SECURE CODING LAB

LAB-10

SLOT-L39+L40

18BCN7128

SEGU NAIMISHA

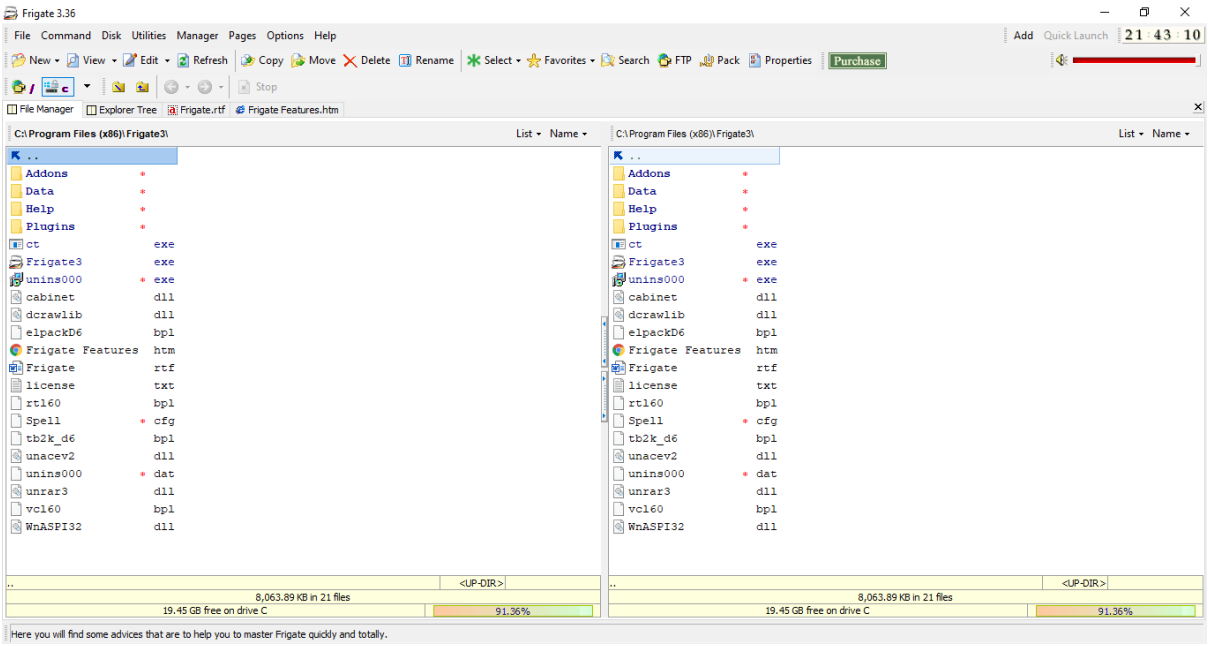
Lab experiment - Working with the memory vulnerabilities – Part IV

Task

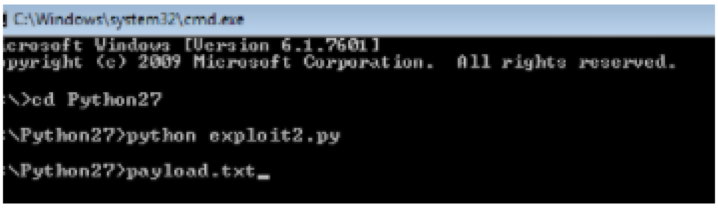
- Download Frigate3_Pro_v36 from teams (check folder named 19.04.2021).
- Deploy a virtual windows 7 instance and copy the Frigate3_Pro_v36 into it.
- Install Immunity debugger or ollydbg in windows7
- Install Frigate3_Pro_v36 and Run the same
- Download and install python 2.7.* or 3.5.*
- Run the exploit script II (exploit2.py- check today's folder) to generate the payload

