SECURE CODING CSE2010

LAB-10

CH.SAI SUMEDH

REG NO:-18BCN7092

SLOT:-L39+L40

Lab experiment - Working with the memory vulnerabilities – Part IV

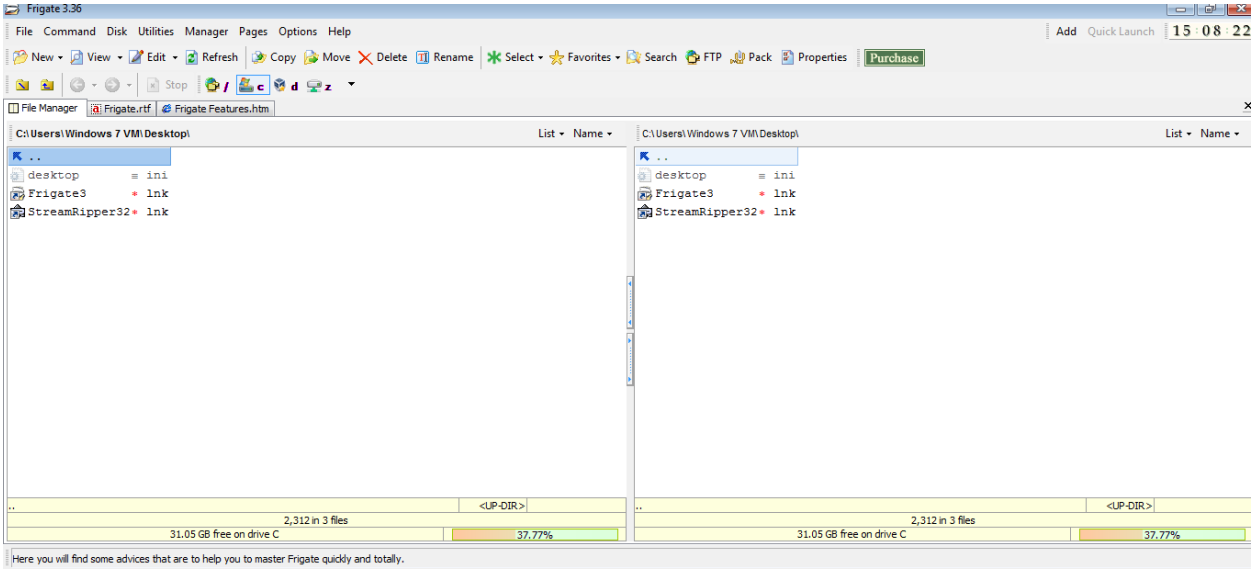
Task

- 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

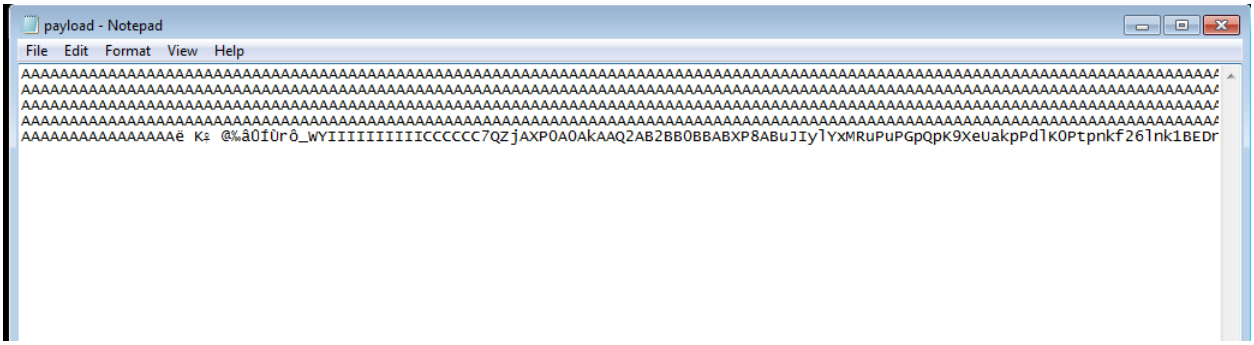
