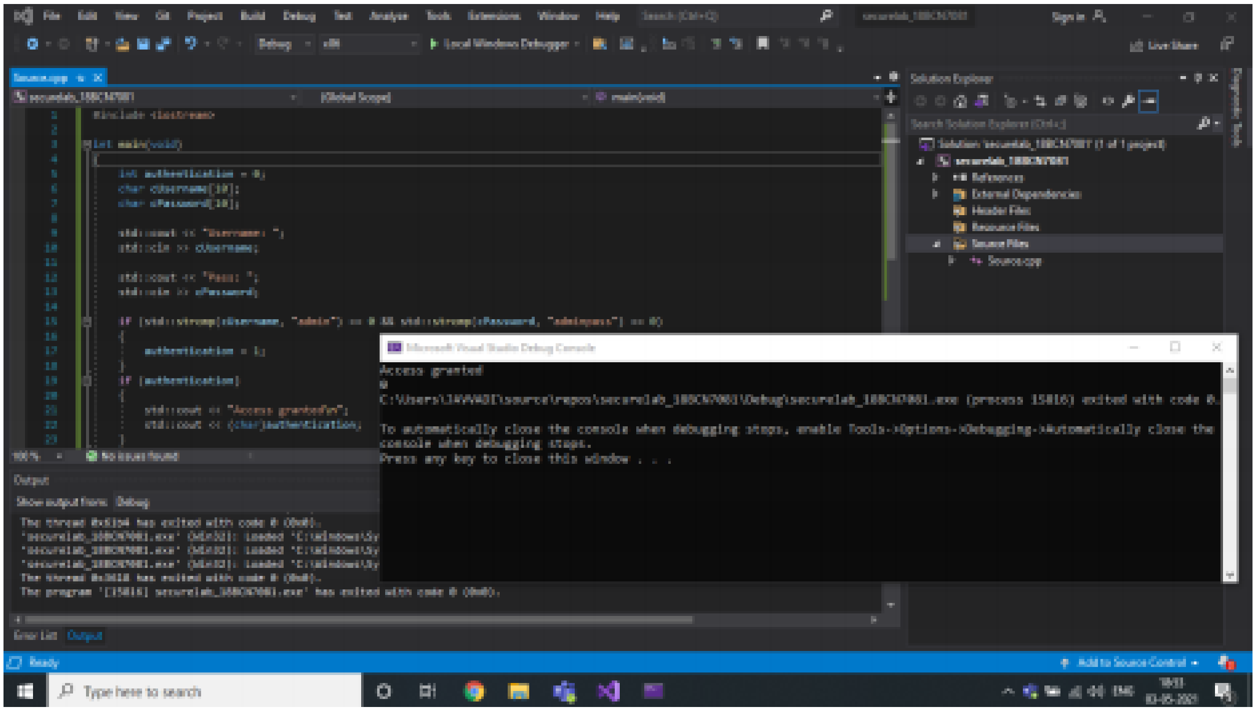
Secure Coding Lab-11

G.CHAITANYA

Lab experiment – Creating secure and safe executable

1) C++ Code & building the Executable

```
#include <iostream>

int main(void)
{
     int authentication = 0;
     char cUsername[10];
     char cPassword[10];

     std::cout << "Username: ";
     std::cin >> cUsername;

     std::cout << "Pass: ";
     std::cin >> cPassword;

     if (std::strcmp(cUsername, "admin") == 0 &&
std::strcmp(cPassword, "adminpass") == 0)
     {
          authentication = 1;
     }
     if (authentication)
     {
          std::cout << "Access granted\n";
          std::cout << (char)authentication;
     }
     else
     {
          std::cout << "Wrong username and password\n";
     }

     return (0);
}
```



```cpp
#include <iostream>

int main(void)
{
    int authentication = 0;
    char cUsername[10];
    char cPassword[10];

    std::cout << "Username: ";
    std::cin >> cUsername;

    std::cout << "Pass: ";
    std::cin >> cPassword;

    if (std::strcmp(cUsername, "admin") == 0 && std::strcmp(cPassword, "adminpass") == 0)
    {
        authentication = 1;
    }
    if (authentication)
    {
        std::cout << "Access granted\n";
        std::cout << (char)authentication;
    }
```