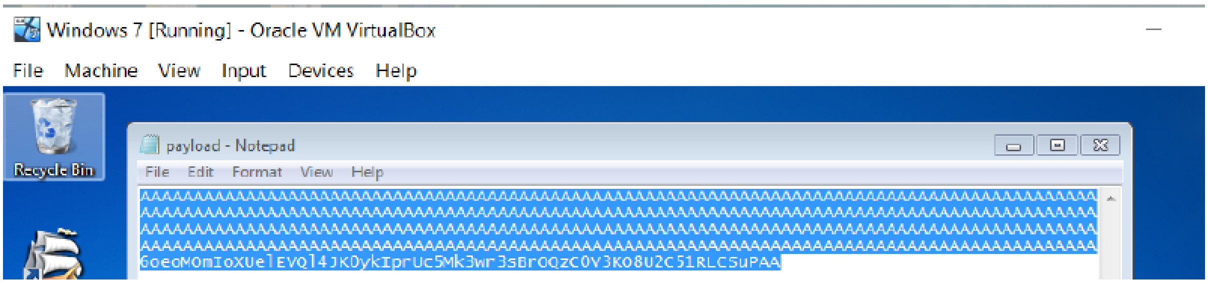
Sol:

Downloaded Frigate3_pr_v36



Running exploit2.py and opening command prompt:

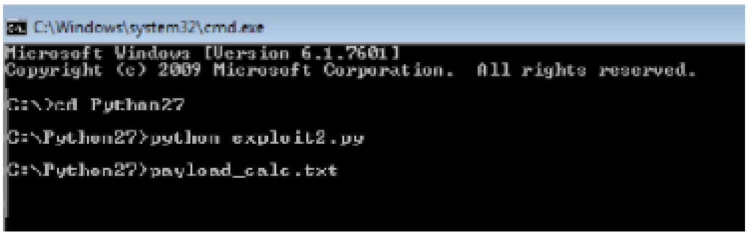


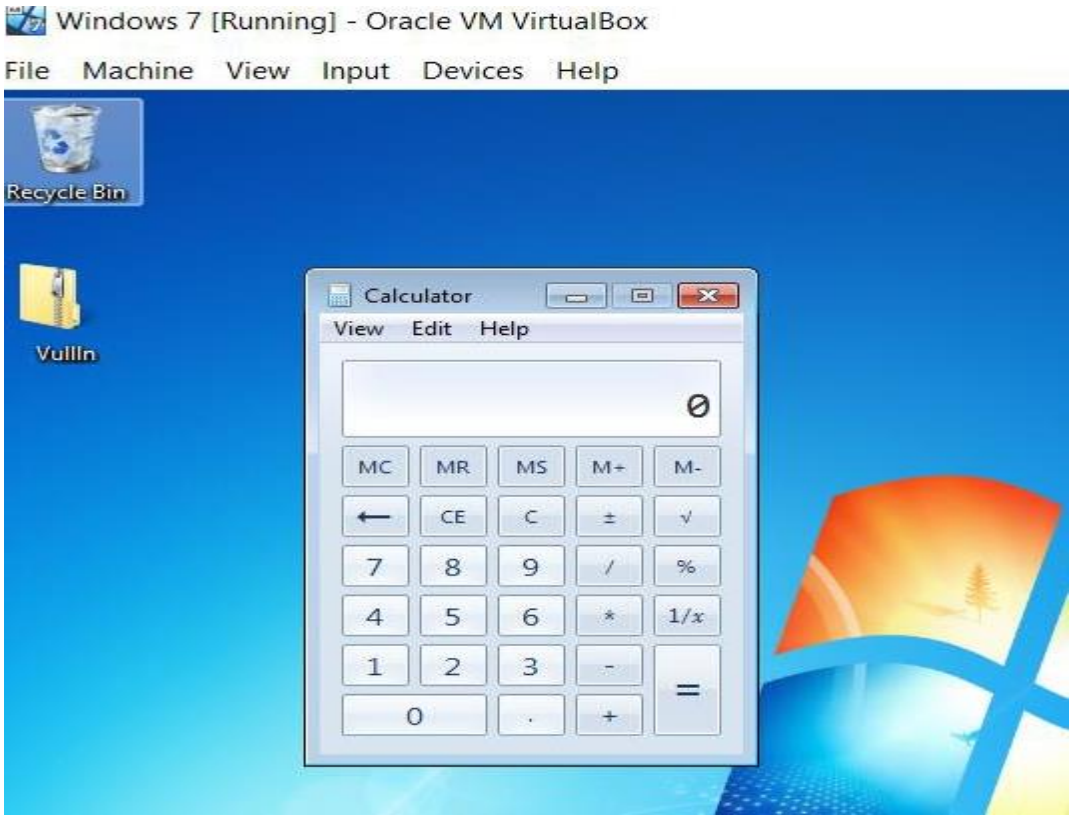


After running the commands in Linux, Frigate3 Stopped (Buffer overflow)

