

SECURE CODING LAB-11

26-04-2021

SLOT-L39+L40

18BCN7134

NIHARIKA VISWANADHUNI

Lab experiment - Creating secure and safe executable

QUESTION

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

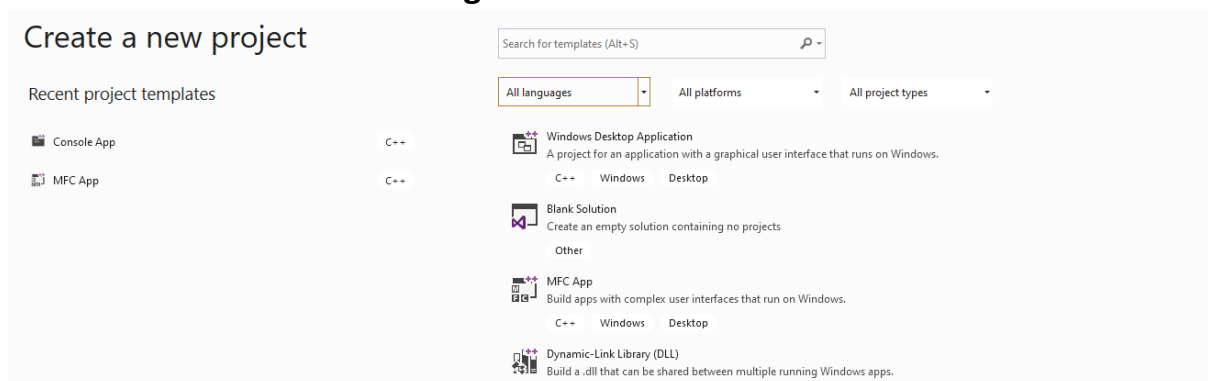
Enable software DEP, ASLR and SEH in the visual studio and rebuild the same executable

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

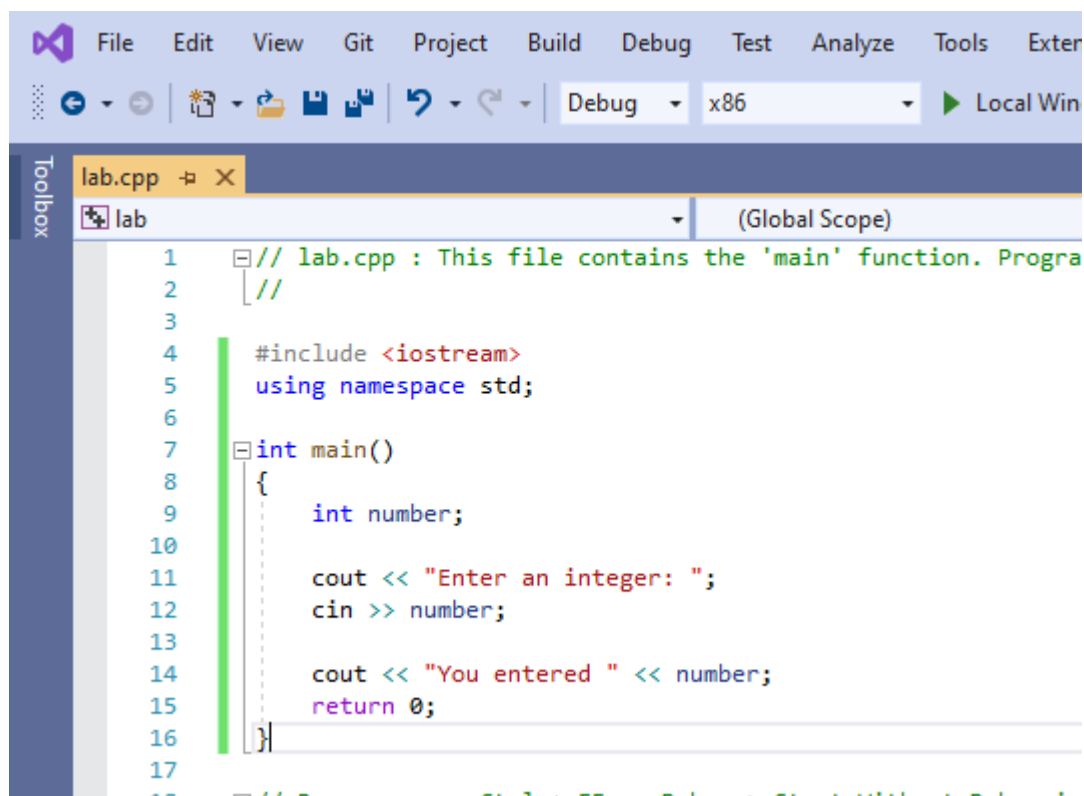
Report the same with separate screenshot - before and after enabling DEP & ASLR.

