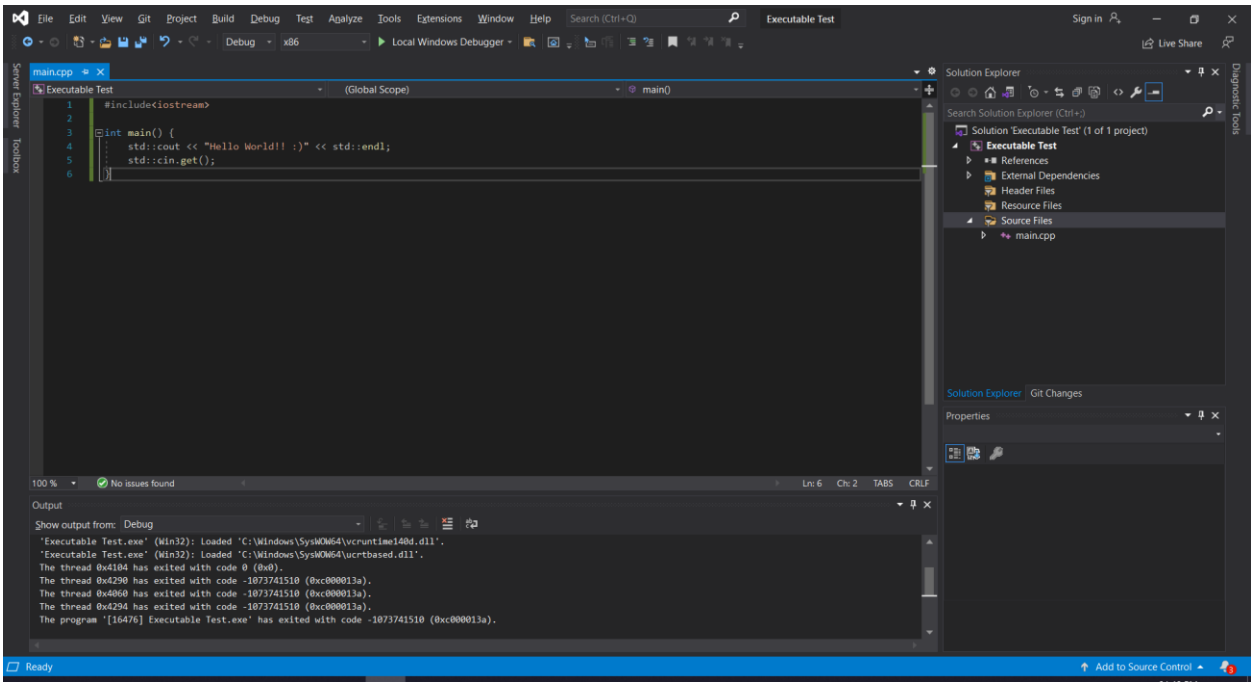
Secure Coding Lab – 11

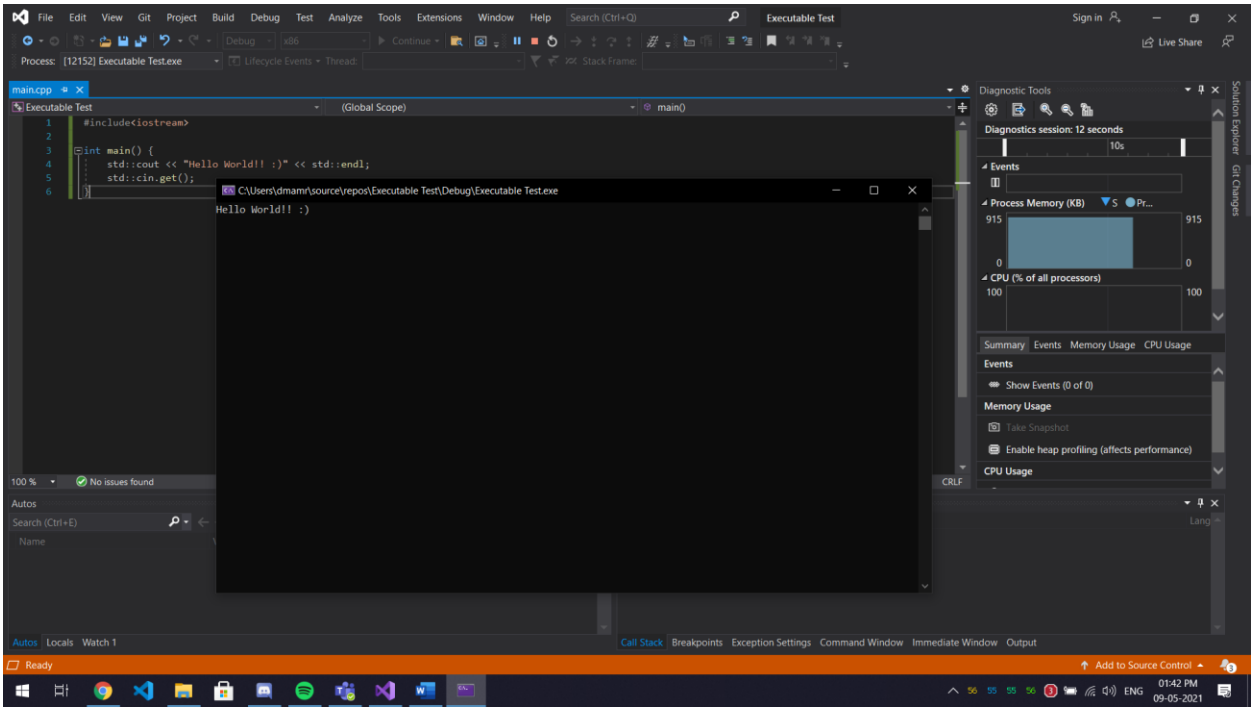
