

Secure Coding Lab - 10

Name: Tejeswar Allaka

Reg No: 18BCN7033

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

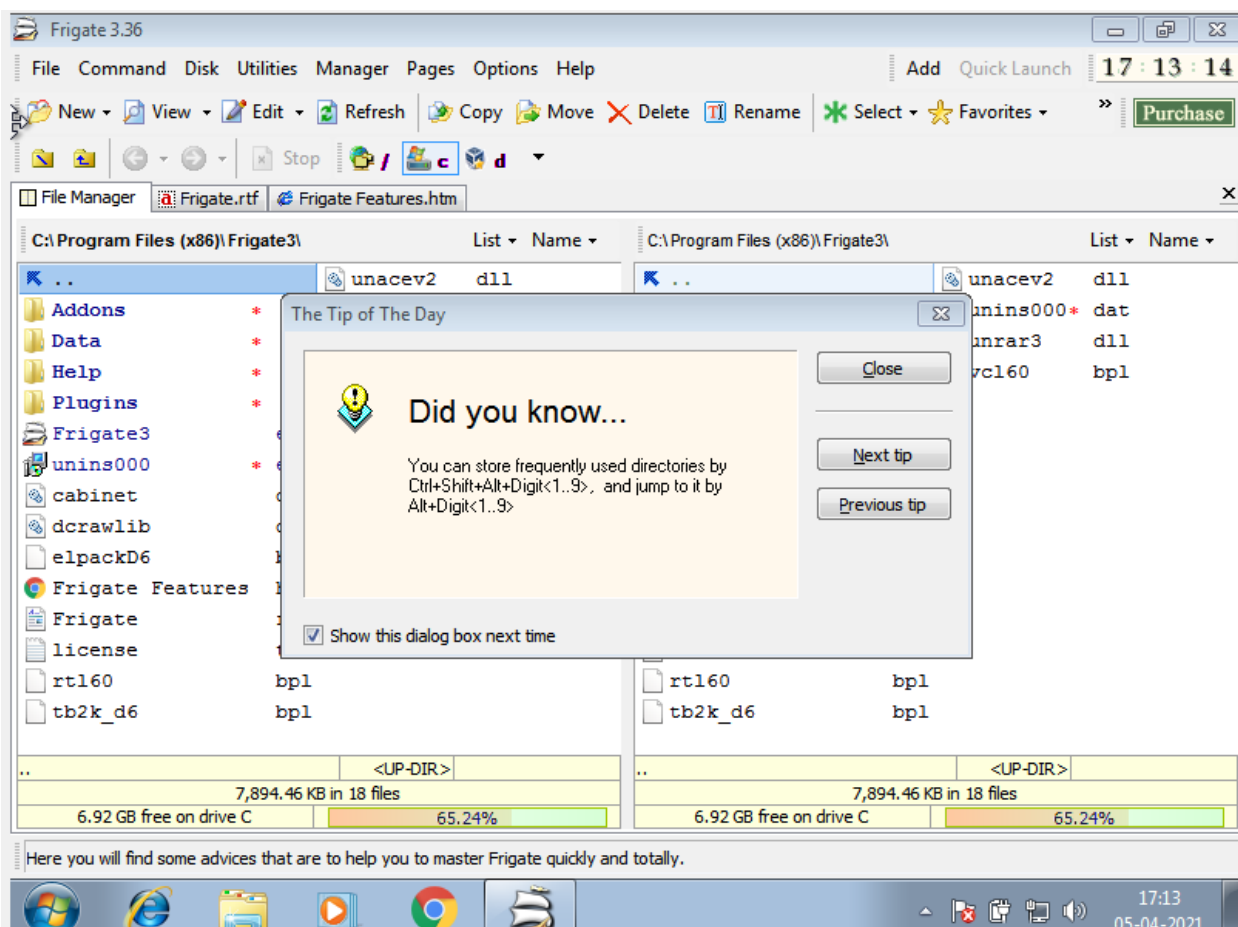
- Try to crash the **Frigate3_Pro_v36** and exploit it.
- Change the default trigger from **cmd.exe** to **calc.exe** (Use **msfvenom** in Kali linux).