OUTPUT

- **Download and installing visual studio**



C++ code

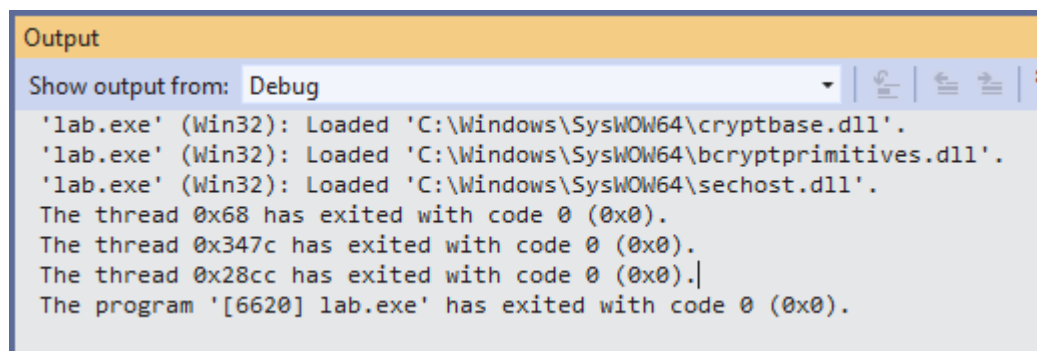


```
1 // lab.cpp : This file contains the 'main' function. Program  
2 //  
3  
4 #include <iostream>  
5 using namespace std;  
6  
7 int main()  
8 {  
9     int number;  
10  
11     cout << "Enter an integer: ";  
12     cin >> number;  
13  
14     cout << "You entered " << number;  
15     return 0;  
16 }  
17  
18 // Run program: Ctrl + F5 or Debug > Start Without Debugging
```

Run and executing the code:

Microsoft Visual Studio Debug Console

```
Enter an integer: 3  
You entered 3
```



Output

Show output from: Debug

```
'lab.exe' (Win32): Loaded 'C:\Windows\SysWOW64\cryptbase.dll'.  
'lab.exe' (Win32): Loaded 'C:\Windows\SysWOW64\bcryptprimitives.dll'.  
'lab.exe' (Win32): Loaded 'C:\Windows\SysWOW64\sechost.dll'.  
The thread 0x68 has exited with code 0 (0x0).  
The thread 0x347c has exited with code 0 (0x0).  
The thread 0x28cc has exited with code 0 (0x0).  
The program '[6620] lab.exe' has exited with code 0 (0x0).
```

Download process explorer

Process Explorer - Sysinternals: www.sysinternals.com [NAIMISHA\Naimisha Segu]