Microsoft Visual Studio Debug Console

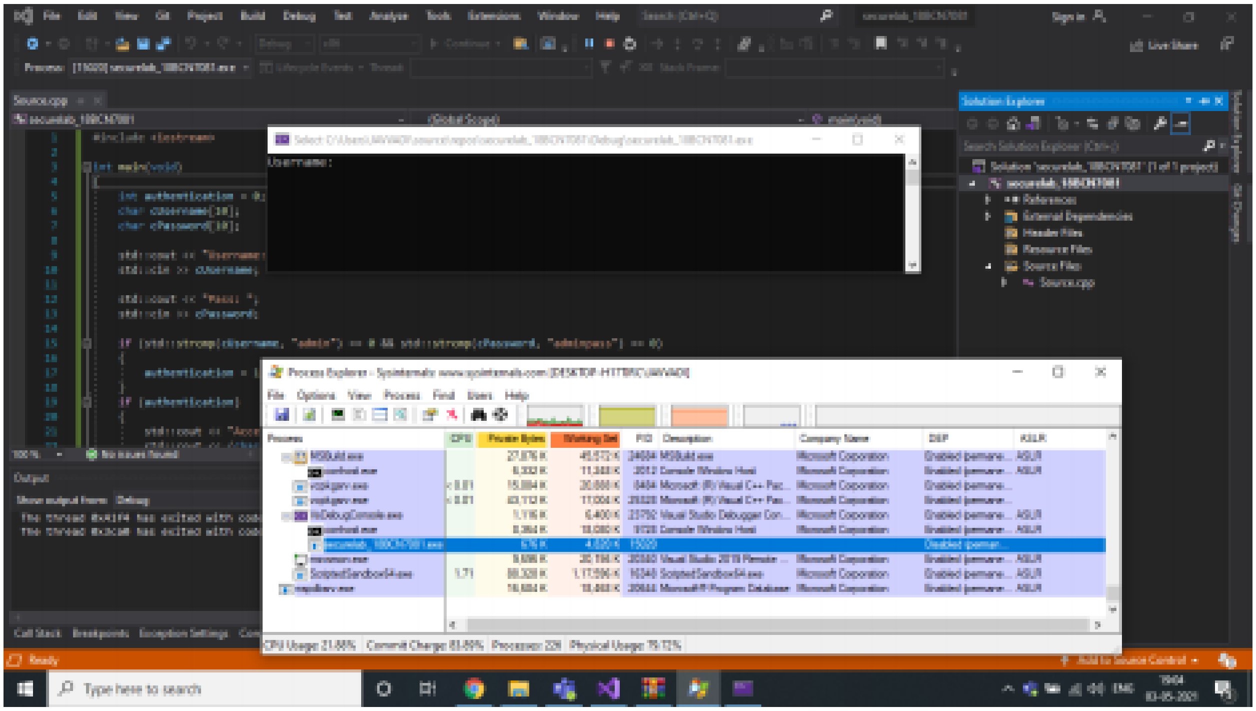
```
Access granted
☺
C:\Users\JAVVADI\source\repos\securelab_188CN7081\Debug\securelab_188CN7081.exe (process 15816) exited with code 0.

To automatically close the console when debugging stops, enable Tools->Options->Debugging->Automatically close the
console when debugging stops.
Press any key to close this window . . .
```

Output

Show output from: Debug

```
The thread 0x51b4 has exited with code 0 (0x0).
'securelab_188CN7081.exe' (Win32): Loaded 'C:\Windows\Sy
'securelab_188CN7081.exe' (Win32): Loaded 'C:\Windows\Sy
'securelab_188CN7081.exe' (Win32): Loaded 'C:\Windows\Sy
The thread 0x3618 has exited with code 0 (0x0).
The program '[15816] securelab_188CN7081.exe' has exited with code 0 (0x0).
```

