

**NAME-SLVN YASWANTH**

**REG NO-19BCN7114**

**LAB EXPERIMENT 11**

Lab experiment – Creating secure and safe executable

Download and install visual studio (recent edition)

Write a C++ code of your own to build an executable and run the same.

Download process explorer and verify the DEP & ASLR status

Enable software DEP, ASLR and SEH in the visual studio and rebuild the same executable

Again, verify the DEP & ASLR status in the process explorer

Report the same with separate screenshot - before and after enabling DEP & ASLR.

Happy Learning!!!

Experiment analysis:

1) Create an executable

Executable created: Factorial.exe

Select C++ as the language and open an empty CLR project and select Windows Form.

Then create the above GUI by adding labels, textbox and button and make the modifications accordingly.

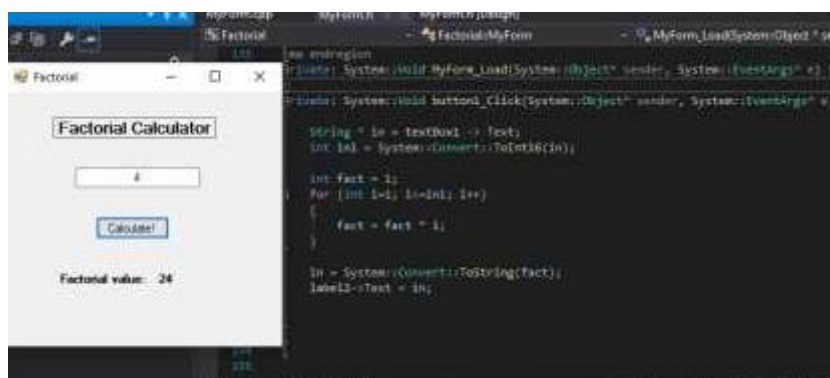
While making the form the code gets auto generated. Later click on particular control option and add functionality to it.

Right click on the Factorial in solution explorer and select “Properties”.

Select Linker and then Select System.

In Sub System option select Windows

Then go to Advanced option and give “main” in the Entry point option.



Now turning DEP and ASLR ON

Now open Process Explorer (Sysinternals) and check the DEP and ASLR status for Factorial.exe

