

Secure Coding Lab - 11

Name : Meghana V

Reg no : 18BCN7070

Task :

Download and install visual studio (recent edition)

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

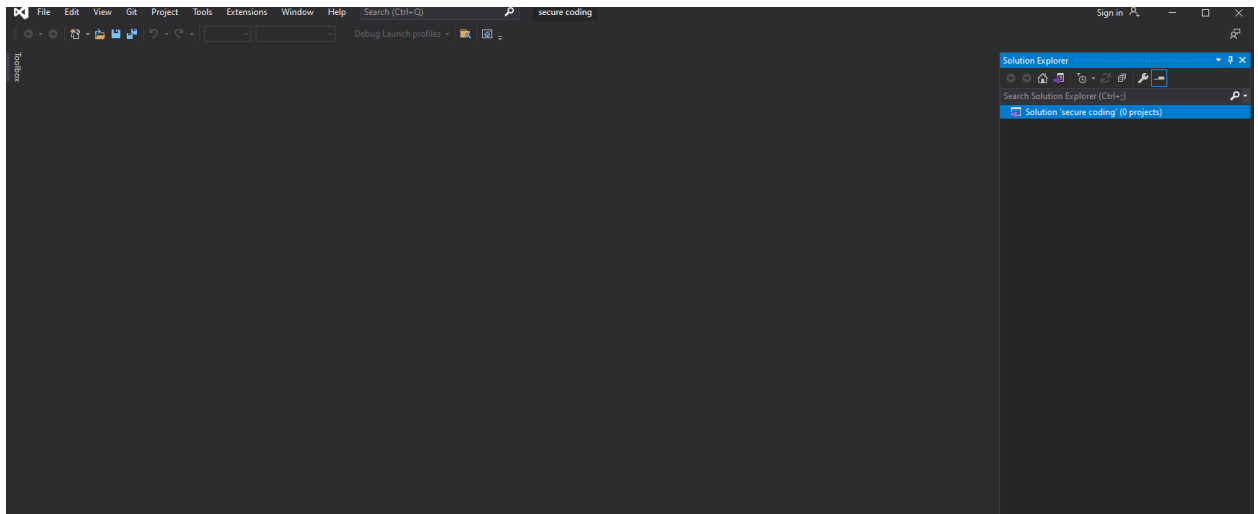
Download process explorer and verify the DEP & ASLR status

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

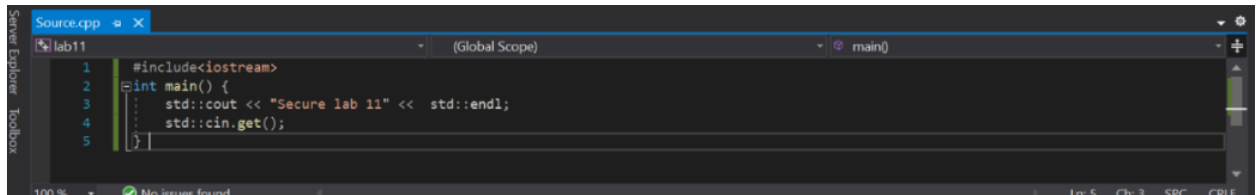
Again, verify the DEP & ASLR status in the process explorer

