Ex.No:10 **Name:** Ganga Suresh Kumar Nair
Date: 19-04-2021 **Reg.No:** 18BCN7014

Secure Coding

Lab experiment - Working with the memory vulnerabilities – Part IV

Task

- **Download Frigate3_Pro_v36 from teams (check folder named 19.04.2021).**
- **Deploy a virtual windows 7 instance and copy the Frigate3_Pro_v36 into it.**
- **Install Immunity debugger or ollydbg in windows7**
- **Install Frigate3_Pro_v36 and Run the same**
- **Download and install python 2.7.* or 3.5.***
- **Run the exploit script II (exploit2.py- check today's folder) to generate the payload**

Analysis

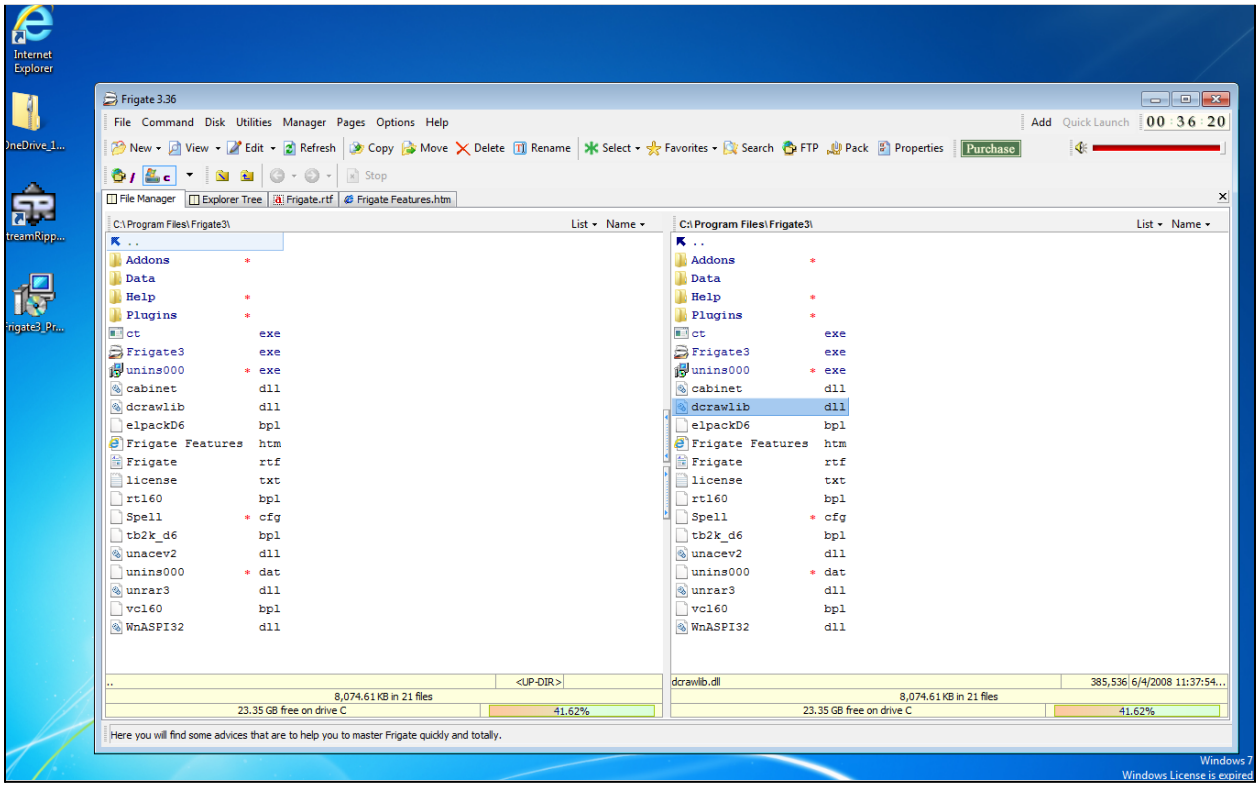
- **Try to crash the Frigate3_Pro_v36 and exploit it.**
- **Change the default trigger from cmd.exe to calc.exe (Use msfvenom in Kali linux).**

