Secure Coding

Lab-10

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**

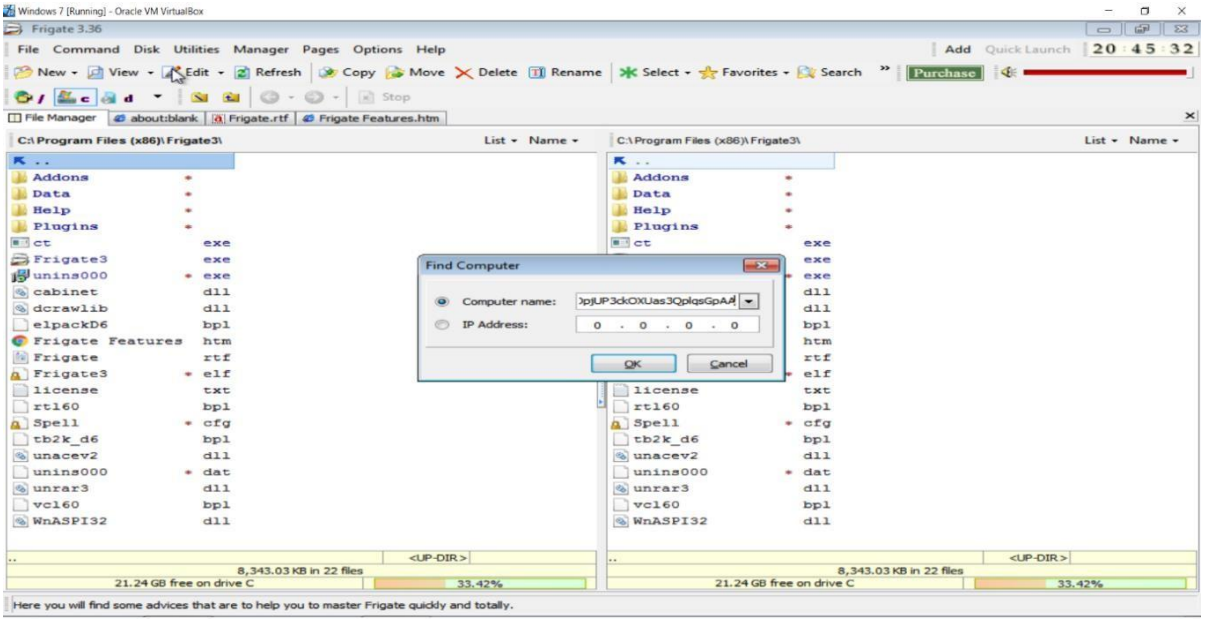
Analysis

- **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).**

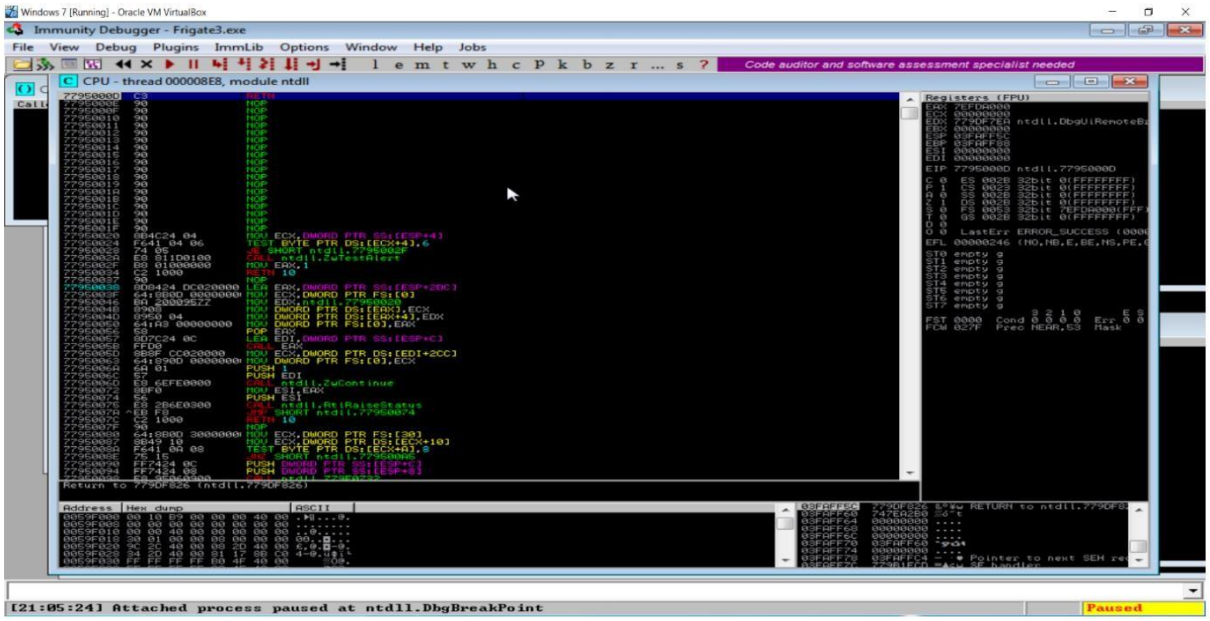
  Example: msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python