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

- 1) Install and run visual studio

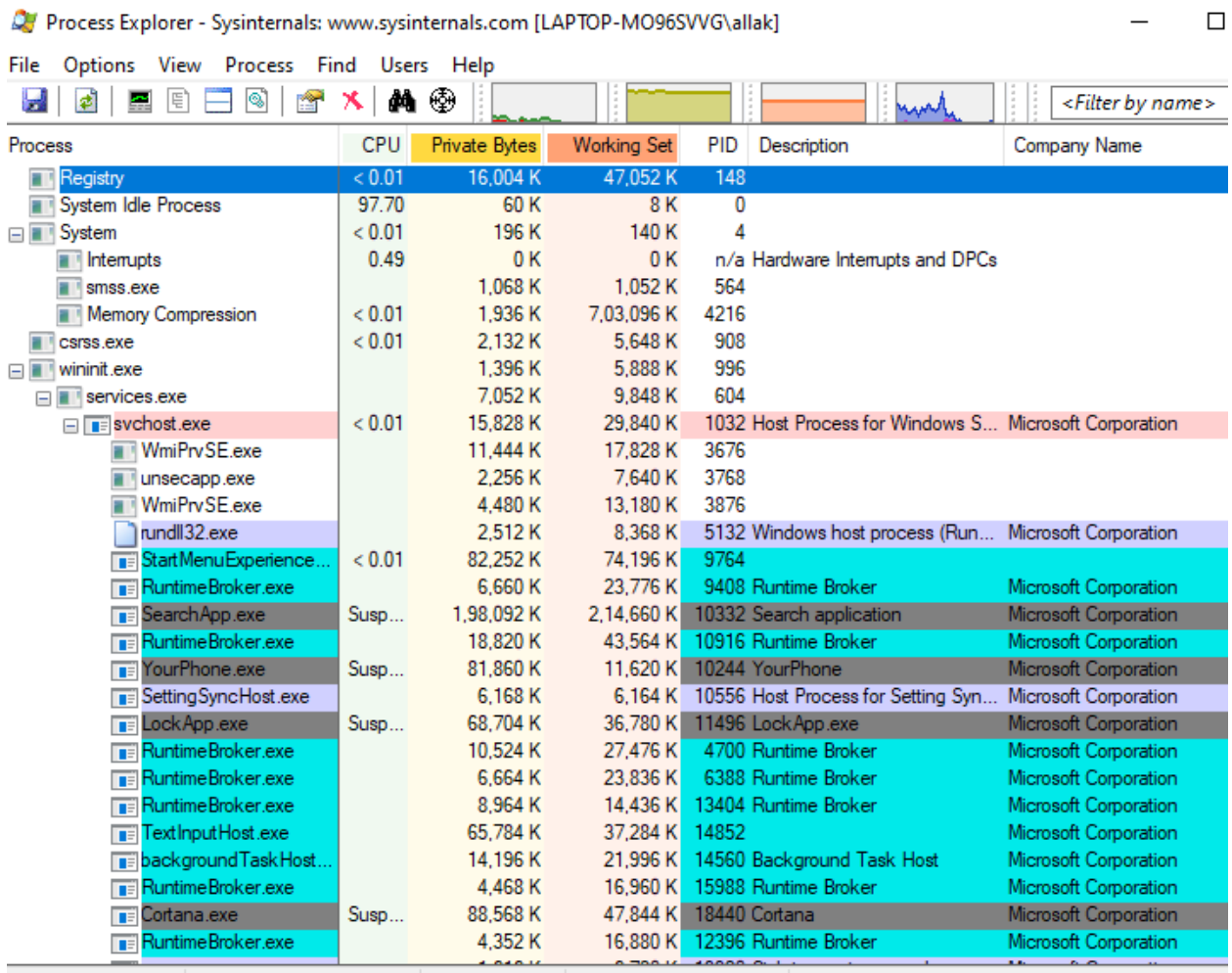


2) Write a simple C++ code in your VS



```
1 #include<iostream>
2 int main() {
3     std::cout << "Secure lab 11" << std::endl;
4     std::cin.get();
5 }
```

3) The execute will run perfectly now. View it on your process explorer



Process Explorer - Sysinternals: www.sysinternals.com [LAPTOP-MO96SVVG\allak]

File Options View Process Find Users Help

<Filter by name>

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry	< 0.01	16,004 K	47,052 K	148		
System Idle Process	97.70	60 K	8 K	0		
System	< 0.01	196 K	140 K	4		
Interrupts	0.49	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1,068 K	1,052 K	564		
Memory Compression	< 0.01	1,936 K	7,03,096 K	4216		
csrss.exe	< 0.01	2,132 K	5,648 K	908		
wininit.exe		1,396 K	5,888 K	996		
services.exe		7,052 K	9,848 K	604		
svchost.exe	< 0.01	15,828 K	29,840 K	1032	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe		11,444 K	17,828 K	3676		
unsecapp.exe		2,256 K	7,640 K	3768		
WmiPrvSE.exe		4,480 K	13,180 K	3876		
rundll32.exe		2,512 K	8,368 K	5132	Windows host process (Run...	Microsoft Corporation
StartMenuExperience...	< 0.01	82,252 K	74,196 K	9764		
RuntimeBroker.exe		6,660 K	23,776 K	9408	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	1,98,092 K	2,14,660 K	10332	Search application	Microsoft Corporation
RuntimeBroker.exe		18,820 K	43,564 K	10916	Runtime Broker	Microsoft Corporation
YourPhone.exe	Susp...	81,860 K	11,620 K	10244	YourPhone	Microsoft Corporation
SettingSyncHost.exe		6,168 K	6,164 K	10556	Host Process for Setting Syn...	Microsoft Corporation
LockApp.exe	Susp...	68,704 K	36,780 K	11496	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		10,524 K	27,476 K	4700	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		6,664 K	23,836 K	6388	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		8,964 K	14,436 K	13404	Runtime Broker	Microsoft Corporation
TextInputHost.exe		65,784 K	37,284 K	14852		Microsoft Corporation
backgroundTaskHost...		14,196 K	21,996 K	14560	Background Task Host	Microsoft Corporation
RuntimeBroker.exe		4,468 K	16,960 K	15988	Runtime Broker	Microsoft Corporation
Cortana.exe	Susp...	88,568 K	47,844 K	18440	Cortana	Microsoft Corporation
RuntimeBroker.exe		4,352 K	16,880 K	12396	Runtime Broker	Microsoft Corporation

4) After you disable DEP and ASLR and SEH

Manifest File	CLR Shadow Stack Compatibility	
Debugging	CLR Image Type	Default image type
System	CLR Thread Attribute	
Optimization	CLR Unmanaged Code Check	
Embedded IDL	Create Hot Patchable Image	
Windows Metadata	Data Execution Prevention (DEP)	No (/NXCOMPAT)
Advanced	Debuggable Assembly	
All Options	Delay Loaded DLLs	
Command Line	Delay Sign	

Manifest File	Ignore All Default Libraries	
Debugging	Ignore Embedded IDL	No
System	Ignore Import Library	No
Optimization	Ignore Specific Default Libraries	
Embedded IDL	Image Has Safe Exception Handlers	YES
Windows Metadata	Import Library	
Advanced	Incremental Link Database File	
All Options	Key Container	
Command Line	Key File	

Rebuild and application and run it again.

As intended, the build will fail.

5) Now ,after re-enabling the DEP and ASLR, if you build the file again, it works fine