Example:

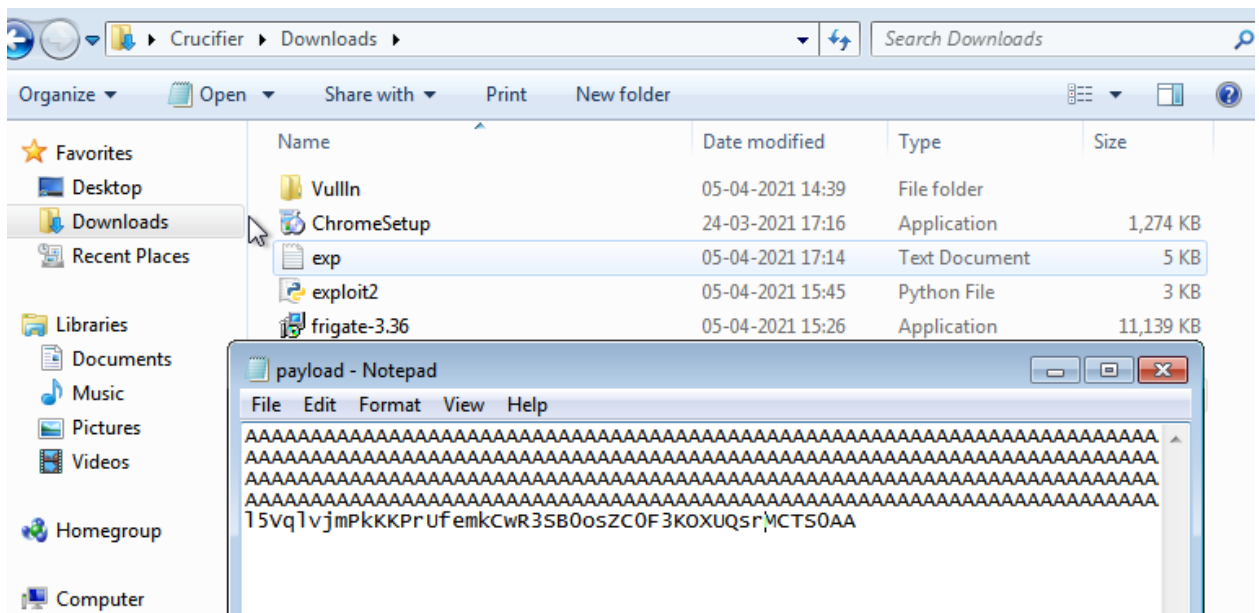
```
msfvenom -a x86 --platform windows -p windows/exec  
CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f  
python
```

