

**PROJ 8: Disassembling C on Windows**

*Prof. Alberto LaCava*

**CY -640**

**MALWARE ANALYSIS & DEFENSE**

*Nikhil Patel*

10/11/2022

**Introduction:** In this lab, we are going to compile a C program on a Windows 2008 server using Visual Studio Express 2008 and also we are going to examine it in the IDA Pro disassembler to learn what it looks like in assembly language.

## **Procedure :**

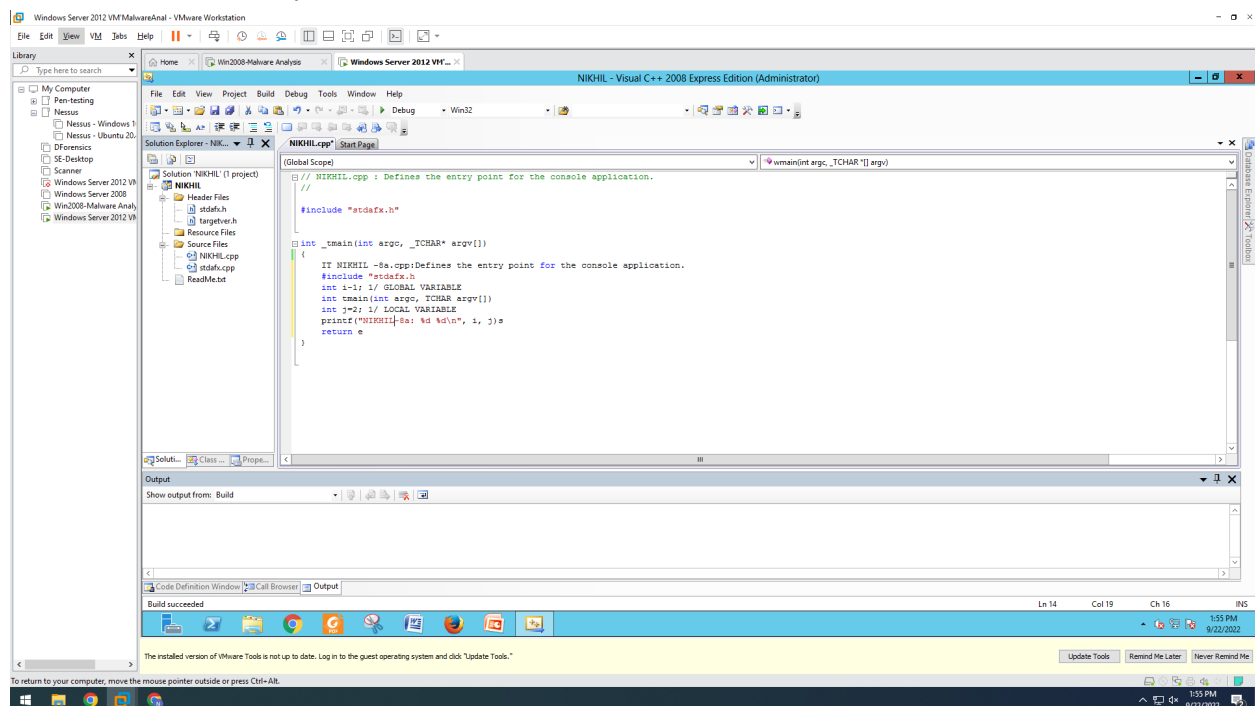
### **Launching Visual Studio Express 2008**

- Go to Start and Type Visual Studio Express 2008 to open the application.

