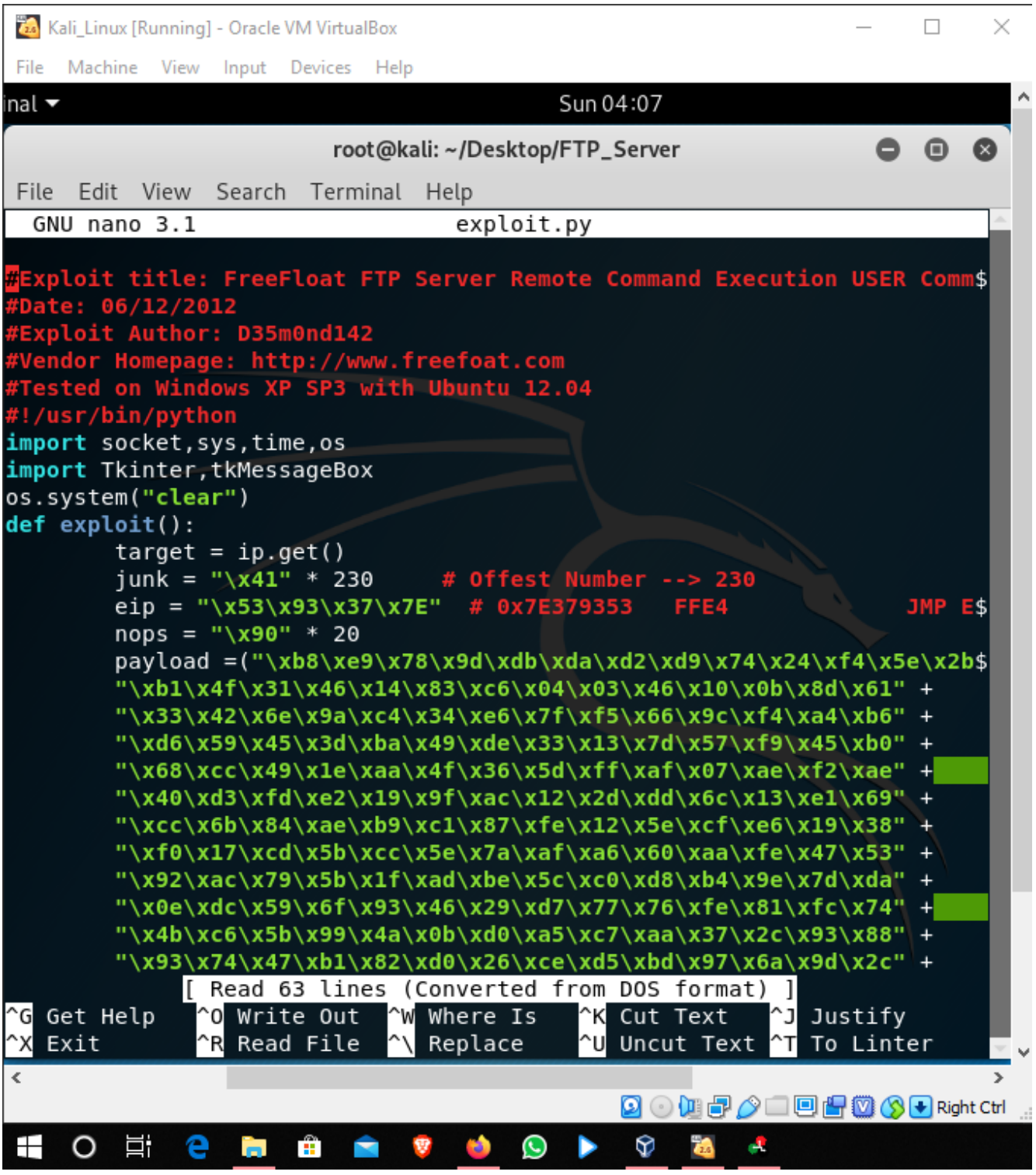

Figure 4

5. Find the ftp port number using nmap

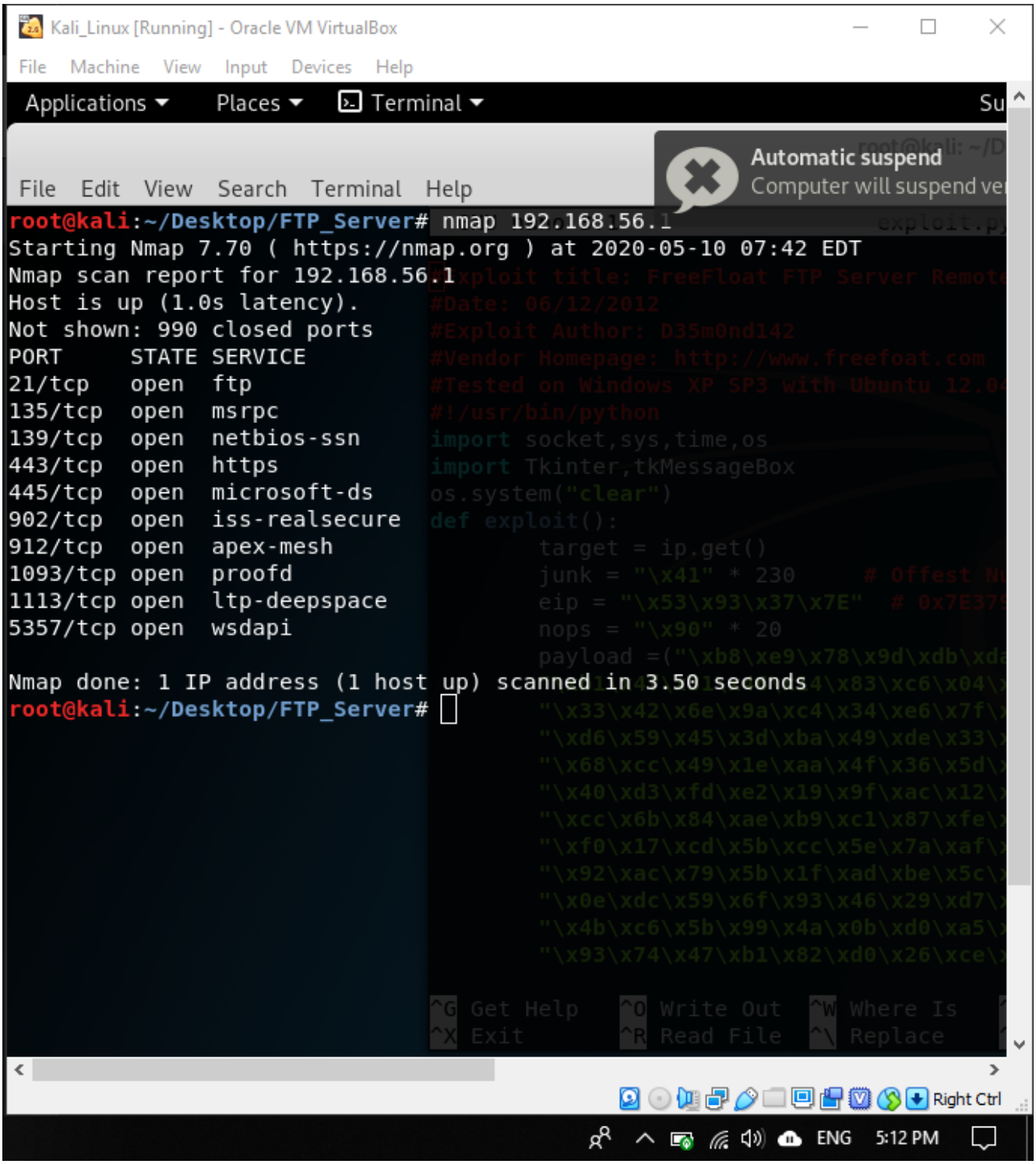

Figure 5