Opening Cal (.exe file):

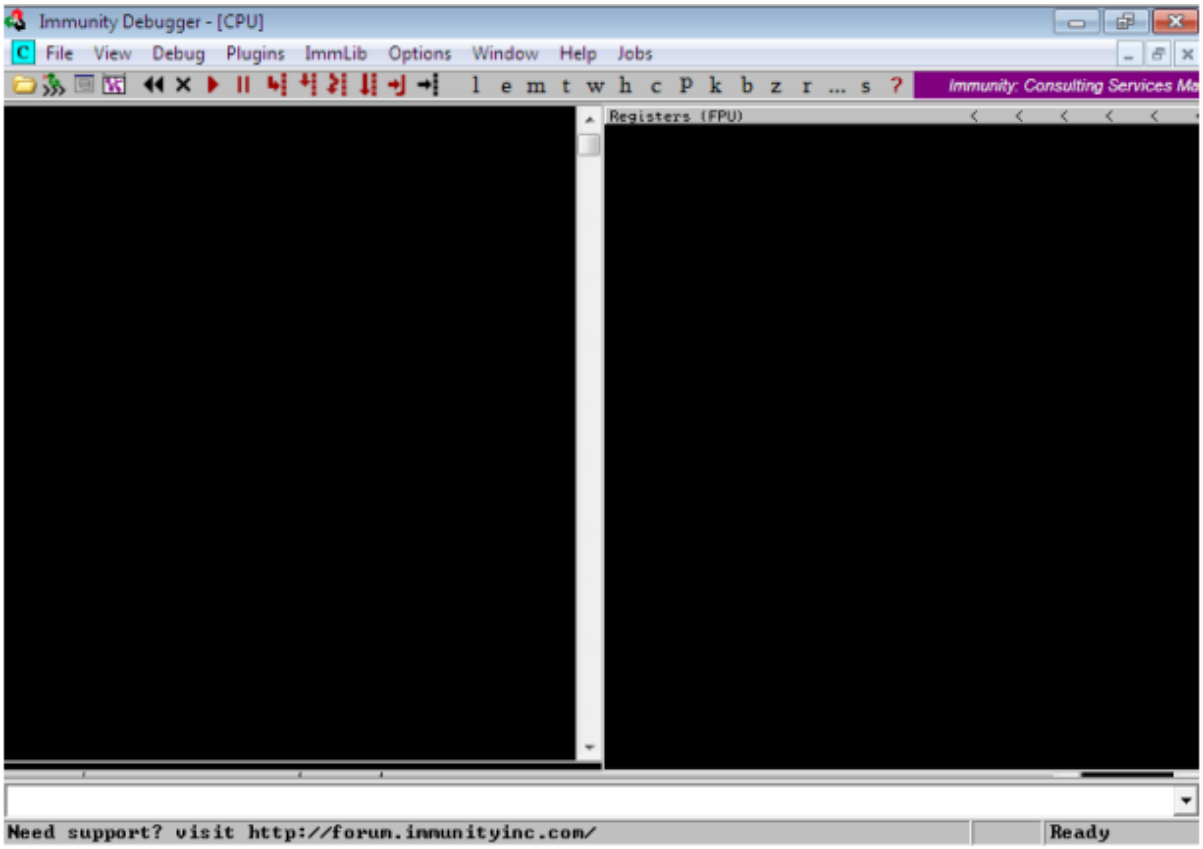
msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python

