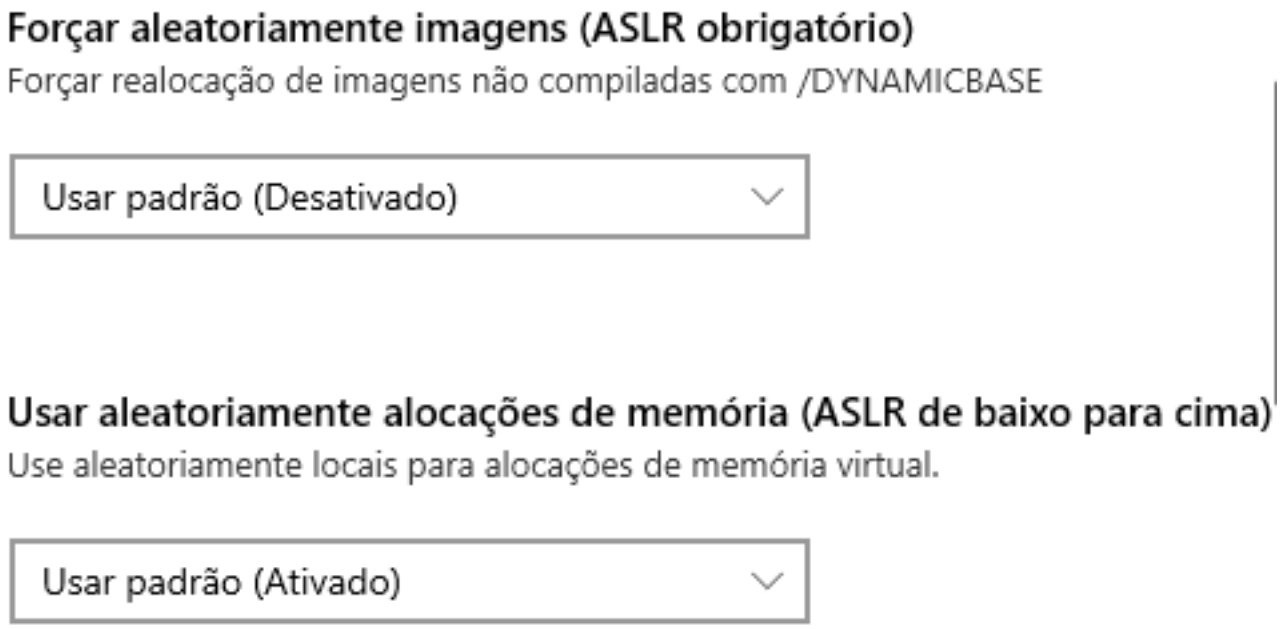
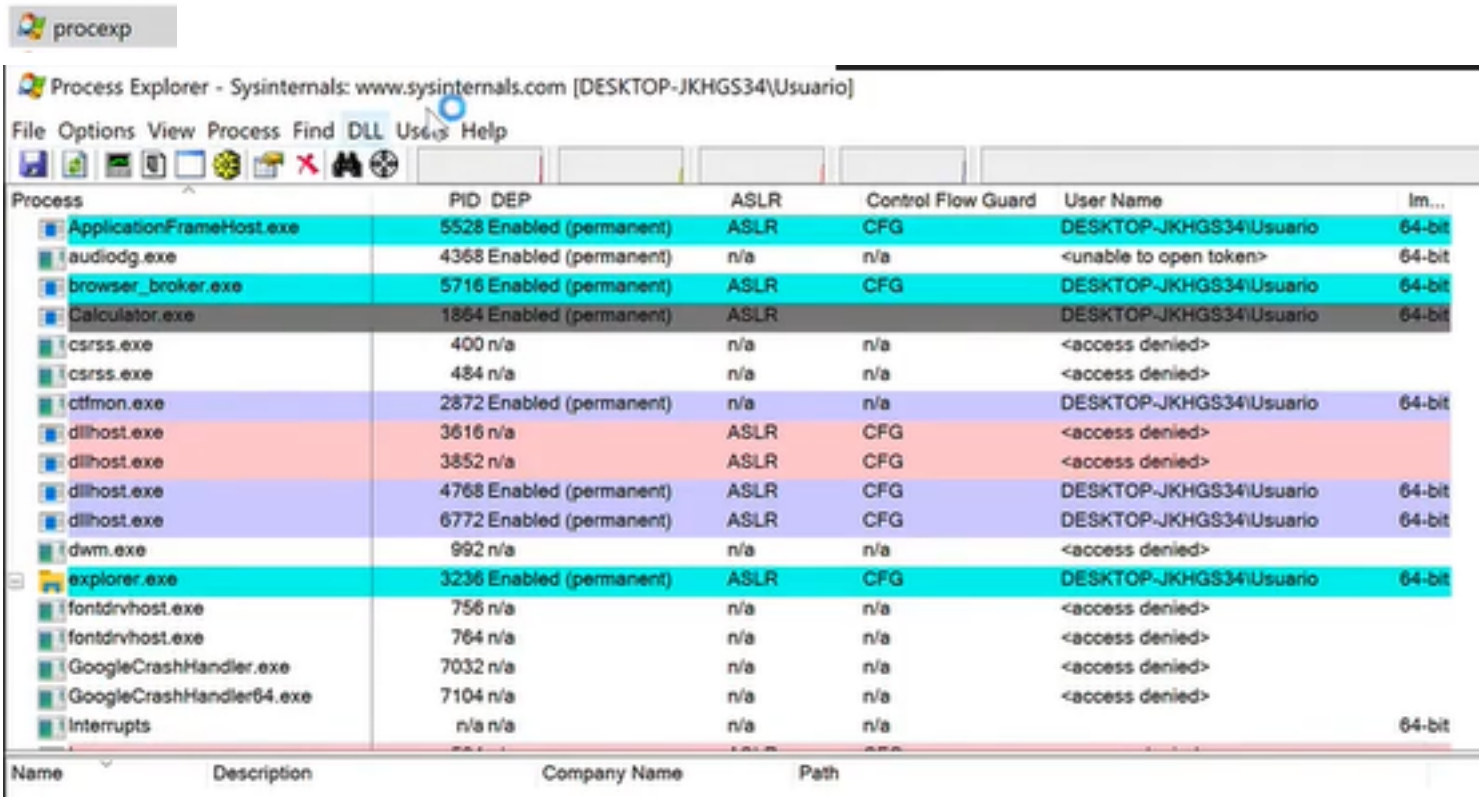
Estudo Prático: ASLR

