# **PROJ 15: Malware Behavior**

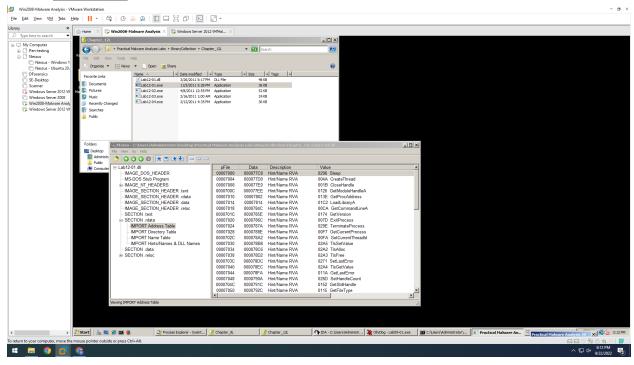
Prof. Alberto LaCava
CY -640
MALWARE ANALYSIS & DEFENSE

*Nikhil Patel* 11/15/2022

**Introduction:** In this lab, we will Lab12-01 file and examine its behavior using IDA Pro and Process Monitor.

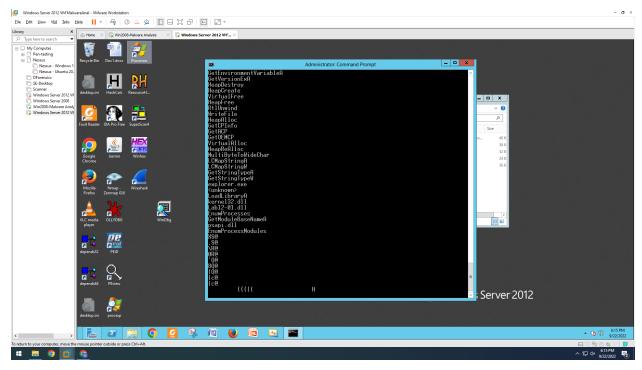
## **Procedure:**

#### **IMPORTS**



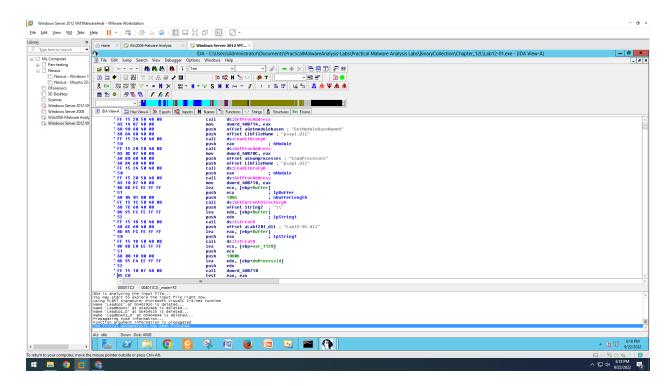
### **Strings**

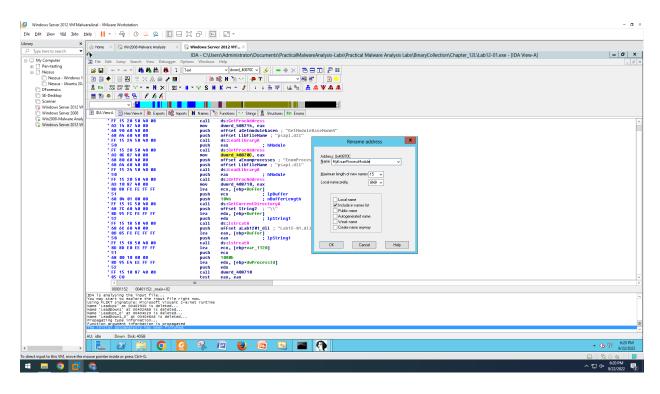
• Examine the file named Lab 12-01.exe.