2) Verifying the DEP & ASLR status in Process Explorer



Select C:\Users\JAVVADI\source\repos\securelab_188CN7081\Debug\securelab_188CN7081.exe

```
Username:
```

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-H1TT8RC\JAVVADI]

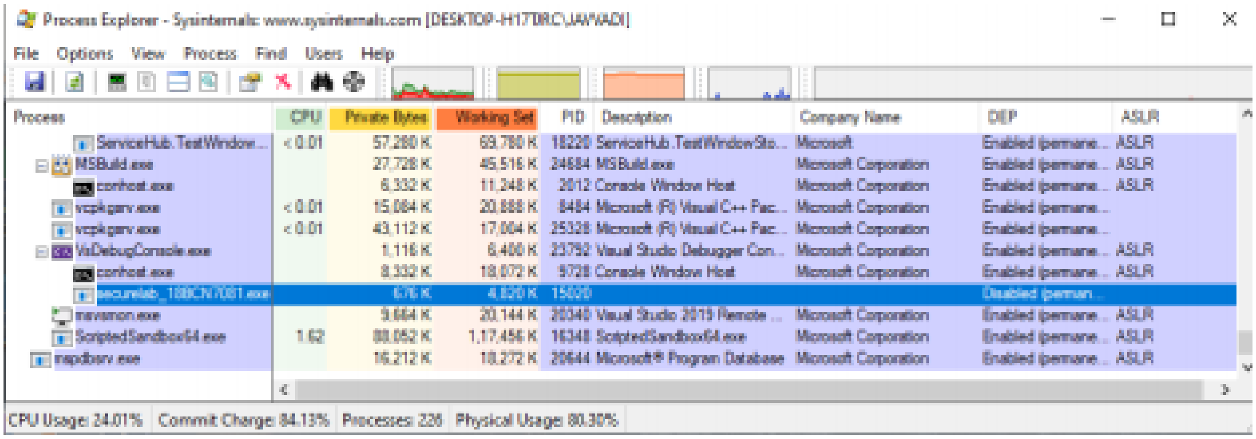
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	DEP	ASLR
MSBuild.exe		27,876 K	45,572 K	24684	MSBuild.exe	Microsoft Corporation	Enabled (permane...	ASLR
conhost.exe		6,332 K	11,348 K	2012	Console Window Host	Microsoft Corporation	Enabled (permane...	ASLR
vcpkgsrv.exe	< 0.01	15,084 K	20,000 K	6404	Microsoft (R) Visual C++ Pac...	Microsoft Corporation	Enabled (permane...	
vcpkgsrv.exe	< 0.01	43,112 K	17,004 K	25328	Microsoft (R) Visual C++ Pac...	Microsoft Corporation	Enabled (permane...	
VsDebugConsole.exe		1,116 K	6,400 K	23792	Visual Studio Debugger Con...	Microsoft Corporation	Enabled (permane...	ASLR
conhost.exe		8,364 K	18,080 K	9728	Console Window Host	Microsoft Corporation	Enabled (permane...	ASLR
securelab_188CN7081.exe		676 K	4,020 K	15020			Disabled (perman...	
msvsmon.exe		9,696 K	20,196 K	20380	Visual Studio 2019 Remote ...	Microsoft Corporation	Enabled (permane...	ASLR
ScriptedSandbox64.exe	1.71	88,328 K	1,17,596 K	16348	ScriptedSandbox64.exe	Microsoft Corporation	Enabled (permane...	ASLR
mspdbsrv.exe		16,604 K	18,468 K	20844	Microsoft® Program Database	Microsoft Corporation	Enabled (permane...	ASLR

CPU Usage: 21.86% | Commit Charge: 83.89% | Processes: 228 | Physical Usage: 79.72%

Output

Show output from: Debug

```
The thread 0x41f4 has exited with code
The thread 0x3ca0 has exited with code
```



