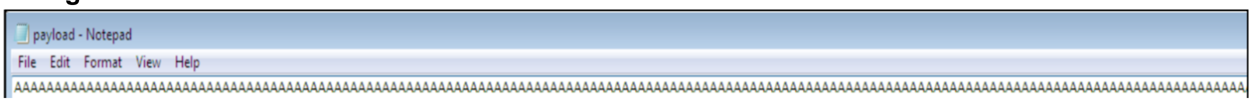
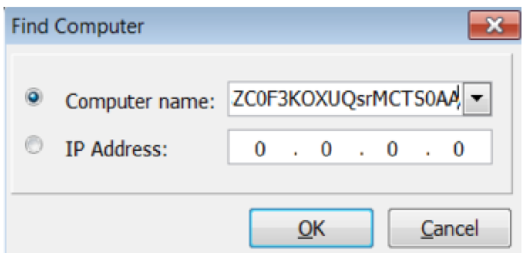
LAB 10

Chaturya Chinta
19BCE7528
L23+L24

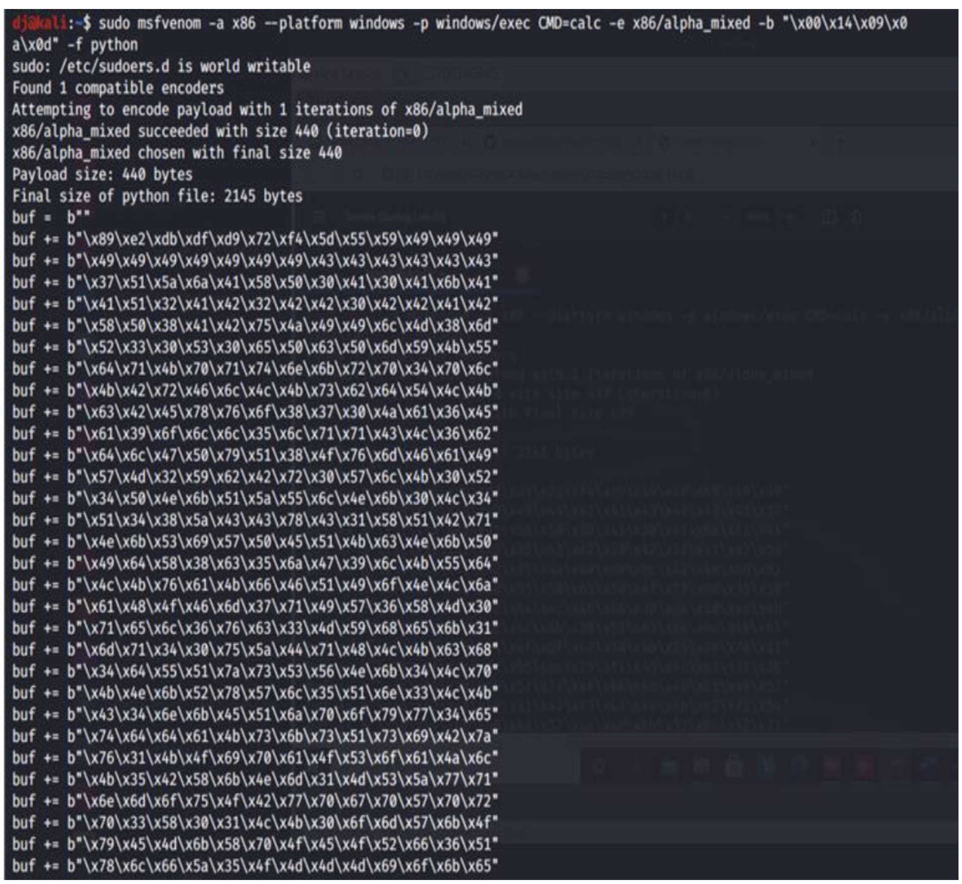
<u>Working with memory vulnerabilities:</u>

Install Frigate. Use the payload generated from exploit2.py and paste it in the vulnerable point of Frigate.

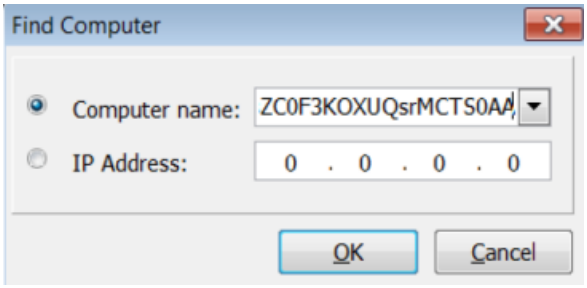




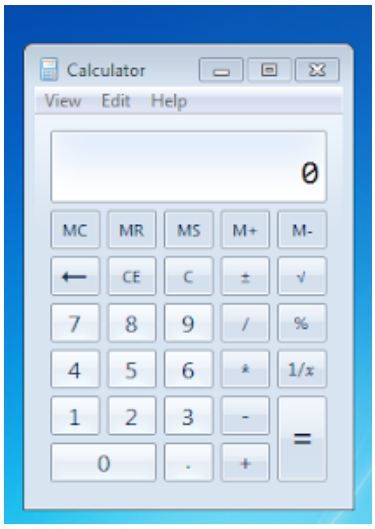
Code exploit(Use msfvenom in Kali linux).



