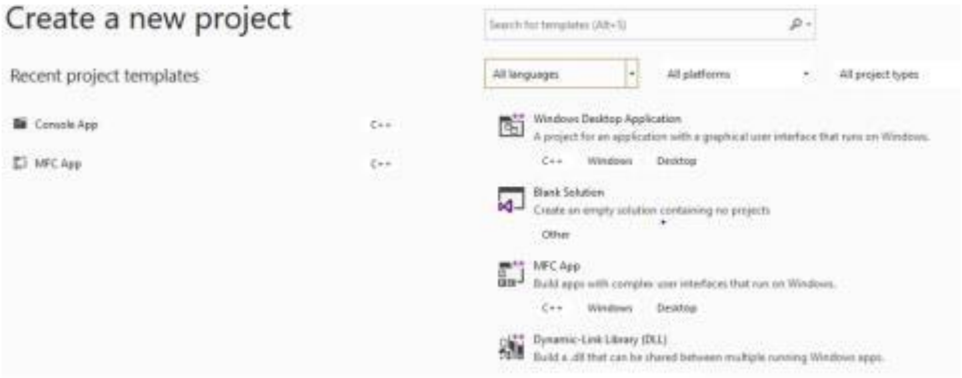
SECURE CODING CSE2010

LAB-11

CH.SAI SUMEDH
REG NO:-18BCN7092
SLOT:-L39+L40

Creating a secure executable application

1. Download visual studio.



Create a new project

Recent project templates

Console App C++

MFC App C++

Search for templates (Alt+S)

All languages | All platforms | All project types

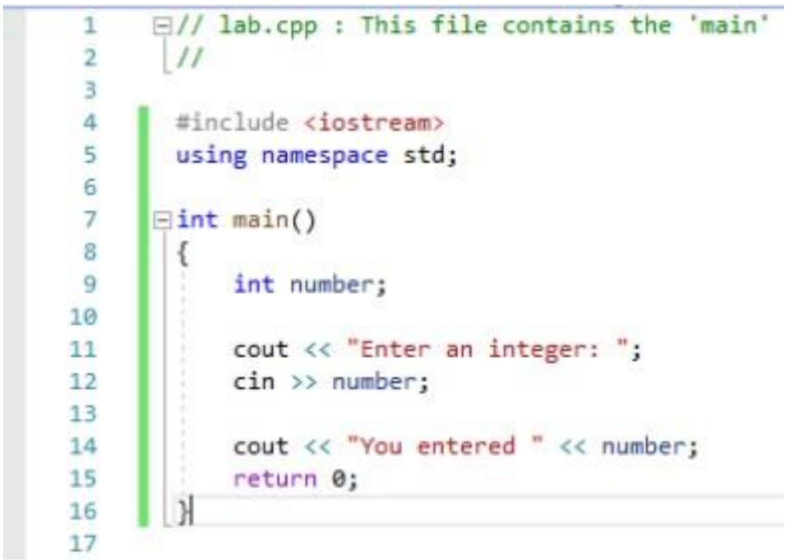
Windows Desktop Application
A project for an application with a graphical user interface that runs on Windows.
C++ Windows Desktop

Blank Solution
Create an empty solution containing no projects
Other

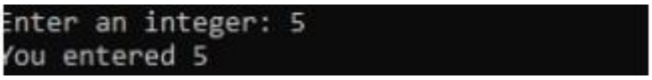
MFC App
Build apps with complex user interfaces that run on Windows.
C++ Windows Desktop

Dynamic-Link Library (DLL)
Build a .dll that can be shared between multiple running Windows apps.

C++ code in an executable file

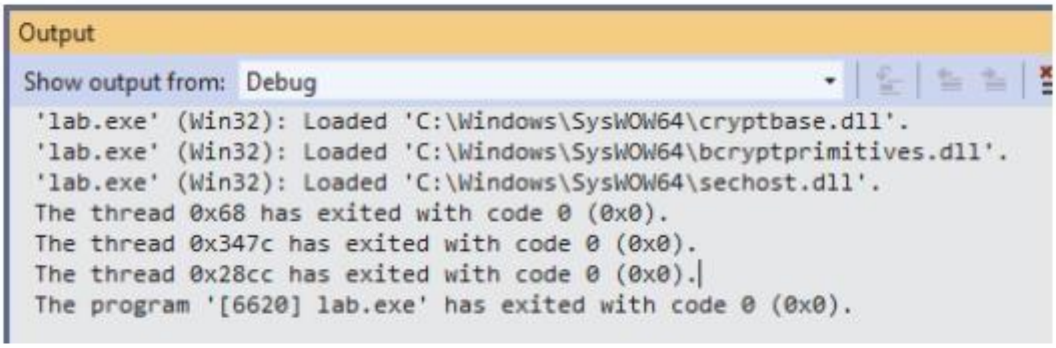


```
// lab.cpp : This file contains the 'main'
//

#include <iostream>
using namespace std;

int main()
{
    int number;

    cout << "Enter an integer: ";
    cin >> number;

    cout << "You entered " << number;
    return 0;
}
```