Analysis

- 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 → SEH

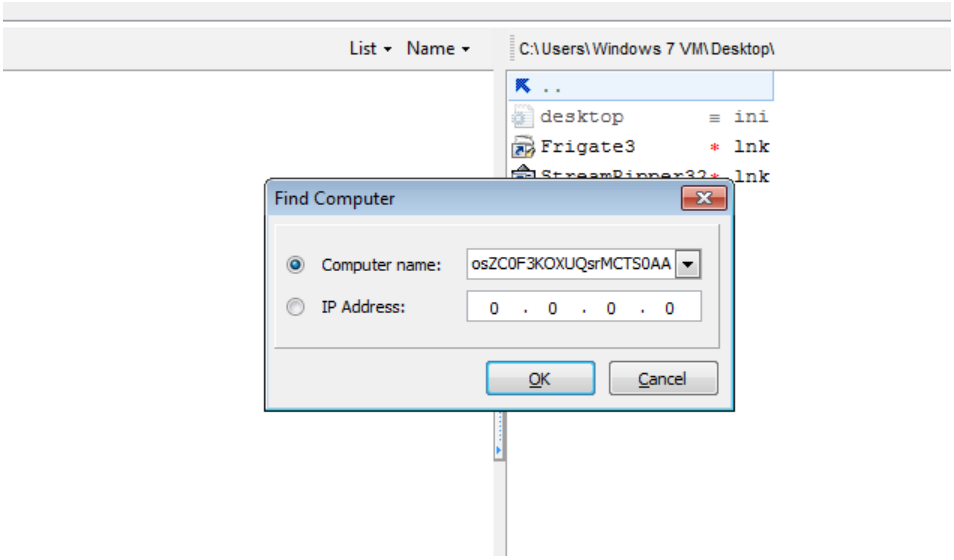
Download and install Frigate software.



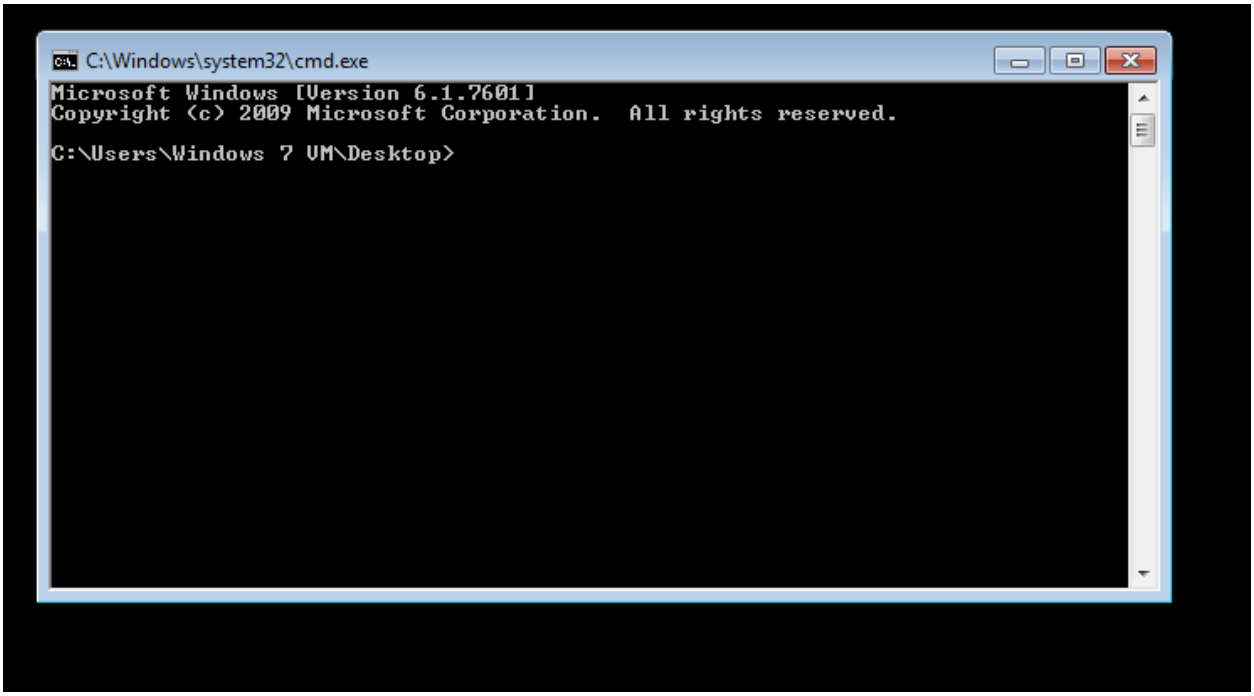
This is the payload generated after executing the script file.