Firstly let us check the status by turning on ASLR and DEP

Check Randomized base address and DEP and make sure it is YES

View Status in process Explorer

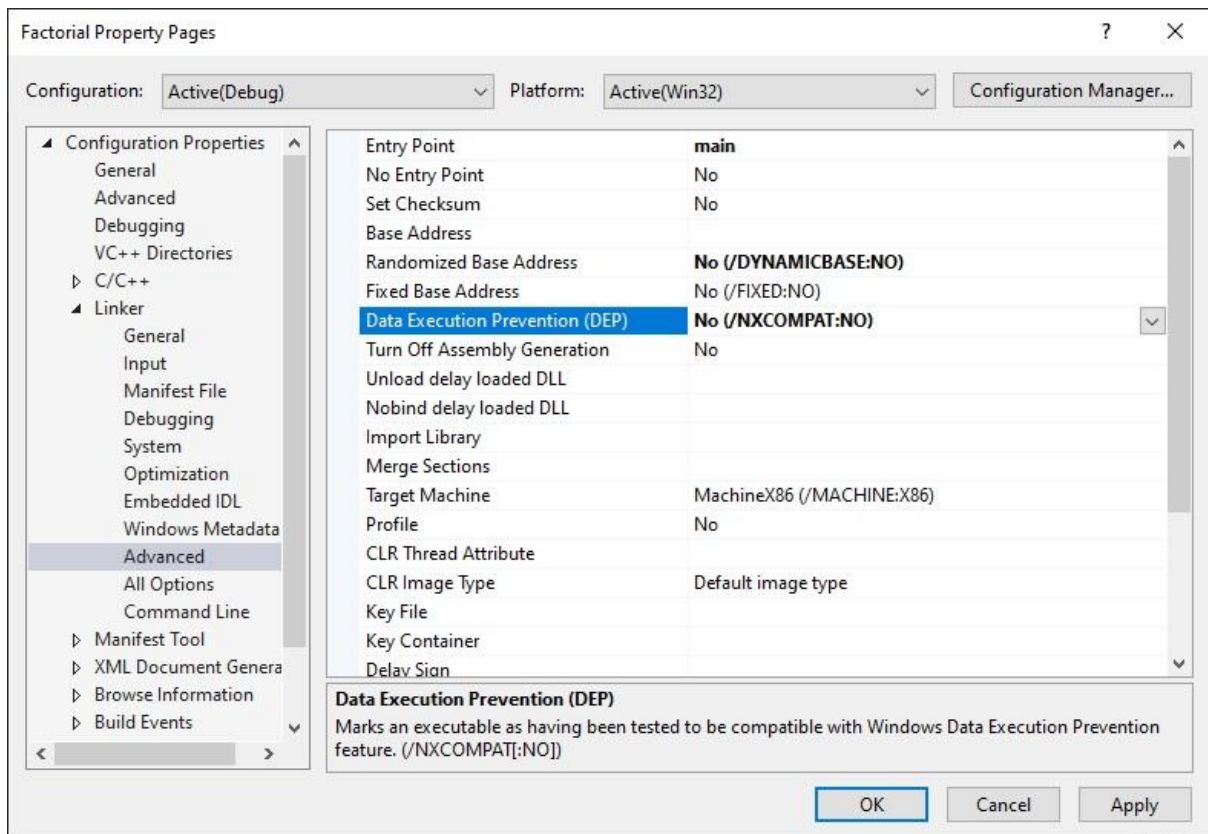
Factorial.exe status

conhost.exe	6,348 K	6,696 K	8936	Console Window Host	Microsoft Corporation	10.0.19041.964	Running	Enabled (permane... ASLR
Factorial.exe	15,368 K	26,704 K	8086					Enabled (permane... ASLR
ScriptedSandbox64.exe	14.87	119,712 K	148,468 K	9312	ScriptedSandbox64.exe	Microsoft Corporation	16.0.31227.257	Enabled (permane... ASLR
process.exe	4.180 K	11.188 K	4628	Sysinternals Process Explorer	Sysinternals - www.sysinter...	16.32.0.0		Enabled (permane... ASLR

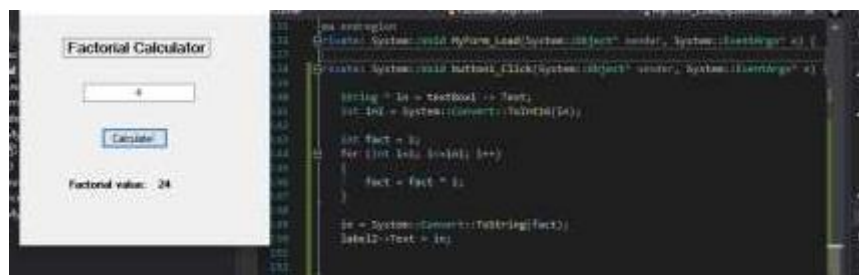
It is enabled

Now lets turn off Dep and ASLR and see

Now let us disable the DEP and ASLR and see if it is reflecting in Process Explorer



Run the exe again



Check ASLR and DEP status

MSBuild.exe	26,880 K	43,164 K	1196	MSBuild.exe	Microsoft Corporation	16.9.0.16/03	Enabled (permane...	
conhost.exe	6,332 K	10,728 K	10276	Console Window Host	Microsoft Corporation	10.0.19041.364	Enabled (permane...	
Factorial.exe	15,304 K	27,136 K	5824			Running	Disabled (permane...	
ScriptedSandbox64.exe	5.86	85,916 K	115,568 K	10584	ScriptedSandbox64.exe	Microsoft Corporation	16.0.31227.257	Enabled (permane...
vsmon.exe	0.01	19,320 K	29,012 K	8136	Microsoft (R) Visual C++ Pac...	Microsoft Corporation	16.0.31229.75	Enabled (permane...