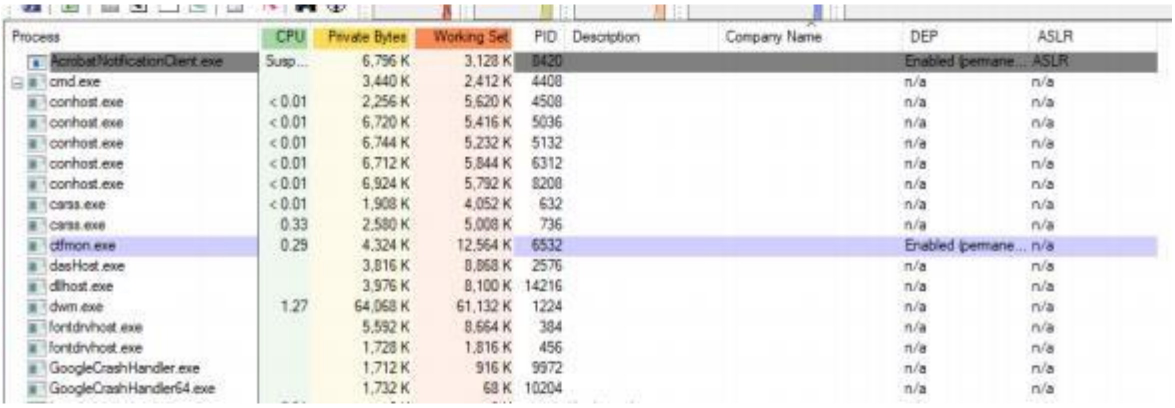
```
Enter an integer: 5
You entered 5
```