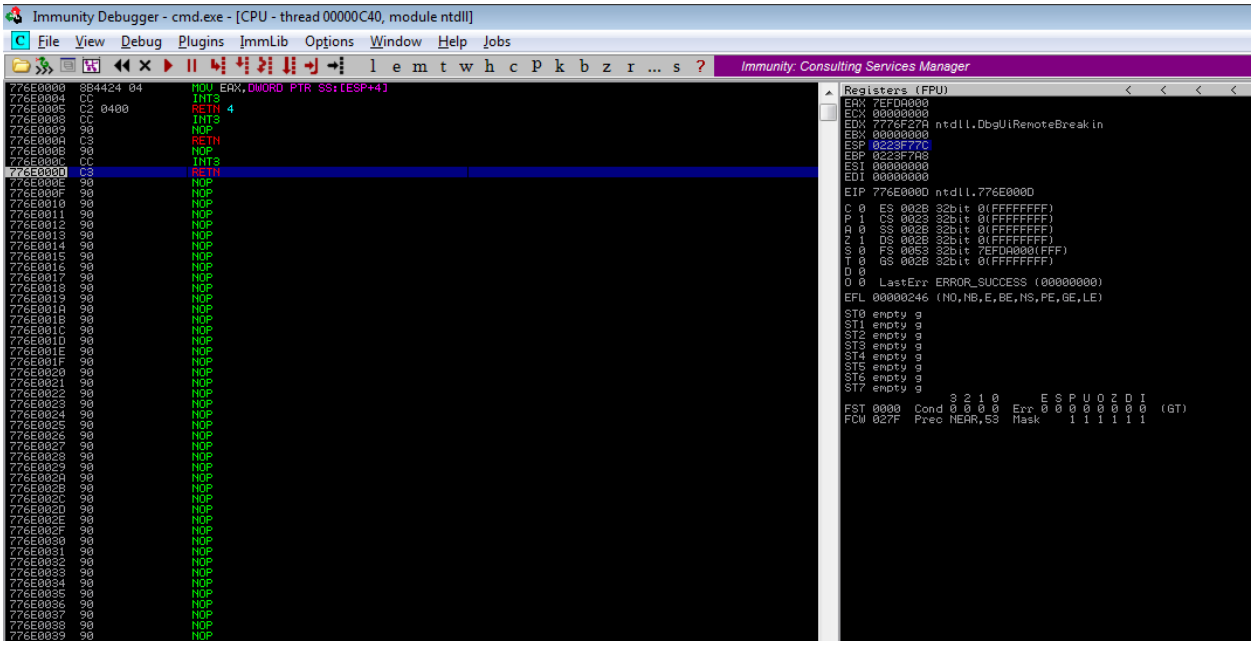
Copy and paste the payload in the frigate software by going to the option disks and click on find computer.



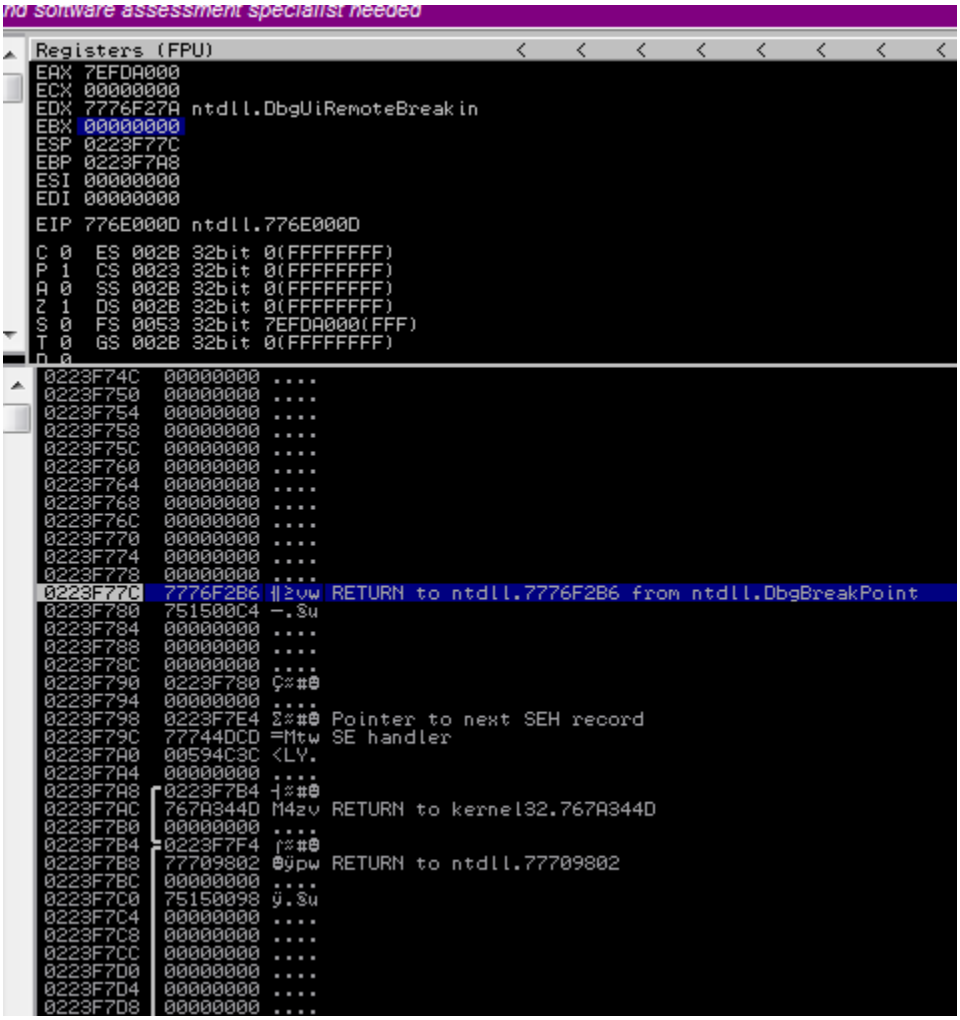
After clicking ok it will crash the software and this command prompt will be displayed.