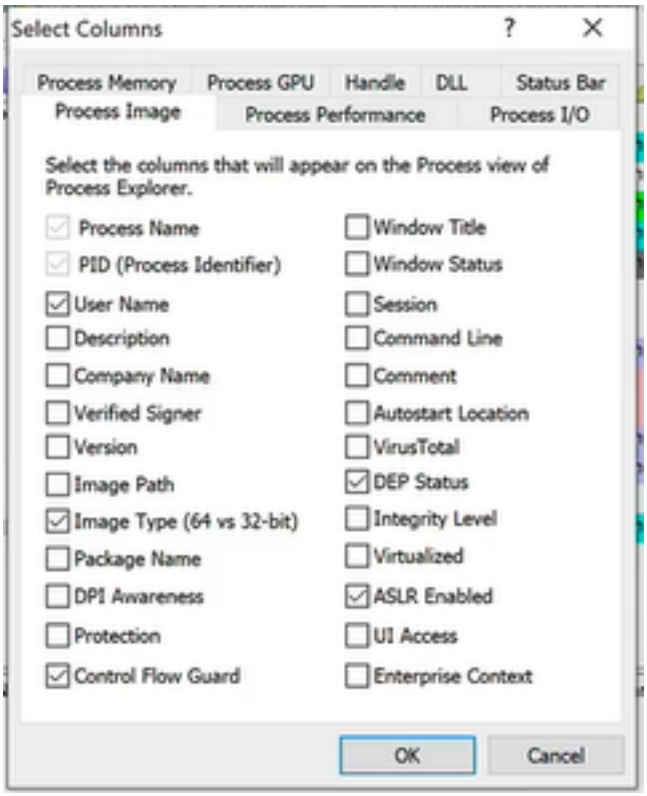
Este computador → botão direito do mouse → Detalhes em Segurança do Windows →
Controle de Aplicativos e do Navegador → Exploit Protection → Config. Exploit Protection →