Build or debug

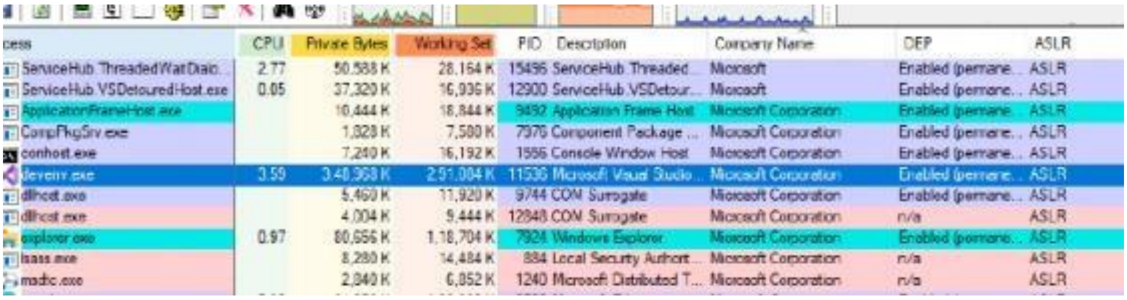


```
'lab.exe' (Win32): Loaded 'C:\Windows\SysWOW64\cryptbase.dll'.
'lab.exe' (Win32): Loaded 'C:\Windows\SysWOW64\bcryptprimitives.dll'.
'lab.exe' (Win32): Loaded 'C:\Windows\SysWOW64\sechost.dll'.
The thread 0x68 has exited with code 0 (0x0).
The thread 0x347c has exited with code 0 (0x0).
The thread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

3. Download the process and explorer and verify the DEP and ASLR status.

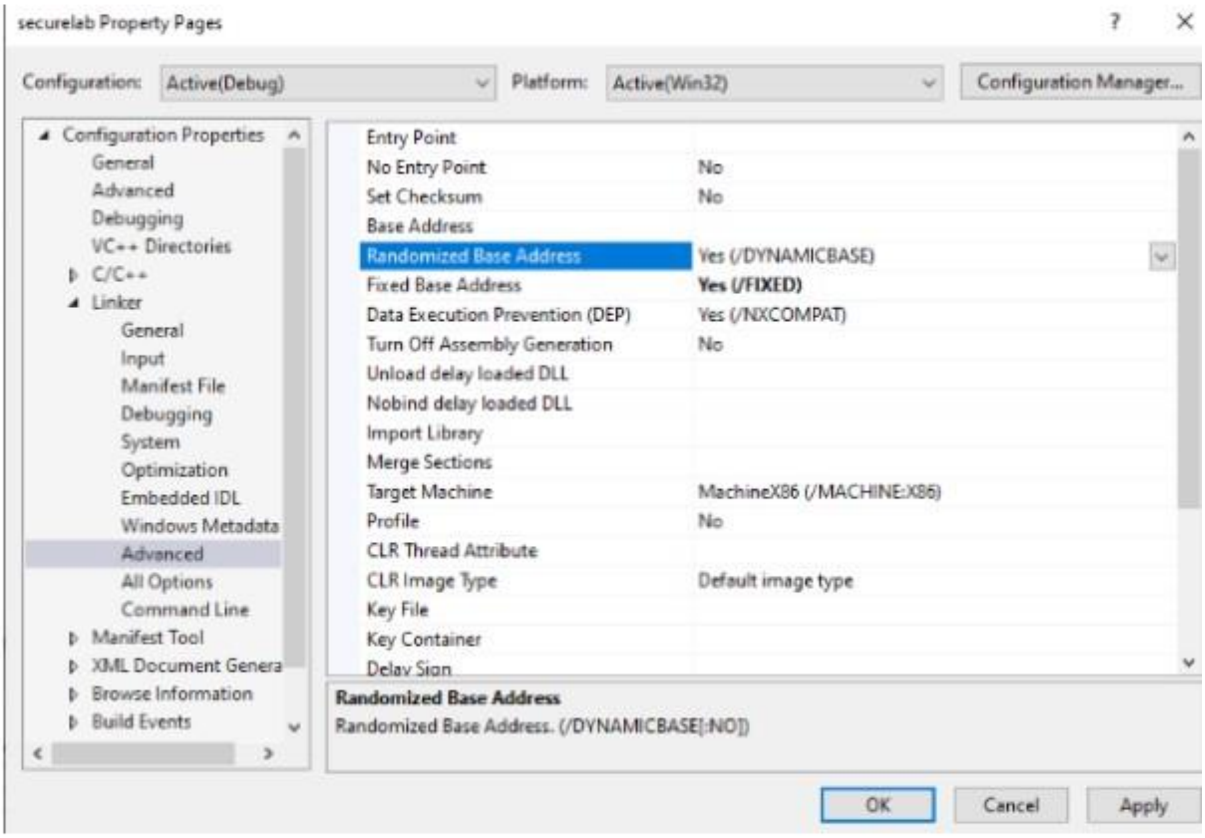


Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	DEP	ASLR
AcrobatNotificationClient.exe	Susp...	6,796 K	3,128 K	8420			Enabled (permane...	ASLR
cmd.exe		3,440 K	2,412 K	4408			n/a	n/a
conhost.exe	< 0.01	2,256 K	5,620 K	4508			n/a	n/a
conhost.exe	< 0.01	6,720 K	5,416 K	5036			n/a	n/a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



cess	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	3,48,968 K	2,91,004 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 Authorit...	Microsoft Corporation	n/a	ASLR
msdtc.exe		2,840 K	6,852 K	1240	Microsoft Distributed T...	Microsoft Corporation	n/a	ASLR

Now, enable the software DEP , ASLR and SEH in the visual studio and rebuild the same executable.



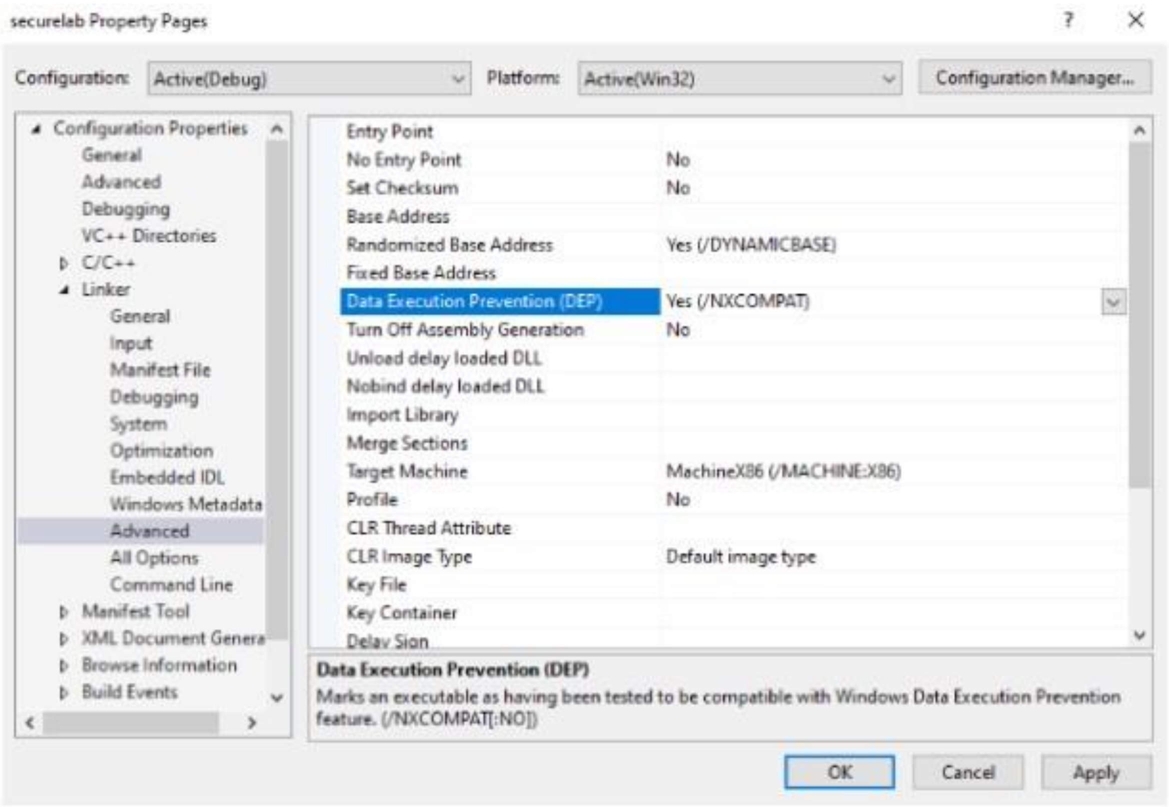
securelab Property Pages

Configuration: Active(Debug) Platform: Active(Win32)