6. Run the bed -s FTP -t192.168.56.1 -p 21 -u anonymous -v anonymous

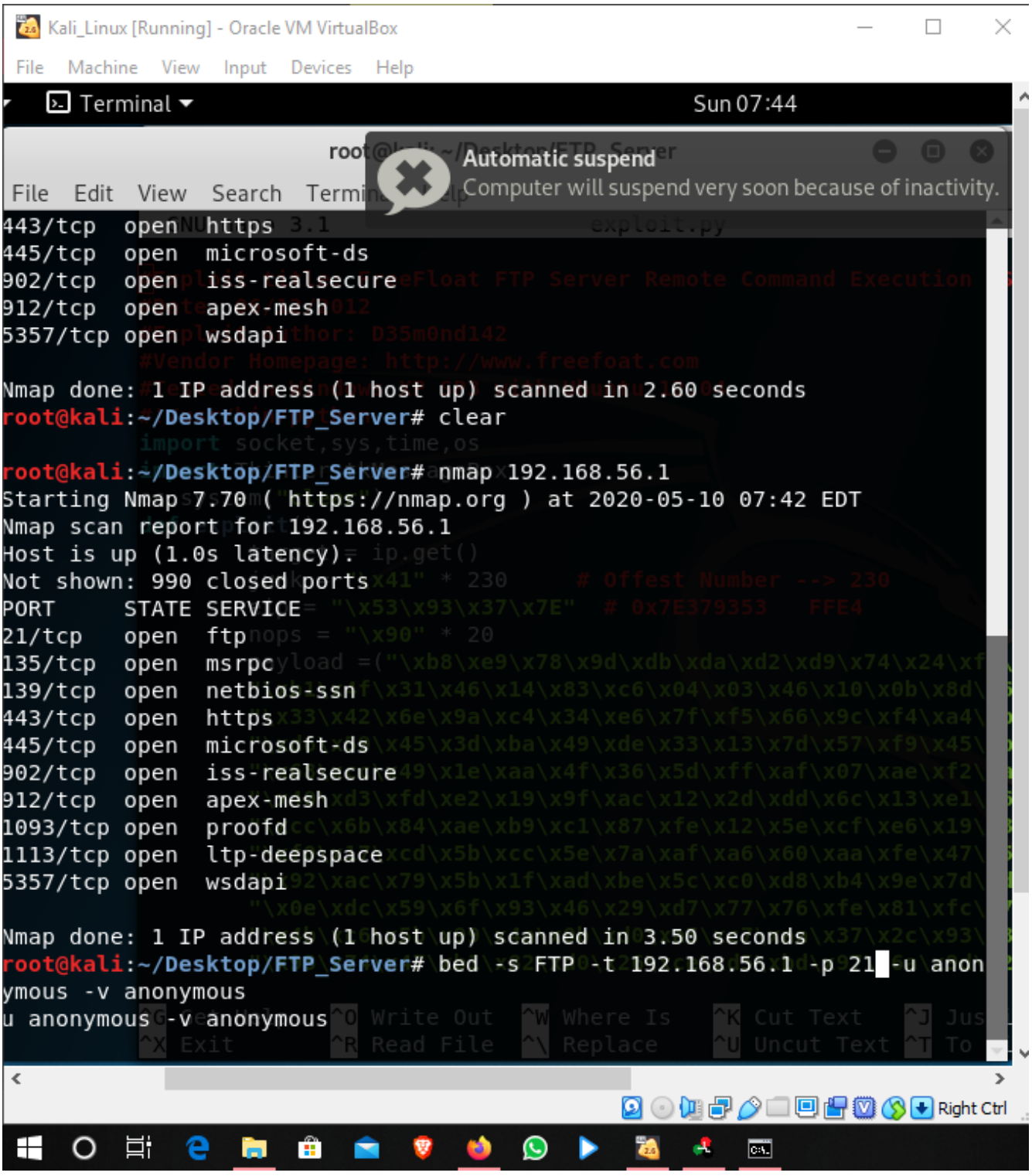

Figure 6

7. It’s Exploit the FTP server

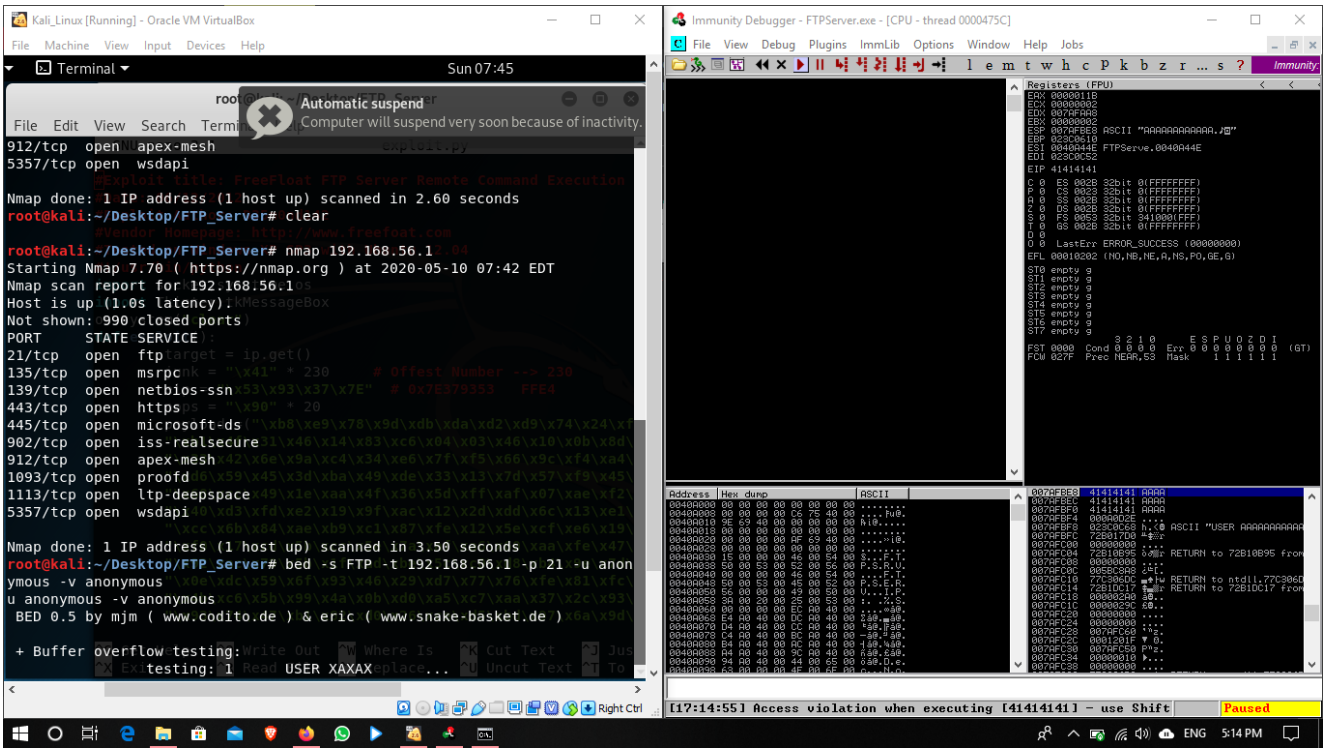