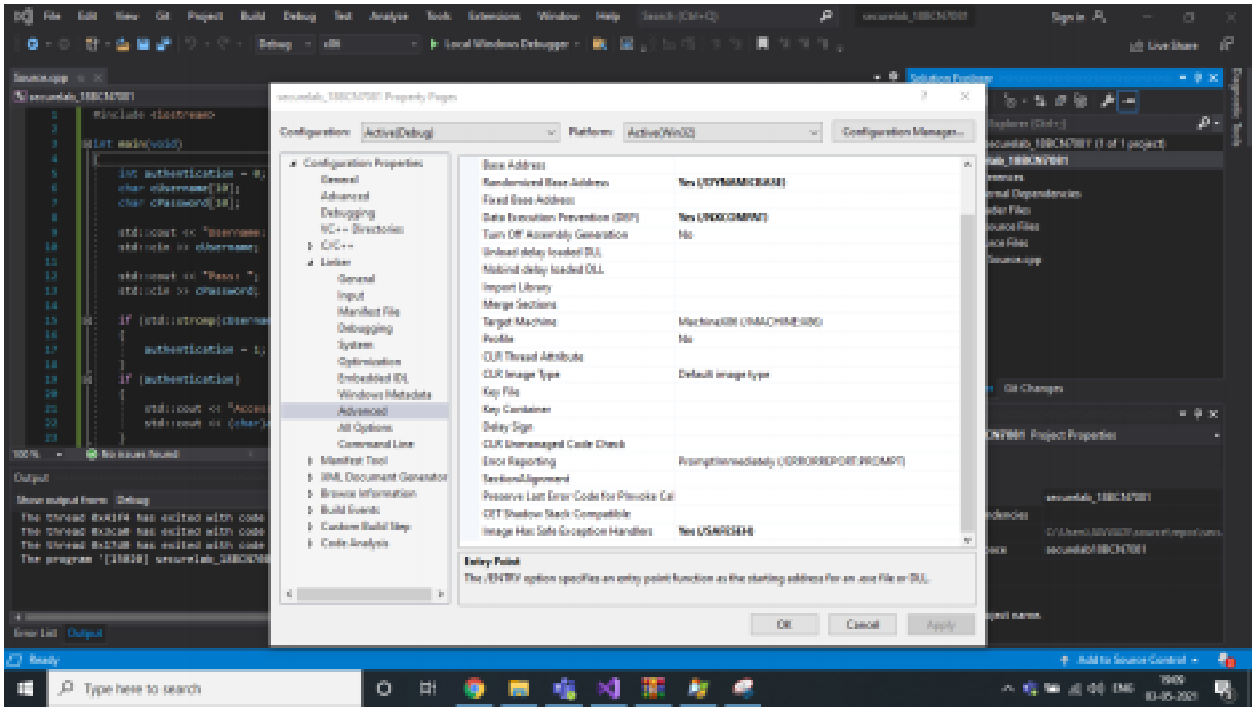
Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-H17DRC\JAWADI]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	DEP	ASLR
ServiceHub.TestWindow...	< 0.01	57,280 K	69,780 K	18220	ServiceHub.TestWindowSto...	Microsoft	Enabled (permane...	ASLR
MSBuild.exe		27,728 K	45,516 K	24684	MSBuild.exe	Microsoft Corporation	Enabled (permane...	ASLR
conhost.exe		6,332 K	11,248 K	2012	Console Window Host	Microsoft Corporation	Enabled (permane...	ASLR
vcpkgsrv.exe	< 0.01	15,084 K	20,888 K	8484	Microsoft (R) Visual C++ Pac...	Microsoft Corporation	Enabled (permane...	
vcpkgsrv.exe	< 0.01	43,112 K	17,004 K	25328	Microsoft (R) Visual C++ Pac...	Microsoft Corporation	Enabled (permane...	
VsDebugConsole.exe		1,116 K	6,400 K	23792	Visual Studio Debugger Con...	Microsoft Corporation	Enabled (permane...	ASLR
conhost.exe		8,332 K	18,072 K	9728	Console Window Host	Microsoft Corporation	Enabled (permane...	ASLR
securelab_18BCN7081.exe		676 K	4,820 K	15020			Disabled (perman...	
msvsmon.exe		9,664 K	20,144 K	20340	Visual Studio 2019 Remote ...	Microsoft Corporation	Enabled (permane...	ASLR
ScriptedSandbox64.exe	1.62	88,052 K	1,17,456 K	16348	ScriptedSandbox64.exe	Microsoft Corporation	Enabled (permane...	ASLR
mspdbsrv.exe		16,212 K	18,272 K	20644	Microsoft® Program Database	Microsoft Corporation	Enabled (permane...	ASLR

CPU Usage: 24.01% | Commit Charge: 84.13% | Processes: 226 | Physical Usage: 80.30%

You can see DEP disabled & No ASLR.