Example:

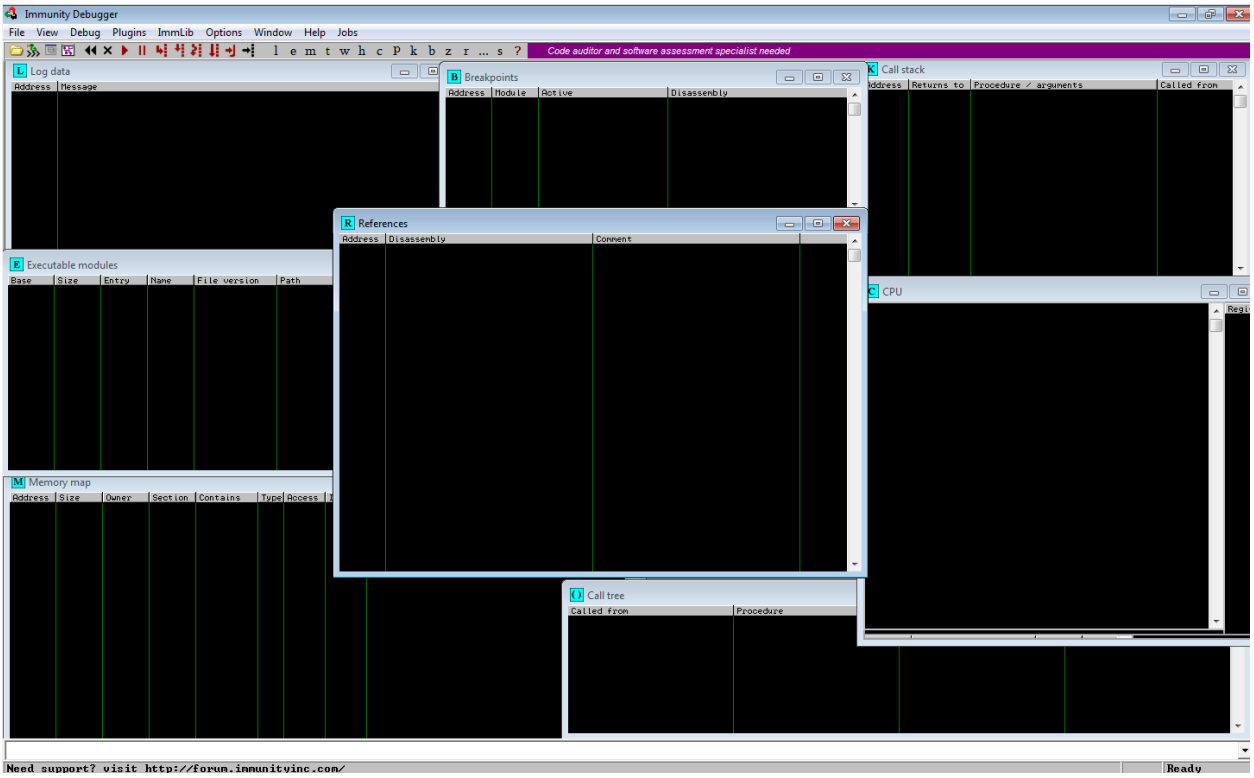
msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python

- **Attach the debugger (immunity debugger or ollydbg) and analyse the address of various registers listed below**
- **Check for EIP address**
- **Verify the starting and ending addresses of stack frame**
- **Verify the SEH chain and report the dll loaded along with the addresses. For viewing SEH chain, goto view à SEH**

