

# 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 →

## Forçar aleatoriamente imagens (ASLR obrigatório)

Forçar realocação de imagens não compiladas com /DYNAMICBASE

Usar padrão (Desativado)

## Usar aleatoriamente alocações de memória (ASLR de baixo para cima)

Use aleatoriamente locais para alocações de memória virtual.

Usar padrão (Ativado)

→ Veja que o ASLR obrigatório ou mandatário 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](#)

procexp

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-JKHGS34\Usuario]

File Options View Process Find DLL Usage Help

Process	PID	DEP	ASLR	Control Flow Guard	User Name	Im...
ApplicationFrameHost.exe	5528	Enabled (permanent)	ASLR	CFG	DESKTOP-JKHGS34\Usuario	64-bit
audiodg.exe	4368	Enabled (permanent)	n/a	n/a	<unable to open token>	64-bit
browser_broker.exe	5716	Enabled (permanent)	ASLR	CFG	DESKTOP-JKHGS34\Usuario	64-bit
Calculator.exe	1864	Enabled (permanent)	ASLR		DESKTOP-JKHGS34\Usuario	64-bit
csrss.exe	400	n/a	n/a	n/a	<access denied>	
csrss.exe	484	n/a	n/a	n/a	<access denied>	
ctfmon.exe	2872	Enabled (permanent)	n/a	n/a	DESKTOP-JKHGS34\Usuario	64-bit
dllhost.exe	3616	n/a	ASLR	CFG	<access denied>	
dllhost.exe	3852	n/a	ASLR	CFG	<access denied>	
dllhost.exe	4768	Enabled (permanent)	ASLR	CFG	DESKTOP-JKHGS34\Usuario	64-bit
dllhost.exe	6772	Enabled (permanent)	ASLR	CFG	DESKTOP-JKHGS34\Usuario	64-bit
dwm.exe	992	n/a	n/a	n/a	<access denied>	
explorer.exe	3236	Enabled (permanent)	ASLR	CFG	DESKTOP-JKHGS34\Usuario	64-bit
fontdrvhost.exe	756	n/a	n/a	n/a	<access denied>	
fontdrvhost.exe	764	n/a	n/a	n/a	<access denied>	
GoogleCrashHandler.exe	7032	n/a	n/a	n/a	<access denied>	
GoogleCrashHandler64.exe	7104	n/a	n/a	n/a	<access denied>	
Interrupts	n/a	n/a	n/a	n/a		64-bit

Name Description Company Name Path

Configurações: Viwev → Show Lower Pane; Select Columns



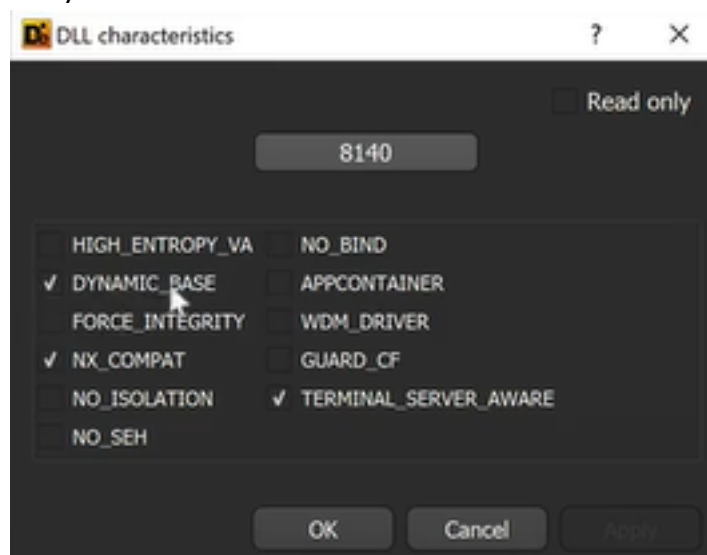
→ Observando o Putty, por exemplo, vemos que nele há o ASLR e o DEP ativos

→ Vamos ver que isso é apontado no Putty e n é no SyncBreeze

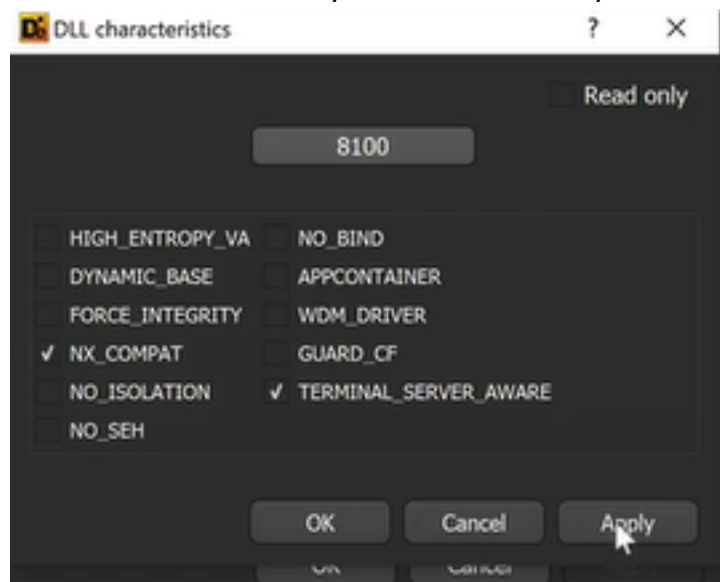
Process	PID	DEP	ASLR	Control Flow Guard	User Name
svchost.exe	4628	n/a	ASLR	CFG	<access denied>
svchost.exe	1012	n/a	ASLR	CFG	<access denied>
svchost.exe	5948	Enabled (permanent)	ASLR	CFG	DESKTOP-JKHGS34\Usuario
svchost.exe	7584	n/a	ASLR	CFG	<access denied>
svchost.exe	5020	n/a	ASLR	CFG	<access denied>
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>
syncbreeze.exe	3000	n/a	n/a	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]

