PROJ 9: Disassembling C on Windows Part 2

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:

Launch Visual Studio Express 2008

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

Creating a simple C Program

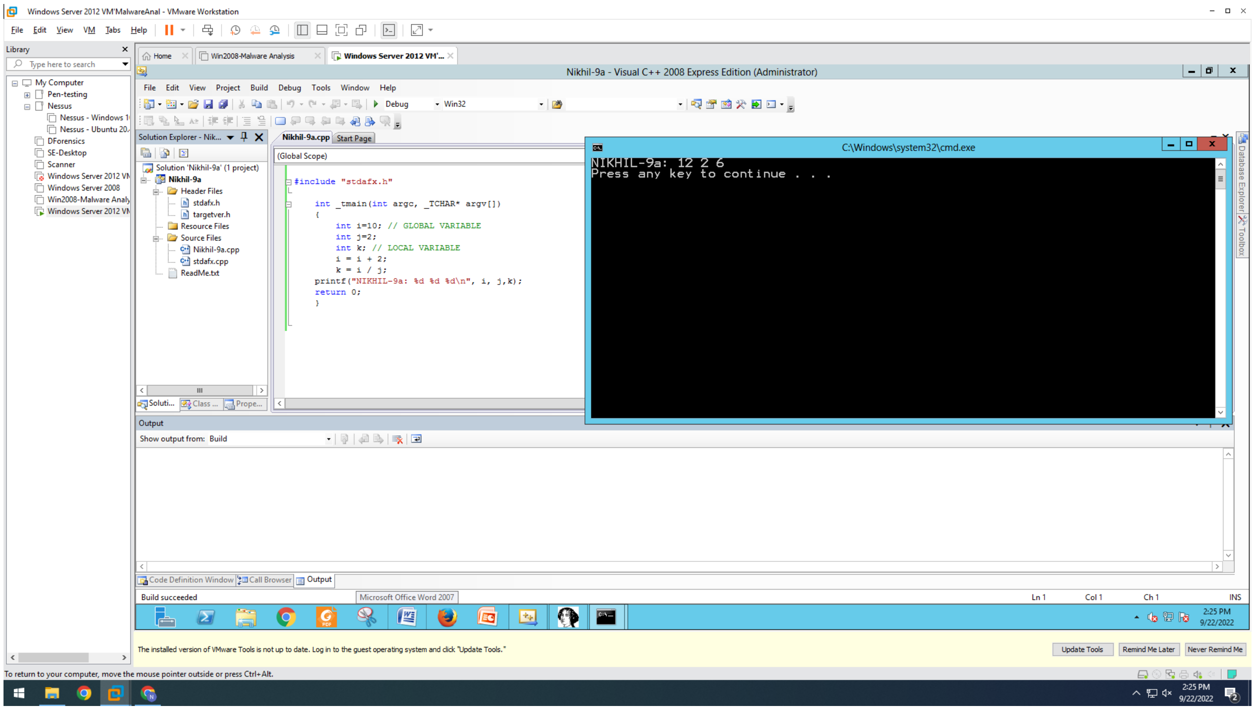
- In the menu bar click on File/New Project.
- A new window will pop up and select Win32 on the left panel and Win32 Console on the right panel.
- Now Type “Nikhil-9a” in the name and click OK/ Next/Finish
- Now we will write a code in c :

```
#include “stdafx.h”

int _tmain(int argc, _TCHAR* argv[])
{
        int i =10;
        int j = 2;
        int k;
        i = i +2;
        k = i / j;
        printf(“Nikhil-8a: %d %d %d\n”, i, j,k);
        return  0;
}
```

Compiling your Program

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


Windows Server 2012 VM'MalwareAnal - VMware Workstation
Nikhil-9a - Visual C++ 2008 Express Edition (Administrator)
Nikhil-9a.cpp
Start Page
(Global Scope)
C:\Windows\system32\cmd.exe

```
#include "stdafx.h"

    int _tmain(int argc, _TCHAR* argv[])
    {
        int i=10; // GLOBAL VARIABLE
        int j=2;
        int k; // LOCAL VARIABLE
        i = i + 2;
        k = i / j;
    printf("NIKHIL-9a: %d %d %d\n", i, j,k);
    return 0;
    }
```

```
NIKHIL-9a: 12 2 6
Press any key to continue . . .
```

Build succeeded

The installed version of VMware Tools is not up to date. Log in to the guest operating system and click "Update Tools."