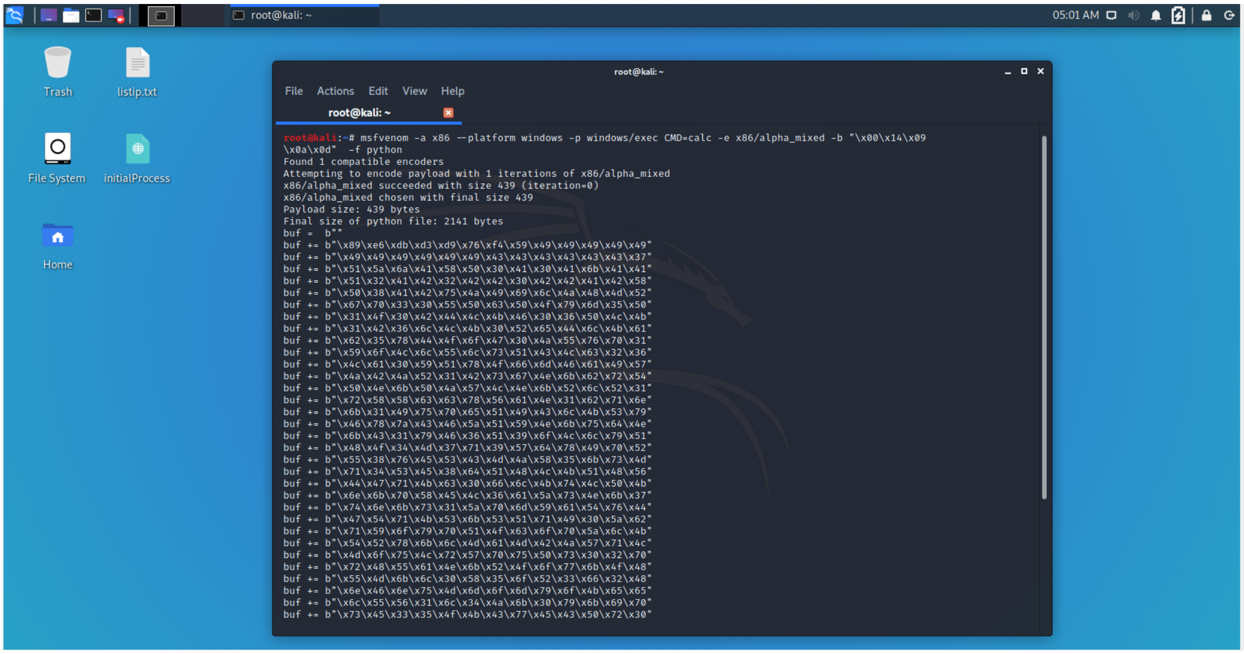
Frigate 3



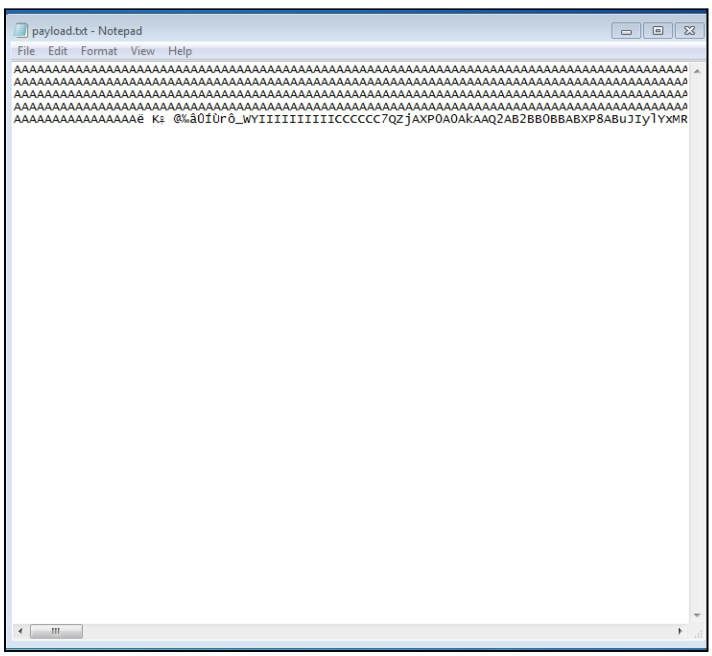
Immunity debugger



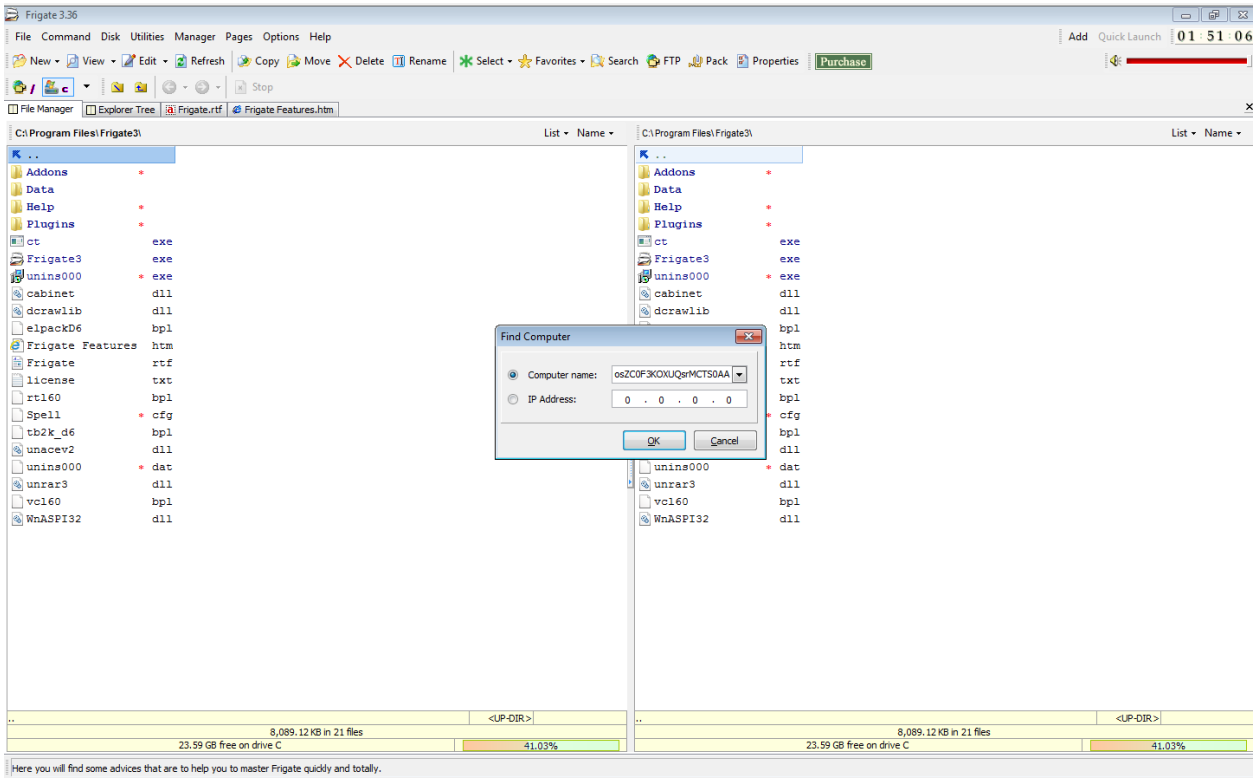
