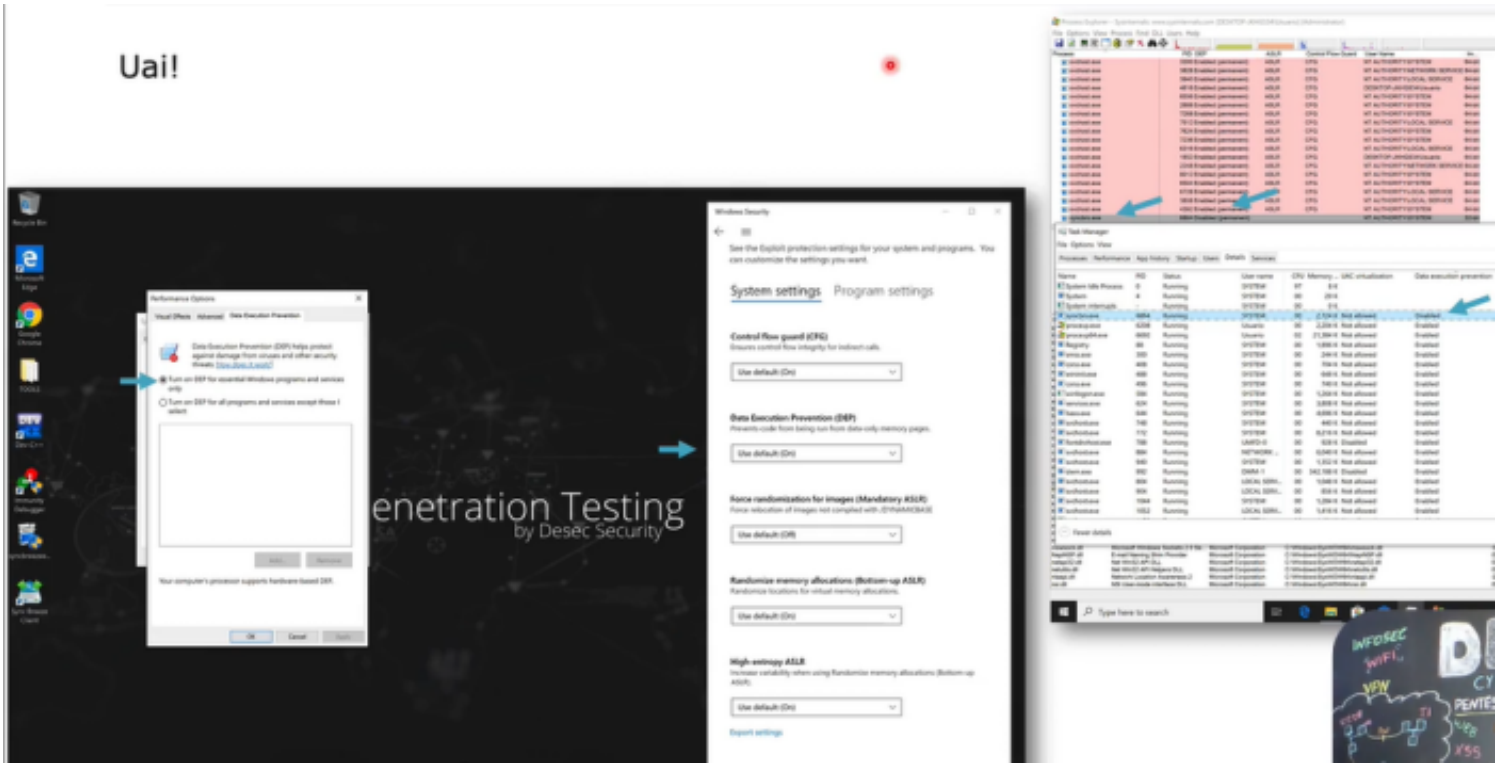
Mecanismos de Proteção: DEP e ASLR

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

DEP - Data Execution Prevention

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Também conhecido como non-execute (NX) tem como objetivo prevenir a execução de códigos em memória



→ O DEP vem habilitado por padrão da Microsoft, mas apenas para programas locais (próprios), para que haja uma maior compatibilidade de Softwares. Então uma boa prática de segurança é habilitar o DEP para todos e em seguida sair selecionando os softwares que não são compatíveis com o DEP para desabilitá-lo somente neles

→ Se o software compila com essa opção acima, então o Windows entender que ele é de fato compatível com o DEP e pode "ligar" o DEP para executá-lo