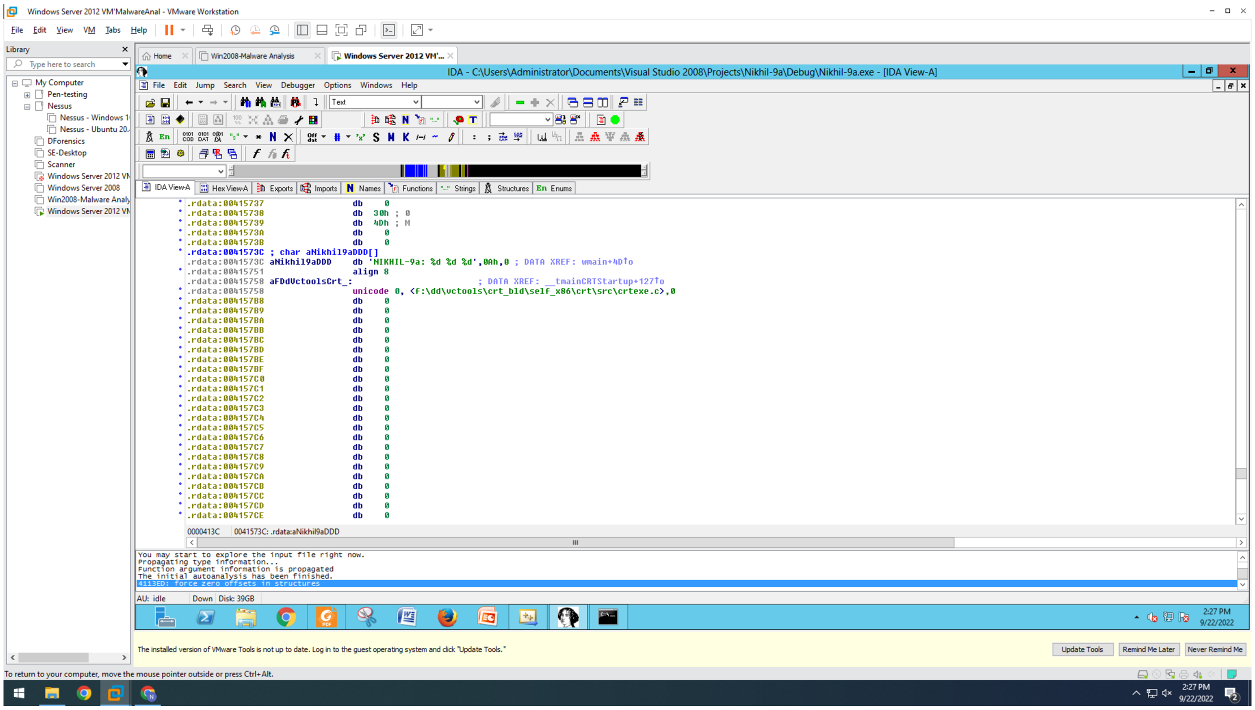
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

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-9a”.
- IDA-Pro will be loaded in Graph mode, Expand the strings windows and find “Nikhil-9a %d %d %d\n” and double click on it.



```
.rdata:00415737                 db    0
.rdata:00415738                 db  30h ; 0
.rdata:00415739                 db  4Dh ; M
.rdata:0041573A                 db    0
.rdata:0041573B                 db    0
.rdata:0041573C ; char aNikhil9aDDD[]
.rdata:0041573C aNikhil9aDDD    db 'NIKHIL-9a: %d %d %d',0Ah,0 ; DATA XREF: wmain+4D↑o
.rdata:00415751                 align 8
.rdata:00415758 aFDdVctoolsCrt_:                        ; DATA XREF: __tmainCRTStartup+127↑o
.rdata:00415758                 unicode 0, <f:\dd\vctools\crt_bld\self_x86\crt\src\crtexe.c>,0
.rdata:004157B8                 db    0
.rdata:004157B9                 db    0
.rdata:004157BA                 db    0
.rdata:004157BB                 db    0
.rdata:004157BC                 db    0
.rdata:004157BD                 db    0
.rdata:004157BE                 db    0
.rdata:004157BF                 db    0
.rdata:004157C0                 db    0
.rdata:004157C1                 db    0
.rdata:004157C2                 db    0
.rdata:004157C3                 db    0
.rdata:004157C4                 db    0
.rdata:004157C5                 db    0
.rdata:004157C6                 db    0
.rdata:004157C7                 db    0
.rdata:004157C8                 db    0
.rdata:004157C9                 db    0
.rdata:004157CA                 db    0
.rdata:004157CB                 db    0
.rdata:004157CC                 db    0
.rdata:004157CD                 db    0
.rdata:004157CE                 db    0
0000413C    0041573C: .rdata:aNikhil9aDDD
```

```
You may start to explore the input file right now.
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.
4113ED: force zero offsets in structures
```

