SECURE CODING LAB 10

MEGHANA CILAGANI

19BCN7157

Lab experiment - Working with the memory vulnerabilities – Part IV

Task

- **Download Frigate3_Pro_v36 from teams (check folder named 17.04.2021).**
- **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

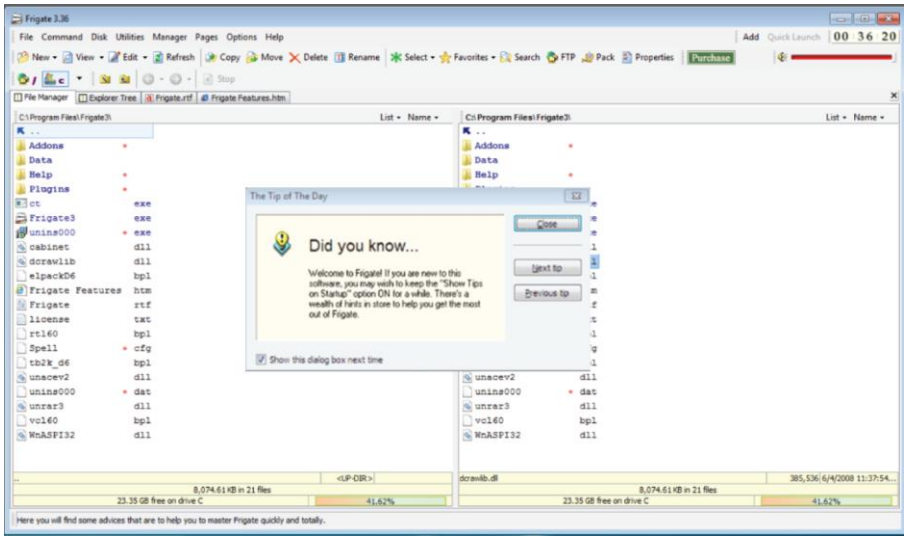
- **Try to crash the Frigate3_Pro_v36 and exploit it.**
- **Change the default trigger from cmd.exe to calc.exe (Use msfvenom in Kali linux).**

Example:

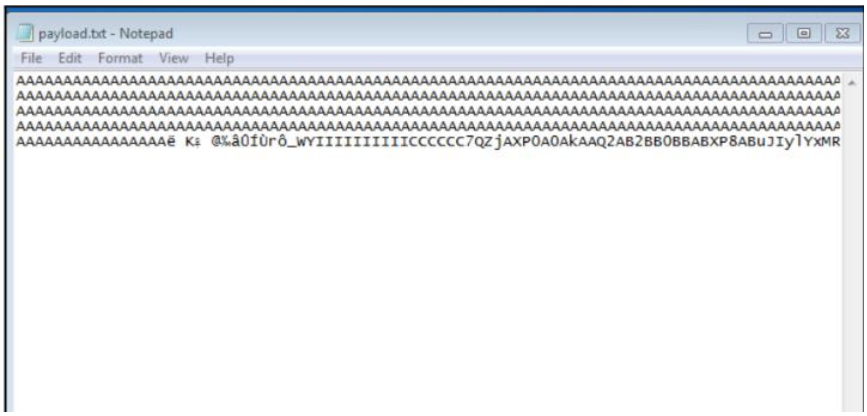
msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python

