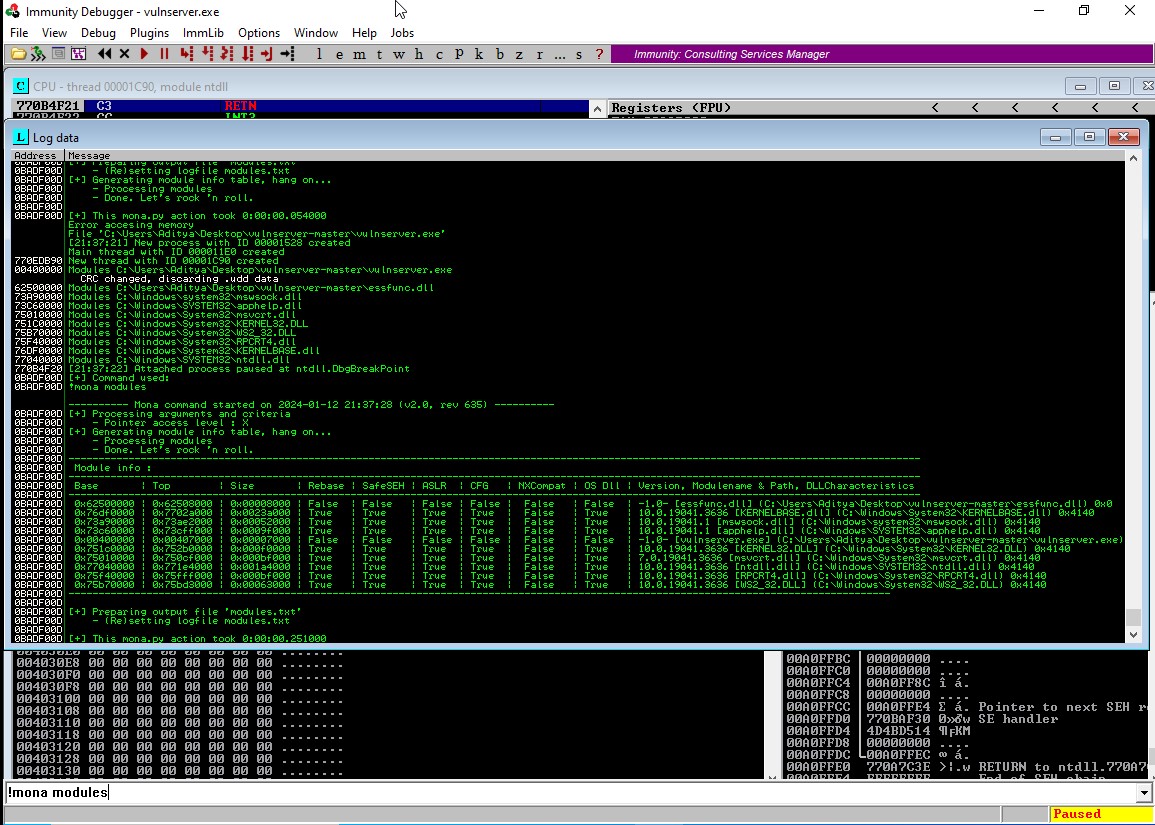
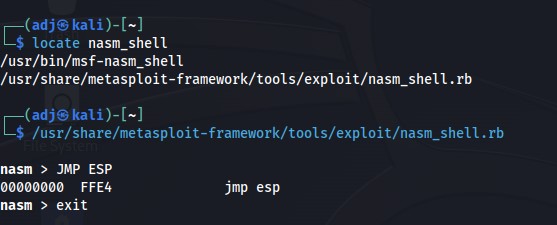
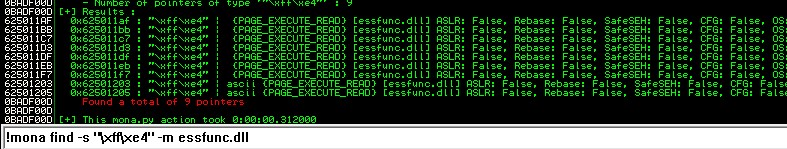
Identify a component that lacks memory protection settings.

To accomplish this, we will utilize the mona tool, which can assist in finding the correct module.  


Our next step involves identifying an opcode equivalent to JMP ESP. To achieve this, we will rely on the Metasploit module name nasm\_shell.rb.  


 We seek is FFE4. To pinpoint the memory address containing the FFE4 (JMP ESP) opcode within essfunc.dll, we can utilize the following mona command:  


We have identified the memory address that contains the JMP ESP opcode, which is 625011AF memory address. Our next goal is to gain full control of the EIP (Extended Instruction Pointer). We can accomplish this by setting a breakpoint at the 625011AF address within Immunity Debugger, overflowing the buffer, and placing 625011AF in EIP to verify if our breakpoint activates. To facilitate this, we can adjust our Python script and insert the return address, which should be in reverse order (\xaf\x11\x50\x62).  
  
  