3) Rebuilding the same executable After enabling DEP & ASLR



Source.cpp

securelab_18BCN7081

```
#include <iostream>

int main(void)
{
    int authentication = 0;
    char cUsername[10];
    char cPassword[10];

    std::cout << "Username:
    std::cin >> cUsername;

    std::cout << "Pass: ";
    std::cin >> cPassword;

    if (std::strcmp(cUserna
    {
        authentication = 1;
    }
    if (authentication)
    {
        std::cout << "Access
        std::cout << (char)
    }
```

100 % No issues found

Output

Show output from: Debug

```
The thread 0x41f4 has exited with code
The thread 0x3c60 has exited with code
The thread 0x17d0 has exited with code
The program '[15020] securelab_18BCN708
```

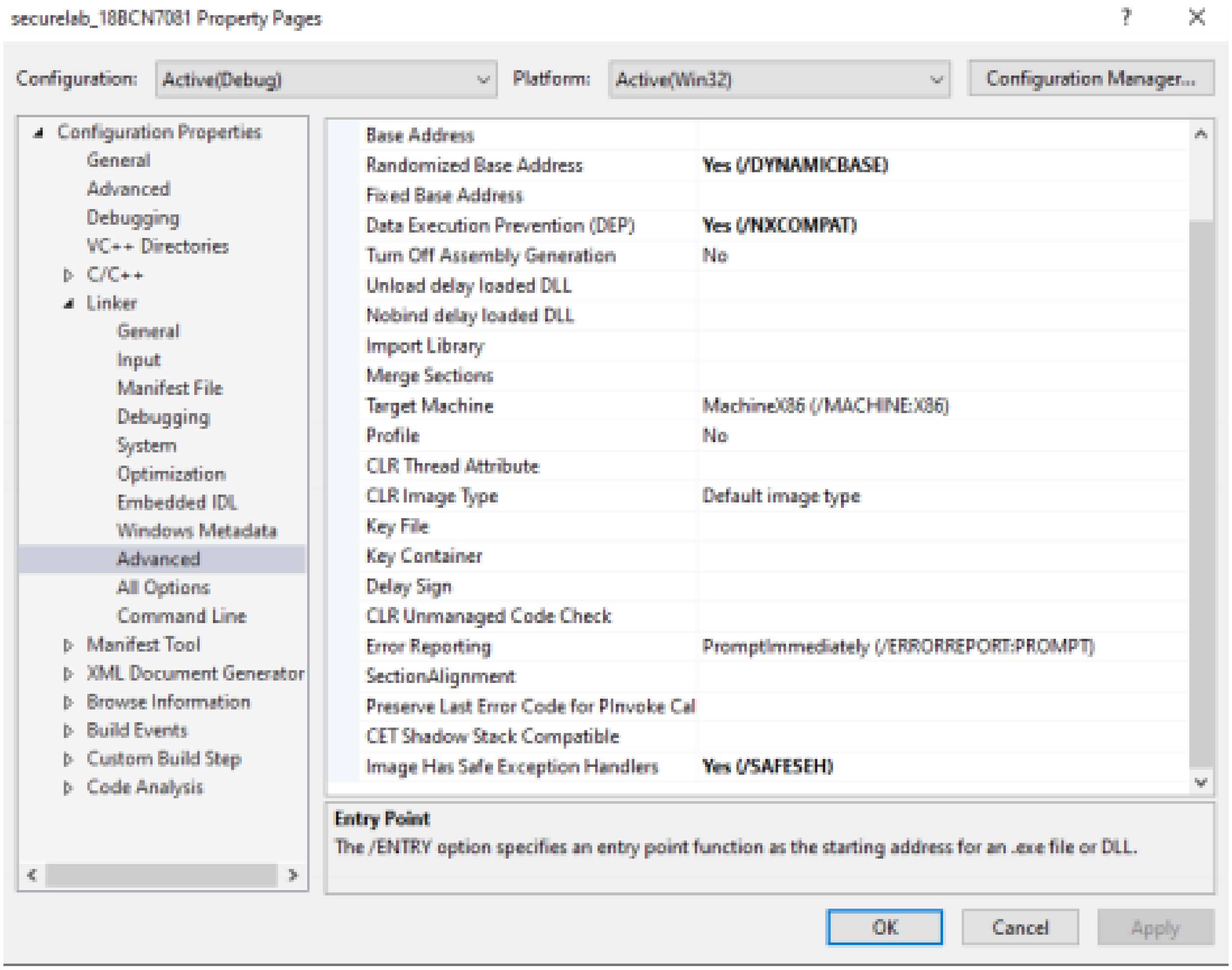
securelab_18BCN7081 Property Pages

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

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	
CLR Unmanaged Code Check	
Error Reporting	PromptImmediately (/ERRORREPORT:PROMPT)