Figure 7

8. Exit from the code

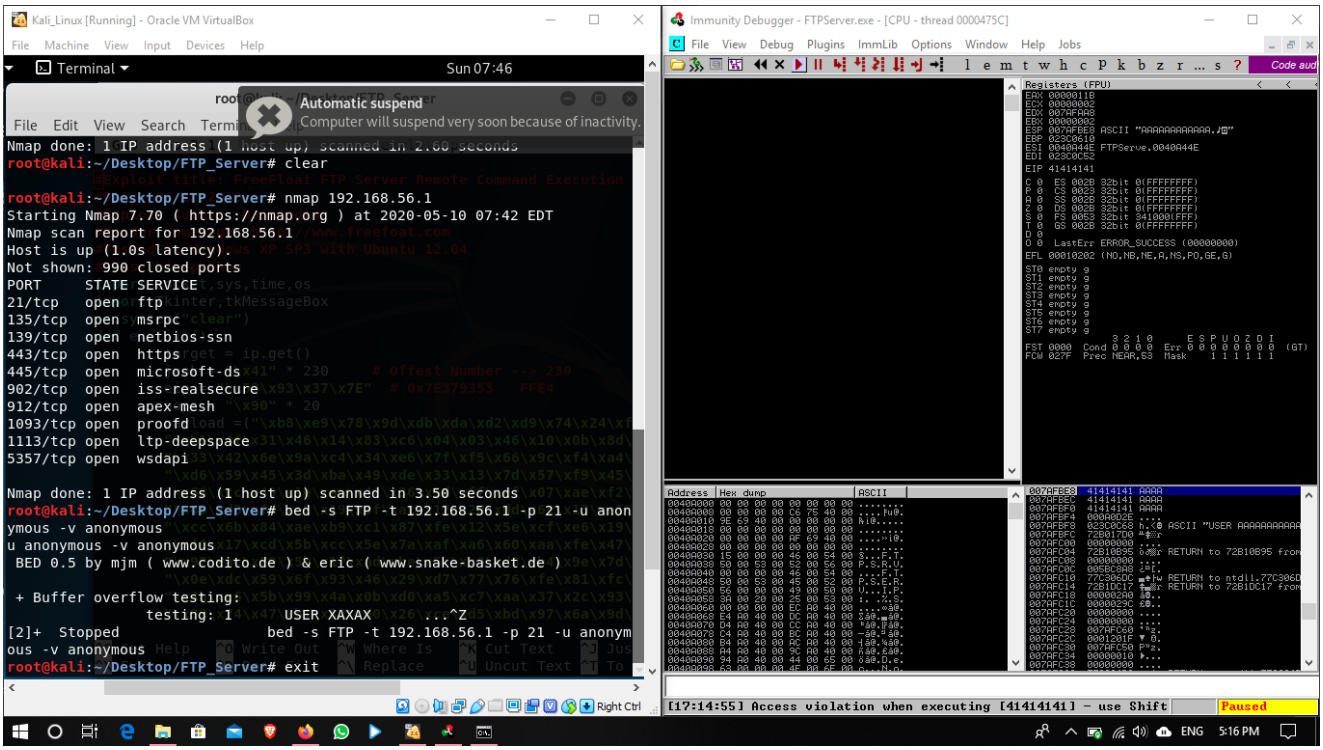

Figure 8

9. Run the python code

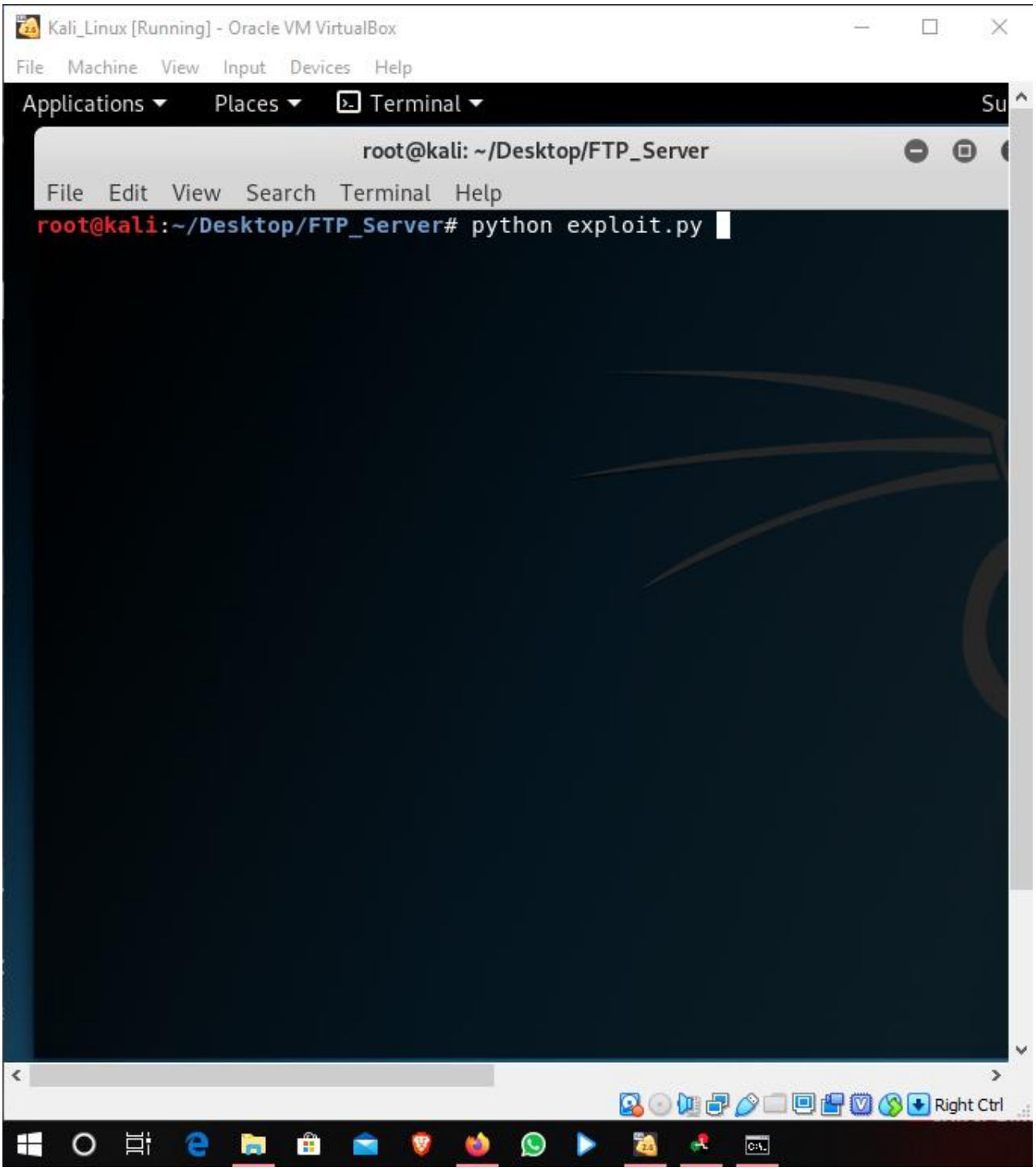

Figure 9