REFERÊNCIAS E DOCUMENTAÇÕES DA PRÓPRIA MICROSOFT:

https://docs.microsoft.com/pt-br/windows/security/threat-protection/overviewer-of-threat-mitigations-in-windows-10

https://docs.microsoft.com/pt-br/previous-versions/windows/embedded/ms913190(v=sinembedded.5

https://docs.microsoft.com/pt-br/windows/win32/Memory/data-execution-prevention

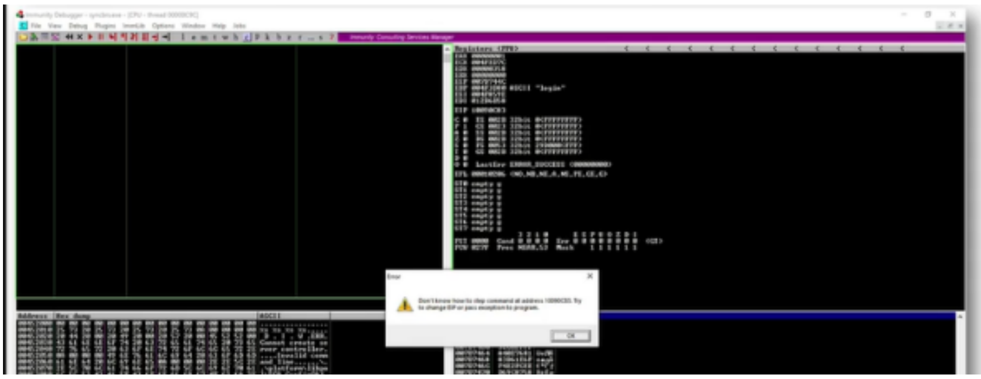
https://docs.microsoft.com/pt-br/cpp/build/reference/nxcompat-compatible-with-data-execution-prevention?view=vs-2019

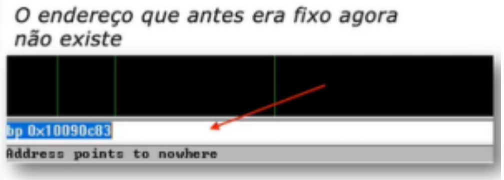
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

