

Lab11

Navya K
18bcn7048
L39+L40

TOPIC : Creating Secure And Safe Executable

- Downloaded visual studio and process explorer.
- Creating a new project.

Create a new project

Recent project templates

A list of your recently accessed templates will be displayed here.

Search for templates (Alt+S)

All languages

All platforms



ASP.NET Web Application (.NET Framework)
Project templates for creating ASP.NET applications, MVC, or Web API applications and add m

Visual Basic Windows C# Web



Empty Project
Start from scratch with C++ for Windows. Provid

C++ Windows Console



Console App
Run code in a Windows terminal. Prints "Hello W

C++ Windows Console



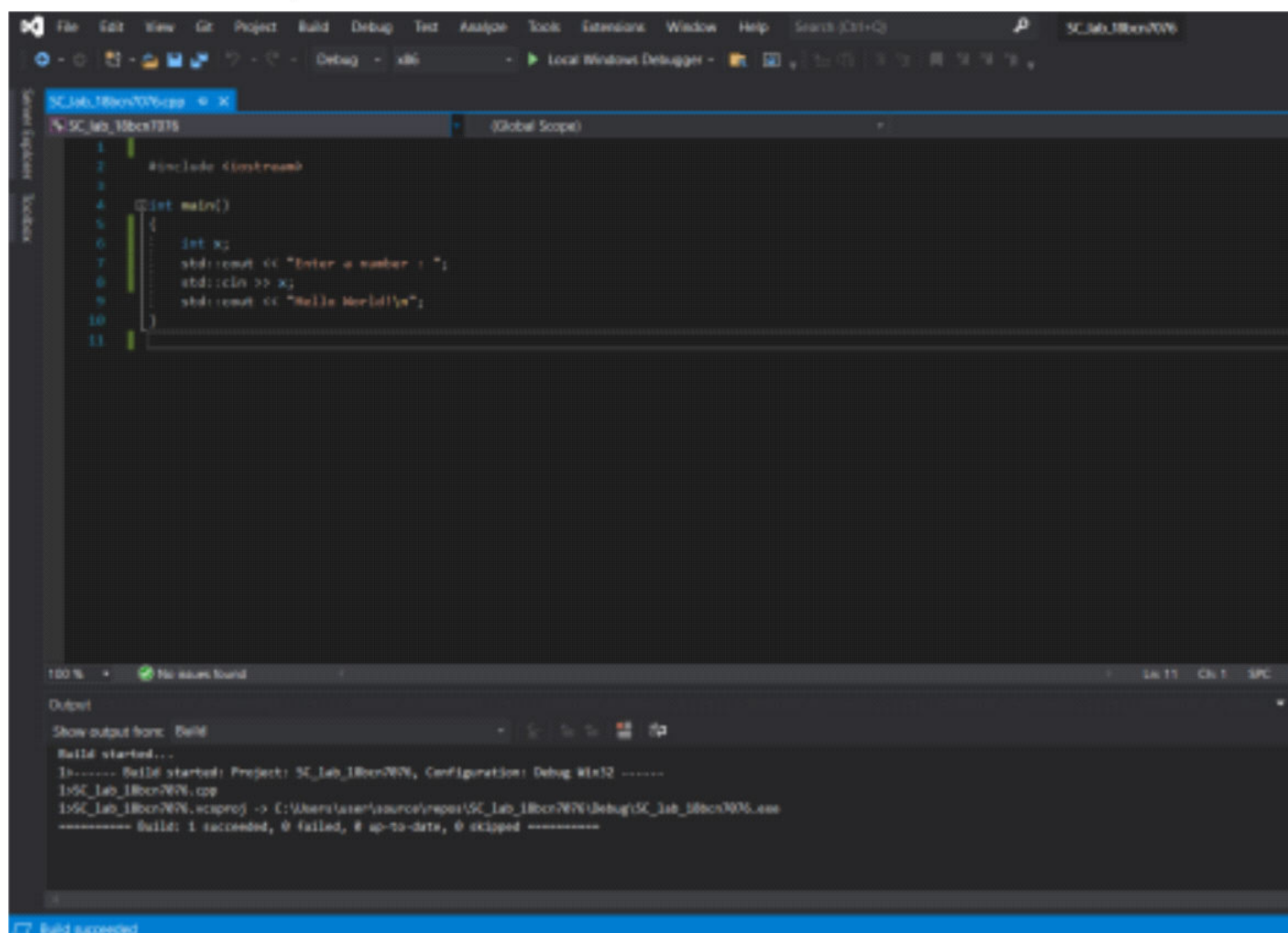
CMake Project
Build modern, cross-platform C++ apps that don