- **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 → SEH**

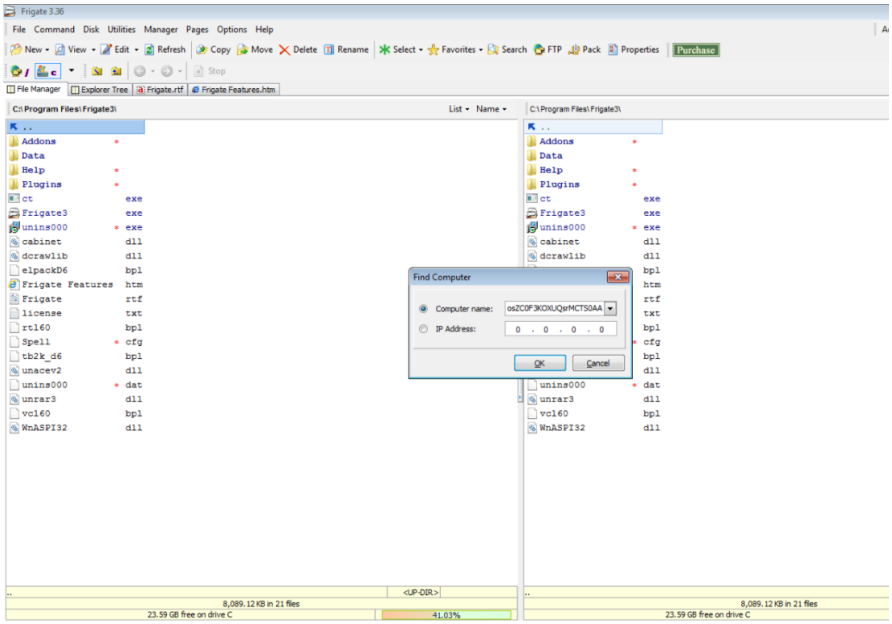
Install Frigate in Vmware



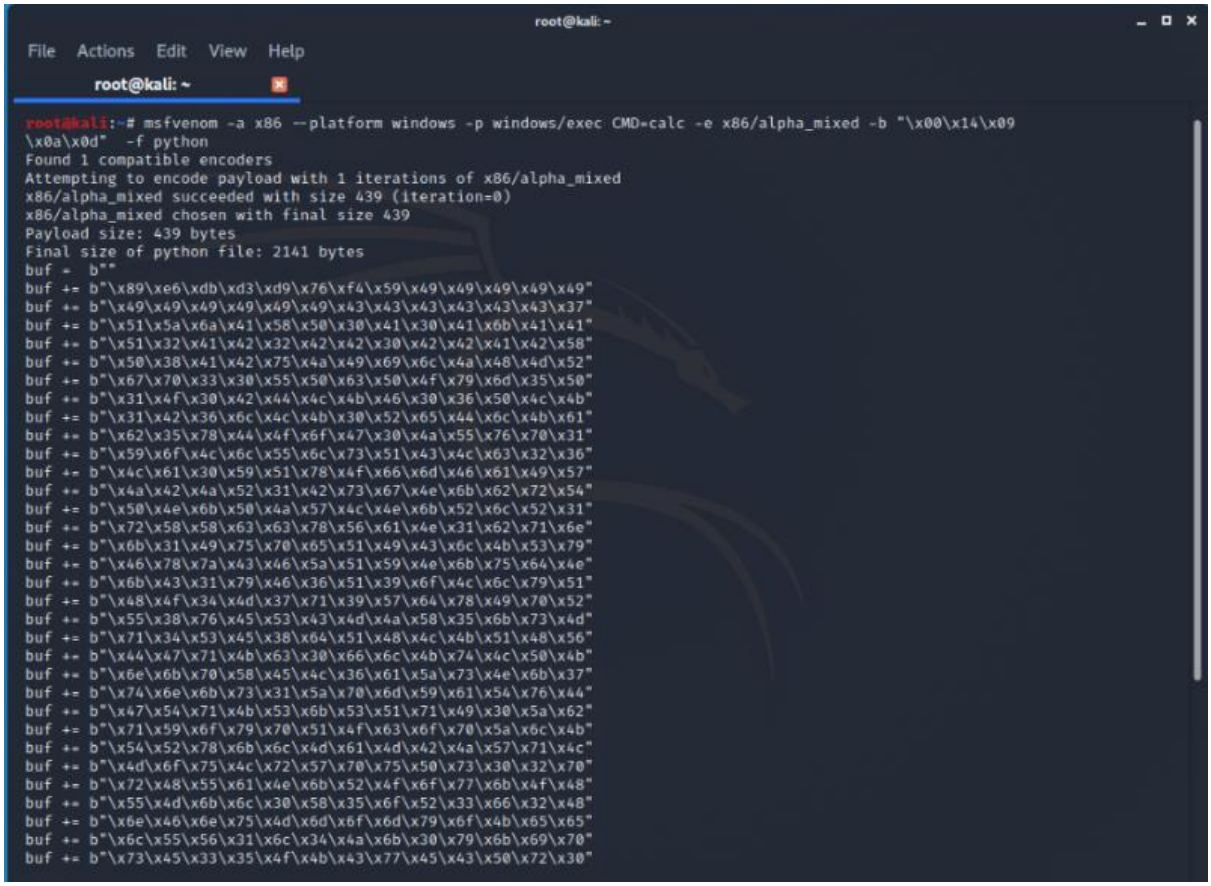
Execute the exploit2.py and generate payload