Getting shell code for exploit from msfvenom kali



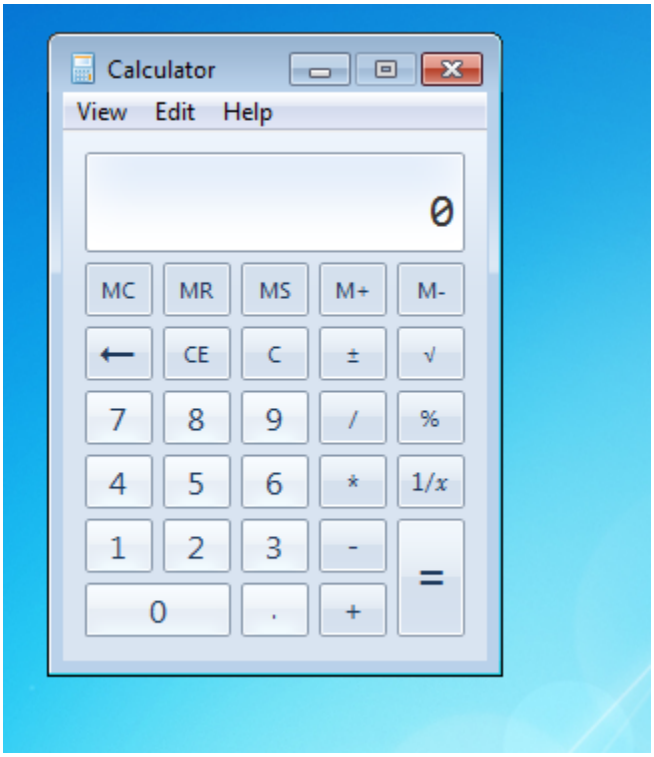
After running exploit2.py , payload is generated



