

Lab-11

K.RAHUL
19BCE7310

Lab experiment – Creating secure and safe executable

1) C++ Code & building the Executable

```
#include <iostream>

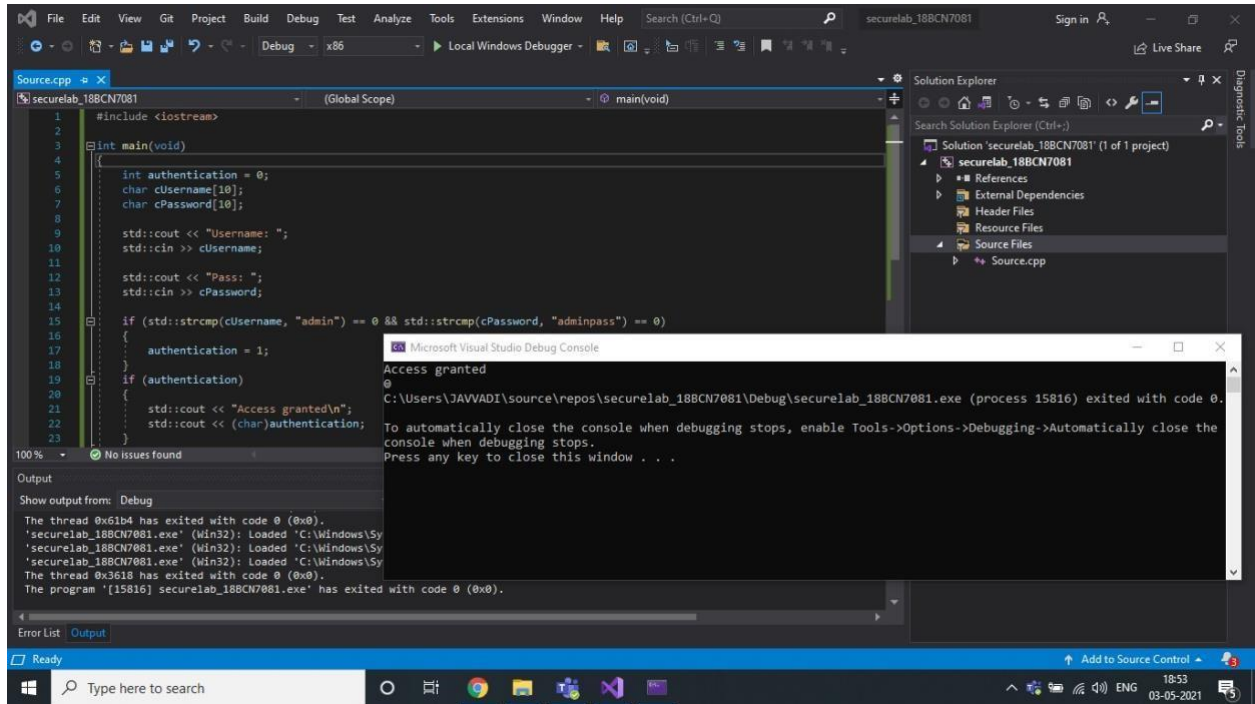
int main(void) { int
authentication = 0; char
cUsername[10]; char
cPassword[10];

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

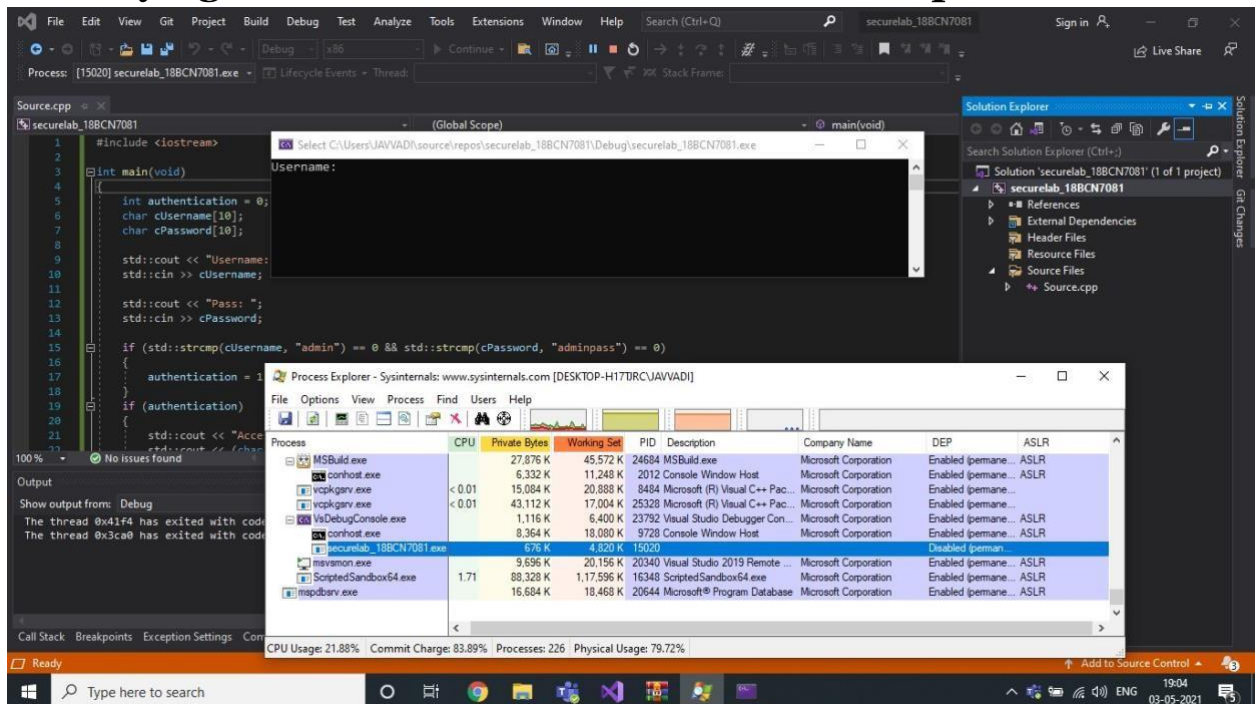
    std::cout << "Pass: "; std::cin
    >> cPassword;

    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); }
```