```
Entry Point
No Entry Point                      No
Set Checksum                        No
Base Address
Randomized Base Address             Yes (/DYNAMICBASE)
Fixed Base Address                  Yes (/FIXED)
Data Execution Prevention (DEP)     Yes (/NXCOMPAT)
Turn Off Assembly Generation        No
Unload delay loaded DLL
Nobind delay loaded DLL
Import Library
Merge Sections
Target Machine                      MachineX86 (/MACHINE:X86)
Profile                             No
CLR Thread Attribute
CLR Image Type                      Default image type
Key File
Key Container
Delay Sign
```

Randomized Base Address

Randomized Base Address. (/DYNAMICBASE[:NO])



securelab Property Pages

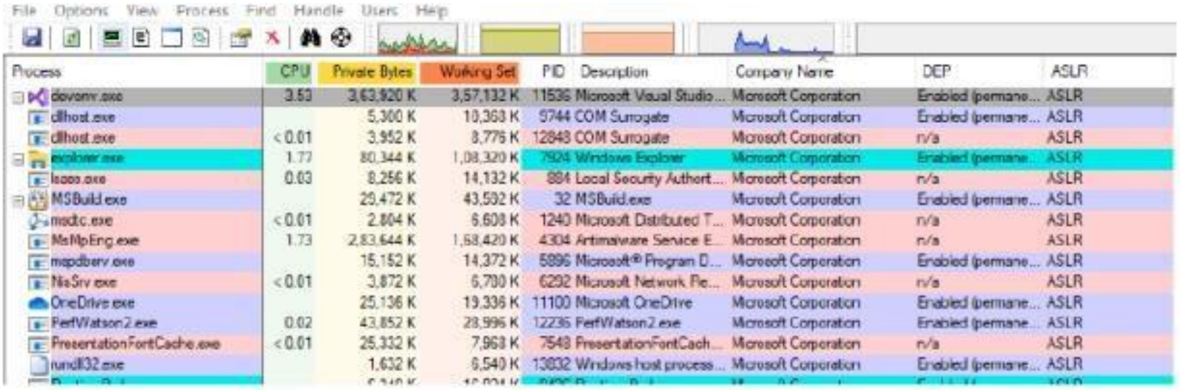
Configuration: Active(Debug) Platform: Active(Win32)

```
Entry Point
No Entry Point                      No
Set Checksum                        No
Base Address
Randomized Base Address             Yes (/DYNAMICBASE)
Fixed Base Address
Data Execution Prevention (DEP)     Yes (/NXCOMPAT)
Turn Off Assembly Generation        No
Unload delay loaded DLL
Nobind delay loaded DLL
Import Library
Merge Sections
Target Machine                      MachineX86 (/MACHINE:X86)
Profile                             No
CLR Thread Attribute
CLR Image Type                      Default image type
Key File
Key Container
Delay Sign
```

Data Execution Prevention (DEP)

Marks an executable as having been tested to be compatible with Windows Data Execution Prevention feature. (/NXCOMPAT[:NO])

Now verify the process explorer of DEP and ASLR.



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	10,363 K	5744	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 Authort...	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	1,68,420 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	6,780 K	6292	Microsoft Network Re...	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	12236	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	13032	Windows host process ...	Microsoft Corporation	Enabled (permane...	ASLR