C++ Windows Linux Console



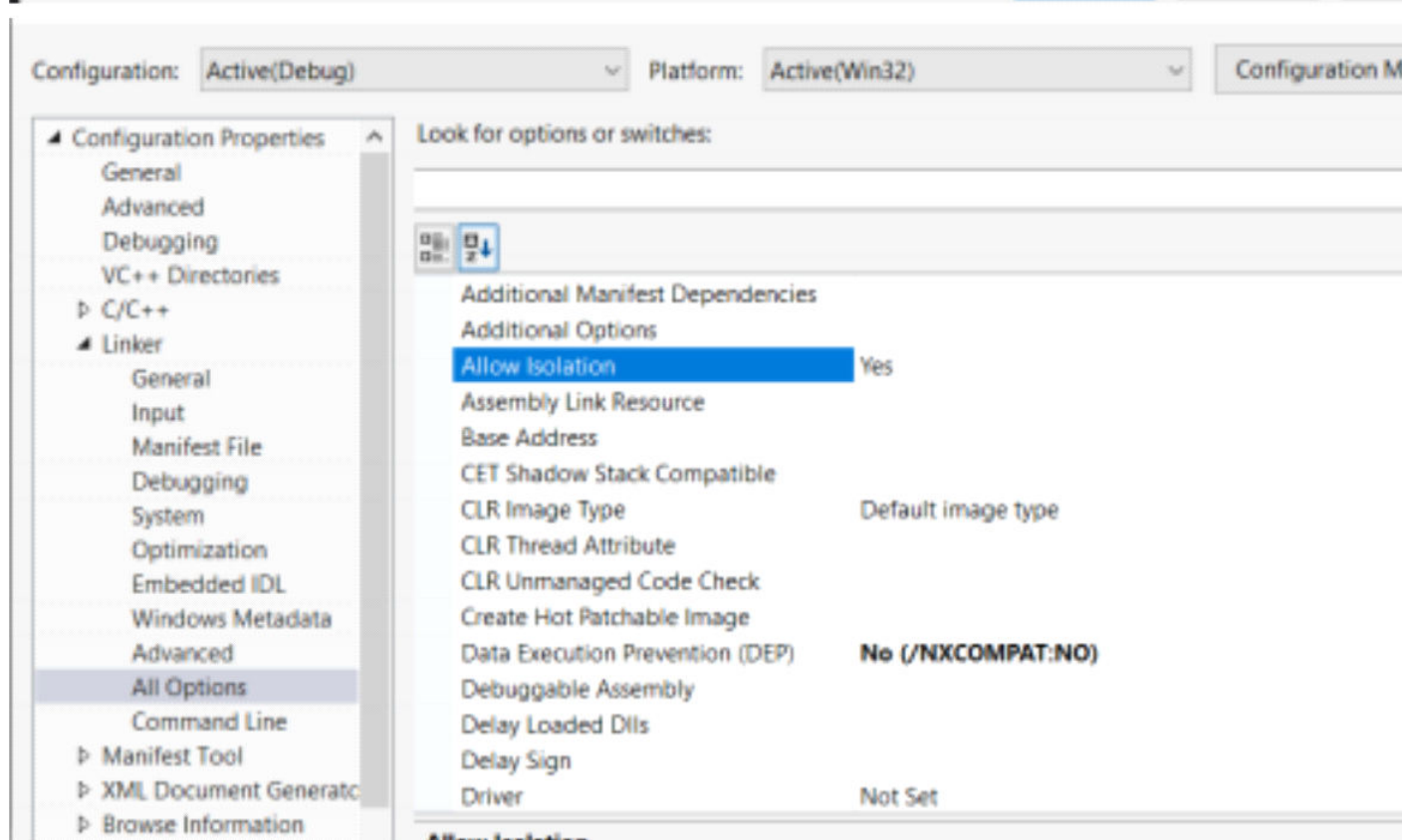