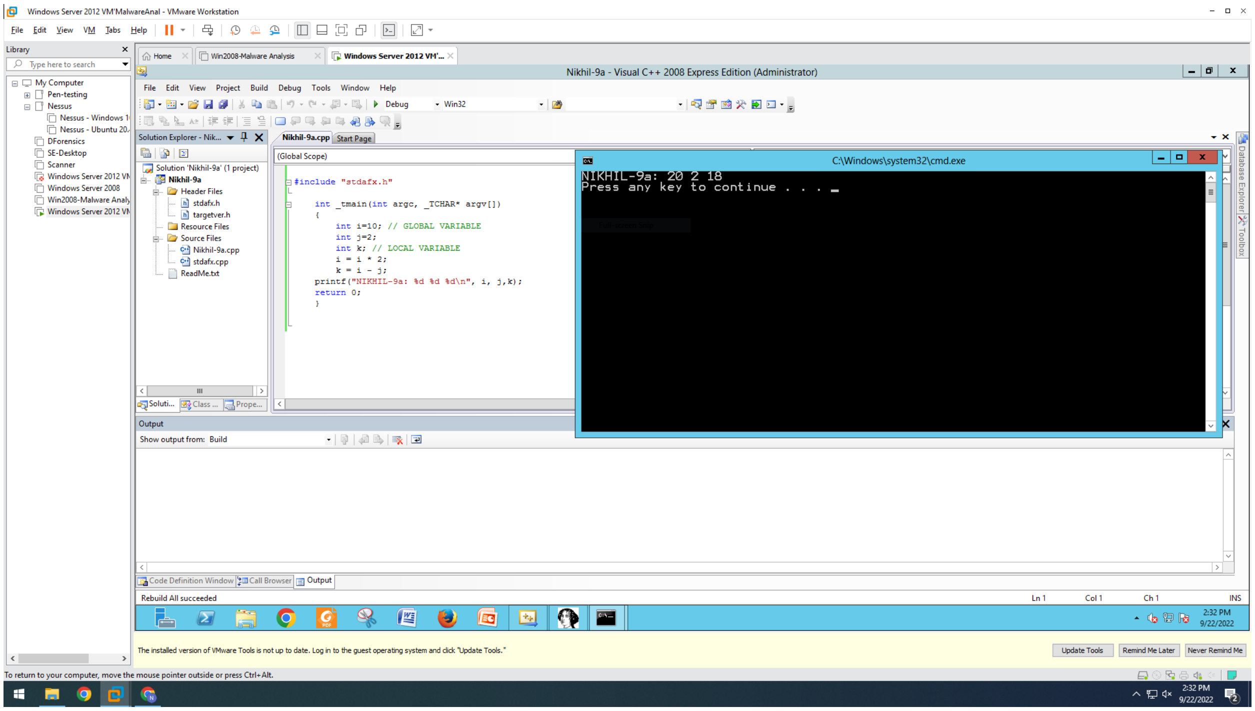
AU: idle   Down   Disk: 39GB

The installed version of VMware Tools is not up to date. Log in to the guest operating system and click "Update Tools."