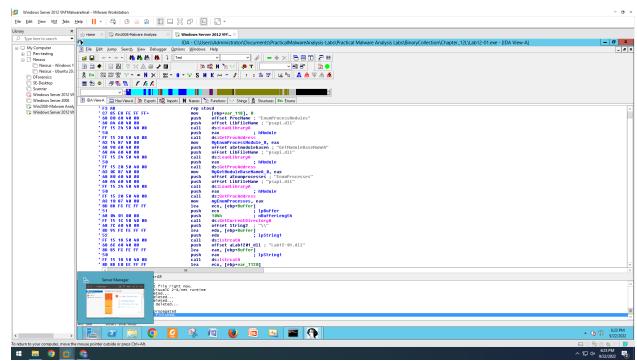


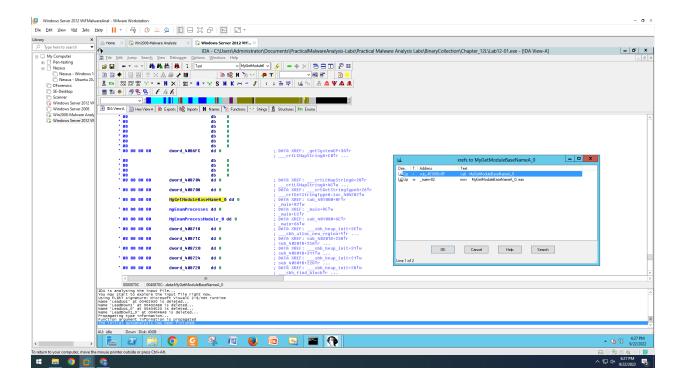
#### IDA Pro

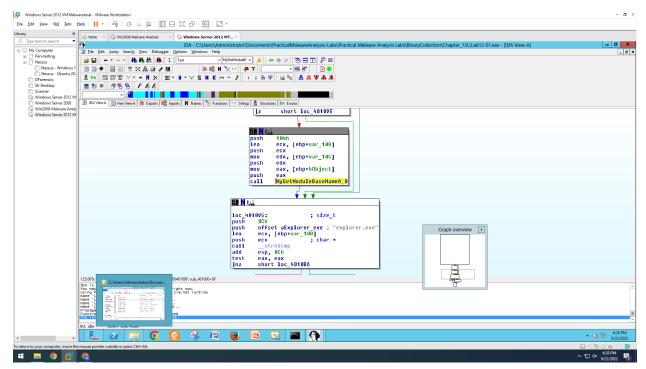
- Open the file named Lab 12-01.exe in IDA Pro.
- Go to options > General, check on the "line prefixes" and set number to "6".
- Then click ok.
- Now we will assign a memory address so named it to myEnumProcessModules.





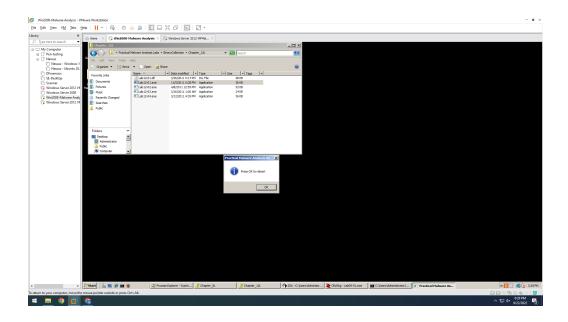


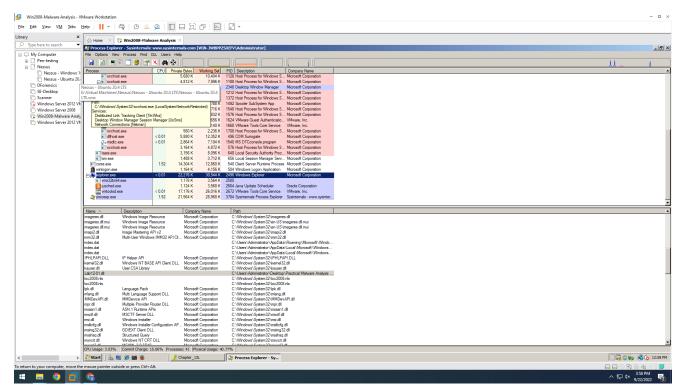




#### **Process Explorer**

- Open IDA Pro. Double-click on Lab 12-01.exe to run the malware.
- And click ok to reboot.
- Now in process monitor go to view > lower pane view > dlls.
- Take a screenshot of the view.





**Conclusion:** To conclude with the lab, we learned how to examine the malware behavior using the IDA Pro & Process Monitor.