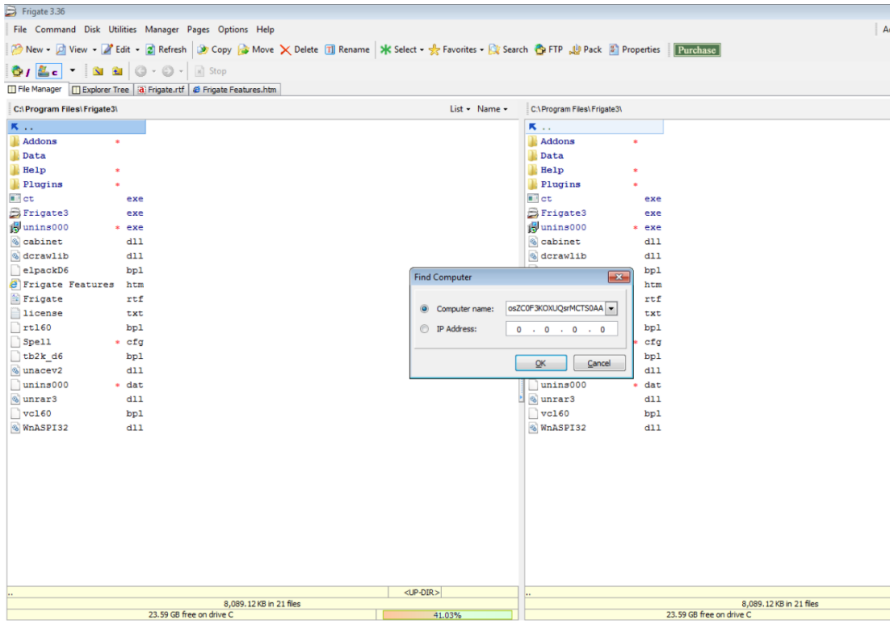
Copy the payload and paste in frigate in find computer