10. Enter IP address and exploit it

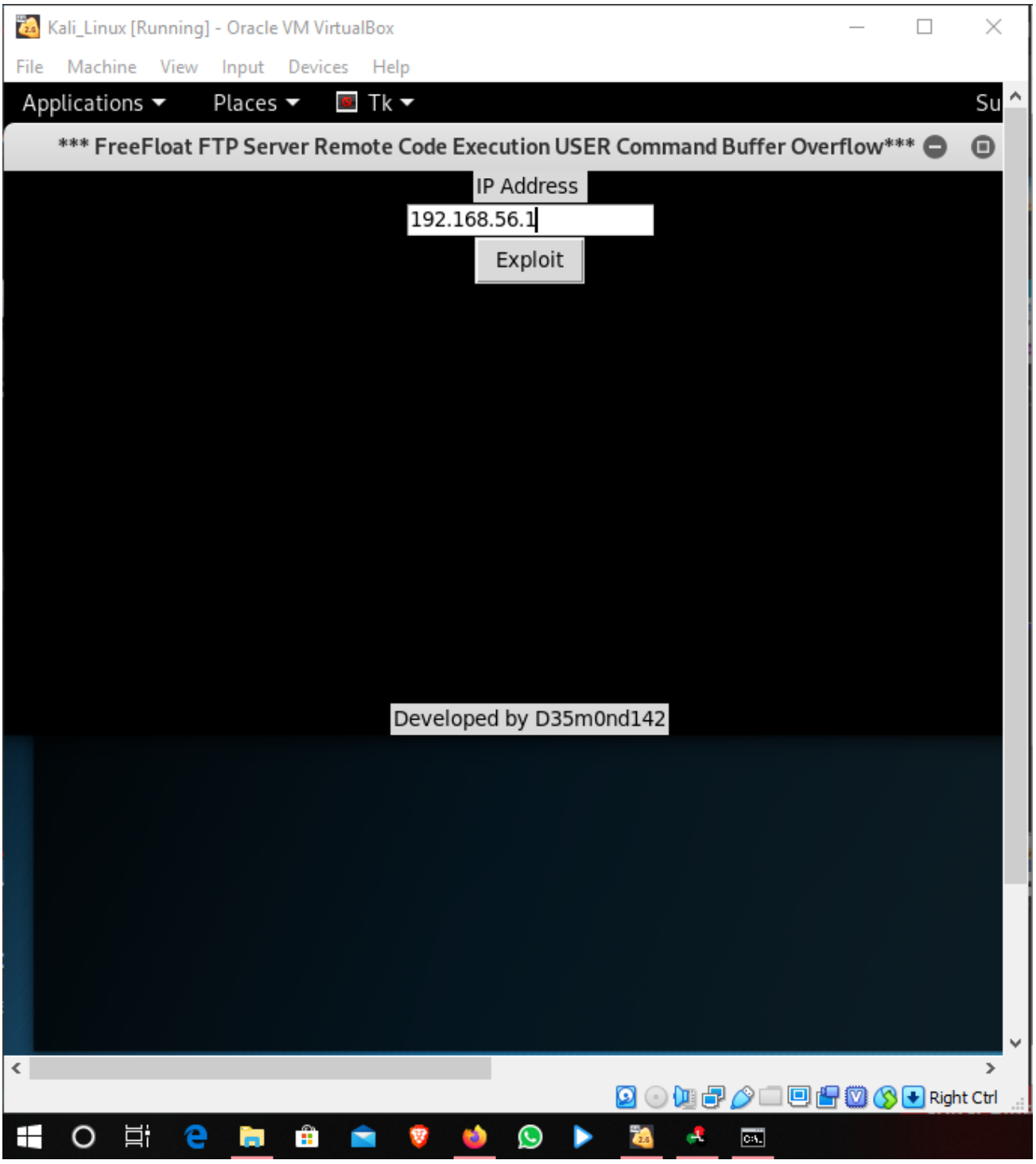

Figure 10

11. Run the msf-patern_create -l 500 code and get the result