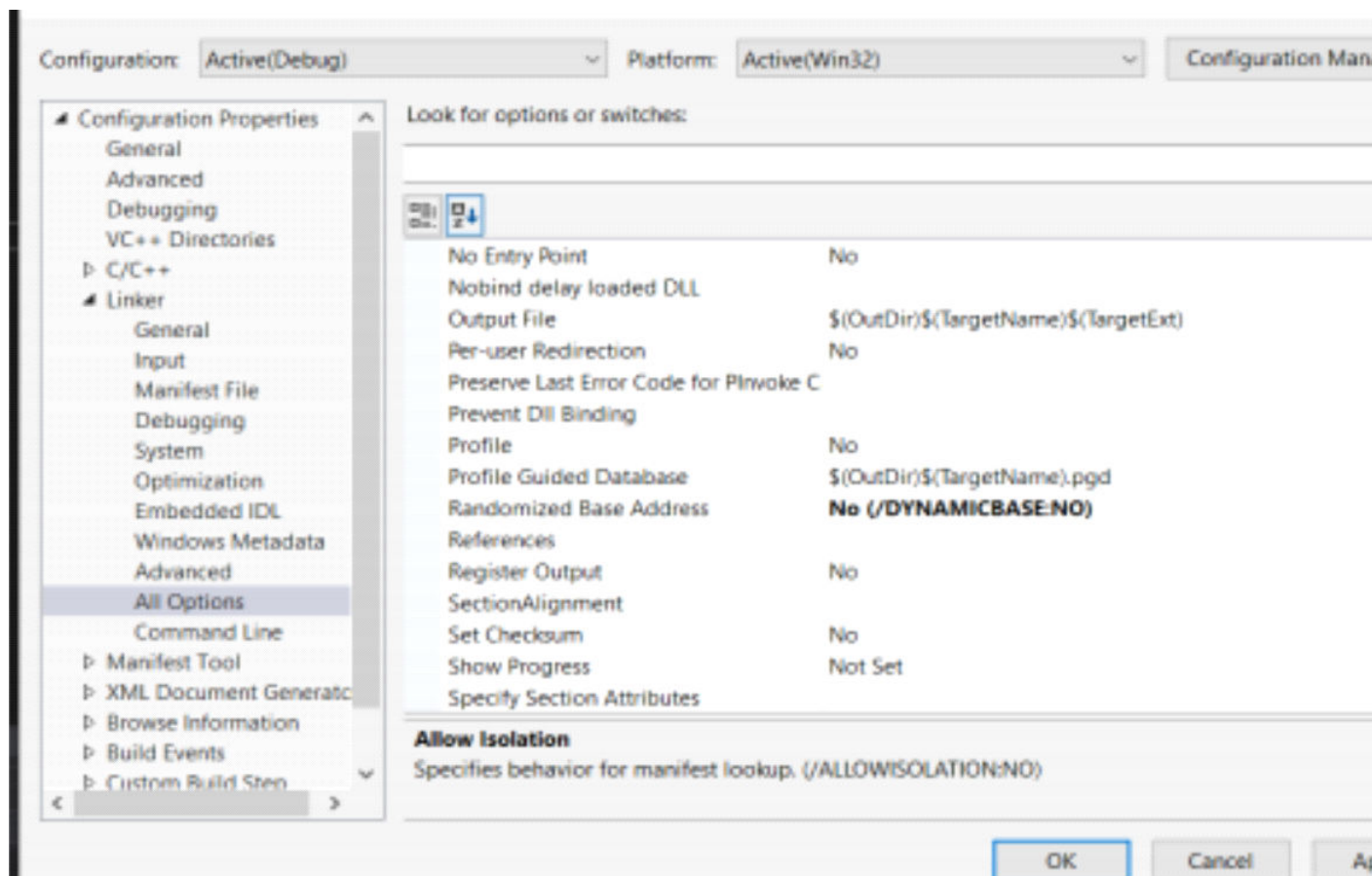
Windows Desktop Wizard
Create your own Windows app using a wizard.

