SECURE CODING (CSE 2010)

LAB REPORT-10

Submitted by : Veneela Adapa

Reg no : 18BCN7127

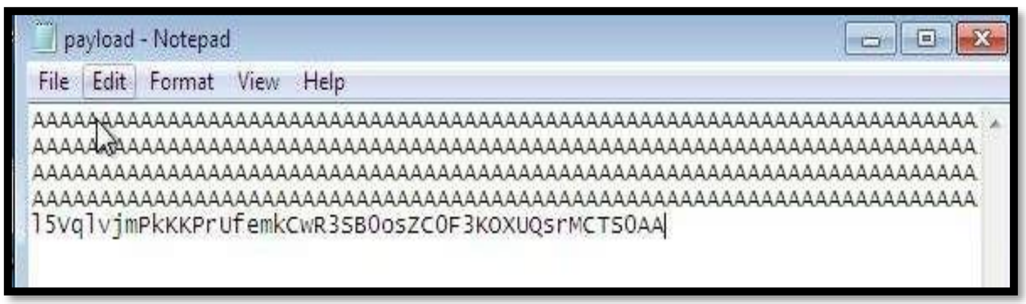
L39+L40 Slot

- *Installing the Immunuity Debugger and Running Frigate3.*

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

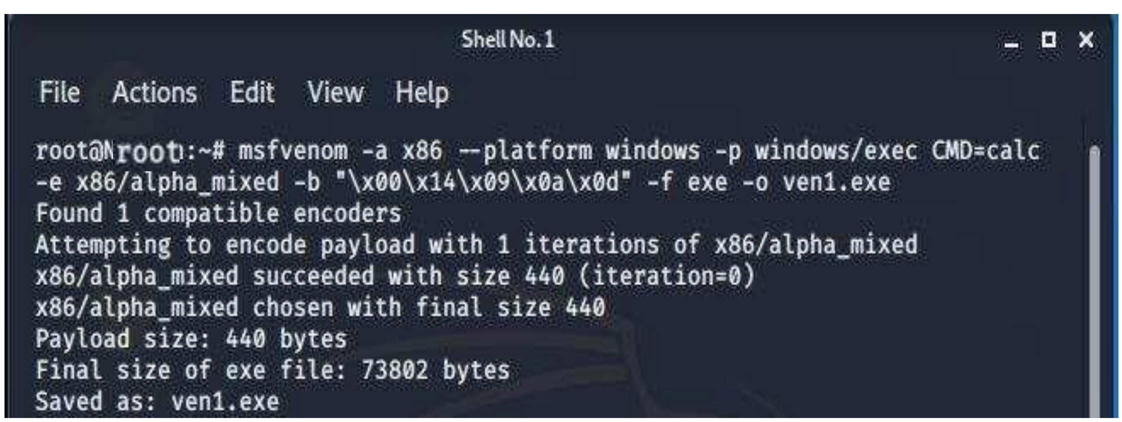
>python exploit2.py

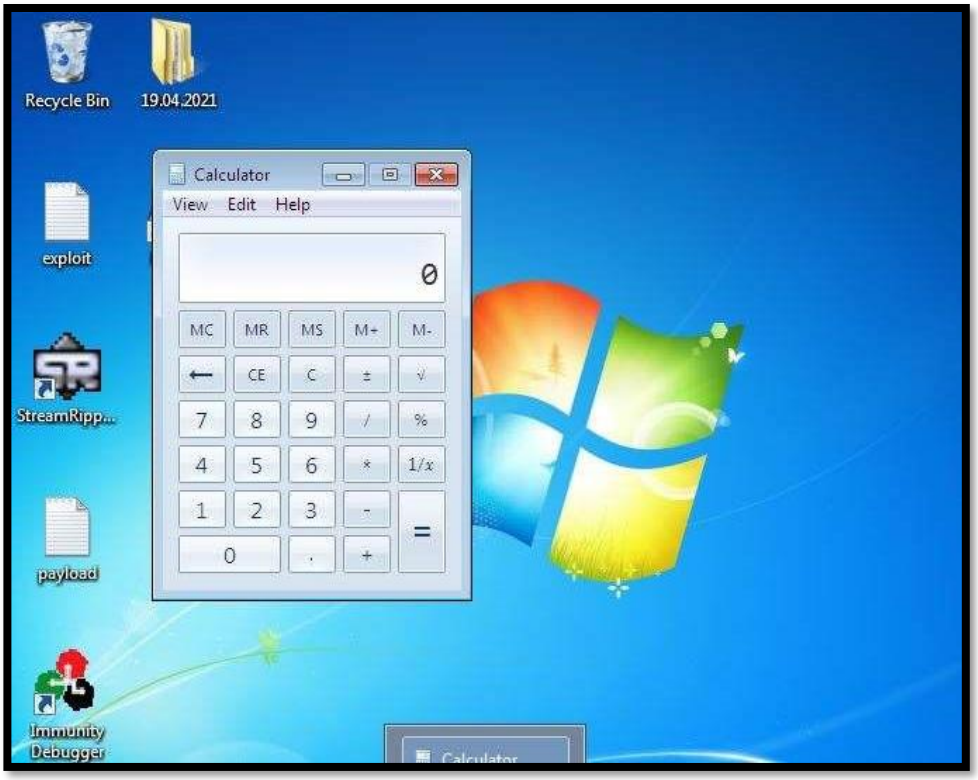
>notepad exploit2.txt



After Running the Exploit2.py The frigate3 stopped working and unable to open the application.