SectionAlignment	
Preserve Last Error Code for PInvoke Cal	
CET Shadow Stack Compatible	
Image Has Safe Exception Handlers	Yes (/SAFESEH)

Entry Point

The /ENTRY option specifies an entry point function as the starting address for an .exe file or DLL.



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

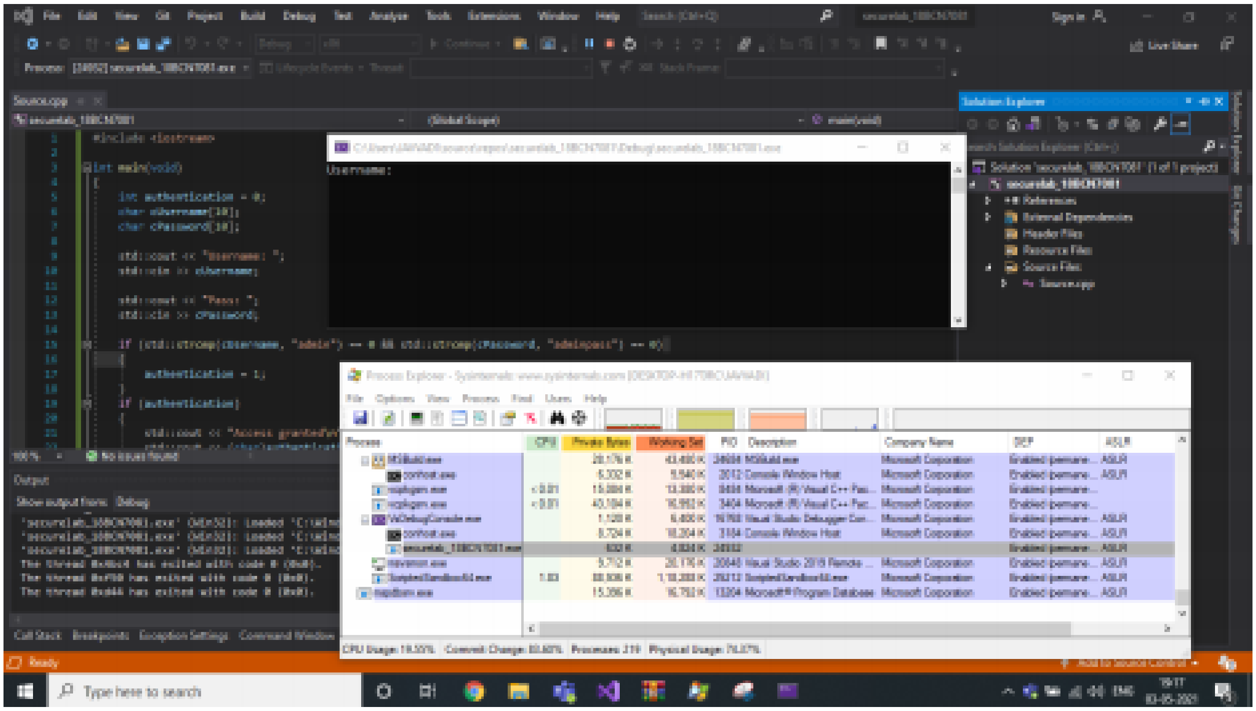
Base Address	
Randomized Base Address	**Yes (/DYNAMICBASE)**
Fixed Base Address	
Data Execution Prevention (DEP)	**Yes (/NXCOMPAT)**
Turn Off Assembly Generation	No
Unload delay loaded DLL	
Nobind delay loaded DLL	
Import Library	
Merge Sections	
Target Machine	MachineX86 (/MACHINE:X86)
Profile	No
CLR Thread Attribute	
CLR Image Type	Default image type
Key File	
Key Container	
Delay Sign	
CLR Unmanaged Code Check	
Error Reporting	PromptImmediately (/ERRORREPORT:PROMPT)
SectionAlignment	
Preserve Last Error Code for PInvoke Cal	
CET Shadow Stack Compatible	
Image Has Safe Exception Handlers	**Yes (/SAFESEH)**