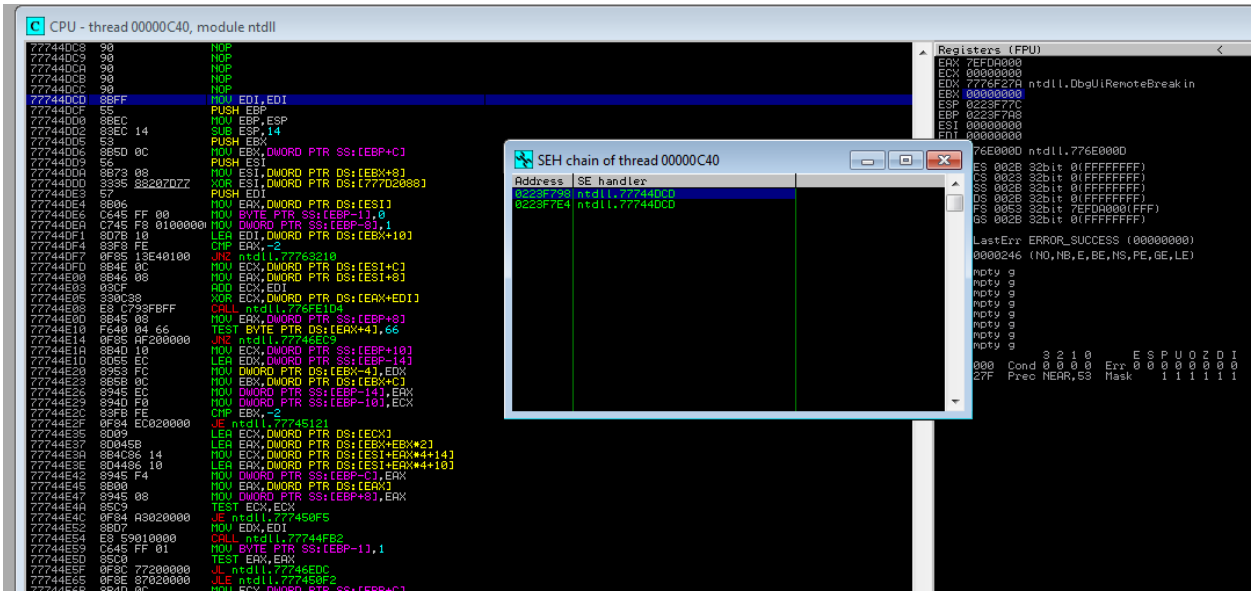
After analysing the executed command prompt:



After checking for that EIP Address:-



SHE Chain:-


CPU - thread 00000C40, module ntdll
SEH chain of thread 00000C40
Address
SE handler
0223F790 ntdll.77744DCD
0223F7E4 ntdll.77744DCD
Registers (FPU)