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

- 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

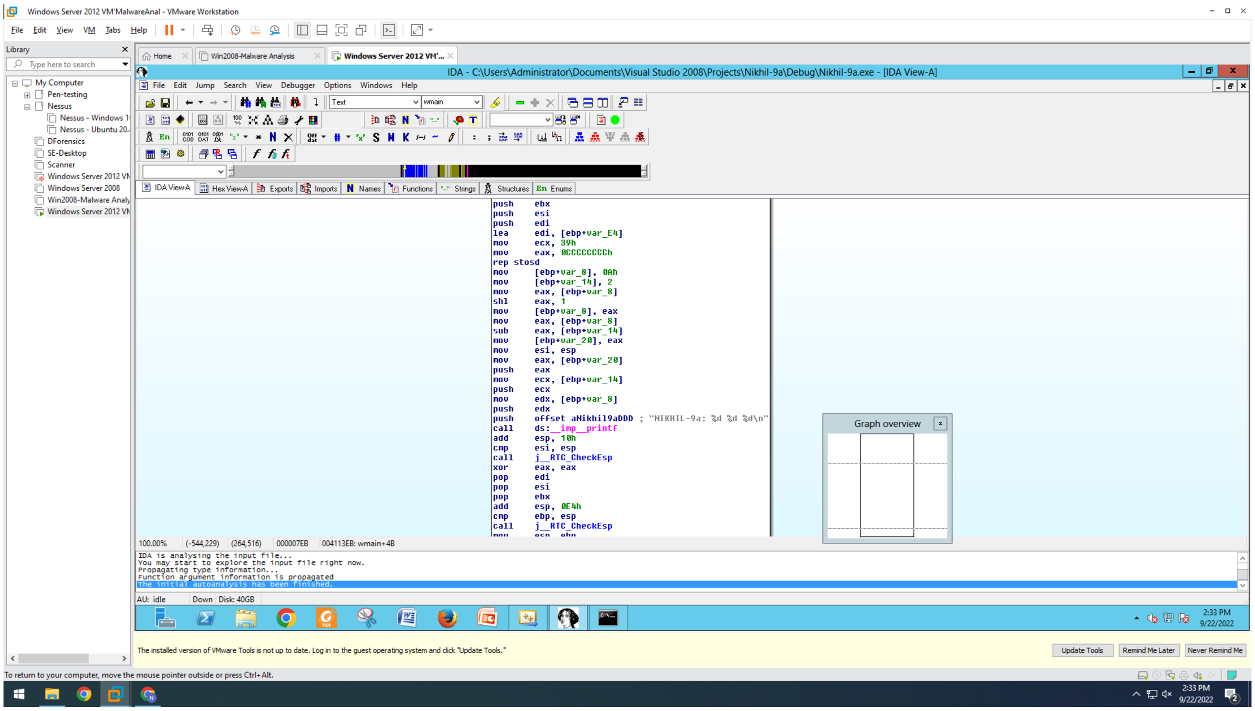

Windows Server 2012 VM'MalwareAnal - VMware Workstation
Nikhil-9a - Visual C++ 2008 Express Edition (Administrator)
Nikhil-9a.cpp
Start Page
(Global Scope)
C:\Windows\system32\cmd.exe
Solution Explorer - Nik...
Rebuild All succeeded

```
#include "stdafx.h"

    int _tmain(int argc, _TCHAR* argv[])
    {
        int i=10; // GLOBAL VARIABLE
        int j=2;
        int k; // LOCAL VARIABLE
        i = i * 2;
        k = i - j;
    printf("NIKHIL-9a: %d %d %d\n", i, j,k);
    return 0;
    }
```

```
NIKHIL-9a: 20 2 18
Press any key to continue . . .
```

The installed version of VMware Tools is not up to date. Log in to the guest operating system and click "Update Tools."


Windows Server 2012 VM'MalwareAnal - VMware Workstation
IDA - C:\Users\Administrator\Documents\Visual Studio 2008\Projects\Nikhil-9a\Debug\Nikhil-9a.exe - [IDA View-A]
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
Enums
Graph overview

```
push    ebx
push    esi
push    edi
lea     edi, [ebp+var_E4]
mov     ecx, 39h
mov     eax, 0CCCCCCCCh
rep stosd
mov     [ebp+var_8], 0Ah
mov     [ebp+var_14], 2
mov     eax, [ebp+var_8]
shl     eax, 1
mov     [ebp+var_8], eax
mov     eax, [ebp+var_8]
sub     eax, [ebp+var_14]
mov     [ebp+var_20], eax
mov     esi, esp
mov     eax, [ebp+var_20]
push    eax
mov     ecx, [ebp+var_14]
push    ecx
mov     edx, [ebp+var_8]
push    edx
push    offset aNikhil9aDDD ; "NIKHIL-9a: %d %d %d\n"
call    ds:__imp__printf
add     esp, 10h
cmp     esi, esp
call    j__RTC_CheckEsp
xor     eax, eax
pop     edi
pop     esi
pop     ebx
add     esp, 0E4h
cmp     ebp, esp
call    j__RTC_CheckEsp
mov     esp, ebp
```

100.00% (-544,229) (264,516) 000007EB 004113EB: wmain+4B

```
IDA is analysing the input file...
You may start to explore the input file right now.
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.
```

AU: idle Down Disk: 40GB

The installed version of VMware Tools is not up to date. Log in to the guest operating system and click "Update Tools."

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.