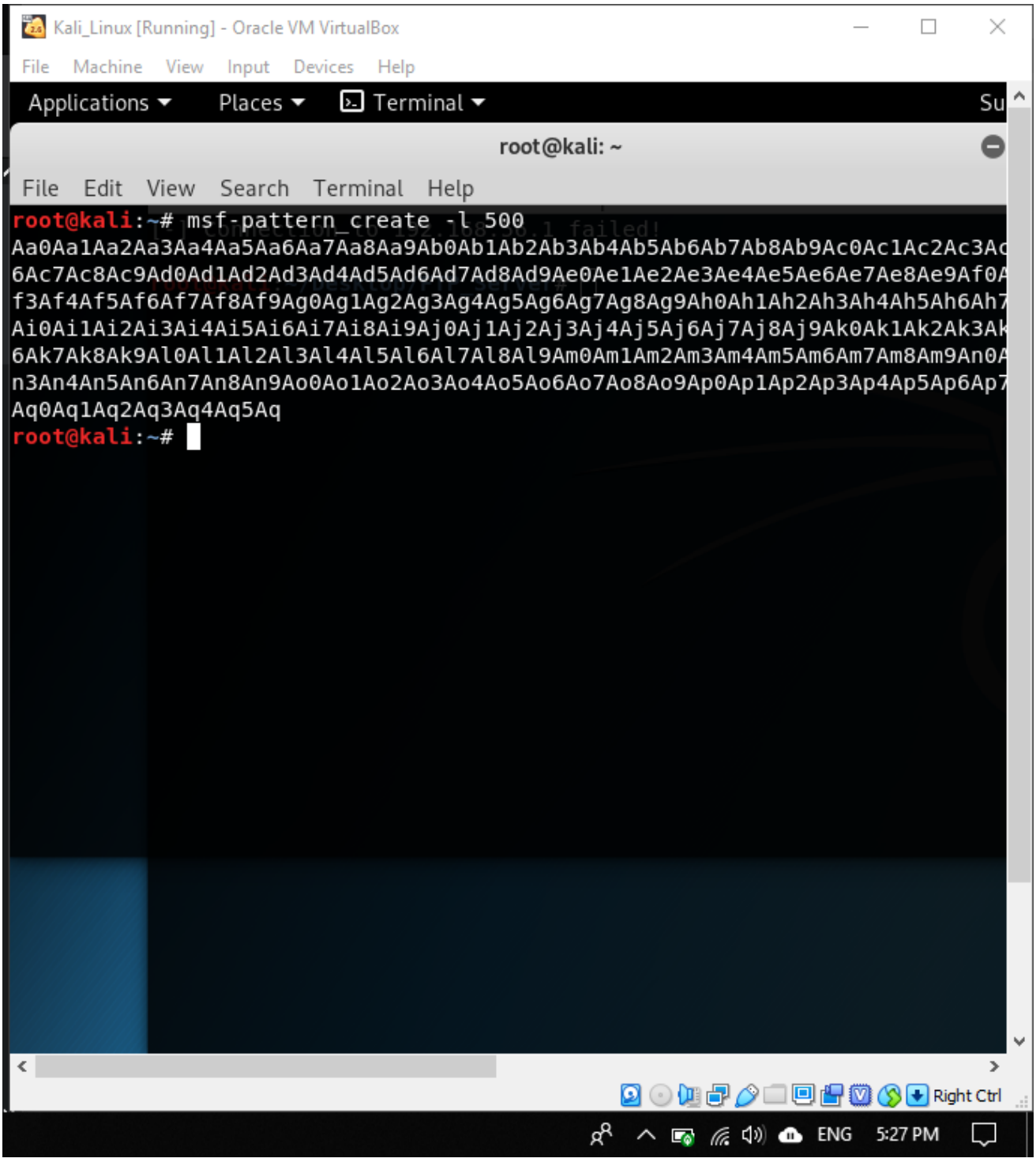

Figure 11

12. Run the msf-patern_offset -q 37684136 code and get the result

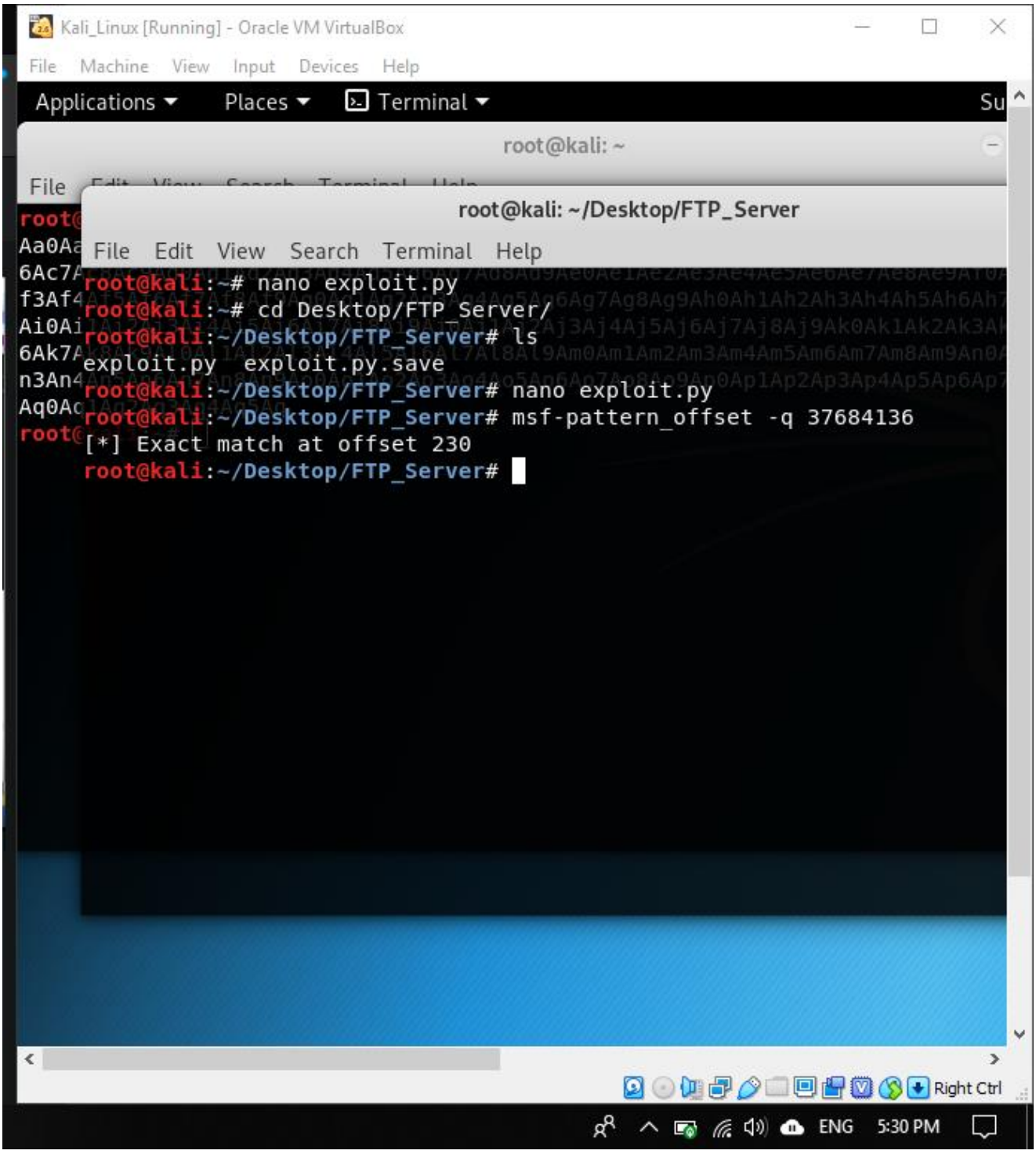

Figure 12

