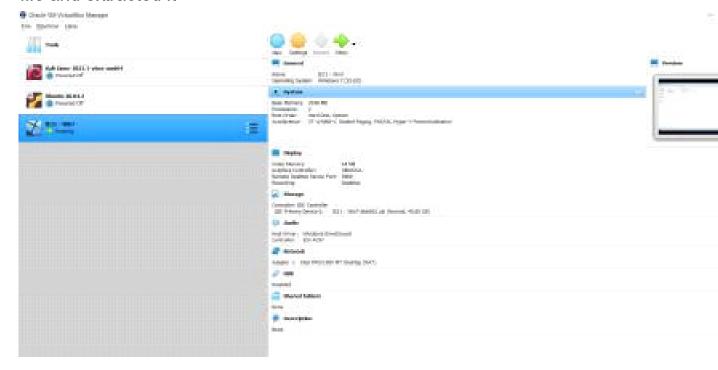
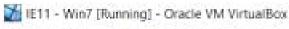
Navya K 18bcn7048 L39+L40

Working With Memory Vulnerabilities

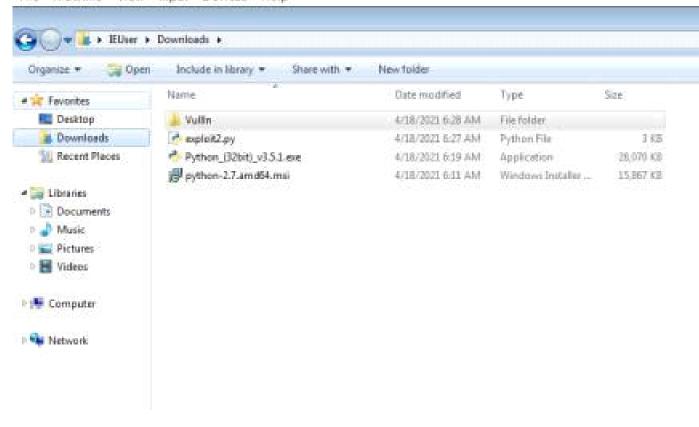
Opened the windows 7 on virtual machine and downloaded the vuln file and extracted it



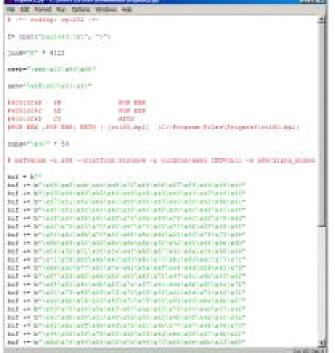
Downloaded python 2.7 and unzipped the Vulln file



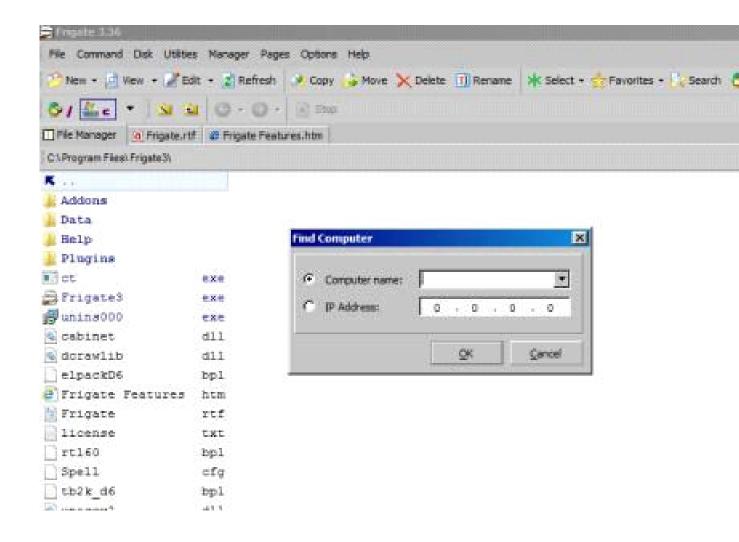
File Machine View Input Devices Help



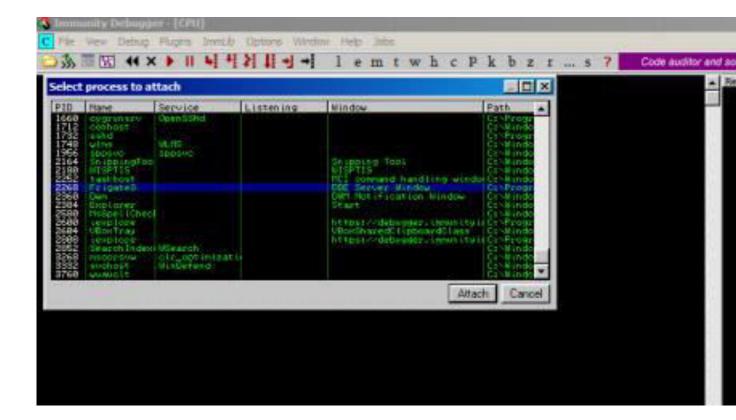
Running the exploit script 2 to generate the payload