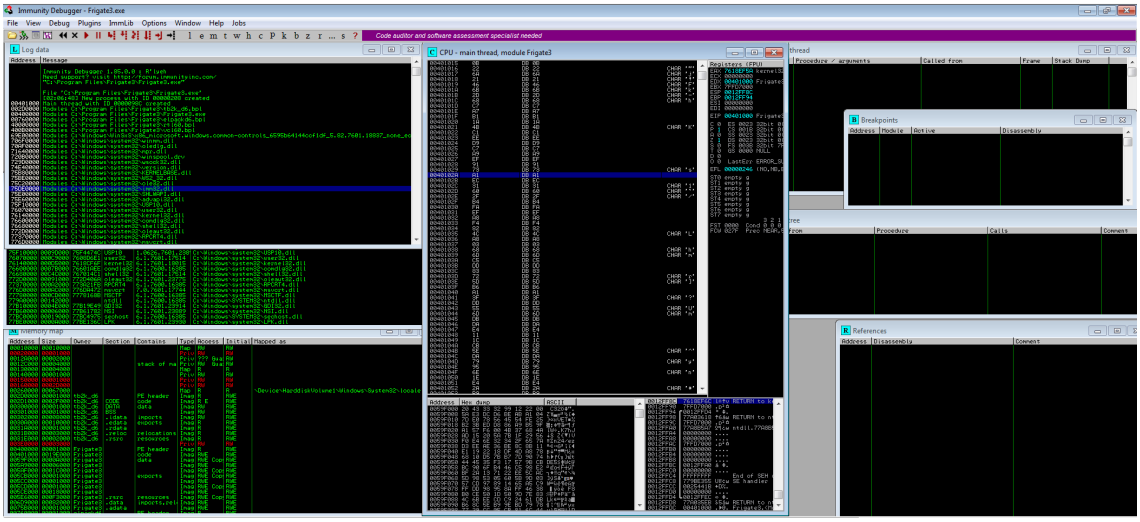
Crashing frigate using the payload generated



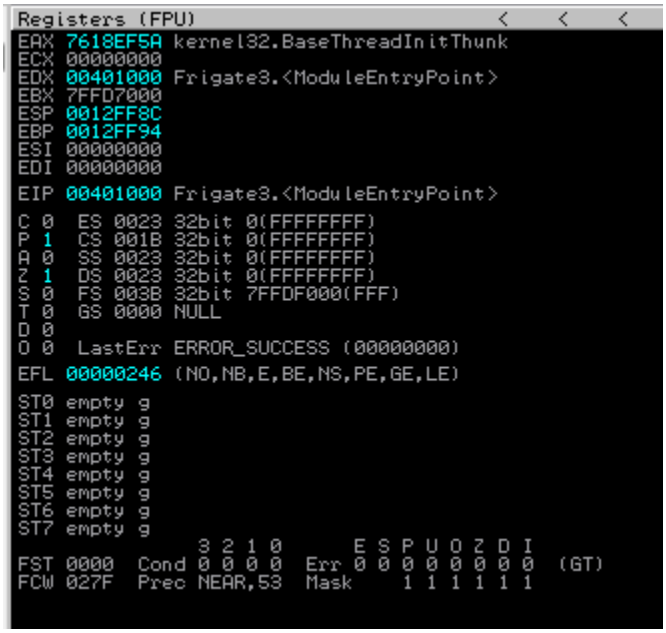
App crashes and calc is triggered



Immunity debugger



Addresses of various registers



EIP- Instruction pointer Address is 00401000

Base pointer of stack frame is 0012FF94 and stack pointer is 0012FF8C

SEH chain, we can see the dll loaded is ntdll