- *Creating .exe file to change the Default Trigger using kali linux.*





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

Attaching the Frigate3 to the Immunity Debugger.

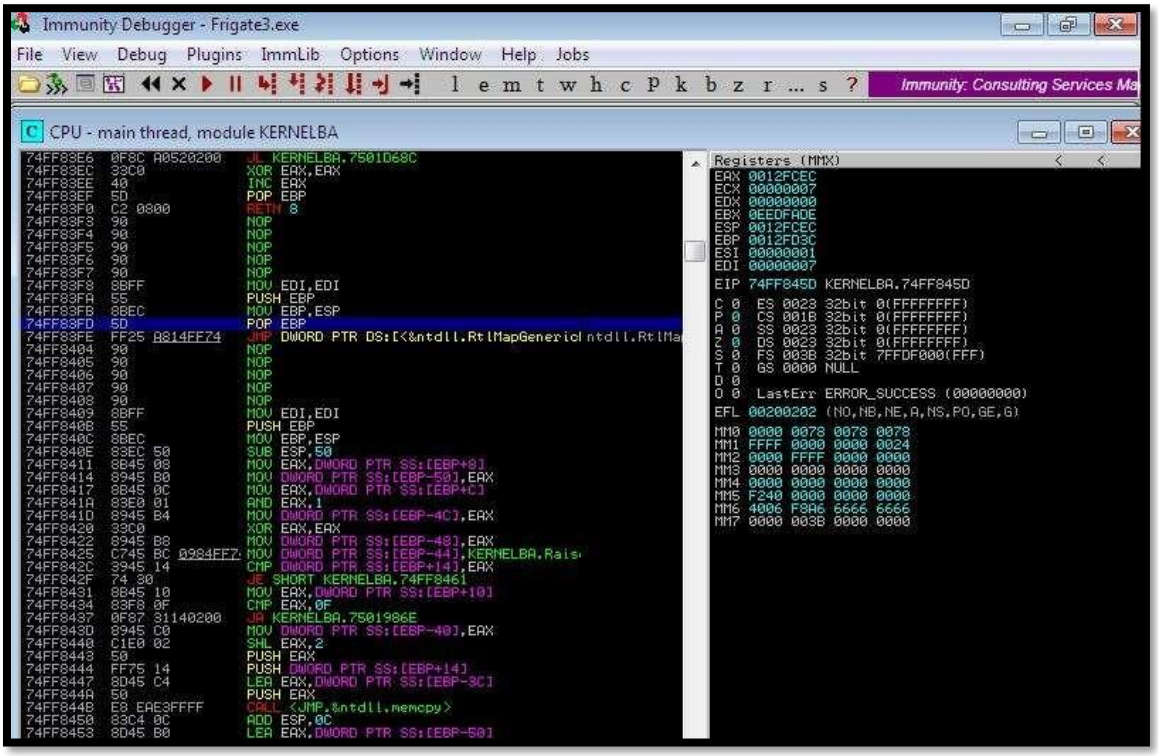
After Attaching the I have get the below details from Immunity Debugger

The EIP Address is:74FF8450

The Starting and Ending of Stack Frame is:

starting address=74FF1000

ending address=75034FFE



SHE Chain:

Address of dll are:0012FFC4