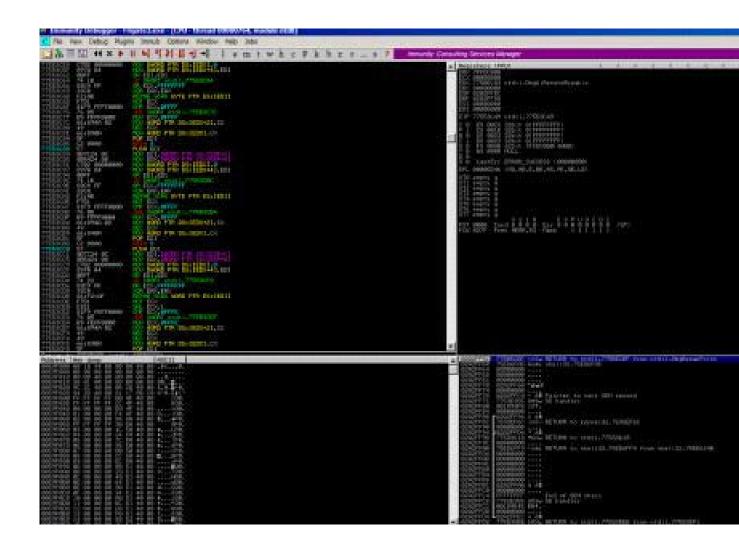
The first control of the control of



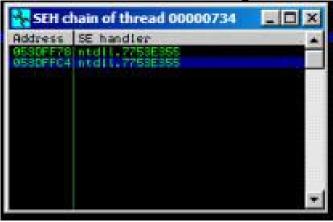
Attaching frigate to immunity debugger



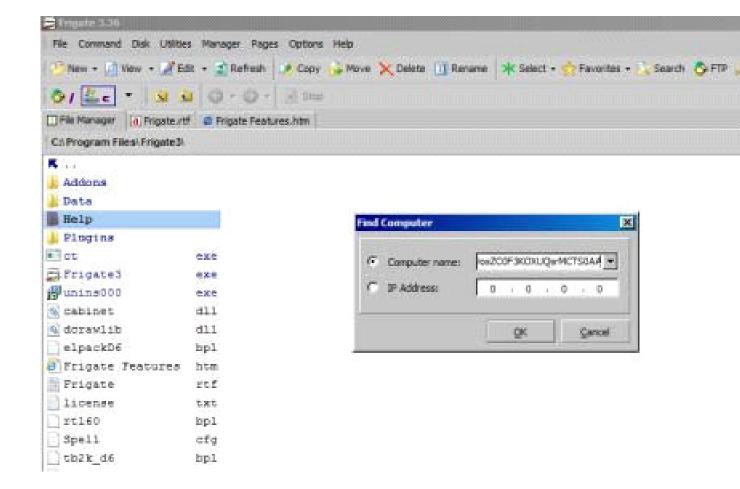
After attaching frigate to immunity debugger



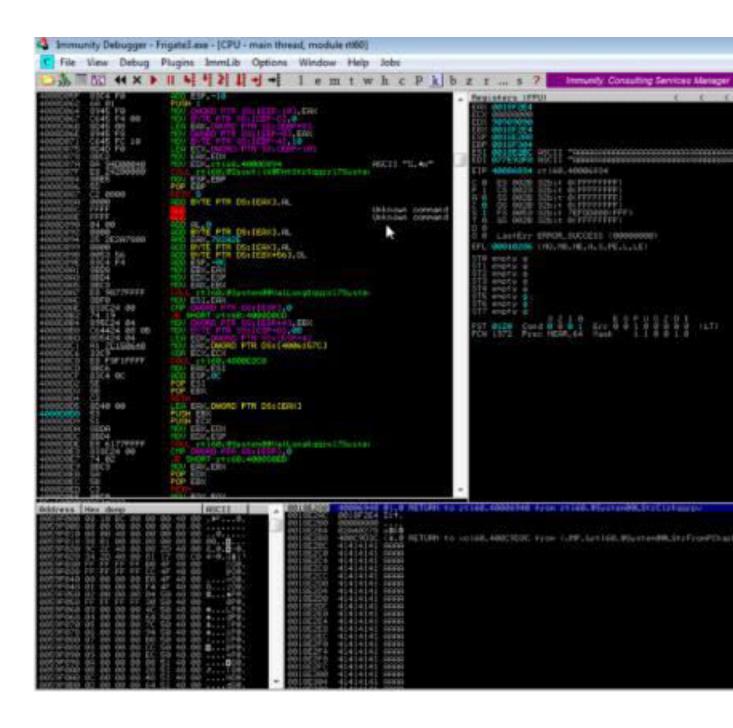
You can see that EIP is loading default exception handler



Now paste the payload in frigate



Checking Immunity Debugger



Now you can see that the EIP has changed and the loaded dll is rtl60