- **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**

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

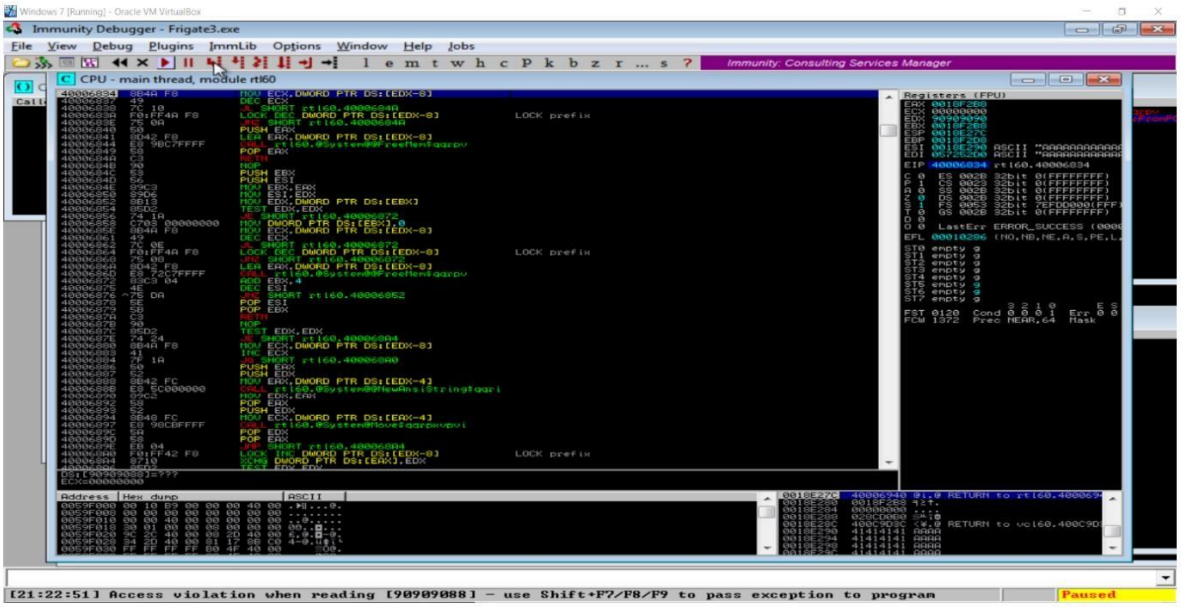
```
Registers (FPU)
EAX 7EFDA000
ECX 00000000
EDX 779DF7EA ntdll.DbgUiRemoteB
EBX 00000000
ESP 03FAFF5C
EBP 03FAFF88
ESI 00000000
EDI 00000000
EIP 7795000D ntdll.7795000D
C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 1  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 7EFDA000(FFF
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (000
EFL 00000246 (NO,NB,E,BE,NS,PE,
ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
```

Verifying the SHE chain.

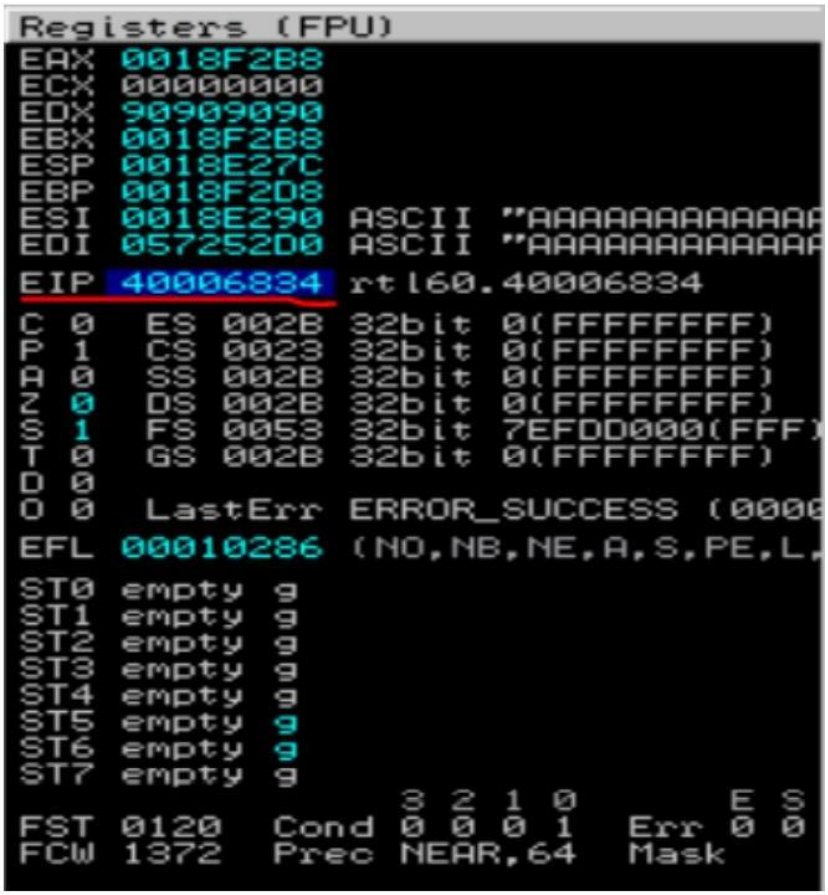
```
SEH chain of thread 000...
Address   SE handler
03FAFF78  ntdll.779B1ECD
03FAFFC4  ntdll.779B1ECD
```

After Execution (Exploitation):

Analysing the address of various registers:



Checkingfor EIP address



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

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

K.Bala Eswar

19BCN7003