- 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

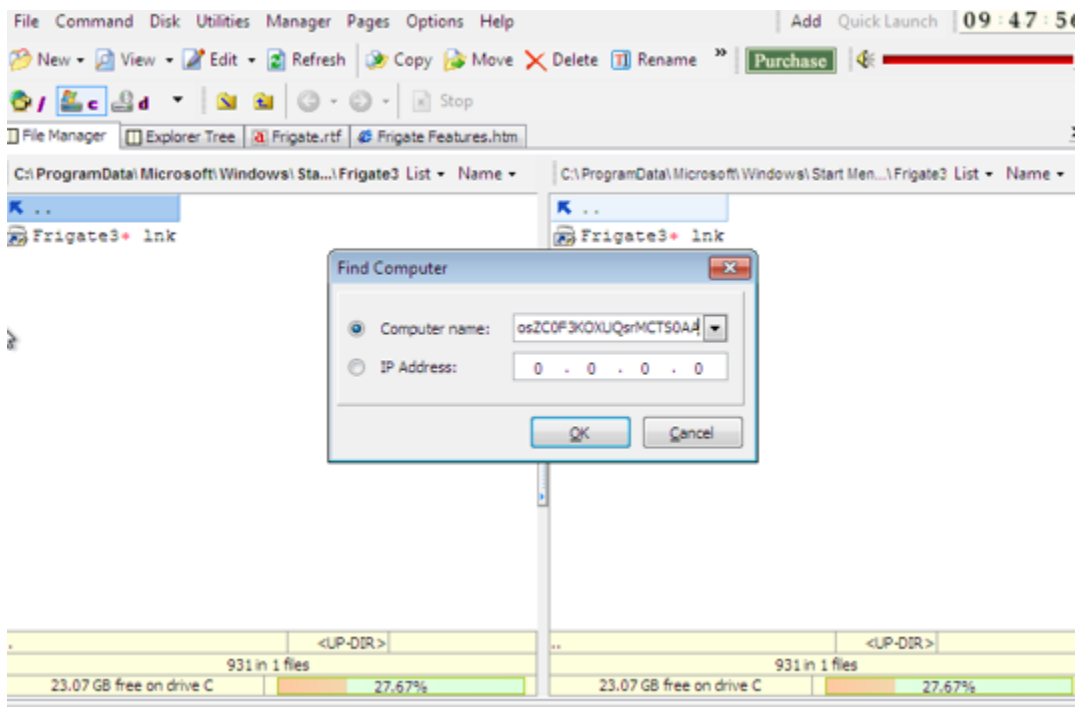
1) Install Frigate on your Windows 7 VM



2) Execute exploit2 for generating a text payload



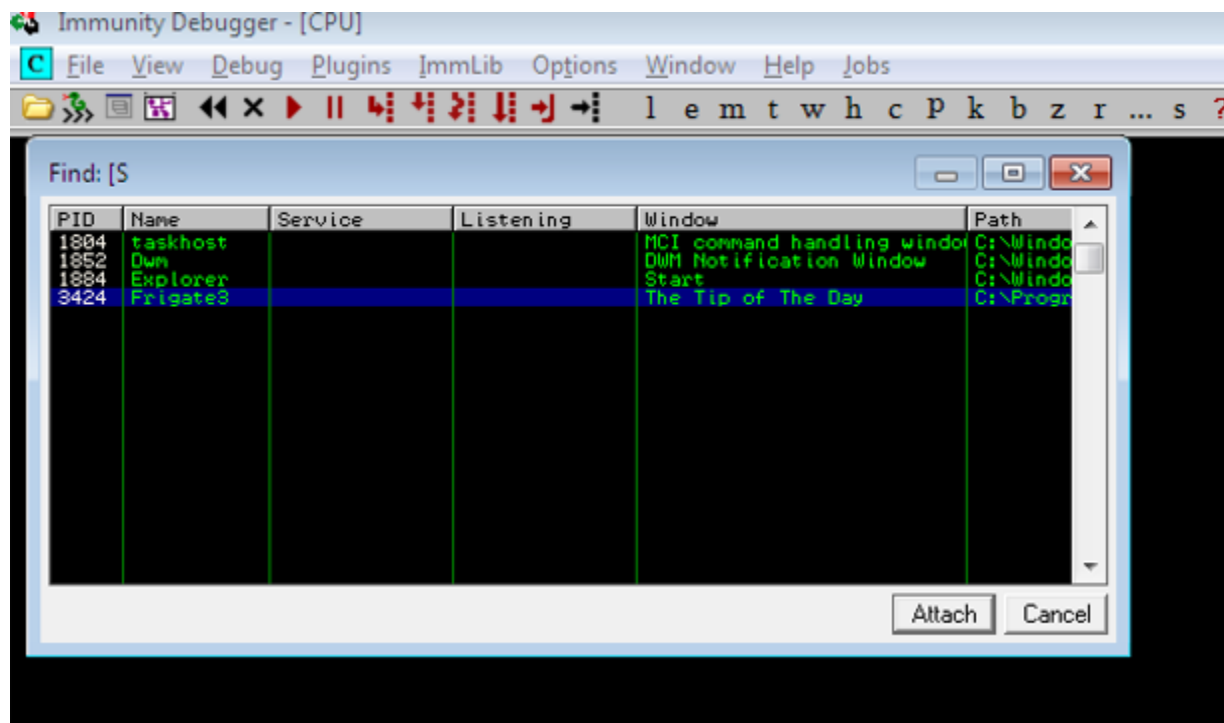
3) Paste the payload in the frigate software



4) App crashes and the calc.exe is triggered



5) Analyse the debugging and registers using immunity debugger



6) Find eip address and overflowing A's

```
EDI 00000000
EIP 00401000 Frigate3.<ModuleEntryPoint>
```

```
EBX 00000001
ESP 0018F3F8
EBP 0018F404
```

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