13. Resulting the msfcode

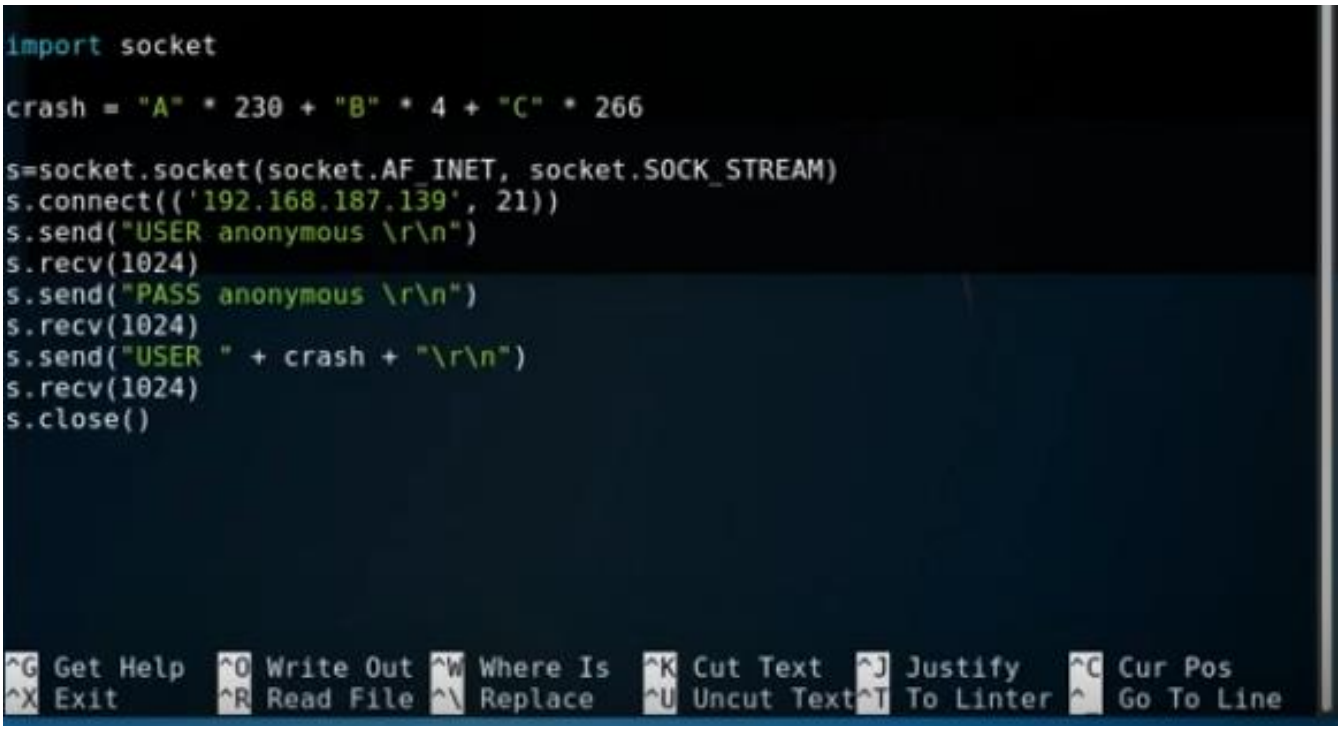

Figure 13

14. Add #JMP ESP SHELL32 75F41C80

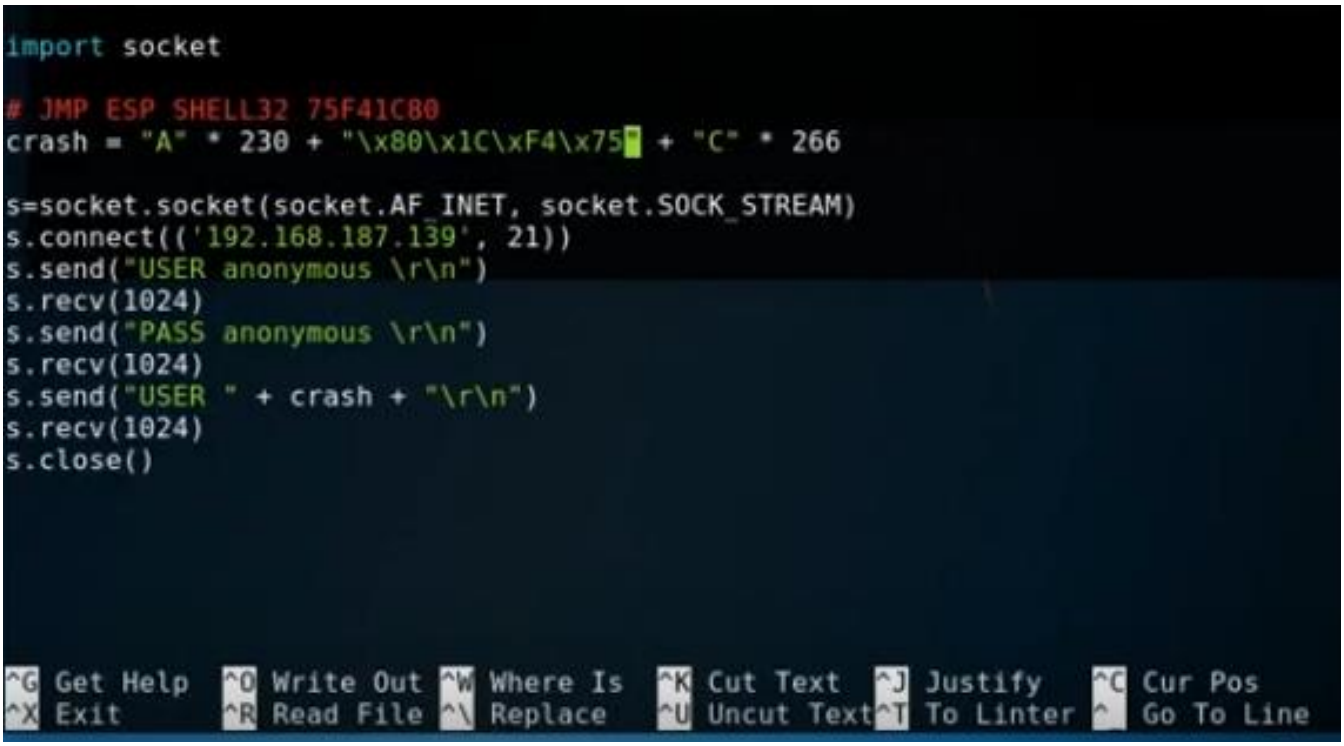

Figure 14