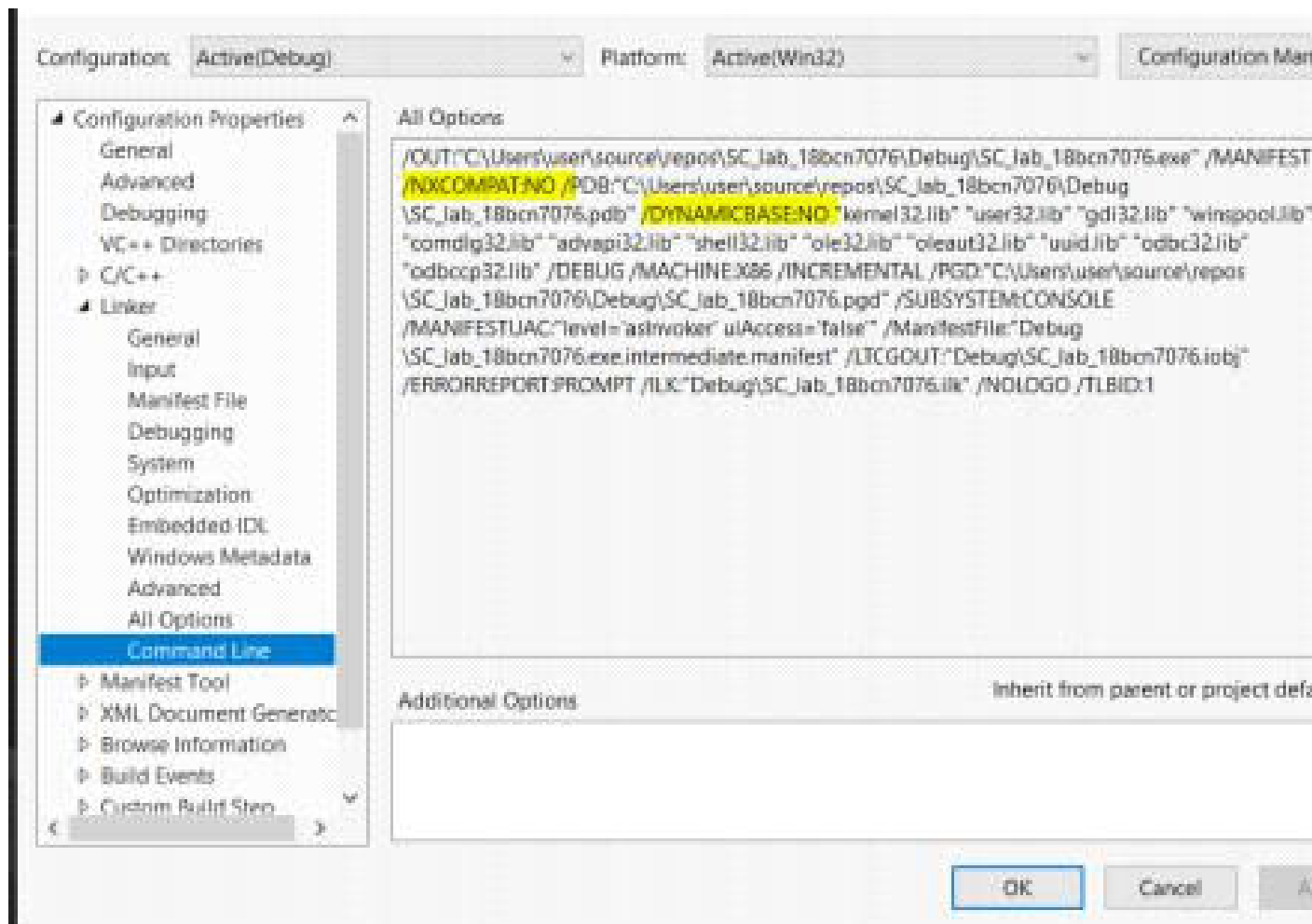
C++ Windows Desktop Console



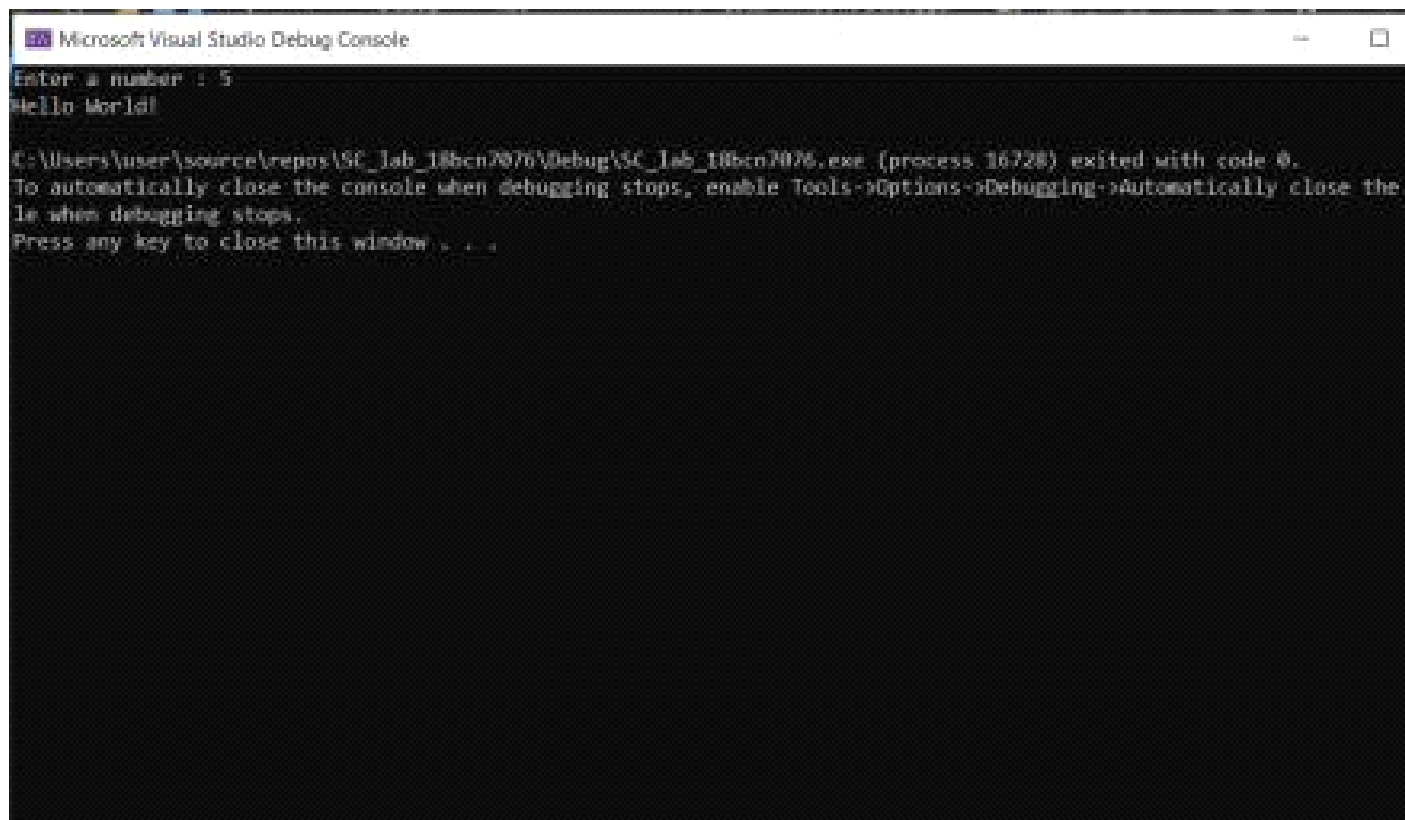
- Visiting the properties of the project and verifying the DEP, ASLR and SEH properties.