### **Creating a simple C Program**

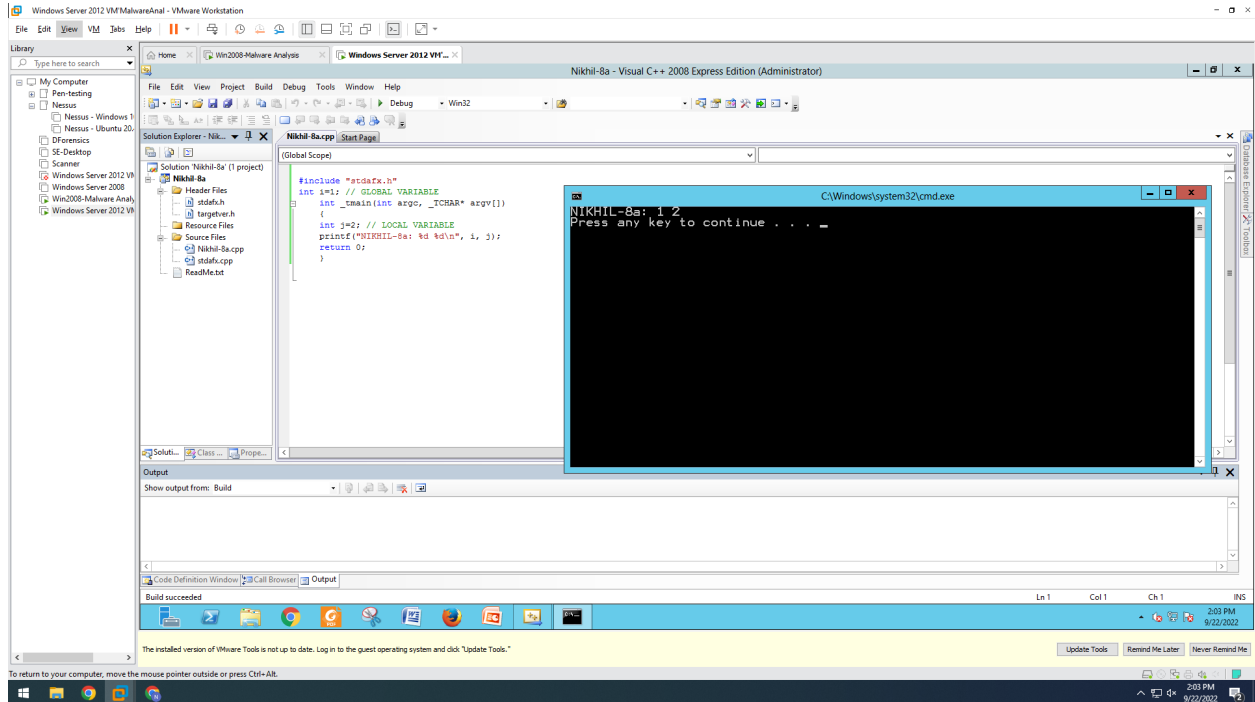
- In the menu bar click on File/New Project.
- A new window will pop up and select Win32 on the left panel and Win32 Console on the right panel.
- Now Type “Nikhil-8a” in the name and click OK/ Next/Finish
- Now we will write a code in c :

```
#include "stdafx.h"
int i=1;
int _tmain(int argc, _TCHAR* argv[])
{
    int j = 2;
    printf("Nikhil-8a: %d %d\n", i, j);
    return 0;
}
```



## Compiling your Program

- Click on Build and Build Solution you see in output 1 success.
- Take a fullscreen screenshot of the desktop.

