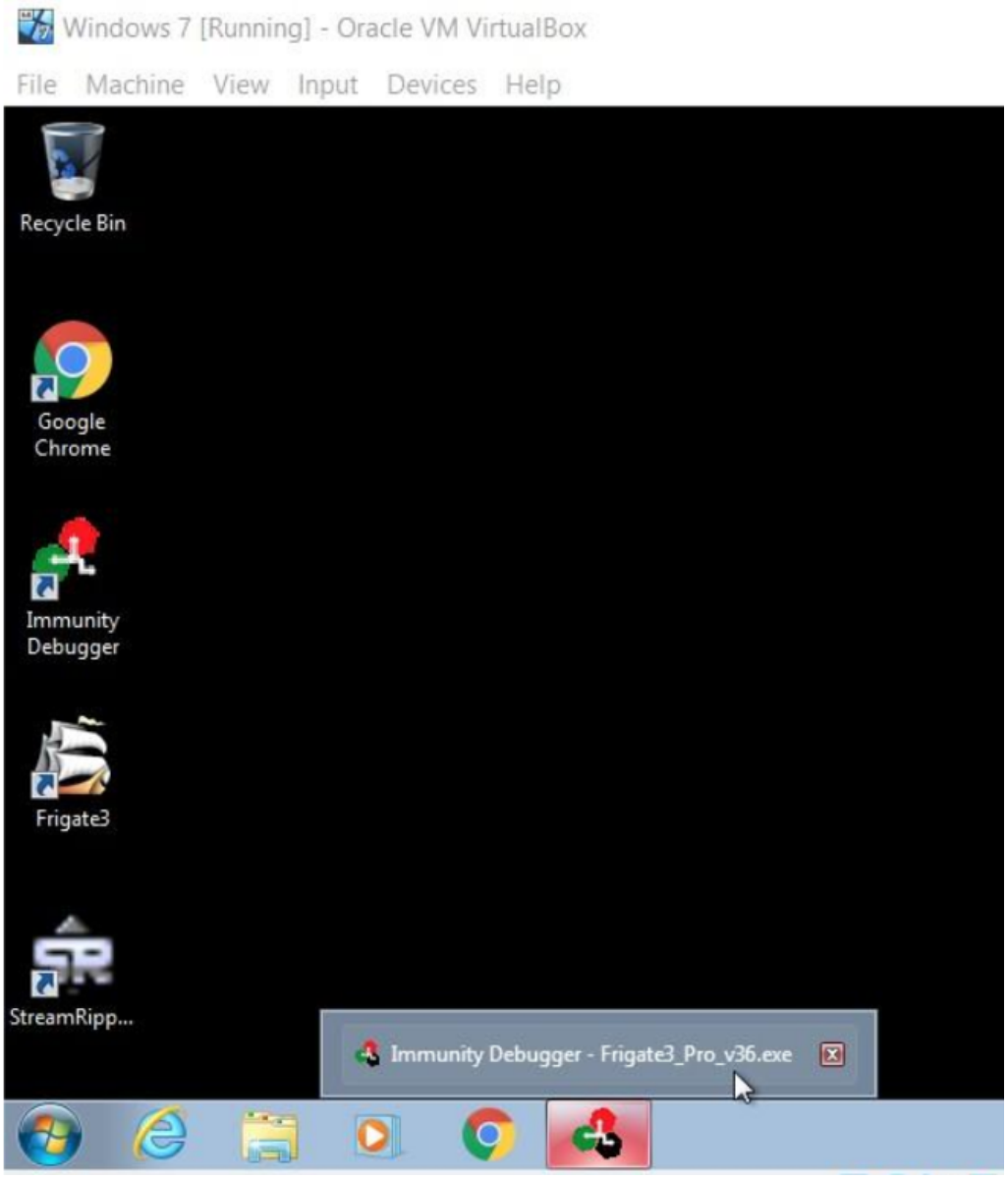
LAB-10: SECURE CODING

N. Satya Pramod
18BCE7293

Step 1:
Installing the Immunity Debugger and Running Frigate3.

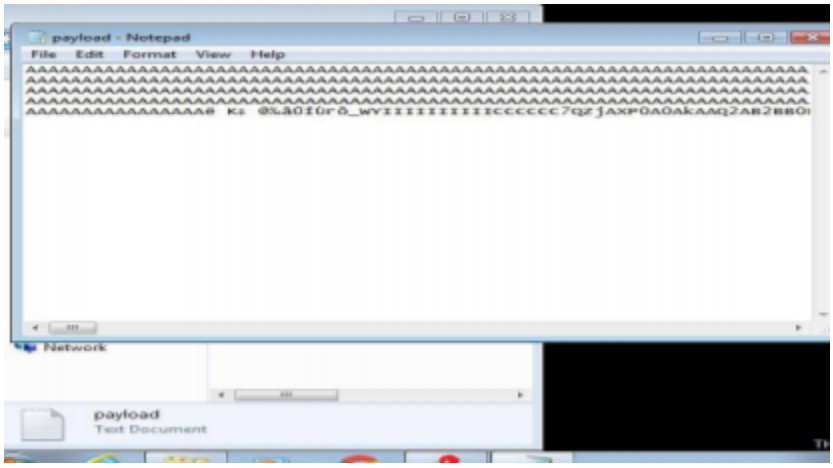


Step 2:

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

Python exploit2.py

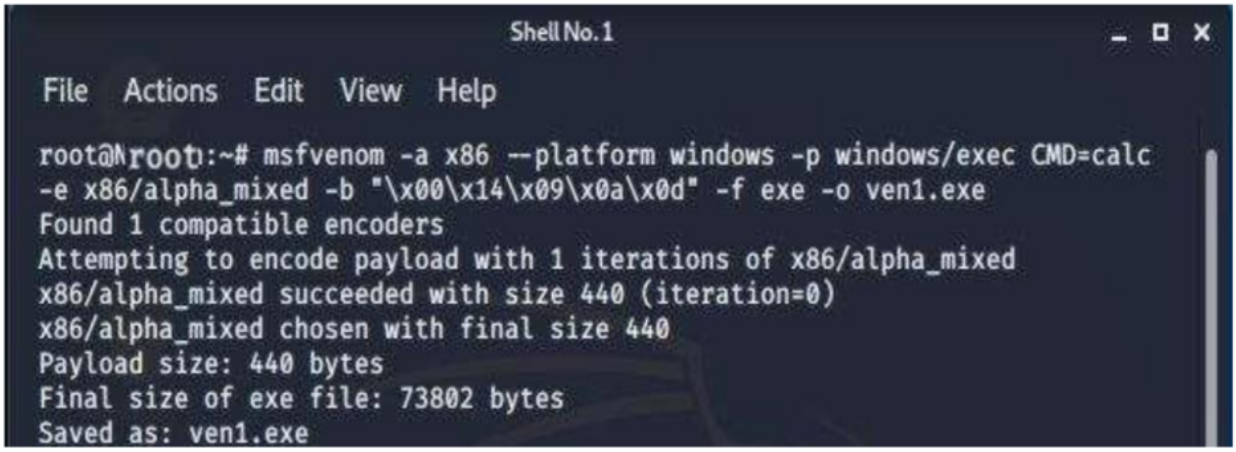
Notepad exploit2.txt

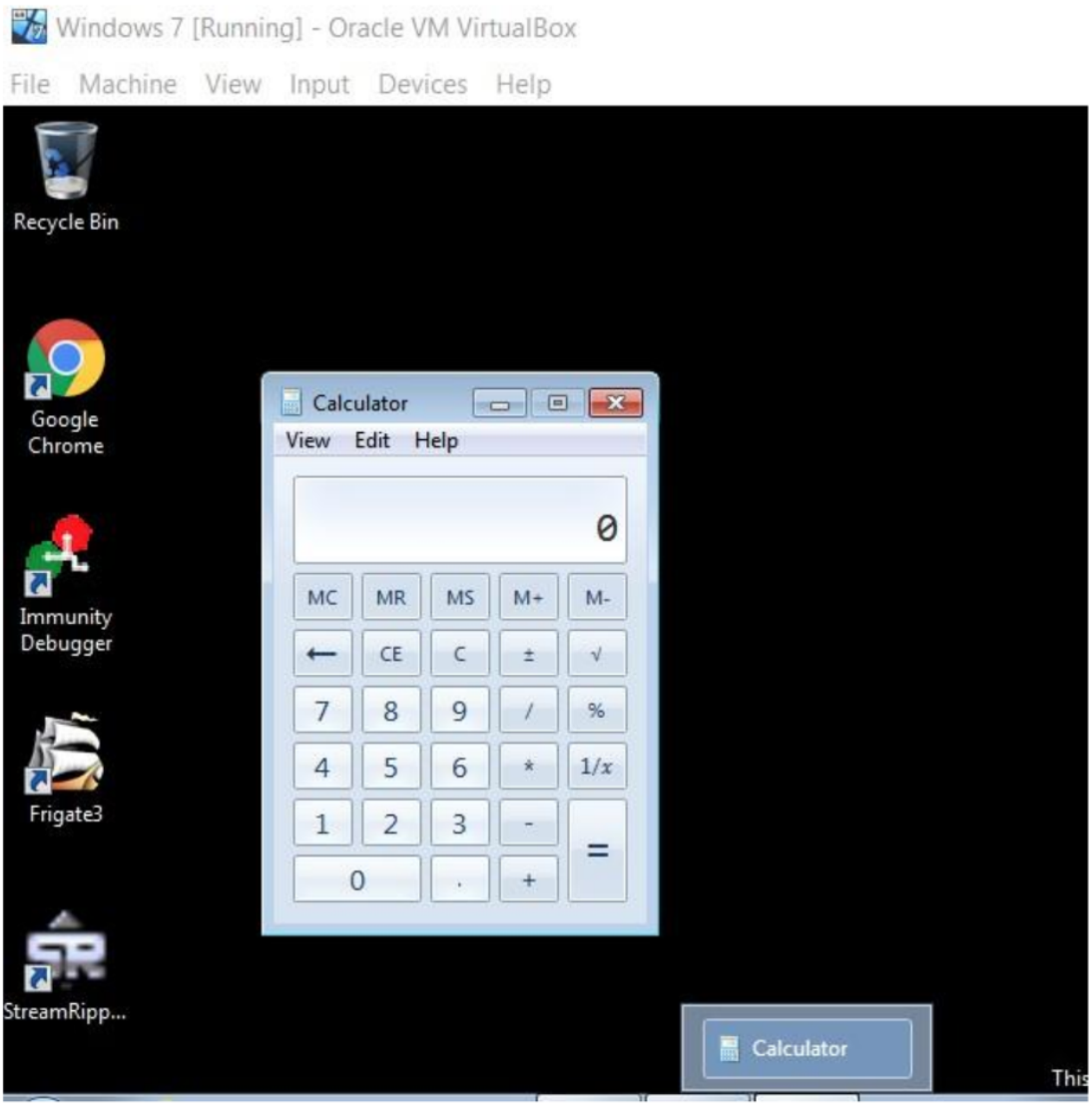


Step 3:

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.