Entry Point
The /ENTRY option specifies an entry point function as the starting address for an .exe file or DLL.

As you can see, I have enabled DEP, ASLR, SEH above.

I have Rebuilded my project and run the same and we can verify the status of DEP, ASLR, SEH.

4) Verifying the DEP & ASLR status in Process Explorer after enabling



```
#include <iostream>

int main(void)
{
    int authentication = 0;
    char cUsername[10];
    char cPassword[10];

    std::cout << "Username: ";
    std::cin >> cUsername;

    std::cout << "Pass: ";
    std::cin >> cPassword;

    if (std::strcmp(cUsername, "admin") == 0 && std::strcmp(cPassword, "adminpass") == 0)
    {
        authentication = 1;
    }
    if (authentication)
    {
        std::cout << "Access granted\n";
        std::cout << (char)authenticat
```

C:\Users\JAWADI\source\repos\securelab_18BCN7081\Debug\securelab_18BCN7081.exe

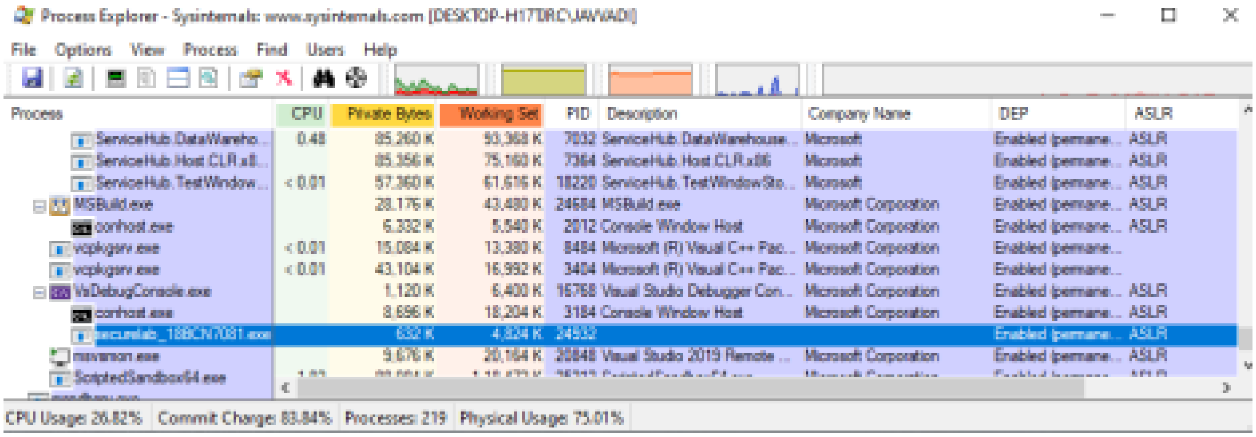
```
Username:
```

```
'securelab_18BCN7081.exe' (Win32): Loaded 'C:\Wind
'securelab_18BCN7081.exe' (Win32): Loaded 'C:\Wind
'securelab_18BCN7081.exe' (Win32): Loaded 'C:\Wind
The thread 0x0bc4 has exited with code 0 (0x0).
The thread 0xf08 has exited with code 0 (0x0).
The thread 0xd44 has exited with code 0 (0x0).
```