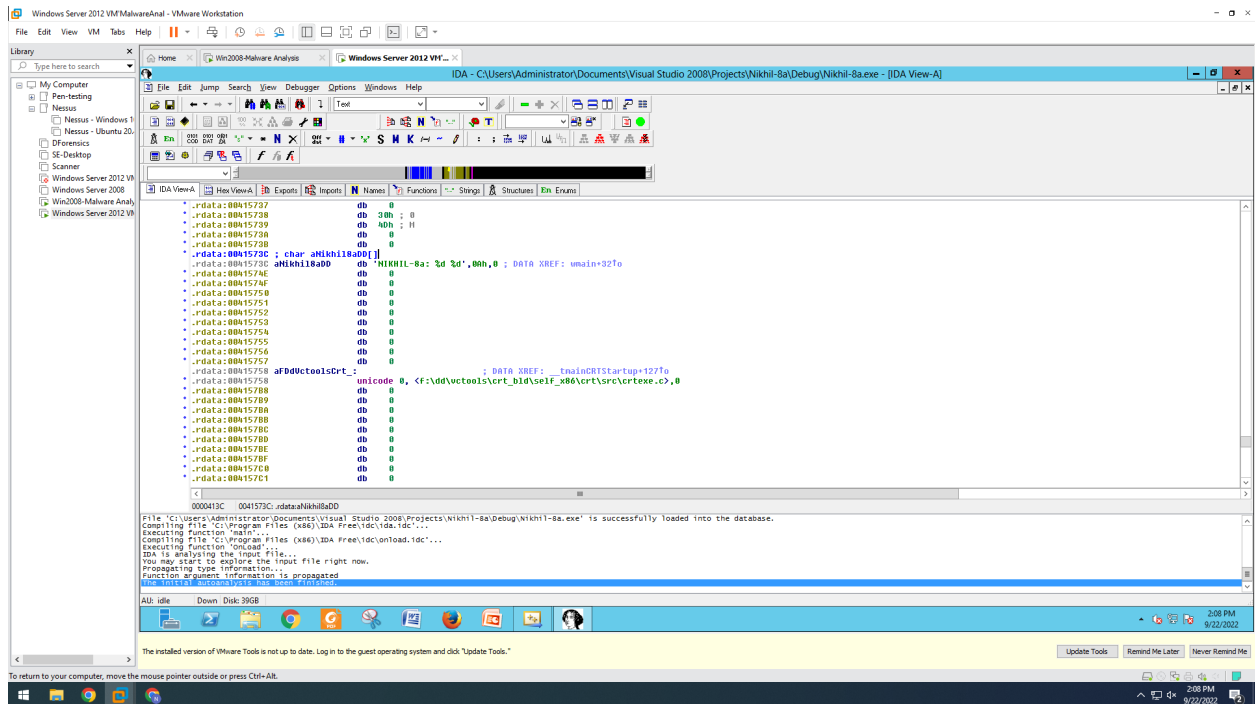


## Running Your Program

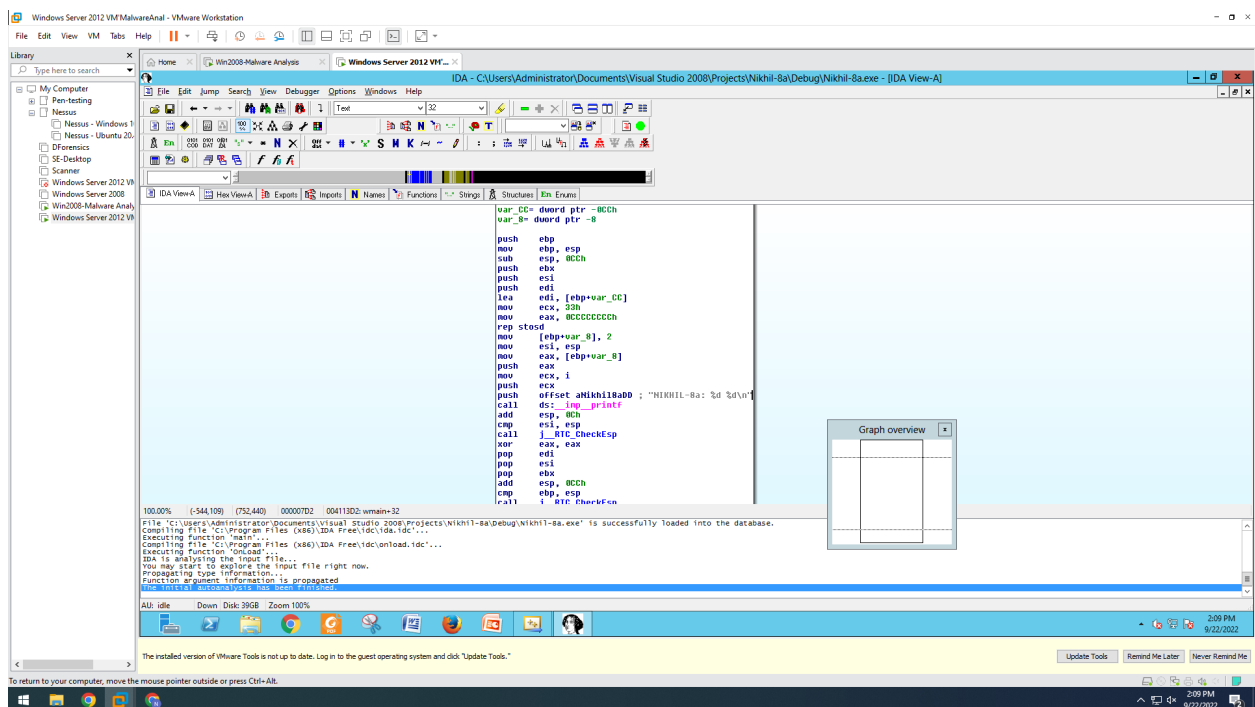
- Click on Debug and Start Without Debugging you see new windows as output.
- Take a fullscreen screenshot of the desktop.