2) Verifying the DEP & ASLR status in Process Explorer



Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-H17DRCJAVVADJ]

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
vcpgkgrv.exe	< 0.01	15,084 K	20,888 K	8484	Microsoft (R) Visual C++ Pac...	Microsoft Corporation	Enabled (permane...	
vcpgkgrv.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...	
msvsmmon.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
mispdbsrv.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

Visual Studio 2019 - Securelab_18BCN7081

Source.cpp

```

1 #include <iostream>
2
3
4 int main(void)
5 {
6     int authentication = 0;
7     char cUsername[10];
8     char cPassword[10];
9
10    std::cout << "Username: ";
11    std::cin >> cUsername;
12
13    std::cout << "Pass: ";
14    std::cin >> cPassword;
15
16    if (std::strcmp(cUsername, "admin") == 0 && std::strcmp(cPassword, "1234") == 0)
17    {
18        authentication = 1;
19    }
20    if (authentication)
21    {
22        std::cout << "Access granted\n";
23        std::cout << (char)cPassword;
24    }
25 }

```

securelab_18BCN7081 Property Pages

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

Configuration Properties

- General
- Advanced
- Debugging
- VC++ Directories
- C/C++
- Linker
 - General
 - Input
 - Manifest File
 - Debugging
 - System
 - Optimization
 - Embedded IDL
 - Windows Metadata
 - Advanced
 - All Options
 - Command Line
- Manifest Tool
- XML Document Generator
- Browse Information
- Build Events
- Custom Build Step
- Code Analysis