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-H17I0RC\JAWADI]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	DEP	ASLR
MSBuild.exe		28,176 K	43,480 K	24684	MSBuild.exe	Microsoft Corporation	Enabled (permane...	ASLR
conhost.exe		6,332 K	5,540 K	2012	Console Window Host	Microsoft Corporation	Enabled (permane...	ASLR
vcpkgsrv.exe	< 0.01	15,084 K	13,380 K	8484	Microsoft (R) Visual C++ Pac...	Microsoft Corporation	Enabled (permane...	
vcpkgsrv.exe	< 0.01	43,104 K	16,992 K	3404	Microsoft (R) Visual C++ Pac...	Microsoft Corporation	Enabled (permane...	
VsDebugConsole.exe		1,120 K	6,400 K	16768	Visual Studio Debugger Con...	Microsoft Corporation	Enabled (permane...	ASLR
conhost.exe		8,724 K	18,204 K	3184	Console Window Host	Microsoft Corporation	Enabled (permane...	ASLR
securelab_18BCN7081.exe		632 K	4,824 K	24932			Enabled (permane...	ASLR
msvsmon.exe		5,712 K	20,176 K	20848	Visual Studio 2019 Remote ...	Microsoft Corporation	Enabled (permane...	ASLR
ScriptedSandbox64.exe	1.03	88,936 K	1,18,200 K	28212	ScriptedSandbox64.exe	Microsoft Corporation	Enabled (permane...	ASLR
mspdbsrv.exe		15,396 K	16,752 K	13204	Microsoft® Program Database	Microsoft Corporation	Enabled (permane...	ASLR

CPU Usage: 19.33% Commit Charge: 83.80% Processes: 219 Physical Usage: 75.07%


Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-H17I0RC\JAWADI]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	DEP	ASLR
ServiceHub.DataWareho...	0.48	85,260 K	93,368 K	7032	ServiceHub.DataWarehouse...	Microsoft	Enabled (permane...	ASLR
ServiceHub.Host.CLR.x8...		85,356 K	75,160 K	7364	ServiceHub.Host.CLR.x86	Microsoft	Enabled (permane...	ASLR
ServiceHub.TestWindow...	< 0.01	57,360 K	61,616 K	18220	ServiceHub.TestWindowSto...	Microsoft	Enabled (permane...	ASLR
MSBuild.exe		28,176 K	43,480 K	24684	MSBuild.exe	Microsoft Corporation	Enabled (permane...	ASLR
conhost.exe		6,332 K	5,540 K	2012	Console Window Host	Microsoft Corporation	Enabled (permane...	ASLR
vcpkgsrv.exe	< 0.01	15,084 K	13,380 K	8484	Microsoft (R) Visual C++ Pac...	Microsoft Corporation	Enabled (permane...	
vcpkgsrv.exe	< 0.01	43,104 K	16,992 K	3404	Microsoft (R) Visual C++ Pac...	Microsoft Corporation	Enabled (permane...	
VsDebugConsole.exe		1,120 K	6,400 K	16768	Visual Studio Debugger Con...	Microsoft Corporation	Enabled (permane...	ASLR
conhost.exe		8,696 K	18,204 K	3184	Console Window Host	Microsoft Corporation	Enabled (permane...	ASLR
securelab_18BCN7081.exe		632 K	4,824 K	24932			Enabled (permane...	ASLR
msvsmon.exe		9,676 K	20,164 K	20848	Visual Studio 2019 Remote ...	Microsoft Corporation	Enabled (permane...	ASLR
ScriptedSandbox64.exe	1.03	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

CPU Usage: 26.82% Commit Charge: 83.84% Processes: 219 Physical Usage: 75.01%