Step 4:

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

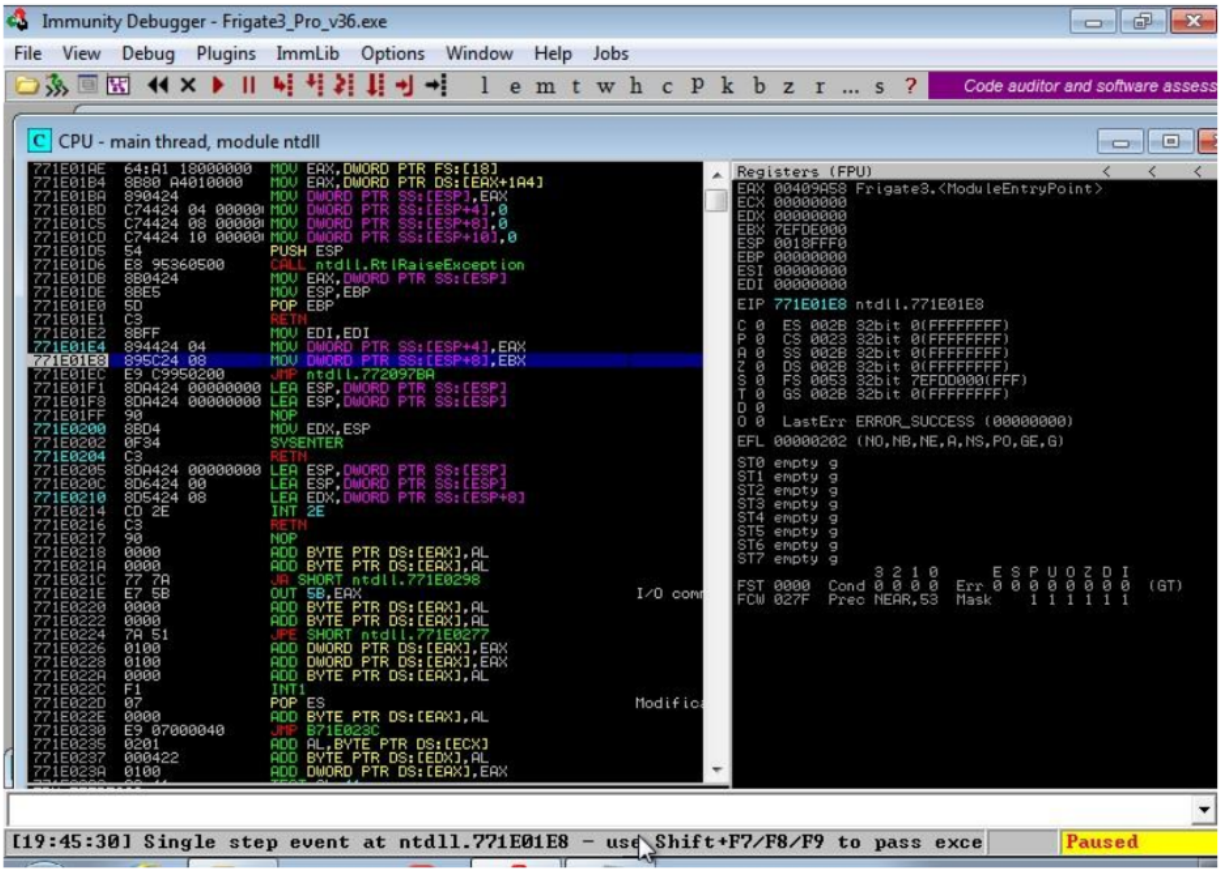
Attaching the Frigate3 to the Immunity Debugger.

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