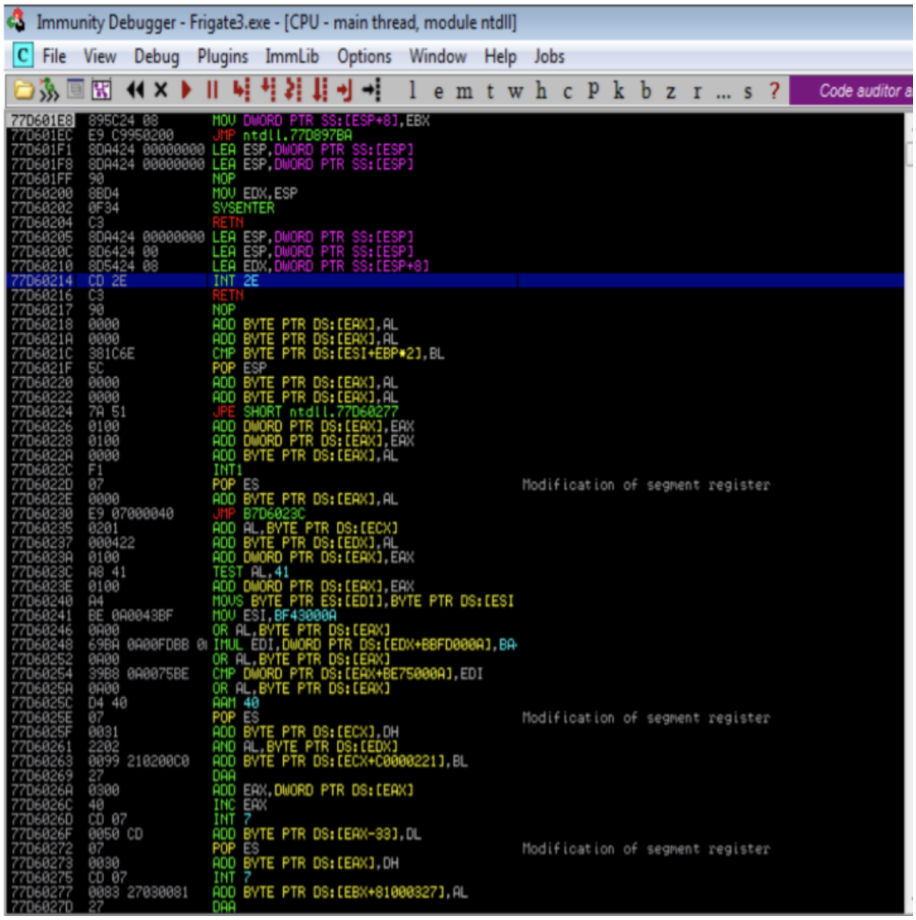
Using payload to exploit frigate



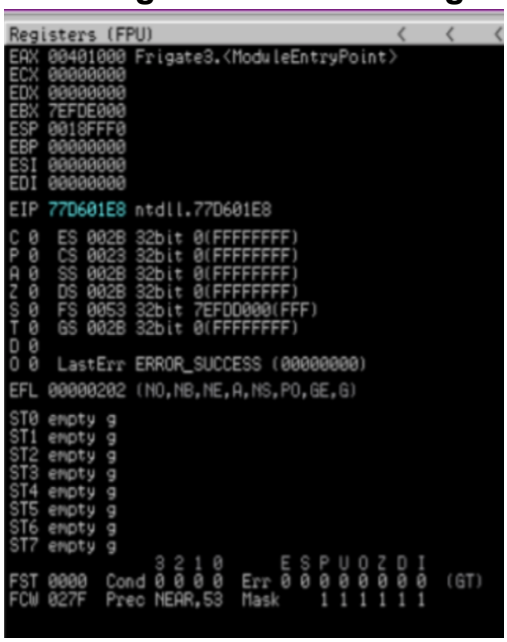
Application crashes and calculator opens



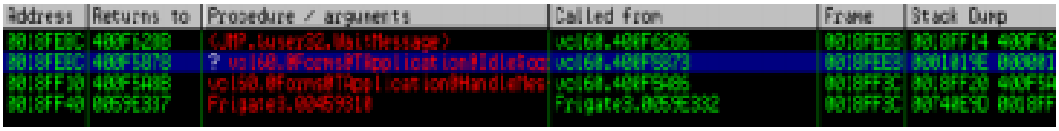
Attach Frigate to the Immunity Debugger.



Checking EIP address along with addresses of other registers



Checking the starting and ending addresses of stack frame.



Checking the SEH chain and report the dll loaded along with the addresses.