

Name: Panwala Harshit Rakesh

Reg. No.: 18BCE7137

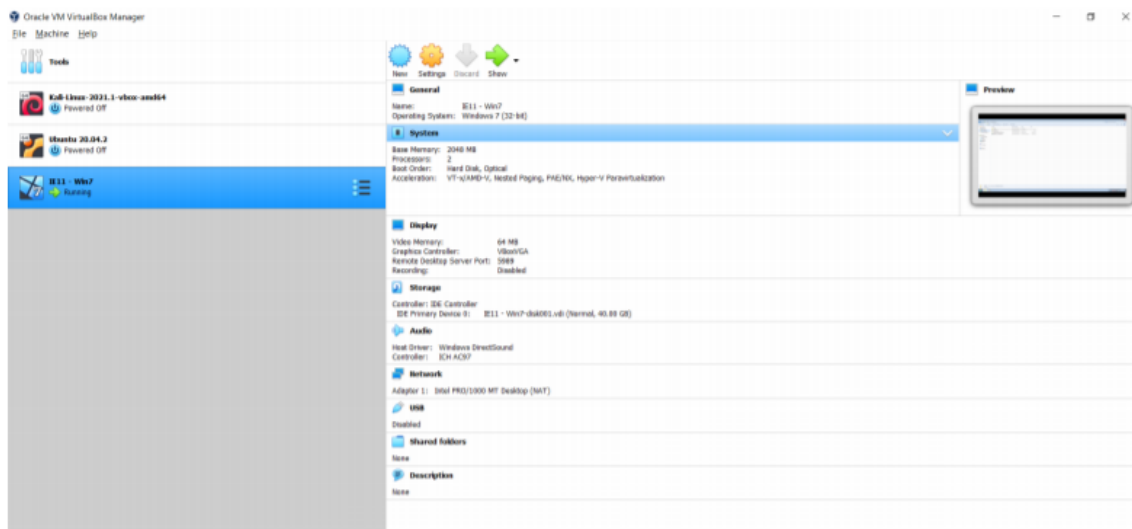
Course code/name: CSE2010/ Secure Coding