Changing the default option to **no** in command line to check them in process explorer





After executing the file .cpp

A screenshot of the Microsoft Visual Studio Debug Console window. The window has a title bar with the Visual Studio icon and the text "Microsoft Visual Studio Debug Console". The console output is as follows:

```
Enter a number : 5  
Hello World!  
  
C:\Users\user\source\repos\SC_lab_18bcn7076\Debug\SC_lab_18bcn7076.exe (process 16728) 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 . . .
```

Checking the DEP and ASLR status in process explorer

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-TSKJKRT\user]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Path
RuntimeBroker.exe	<0.0%	6,064 K	24,272 K	12884	Runtime Broker	Microsoft Corporation	C:\Windows\System32\RuntimeBroker.exe
RuntimeBroker.exe		1,824 K	7,224 K	8032	Runtime Broker	Microsoft Corporation	C:\Windows\System32\RuntimeBroker.exe
RuntimeBroker.exe		4,416 K	19,340 K	11896	Runtime Broker	Microsoft Corporation	C:\Windows\System32\RuntimeBroker.exe
RuntimeBroker.exe		13,020 K	31,820 K	15736	Runtime Broker	Microsoft Corporation	C:\Windows\System32\RuntimeBroker.exe
cmd.exe		2,000 K	9,764 K	2432	Windows command processor (cmd)	Microsoft Corporation	C:\Windows\System32\cmd.exe
RealtekHDAudio.sys		4,876 K	14,960 K	2580	Realtek HD Audio Manager	Realtek Semiconductor	C:\Program Files\Realtek\Audio\HDA\RealtekHDA.sys
process64.exe	1.40	37,460 K	57,272 K	17132	Sysinternals Process Explorer	Sysinternals - www.sysinternals.com	C:\Users\user\AppData\Local\Temp\process64.exe
Microsoft.ServiceHub.Controller.exe		44,540 K	56,368 K	13644	Microsoft ServiceHub Controller	Microsoft	C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\Common7\IDE\VC\VCExpress.exe
Microsoft.Photos.exe	Susp...	62,636 K	2,880 K	2676			C:\Program Files\WindowsApps\Microsoft.Windows.Photos_2020.10.20.0.0.0.0
LockApp.exe	Susp...	15,972 K	50,294 K	4036	LockApp.exe	Microsoft Corporation	C:\Windows\SystemApps\Microsoft.LockApp.LockApp.exe
igfxCI.exe		7,000 K	25,848 K	6520	igfxCI Module	Intel Corporation	C:\Windows\System32\DriverStore\FileRepository\igfx_ci_dll\igfxCI.exe
Hotfix.exe	<0.0%	9,796 K	33,280 K	10194	Microsoft Outlook Connectors	Microsoft Corporation	C:\Program Files\WindowsApps\Microsoft.Outlook.Connectors_100
Hotfix.exe	Susp...	23,628 K	3,184 K	13244	Microsoft Outlook	Microsoft Corporation	C:\Program Files\WindowsApps\Microsoft.Outlook_100
Hotfix.exe	<0.0%	18,440 K	32,176 K	13880	Microsoft Outlook Accounts	Microsoft Corporation	C:\Program Files\WindowsApps\Microsoft.Outlook.Accounts_100
explorer.exe	0.19	86,664 K	1,40,364 K	12188	Windows Explorer	Microsoft Corporation	C:\Windows\explorer.exe
cdm.exe		4,296 K	13,284 K	11788	CDM Surrogate	Microsoft Corporation	C:\Windows\System32\cdm.exe
cdm.exe		3,348 K	15,912 K	7676	CDM Surrogate	Microsoft Corporation	C:\Windows\System32\cdm.exe
cdm.exe	<0.0%	42,504 K	44,156 K	9252			[Access is denied]
Console.exe	Susp...	30,962 K	37,888 K	9208	Console	Microsoft Corporation	C:\Program Files\WindowsApps\Microsoft.Windows.Common-UI_100