ASLR - Address Space Layout Randomization
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

~~~~~~

A ideia por trás do ASLR é tornar os endereços de memória aleatórios dificultando que o atacante consiga um endereço fixo durante a exploração





Sem ASLR

Base	Size	Entry	Name	File version	Path
00400000	00062000	00430484	syncbrs		C:\Program Files (x86)\Sync Breeze Enterprise\bin\syncbrs.exe
00840000	000D4000	008C6417	libpal		C:\Program Files (x86)\Sync Breeze Enterprise\bin\libpal.dll
00A20000	000B4000	00A8D99D	libsync		C:\Program Files (x86)\Sync Breeze Enterprise\bin\libsync.dll
→ 10000000	00223000	10157417	libspp		C:\Program Files (x86)\Sync Breeze Enterprise\bin\libspp.dll

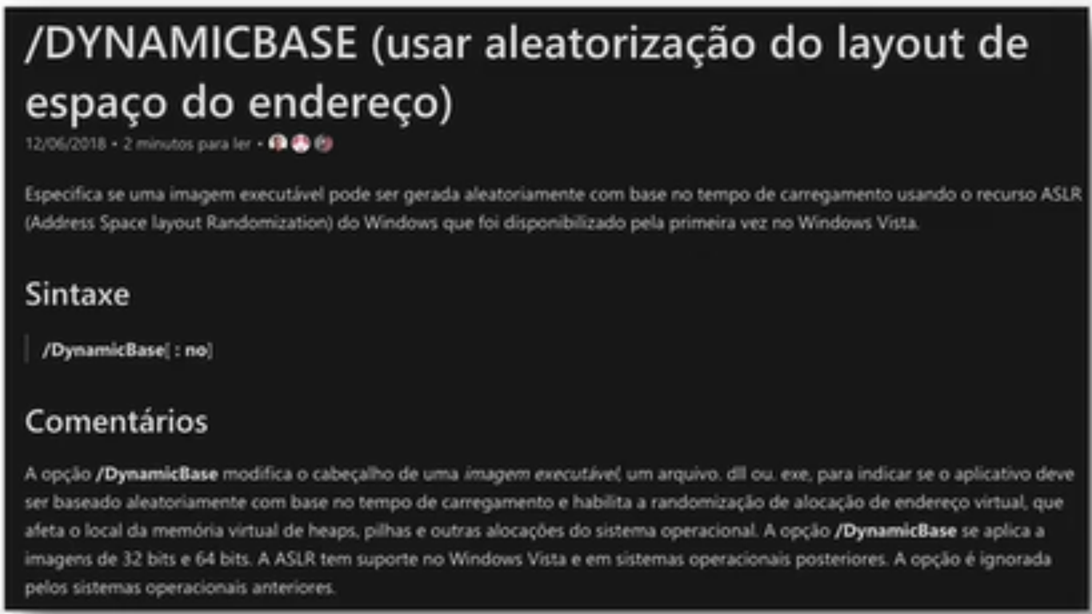
Base	Size	Entry	Name	File version	Path
00400000	00062000	00430484	syncbrs		C:\Program Files (x86)\Sync Breeze Enterprise\bin\syncbrs.exe
00840000	000D4000	008C6417	libpal		C:\Program Files (x86)\Sync Breeze Enterprise\bin\libpal.dll
00A20000	000B4000	00A8D99D	libsync		C:\Program Files (x86)\Sync Breeze Enterprise\bin\libsync.dll
→ 10000000	00223000	10157417	libspp		C:\Program Files (x86)\Sync Breeze Enterprise\bin\libspp.dll

Com ASLR

Base	Size	Entry	Name	File version	Path
00400000	00062000	00430484	syncbrs		C:\Program Files (x86)\Sync Breeze Enterprise\bin\syncbrs.exe
→ 007E0000	00223000	00937417	libspp		C:\Program Files (x86)\Sync Breeze Enterprise\bin\libspp.dll
00A10000	000D4000	00A96417	libpal		C:\Program Files (x86)\Sync Breeze Enterprise\bin\libpal.dll
00BF0000	000B4000	00C5D99D	libsync		C:\Program Files (x86)\Sync Breeze Enterprise\bin\libsync.dll

Base	Size	Entry	Name	File version	Path
00400000	00062000	00430484	syncbrs		C:\Program Files (x86)\Sync Breeze Enterprise\bin\syncbrs.exe
→ 00840000	00223000	00997417	libspp		C:\Program Files (x86)\Sync Breeze Enterprise\bin\libspp.dll
00B70000	000D4000	00BF6417	libpal		C:\Program Files (x86)\Sync Breeze Enterprise\bin\libpal.dll
00C50000	000B4000	00CBD99D	libsync		C:\Program Files (x86)\Sync Breeze Enterprise\bin\libsync.dll

→ Semelhantemente ao DEP, o ASLR também não força os executáveis a carregarem com esse protocolo, por questões de compatibilidade, mas ele já vem ativo no windows por default



/DYNAMICBASE (usar aleatorização do layout de espaço do endereço)

12/06/2018 • 2 minutos para ler •

Especifica se uma imagem executável pode ser gerada aleatoriamente com base no tempo de carregamento usando o recurso ASLR (Address Space layout Randomization) do Windows que foi disponibilizado pela primeira vez no Windows Vista.

Sintaxe

> /DynamicBase[: no]

Comentários

A opção **/DynamicBase** modifica o cabeçalho de uma *imagem executável*, um arquivo. dll ou. exe, para indicar se o aplicativo deve ser baseado aleatoriamente com base no tempo de carregamento e habilita a randomização de alocação de endereço virtual, que afeta o local da memória virtual de heaps, pilhas e outras alocações do sistema operacional. A opção **/DynamicBase** se aplica a imagens de 32 bits e 64 bits. A ASLR tem suporte no Windows Vista e em sistemas operacionais posteriores. A opção é ignorada pelos sistemas operacionais anteriores.
~~~~~~

	Process EXE opts-in to ASLR			Process EXE *does not* opt-in to ASLR		
	Default behavior	Mandatory ASLR	Mandatory ASLR + bottom-up ASLR	Default behavior	Mandatory ASLR	Mandatory ASLR + bottom-up ASLR
ASLR image	Randomized	Randomized	Randomized	Randomized	Randomized	Randomized
Non-ASLR image	Not randomized	Rebased and randomized	Rebased and randomized	Not randomized	Rebased but not randomized	Rebased and randomized

https://docs.microsoft.com/pt-br/windows/security/threat-protection/overviewer-of-threat-mitigations-in-windows-10
https://docs.microsoft.com/pt-br/cpp/build/reference/dynamicbase-use-address-space-layout-randomization?view=vs-2019
https://docs.microsoft.com/en-us/previous-versions/bb430720(v=msdn.10)?redirectedfrom=MSDN#address-space-layout-randomization
https://msrc-blog.microsoft.com/2017/11/21/clarifying-the-behavior-of-mandatory-aslr/

Conclusão

~~~~~~

Apesar do Sistema Operacional ter DEP e ASLR habilitado por default é necessário garantir que o software utilizado foi compilado com as opções de segurança afim de prevenir DEP e ASLR

A recomendação é sempre habilitar as opções mais completas de segurança do Sistema operacional afim de garantir que todos os softwares rodem com as proteções
~~~~~~