15. Remove SHELL32 and Add #JMP ESP KERNEL32 75F41C80

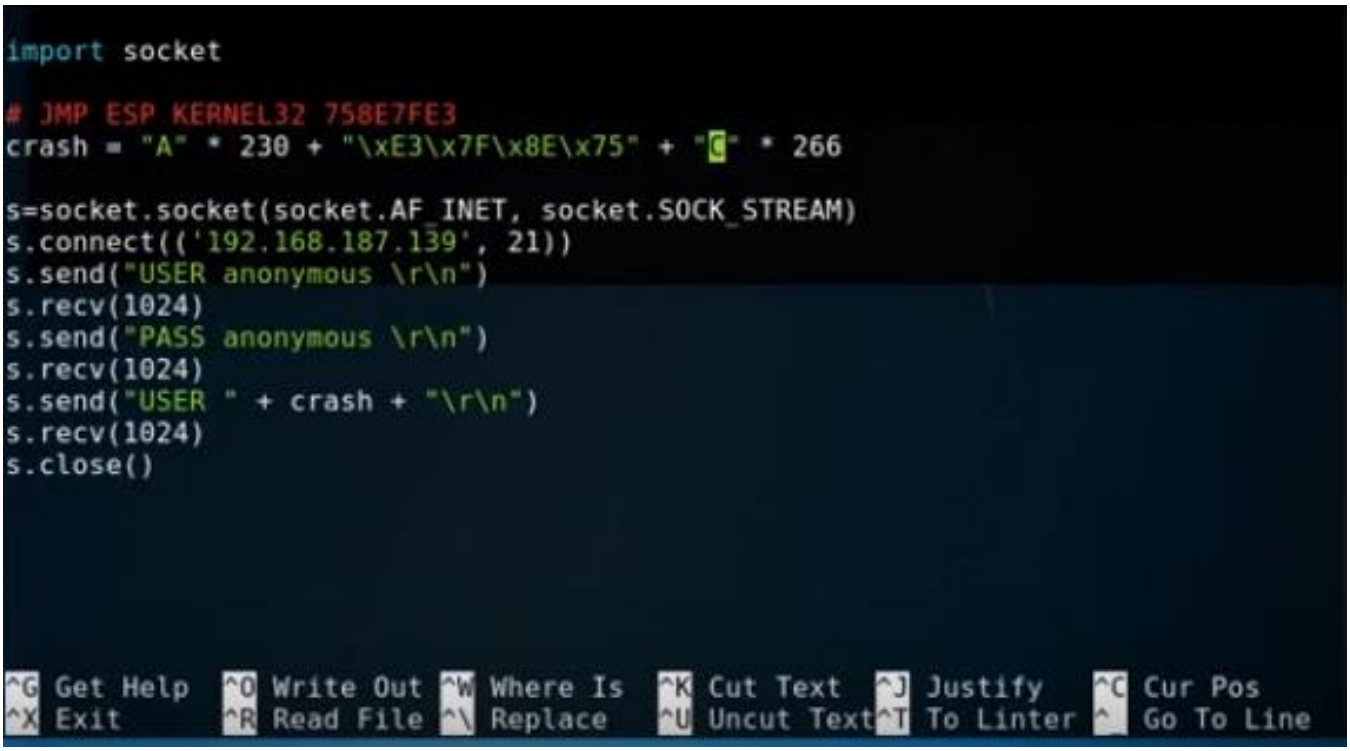

Figure 15

16. Run the msfvenom -p code and get the buffers