Dasari Mohan Amritesh

18BCN7038

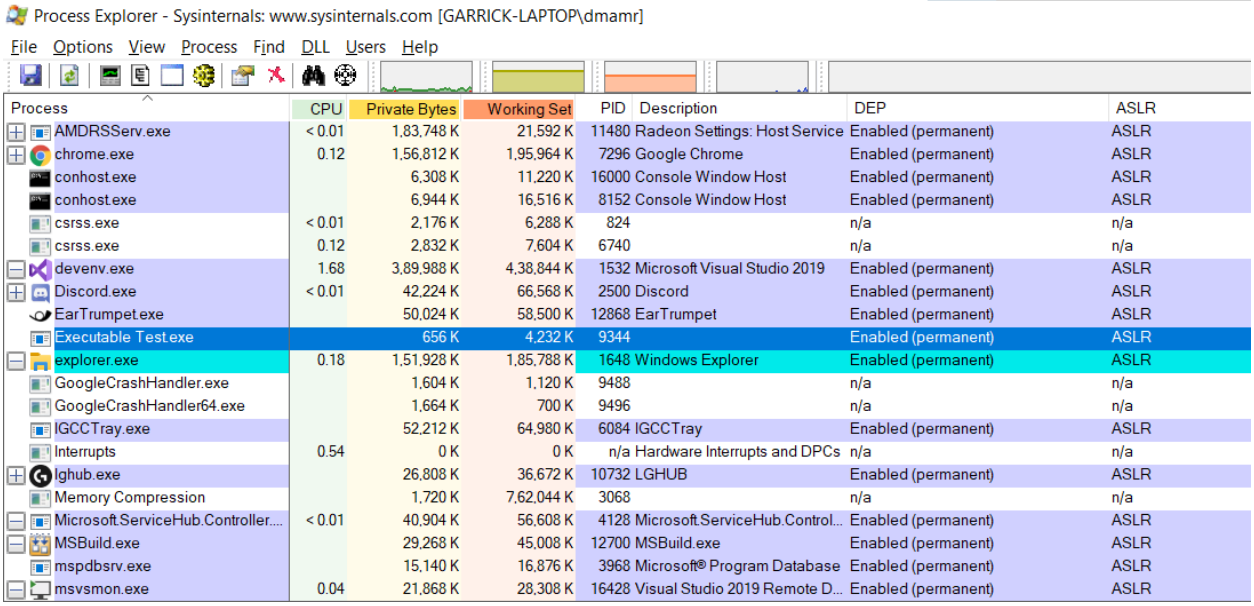
Download and install visual studio (recent edition)