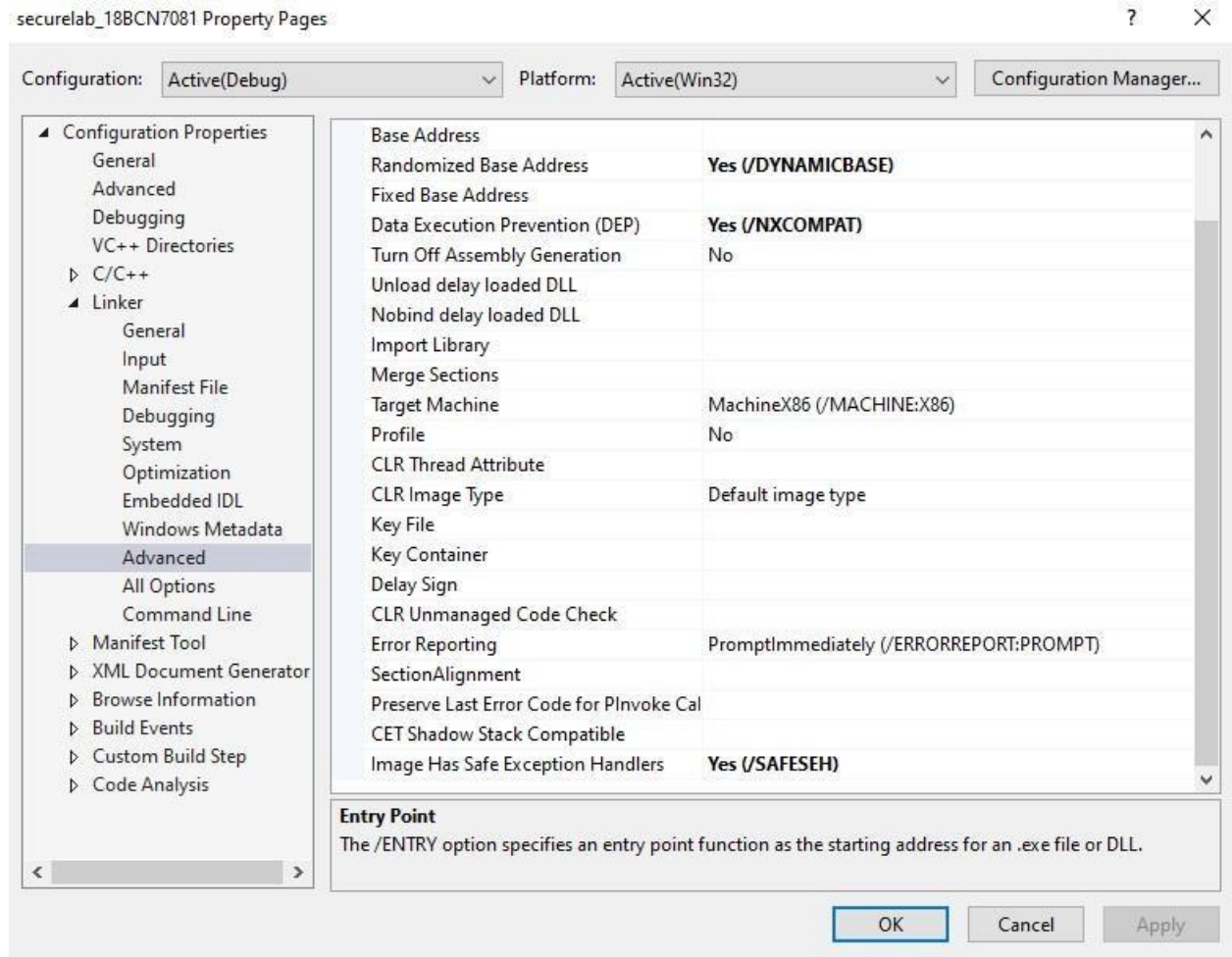
Base Address

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

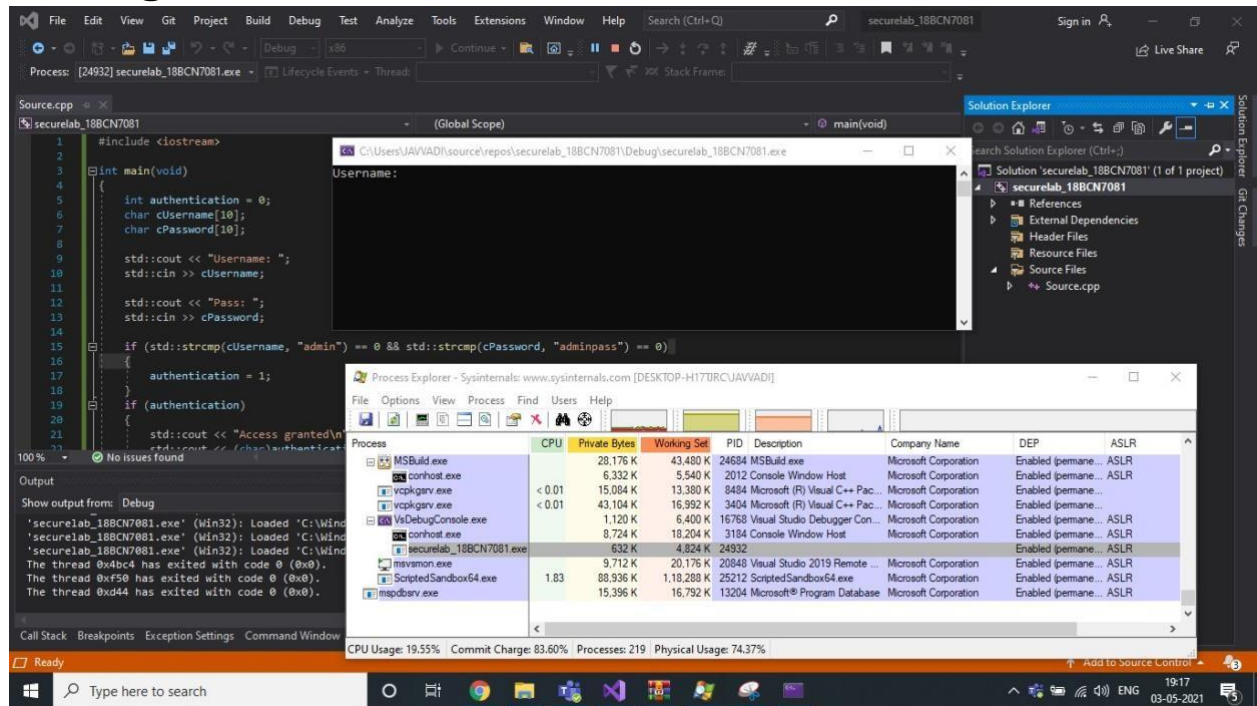
OK Cancel Apply



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

I have Rebuilt 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



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

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
vcpgkgrv.exe	< 0.01	15,084 K	13,380 K	8484	Microsoft (R) Visual C++ Pac...	Microsoft Corporation	Enabled (permane...	ASLR
vcpgkgrv.exe	< 0.01	43,104 K	16,992 K	3404	Microsoft (R) Visual C++ Pac...	Microsoft Corporation	Enabled (permane...	ASLR
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_188CN7081.exe		632 K	4,824 K	24932			Enabled (permane...	ASLR
msvsmom.exe		9,676 K	20,164 K	20848	Visual Studio 2019 Remote ...	Microsoft Corporation	Enabled (permane...	ASLR
ScriptedSandbox64.exe	1.83	88,936 K	1,18,288 K	25212	ScriptedSandbox64.exe	Microsoft Corporation	Enabled (permane...	ASLR

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