conhost.exe		6,528 K	11,536 K	2240	Console Window Host	Microsoft Corporation	C:\Windows\System32\conhost.exe
conhost.exe		7,136 K	17,832 K	6672	Console Window Host	Microsoft Corporation	C:\Windows\System32\conhost.exe
CompPack.exe		1,760 K	9,912 K	12312	Component Package Support	Microsoft Corporation	C:\Windows\System32\CompPack.exe
chrome.exe	0.19	1,82,292 K	1,64,164 K	10880	Google Chrome	Google LLC	C:\Program Files\Google\Chrome\Application\chrome.exe
chrome.exe		2,400 K	7,820 K	15840	Google Chrome	Google LLC	C:\Program Files\Google\Chrome\Application\chrome.exe
chrome.exe		7,65,064 K	7,28,556 K	7760	Google Chrome	Google LLC	C:\Program Files\Google\Chrome\Application\chrome.exe
chrome.exe	<0.0%	23,304 K	41,212 K	12836	Google Chrome	Google LLC	C:\Program Files\Google\Chrome\Application\chrome.exe
chrome.exe		13,072 K	17,552 K	5704	Google Chrome	Google LLC	C:\Program Files\Google\Chrome\Application\chrome.exe
chrome.exe		46,124 K	66,248 K	11940	Google Chrome	Google LLC	C:\Program Files\Google\Chrome\Application\chrome.exe
chrome.exe		1,88,388 K	2,12,688 K	7688	Google Chrome	Google LLC	C:\Program Files\Google\Chrome\Application\chrome.exe
chrome.exe	<0.0%	38,236 K	68,888 K	3182	Google Chrome	Google LLC	C:\Program Files\Google\Chrome\Application\chrome.exe
chrome.exe		36,024 K	65,856 K	16186	Google Chrome	Google LLC	C:\Program Files\Google\Chrome\Application\chrome.exe
chrome.exe		16,324 K	19,880 K	13880	Google Chrome	Google LLC	C:\Program Files\Google\Chrome\Application\chrome.exe
chrome.exe	<0.0%	2,84,572 K	2,26,592 K	15124	Google Chrome	Google LLC	C:\Program Files\Google\Chrome\Application\chrome.exe
chrome.exe		43,440 K	65,888 K	16396	Google Chrome	Google LLC	C:\Program Files\Google\Chrome\Application\chrome.exe
chrome.exe		15,904 K	23,672 K	1280	Google Chrome	Google LLC	C:\Program Files\Google\Chrome\Application\chrome.exe
Calculator.exe	Susp...	24,308 K	2,324 K	12888			C:\Program Files\WindowsApps\Microsoft.Windows.Calculator_100
AvastUI.exe	0.37	36,628 K	58,824 K	2216	Avast! Antivirus	Avast Software	C:\Program Files\Avast Software\Avast\AvastUI.exe
AvastUI.exe		15,528 K	40,852 K	3334	Avast! Antivirus	Avast Software	C:\Program Files\Avast Software\Avast\AvastUI.exe
AvastUI.exe		12,172 K	32,588 K	876	Avast! Antivirus	Avast Software	C:\Program Files\Avast Software\Avast\AvastUI.exe
AvastUI.exe		16,356 K	42,396 K	12880	Avast! Antivirus	Avast Software	C:\Program Files\Avast Software\Avast\AvastUI.exe
audiodg.exe		9,616 K	19,856 K	12630			[Access is denied]
ApplicationFrameHost.exe		23,752 K	39,196 K	12384	Application Frame Host	Microsoft Corporation	C:\Windows\System32\ApplicationFrameHost.exe
cmd.exe		772 K	4,924 K	884			C:\Windows\System32\cmd.exe

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-TSKJKRT\user]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Des...	Company Name	Path
wsc_proxy.exe		4,544 K	5,900 K	3088	Avast ...	AVAST Software	C:\Program
ScriptedSandbox64.exe		27,432 K	32,280 K	20176	Script...	Microsoft Corporation	C:\Program
SC_jab_15bca7076.exe		992 K	4,988 K	864			C:\Users\us

Again enabling the DEP and ASLR status and also the SEH