File Options View Process Find Handle Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	DEP	ASLR
AcrobatNotificationClient.exe	Susp...	6,796 K	3,128 K	8420			Enabled (permane...	ASLR
cmd.exe		3,440 K	2,412 K	4408		n/a	n/a	n/a
conhost.exe	< 0.01	2,256 K	5,620 K	4508		n/a	n/a	n/a
conhost.exe	< 0.01	6,720 K	5,416 K	5036		n/a	n/a	n/a
conhost.exe	< 0.01	6,744 K	5,232 K	5132		n/a	n/a	n/a
conhost.exe	< 0.01	6,712 K	5,844 K	6312		n/a	n/a	n/a
conhost.exe	< 0.01	6,924 K	5,792 K	8208		n/a	n/a	n/a
csrss.exe	< 0.01	1,908 K	4,052 K	632		n/a	n/a	n/a
csrss.exe	0.33	2,580 K	5,008 K	736		n/a	n/a	n/a
ctfmon.exe	0.29	4,324 K	12,564 K	6532		Enabled (permane...	n/a	n/a
dasHost.exe		3,816 K	8,868 K	2576		n/a	n/a	n/a
dllhost.exe		3,976 K	8,100 K	14216		n/a	n/a	n/a
dwm.exe	1.27	64,068 K	61,132 K	1224		n/a	n/a	n/a
fontdrvhost.exe		5,592 K	8,664 K	384		n/a	n/a	n/a
fontdrvhost.exe		1,728 K	1,816 K	456		n/a	n/a	n/a
GoogleCrashHandler.exe		1,712 K	916 K	9972		n/a	n/a	n/a
GoogleCrashHandler64.exe		1,732 K	68 K	10204		n/a	n/a	n/a
Intempts	2.21	0 K	0 K	n/a	Hardware Interrupts an	n/a	n/a	n/a