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





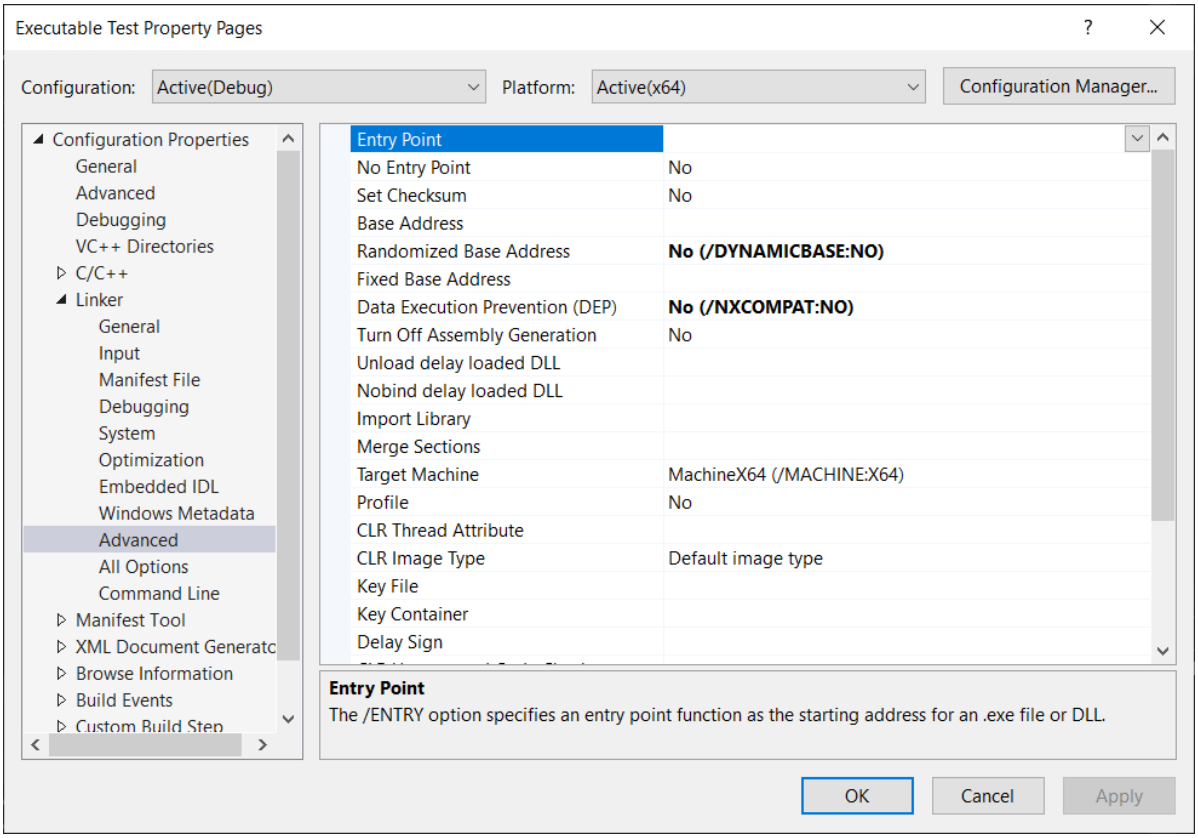
Download process explorer and verify the DEP & ASLR status