## Disassembling the EXE

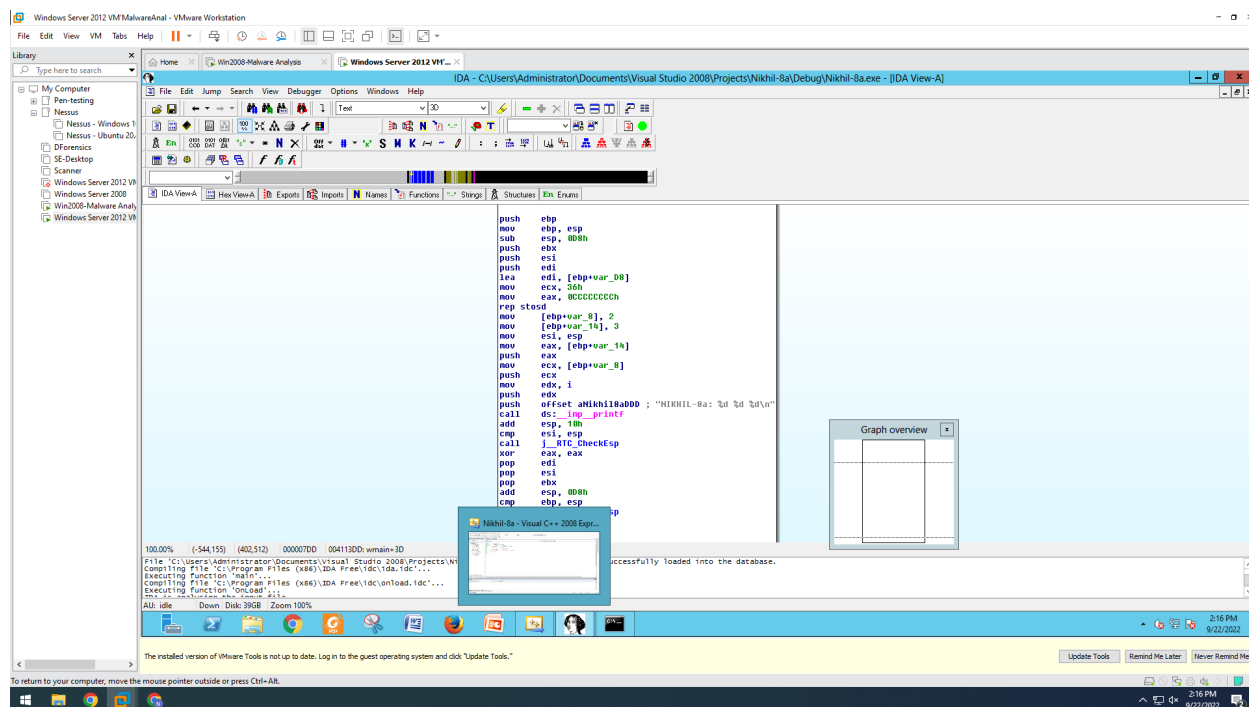
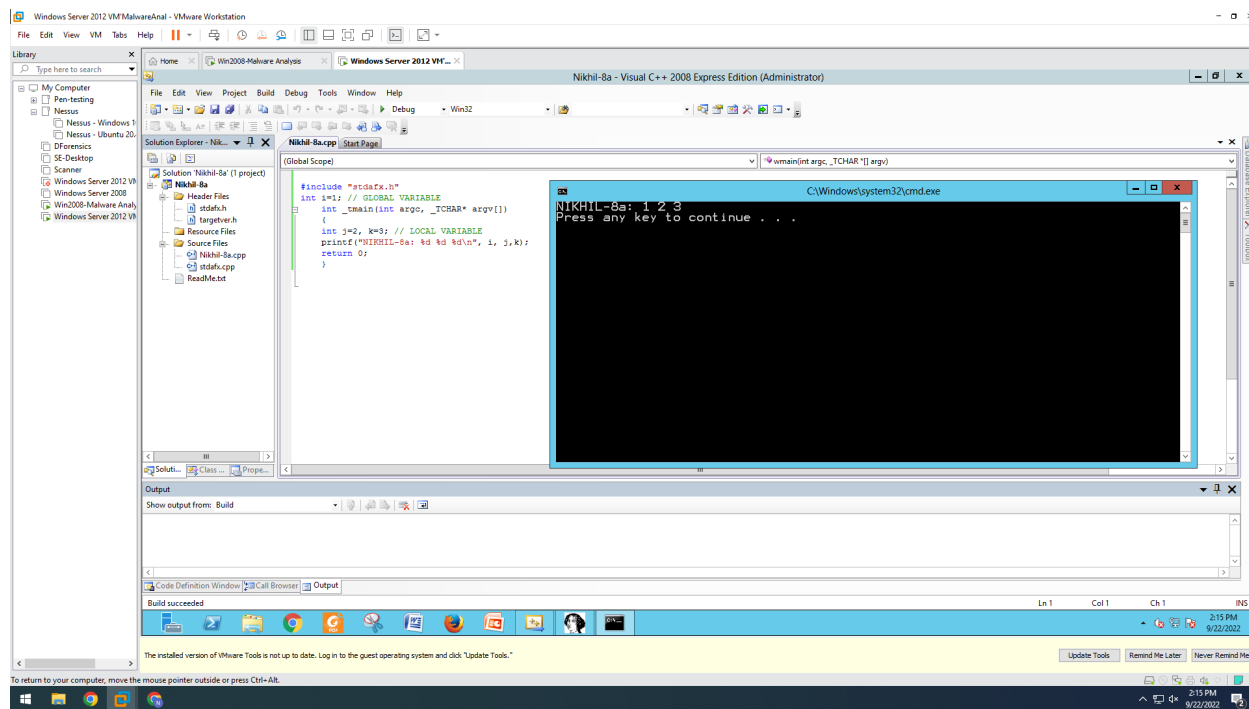
- Now close the window by hitting enter and minimize the Visual Studio.
- Start the IDA Pro Free and in the “About” box, click OK.
- Agree to the license and close the help window.
- In the Welcome to IDA box click New and double click PE Executable.
- Now we have to select the same file we created on Visual Studio i.e. “Nikhil-8a”.
- IDA-Pro will be loaded in Graph mode, Expand the strings windows and find “Nikhil-8a %d %d\n” and double click on it.



- You will have to look for DATA XREF right next to “Nikhil-8a”, take a cursor to “DATA XREF” and you will see a yellow box.
- Now double click on wmain + 32 now you will see the C program appears.
- Save an Image of Push cmd followed by “Nikhil-8a %d %d\n”



# CHALLENGE



**Conclusion:** To Conclude with this lab we learned how to Create, Compile and Run a simple C Program in Visual Studio Express 2008 on the Windows 2008 server and also get to know how the IDA pro disassembler works.