Process explorer and verify the DEP & ASLR status

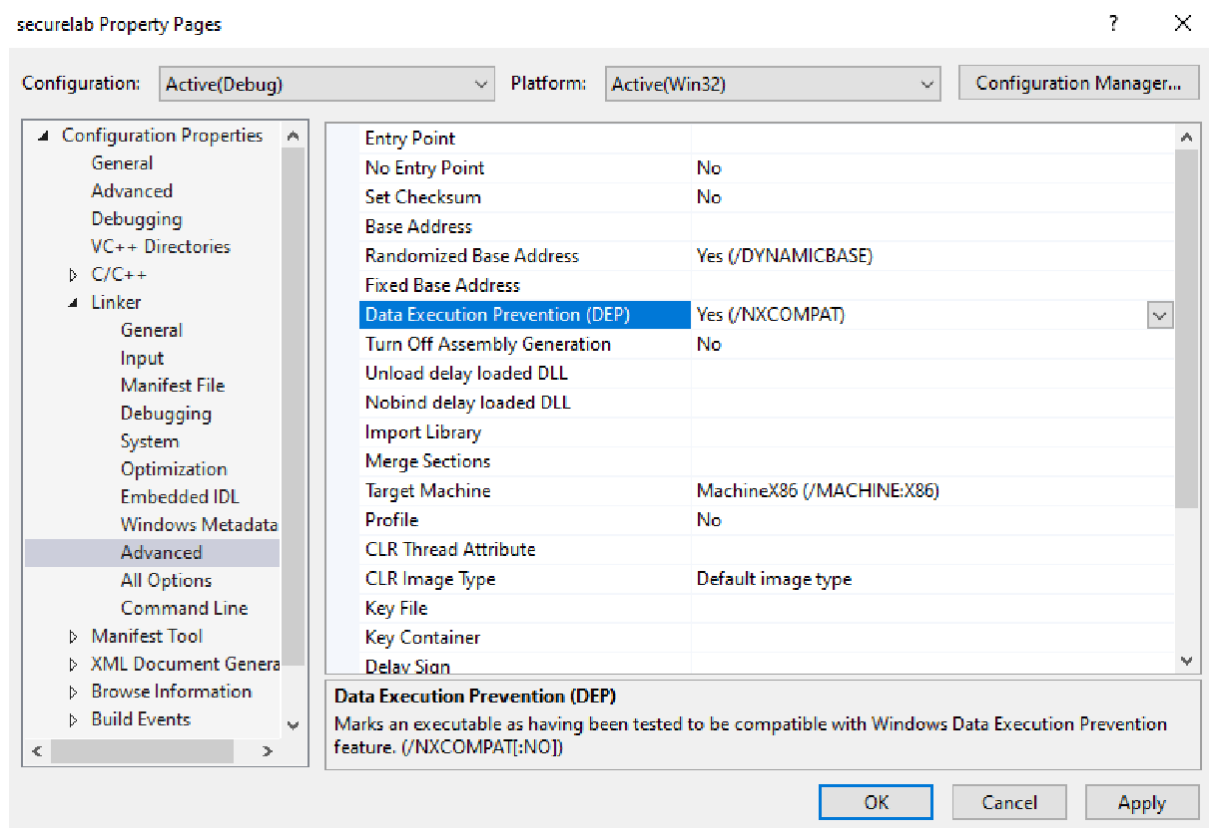
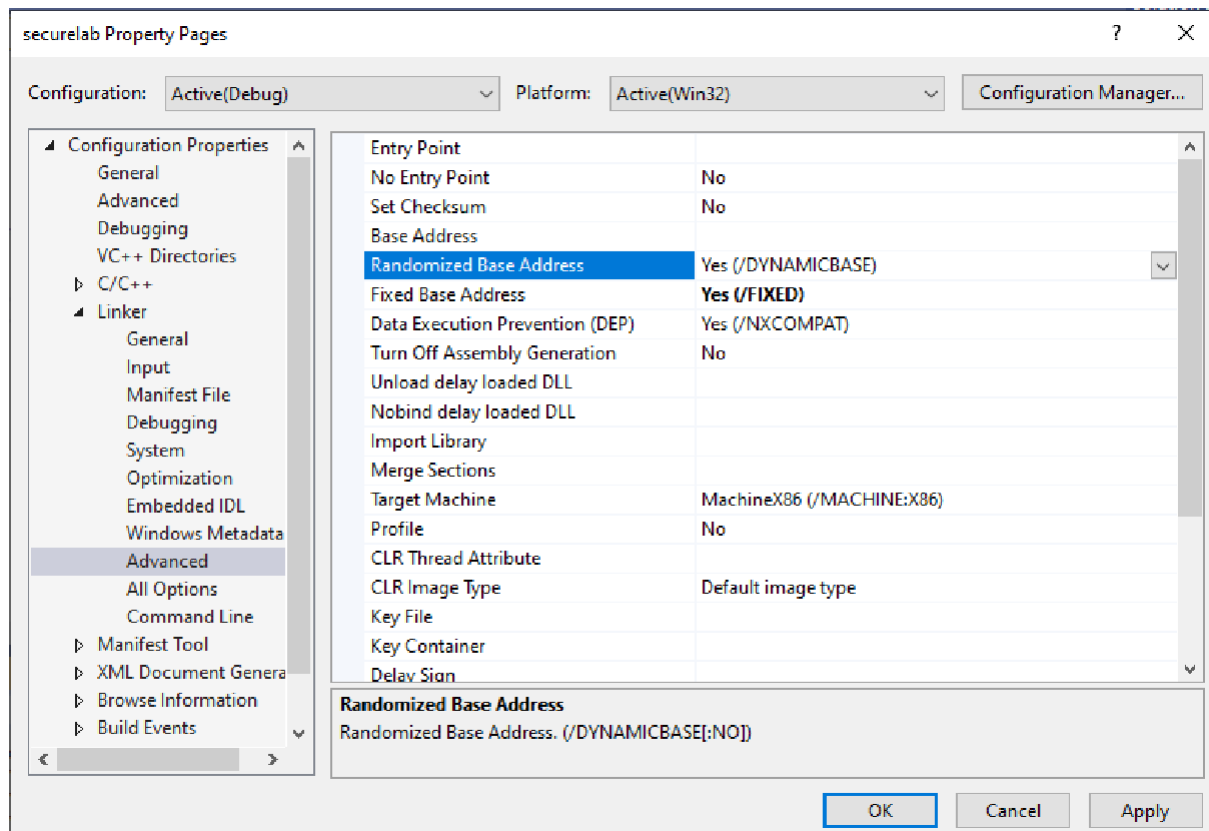
File Options View Process Find DLL Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	DEP	ASLR
ServiceHub.ThreadedWaitDialo...	2.77	50,588 K	28,164 K	15496	ServiceHub.Threaded...	Microsoft	Enabled (permane...	ASLR
ServiceHub.VSDetouredHost.exe	0.05	37,320 K	16,936 K	12900	ServiceHub.VSDetour...	Microsoft	Enabled (permane...	ASLR
ApplicationFrameHost.exe		10,444 K	18,844 K	9492	Application Frame Host	Microsoft Corporation	Enabled (permane...	ASLR
CompPkgSrv.exe		1,828 K	7,580 K	7976	Component Package ...	Microsoft Corporation	Enabled (permane...	ASLR
conhost.exe		7,240 K	16,192 K	1556	Console Window Host	Microsoft Corporation	Enabled (permane...	ASLR
devenv.exe	3.59	348,968 K	2,91,084 K	11536	Microsoft Visual Studio ..	Microsoft Corporation	Enabled (permane...	ASLR
dllhost.exe		5,460 K	11,920 K	9744	COM Surrogate	Microsoft Corporation	Enabled (permane...	ASLR
dllhost.exe		4,004 K	9,444 K	12848	COM Surrogate	Microsoft Corporation	n/a	ASLR
explorer.exe	0.97	80,656 K	1,18,704 K	7924	Windows Explorer	Microsoft Corporation	Enabled (permane...	ASLR
lsass.exe		8,280 K	14,484 K	884	Local Security Authort...	Microsoft Corporation	n/a	ASLR
msdtc.exe		2,840 K	6,852 K	1240	Microsoft Distributed T...	Microsoft Corporation	n/a	ASLR