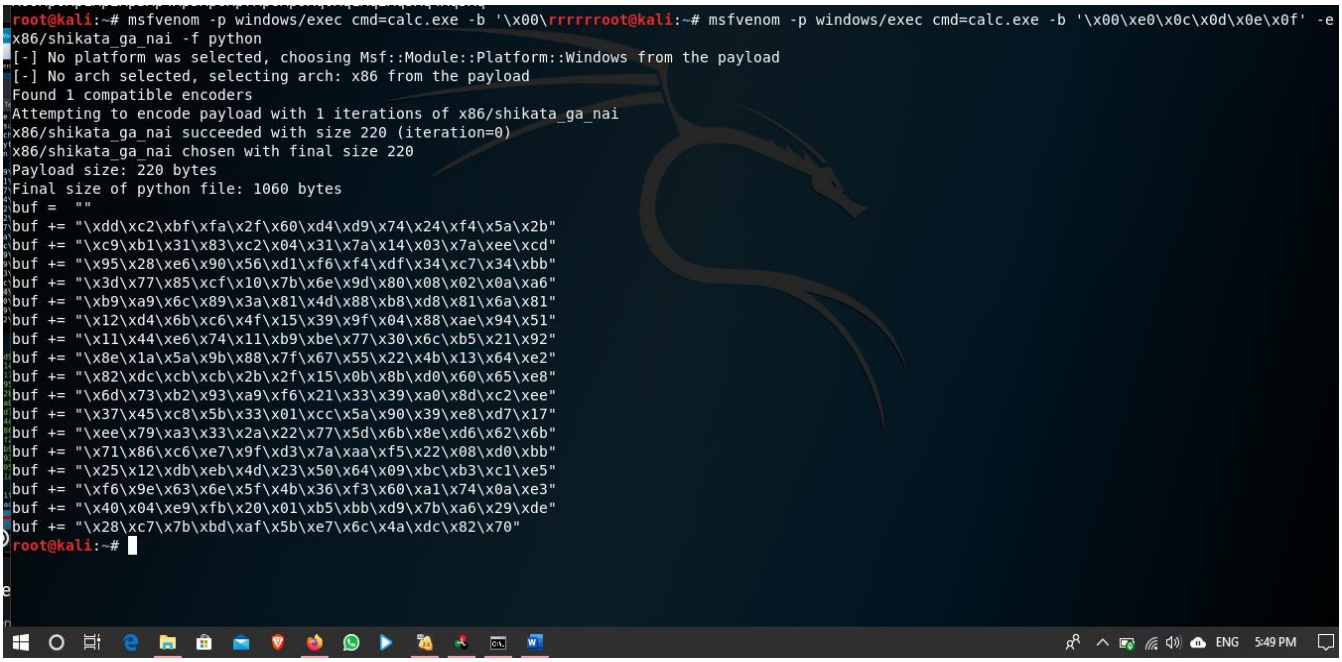

Figure 16

17. Exploitation is Success. It shows in blue line in the right side

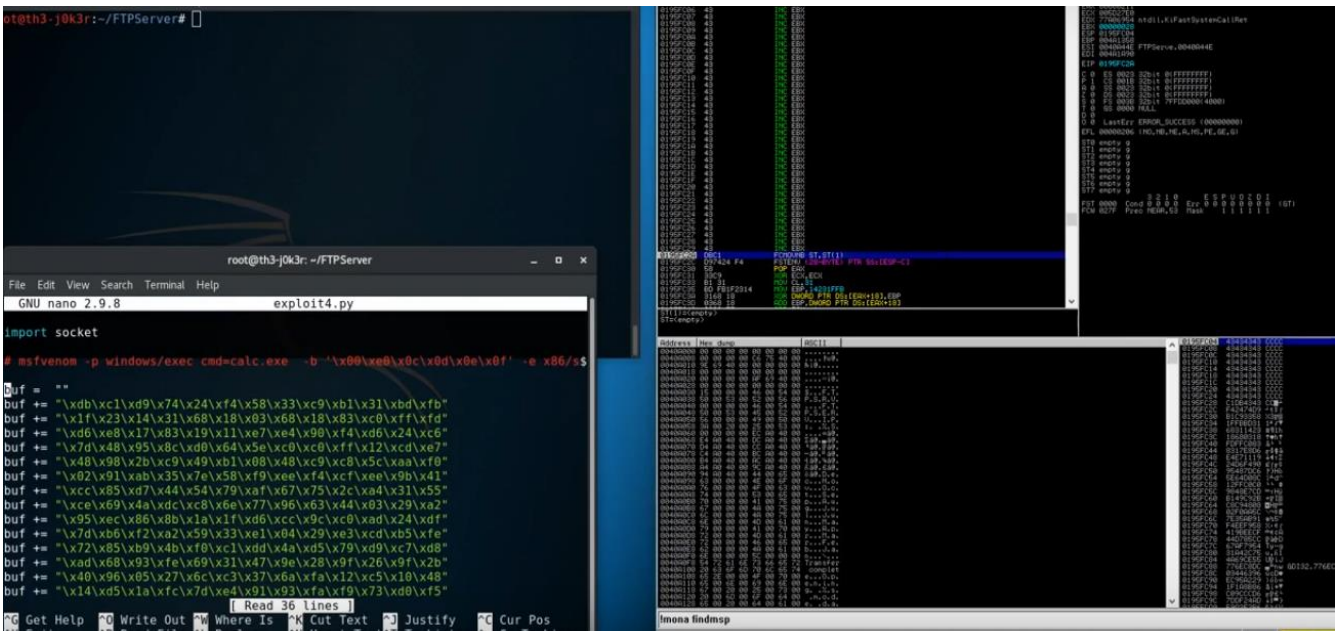

Figure 17