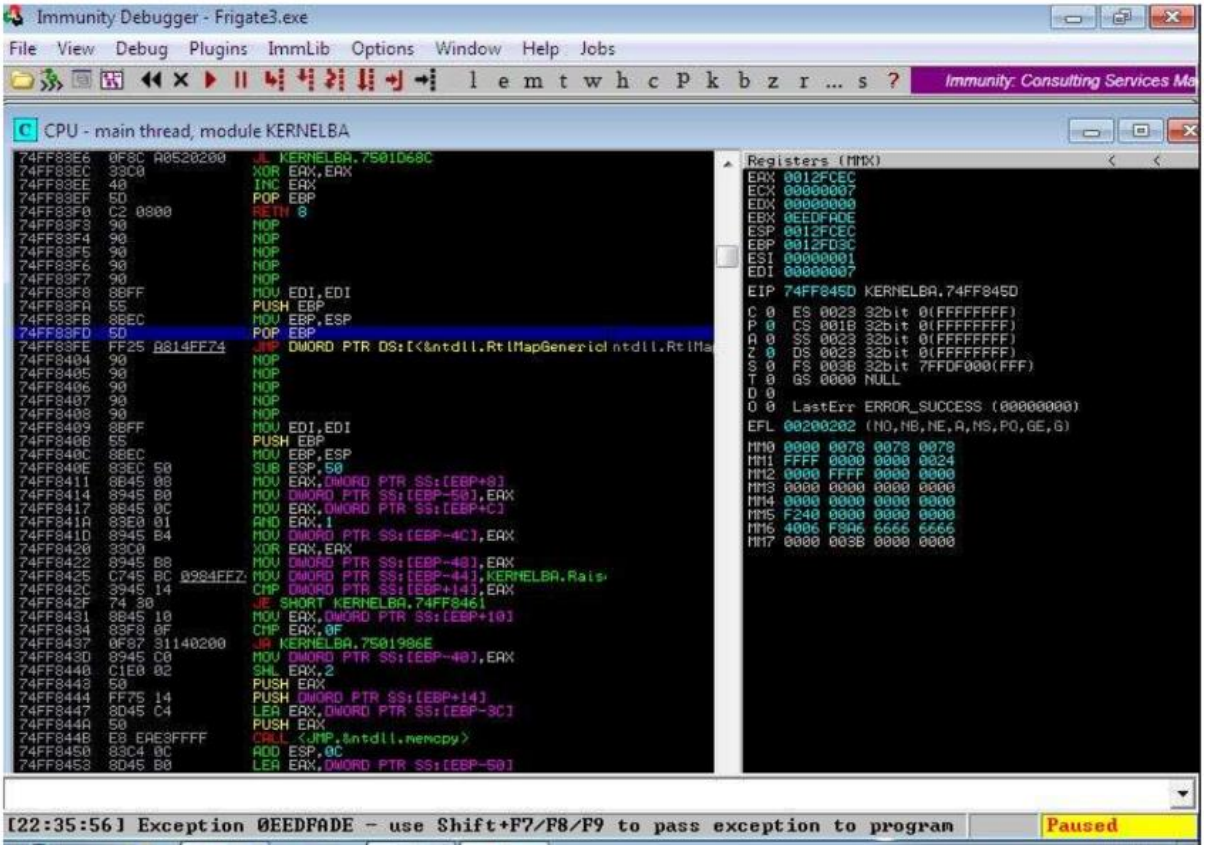




Installing immunity debugger:

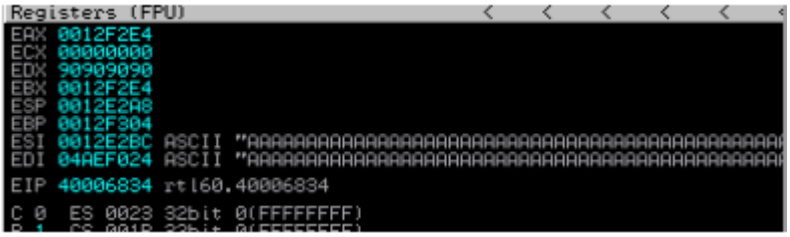
Attaching debugger





Checking for EPI address:

Checking address in stack frame:



SEH chain: verifying SHE and reporting the DLL loaded along with the address