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

Configuration Properties > Linker > Advanced property page

Modifying the Randomized Base Address property.



Again, running the executable

Microsoft Visual Studio Debug Console

```
Enter an integer: 5  
You entered 5
```

And, verifying the DEP & ASLR status in the process explorer

File Options View Process Find Handle Users Help								
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	DEP	ASLR
devenv.exe	3.53	3,63,920 K	3,57,132 K	11536	Microsoft Visual Studio...	Microsoft Corporation	Enabled (permane...	ASLR
dllhost.exe		5,300 K	10,368 K	9744	COM Surrogate	Microsoft Corporation	Enabled (permane...	ASLR
dllhost.exe	< 0.01	3,952 K	8,776 K	12848	COM Surrogate	Microsoft Corporation	n/a	ASLR
explorer.exe	1.77	80,344 K	1,08,320 K	7924	Windows Explorer	Microsoft Corporation	Enabled (permane...	ASLR
lsass.exe	0.03	8,256 K	14,132 K	884	Local Security Author...	Microsoft Corporation	n/a	ASLR
MSBuild.exe		29,472 K	43,592 K	32	MSBuild.exe	Microsoft Corporation	Enabled (permane...	ASLR
msdtc.exe	< 0.01	2,804 K	6,608 K	1240	Microsoft Distributed T...	Microsoft Corporation	n/a	ASLR
MsMpEng.exe	1.73	2,83,644 K	1,58,420 K	4304	Antimalware Service E...	Microsoft Corporation	n/a	ASLR
mspdbsrv.exe		15,152 K	14,372 K	5896	Microsoft® Program D...	Microsoft Corporation	Enabled (permane...	ASLR
NisSrv.exe	< 0.01	3,872 K	6,790 K	6292	Microsoft Network Fle...	Microsoft Corporation	n/a	ASLR
OneDrive.exe		25,136 K	19,336 K	11100	Microsoft OneDrive	Microsoft Corporation	Enabled (permane...	ASLR
PerfWatson2.exe	0.02	43,852 K	28,996 K	12235	PerfWatson2.exe	Microsoft Corporation	Enabled (permane...	ASLR
PresentationFontCache.exe	< 0.01	25,332 K	7,968 K	7548	PresentationFontCach...	Microsoft Corporation	n/a	ASLR
rundll32.exe		1,632 K	6,540 K	13832	Windows host process...	Microsoft Corporation	Enabled (permane...	ASLR