Slot: L23 + L24

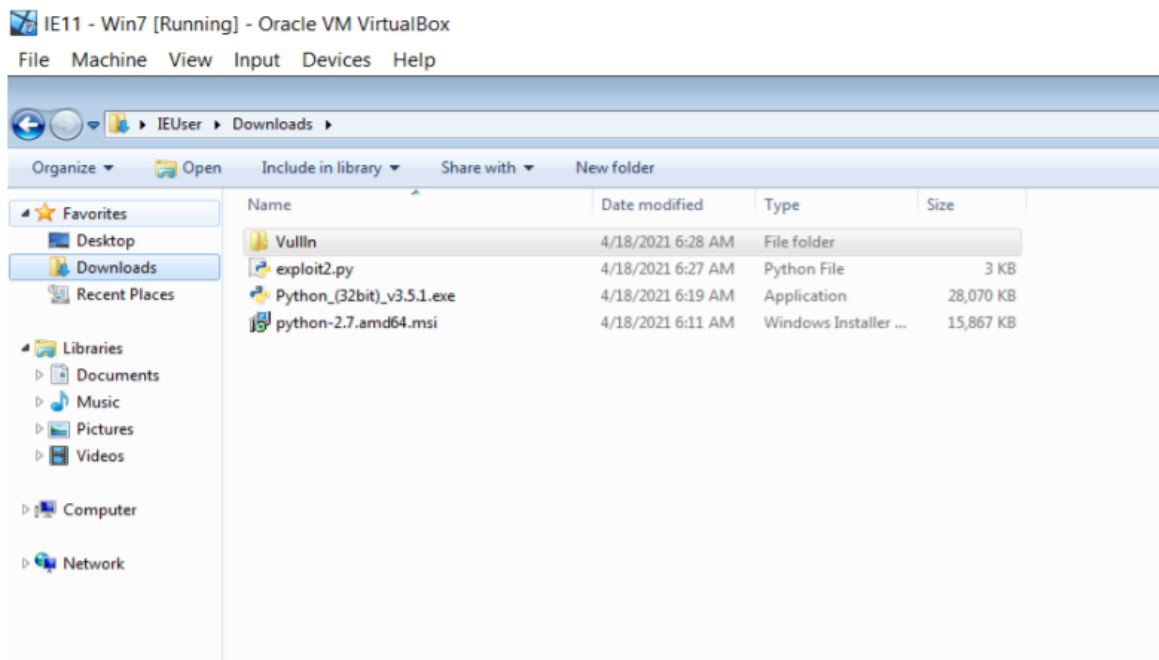
Faculty: Prof. Sibi Chakkaravarthy S

LAB-10

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

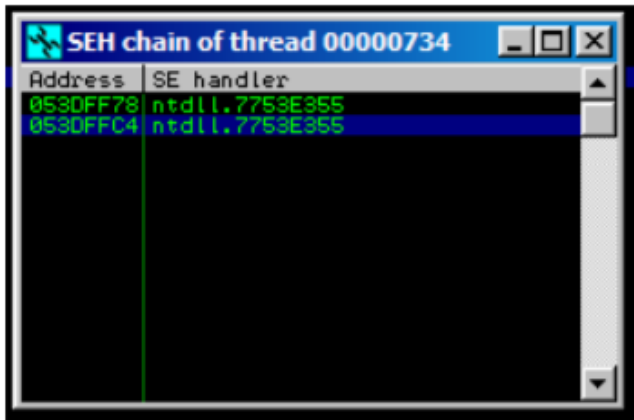


Downloaded python 2.7 and unzipped the Vuln file

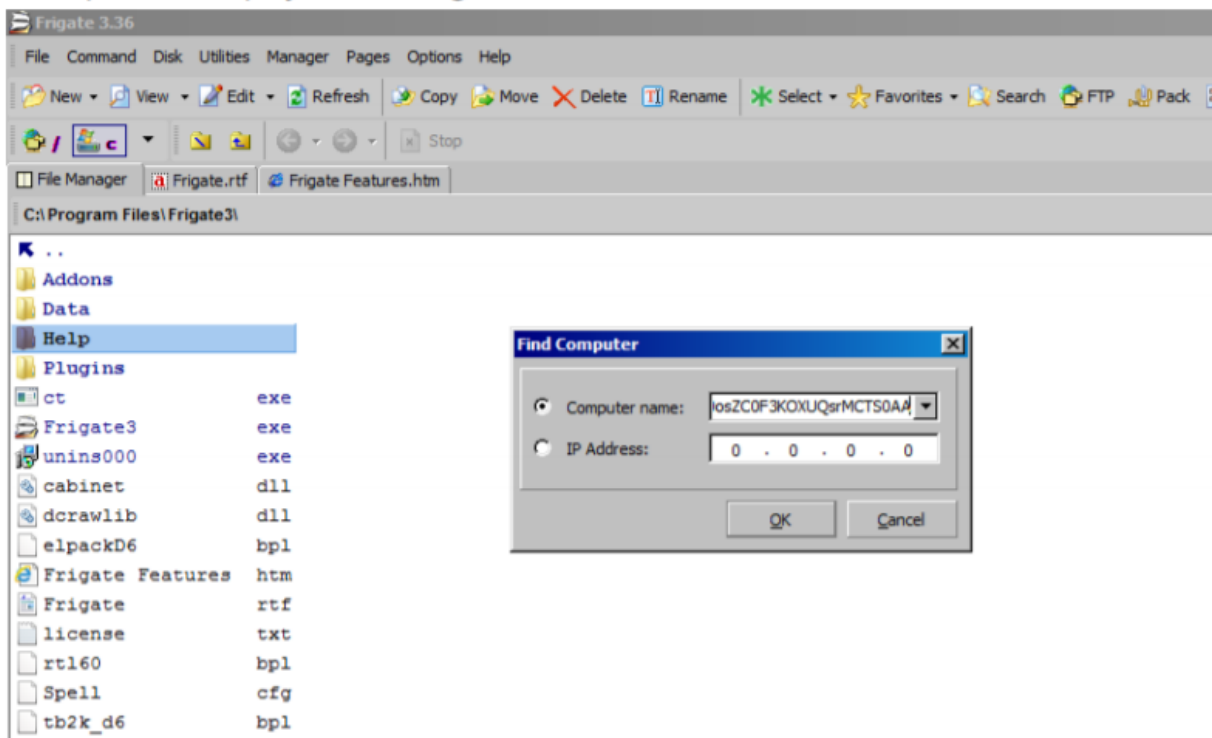


Running the exploit script 2 to generate the payload

You can see that EIP is loading default exception handler



Now paste the payload in frigate



Checking Immunity Debugger

SEH chain of main thread	
Address	SE handler
0018F2F4	rtl60.40010C4B
909020EB	*** CORRUPT ENTRY ***