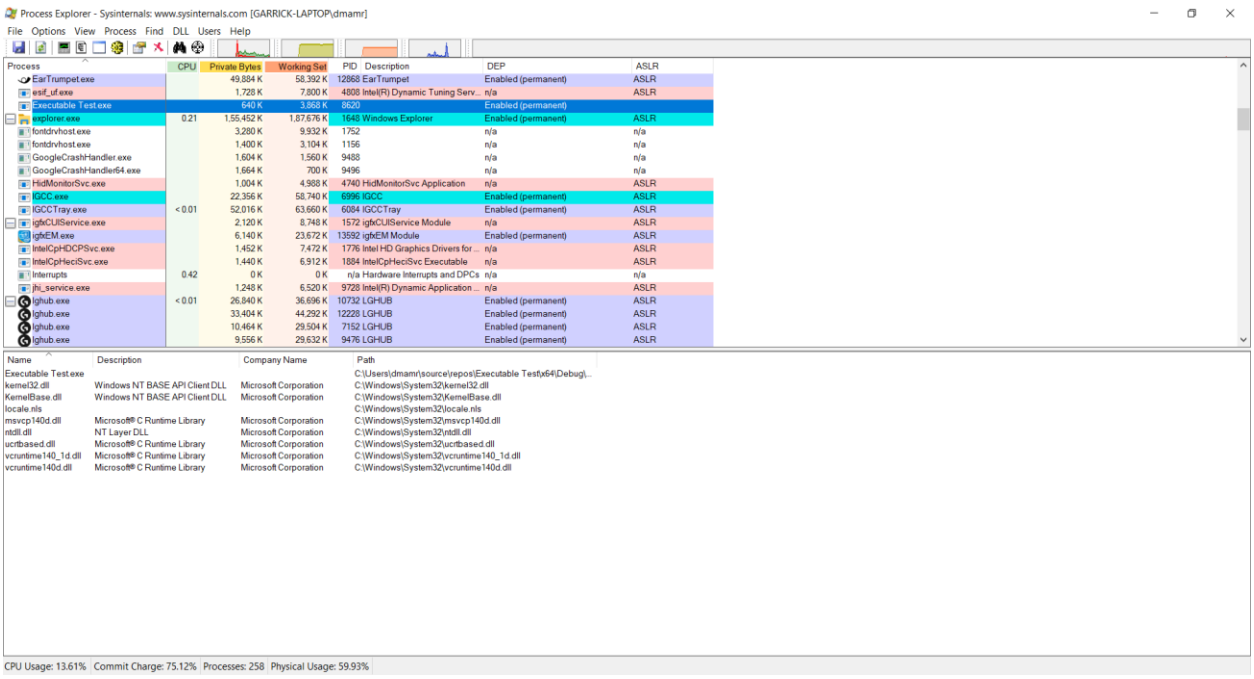


Process	CPU	Private Bytes	Working Set	PID	Description	DEP	ASLR
AMDRSServ.exe	< 0.01	1,83,748 K	21,592 K	11480	Radeon Settings: Host Service	Enabled (permanent)	ASLR
chrome.exe	0.12	1,56,812 K	1,95,964 K	7296	Google Chrome	Enabled (permanent)	ASLR
conhost.exe		6,308 K	11,220 K	16000	Console Window Host	Enabled (permanent)	ASLR
conhost.exe		6,944 K	16,516 K	8152	Console Window Host	Enabled (permanent)	ASLR
csrss.exe	< 0.01	2,176 K	6,288 K	824		n/a	n/a
csrss.exe	0.12	2,832 K	7,604 K	6740		n/a	n/a
devenv.exe	1.68	3,89,988 K	4,38,844 K	1532	Microsoft Visual Studio 2019	Enabled (permanent)	ASLR
Discord.exe	< 0.01	42,224 K	66,568 K	2500	Discord	Enabled (permanent)	ASLR
EarTrumpet.exe		50,024 K	58,500 K	12868	EarTrumpet	Enabled (permanent)	ASLR
Executable Test.exe		656 K	4,232 K	9344		Enabled (permanent)	ASLR
explorer.exe	0.18	1,51,928 K	1,85,788 K	1648	Windows Explorer	Enabled (permanent)	ASLR
GoogleCrashHandler.exe		1,604 K	1,120 K	9488		n/a	n/a
GoogleCrashHandler64.exe		1,664 K	700 K	9496		n/a	n/a
IGCCTray.exe		52,212 K	64,980 K	6084	IGCCTray	Enabled (permanent)	ASLR
Interrupts	0.54	0 K	0 K	n/a	Hardware Interrupts and DPCs	n/a	n/a
lghub.exe		26,808 K	36,672 K	10732	LGHUB	Enabled (permanent)	ASLR
Memory Compression		1,720 K	7,62,044 K	3068		n/a	n/a
Microsoft.ServiceHub.Controller....	< 0.01	40,904 K	56,608 K	4128	Microsoft.ServiceHub.Control...	Enabled (permanent)	ASLR
MSBuild.exe		29,268 K	45,008 K	12700	MSBuild.exe	Enabled (permanent)	ASLR
mspdbsrv.exe		15,140 K	16,876 K	3968	Microsoft® Program Database	Enabled (permanent)	ASLR
msvsmon.exe	0.04	21,868 K	28,308 K	16428	Visual Studio 2019 Remote D...	Enabled (permanent)	ASLR

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

Project > properties > configuration properties > linker





By Default, in project properties, DEP and ASLR properties are enabled and even upon disabling them, DEP is still in affect