Code exploit from msfvenom kali linux

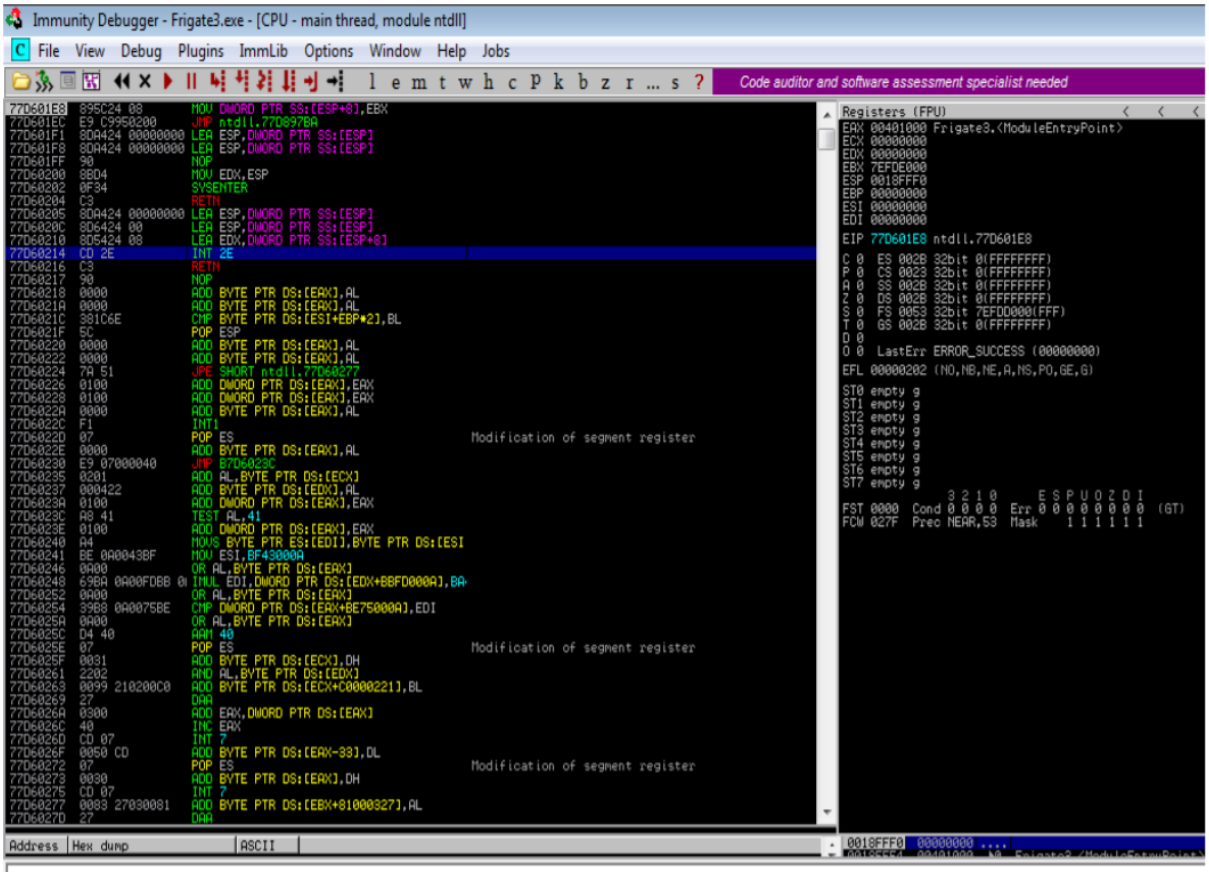


Using payload to exploit friget

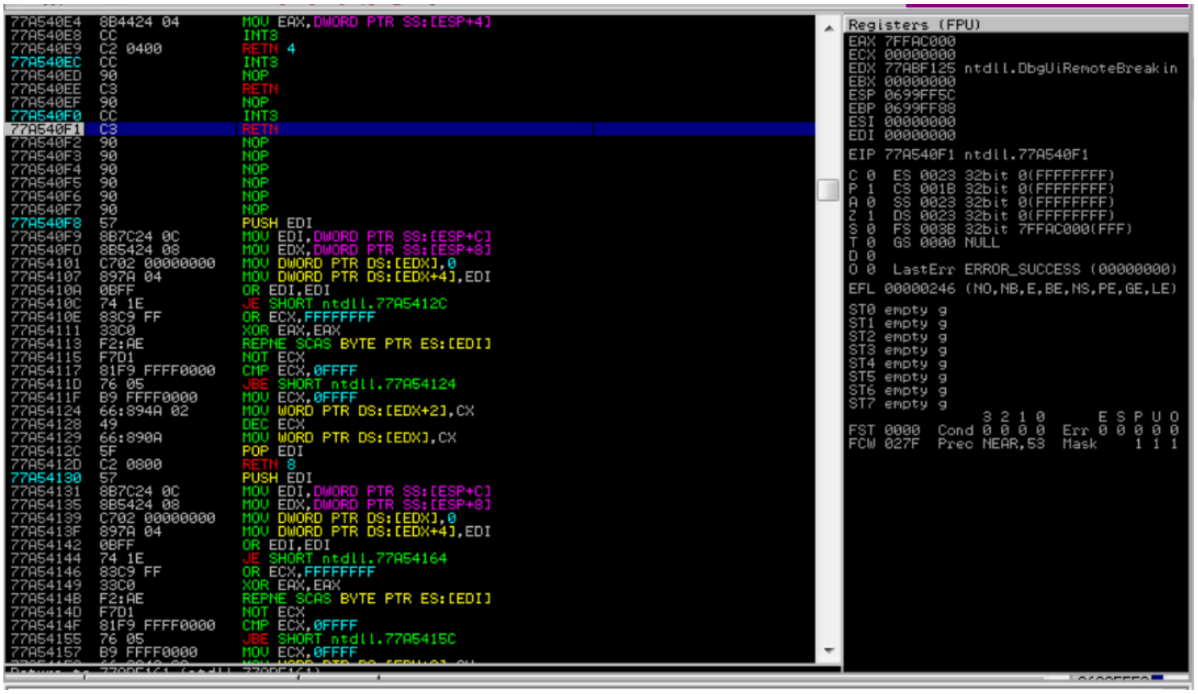


The Application crashes and calculator opens

Attaching the Frigate3 to immunity debugger and analyse the address of various registers listed below :



Check for EIP address



Verify the SEH chain and report the dll loaded along with the addresses. For viewing SEH chain, goto view SEH :