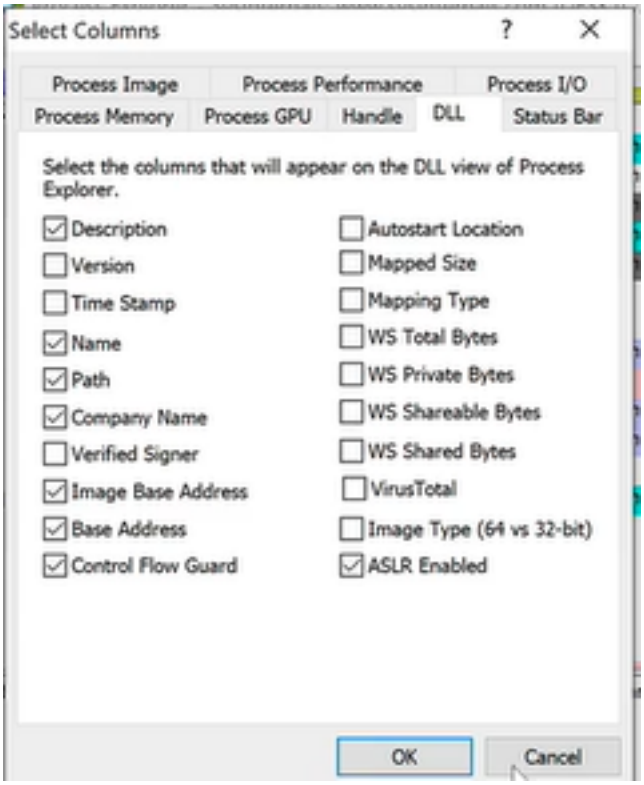
→ Veja que o ASLR obrigatório ou mandatório está, por default, desabilitado
→ Esse é o que força até os programas que não foram configurados com a Dynamic Base a executar o ASLR pra forçar a segurança
+ Para ver todas essas informações, vamos usar o procexp



Configurações: Viwew → Show Lower Pane; Selecet Columns



DLL:

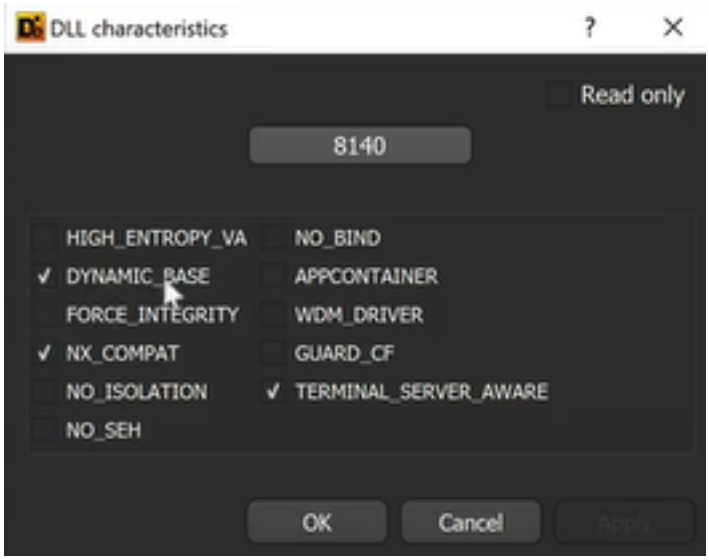


+ Se pegamos um processo qqer, ele indica se tem ou n ASLR ou DEP

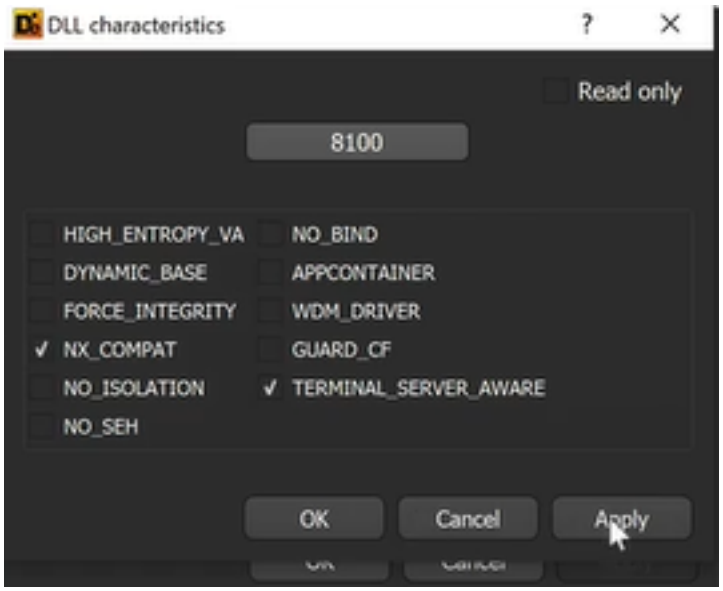
→ Observando o Putty, por exemplo, vemos que nele há o ASLR e o DEP ativos
→ Vamos ver que isso é apontado no Putty e n é no SyncBreeze

Process	PID	DEP	ASLR	Control Flow Guard	User Name
svchost.exe	4628	n/a	ASLR	CFG	<access denied>
svchost.exe	1012	n/a	ASLR	CFG	<access denied>
svchost.exe	5948	Enabled (permanent)	ASLR	CFG	DESKTOP-JKHGS
svchost.exe	7584	n/a	ASLR	CFG	<access denied>
svchost.exe	5020	n/a	ASLR	CFG	<access denied>
svchost.exe	1072	n/a	ASLR	CFG	<access denied>
svchost.exe	1588	n/a	ASLR	CFG	<access denied>
svchost.exe	7048	n/a	ASLR	CFG	<access denied>
syncbrs.exe	3000	n/a			<access denied>
System	4	n/a	n/a	n/a	<access denied>

→ Usaremos novamente o DIE
Putty



→ Se desabilitarmos a Dynamic Base do Putty



Process	PID	DEP	ASLR	Control Flow Guard	User Name	Im...
MicrosoftEdge.exe	5560	Enabled (permanent)	ASLR	CFG	DESKTOP-JKHGS34\Usuario	64-bit
MicrosoftEdgeCP.exe	6180	Enabled (permanent)	ASLR	CFG	DESKTOP-JKHGS34\Usuario	64-bit
MicrosoftEdgeSH.exe	6172	Enabled (permanent)	ASLR	CFG	DESKTOP-JKHGS34\Usuario	64-bit
msdtc.exe	5004	n/a	ASLR	CFG	<access denied>	
MsMpEng.exe	3140	n/a	ASLR	CFG	<access denied>	
NisSrv.exe	4608	n/a	ASLR	CFG	<access denied>	
procexp.exe	3240	Enabled (permanent)	ASLR		DESKTOP-JKHGS34\Usuario	32-bit
procexp64.exe	1300	Enabled (permanent)	ASLR		DESKTOP-JKHGS34\Usuario	64-bit
putty.exe	2900	Enabled (permanent)			DESKTOP-JKHGS34\Usuario	32-bit

→ Temos aí o DEP ativo, mas o ASLR não
[Em essência, o final da aula agora foi apenas testes dos exploits antes e depois de ligar/desligar o ASLR]