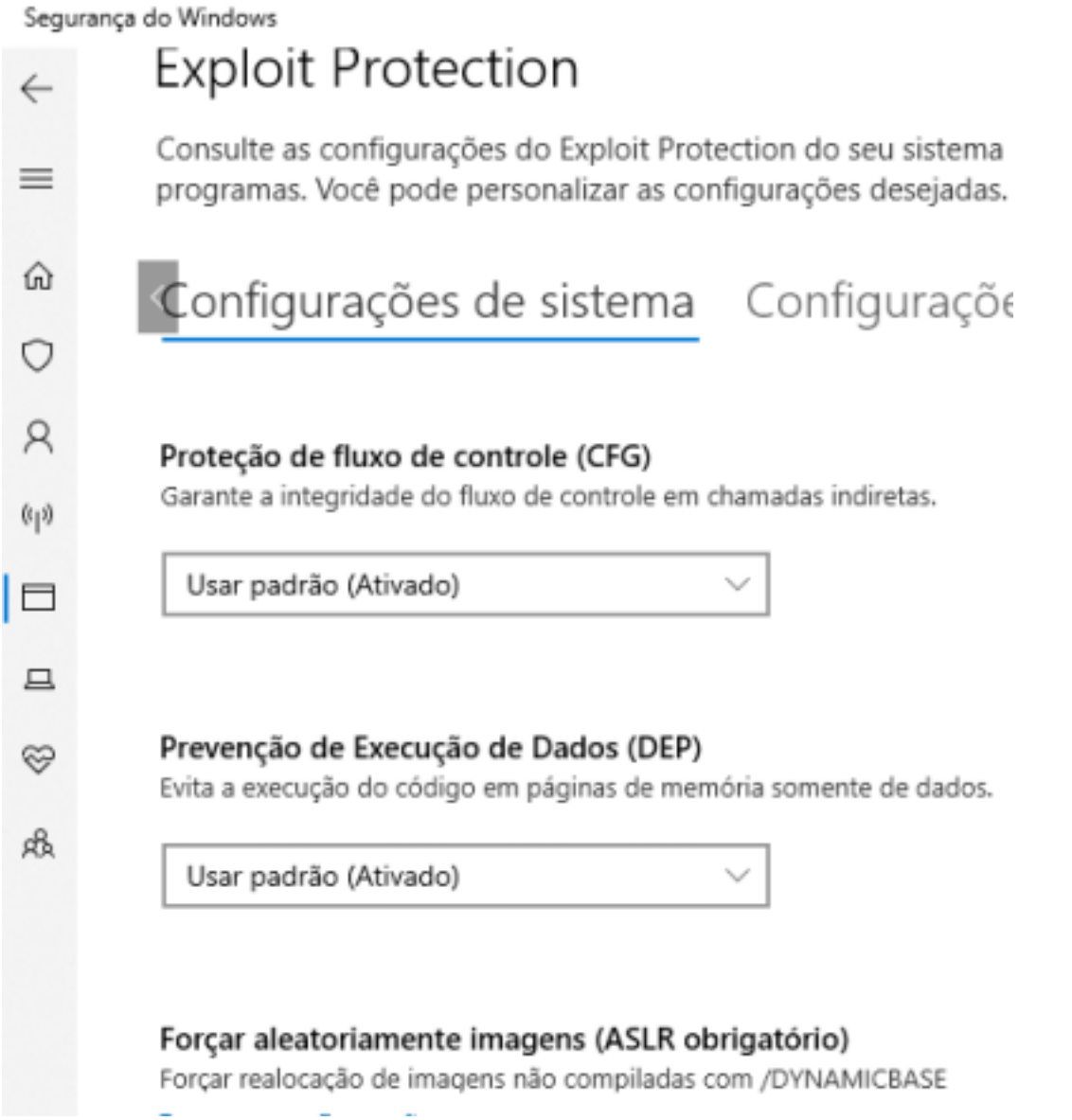
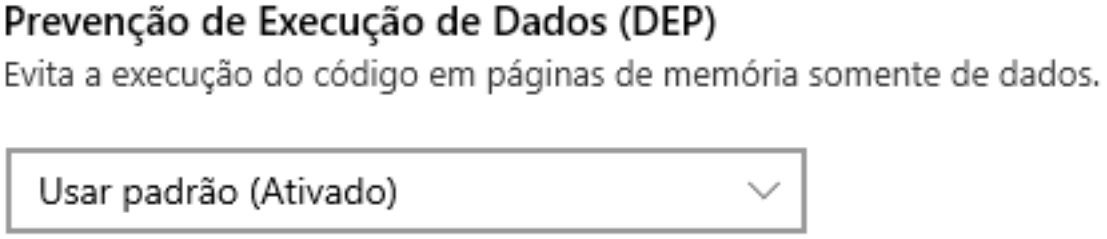
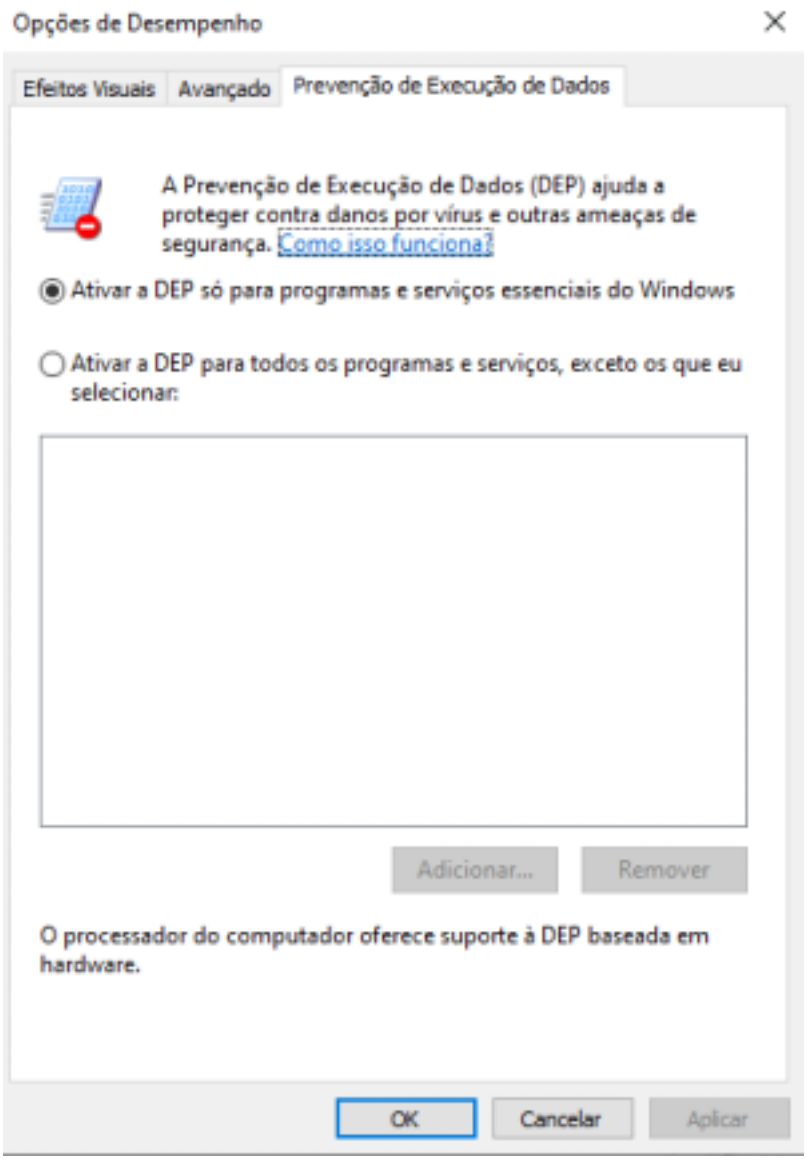
Estudo Prático: DEP

Vamos analisar a segurança do Windows com o seguinte caminho:
Segurança do Windows → Controle de Aplicativos e do Navegador → Exploit Protection → O Windows 10 vem com tudo ativo por default

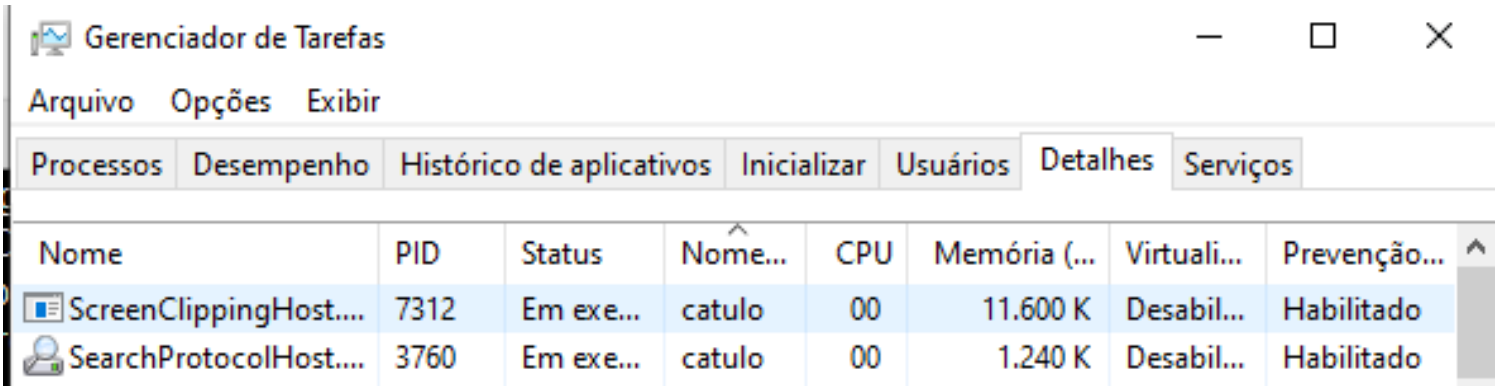




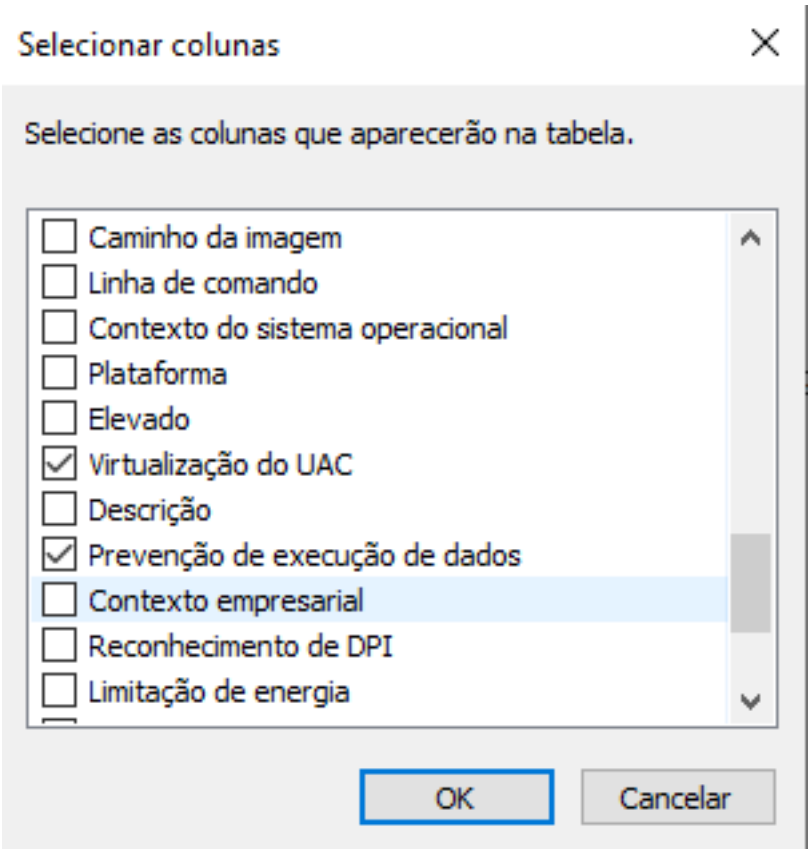
→ Outra maneira de visualizar o DEP:
Este computador → botão direito do mouse → propriedades → configurações avançadas do sistema → avançado → configurações → Prevenção de Execução de Dados



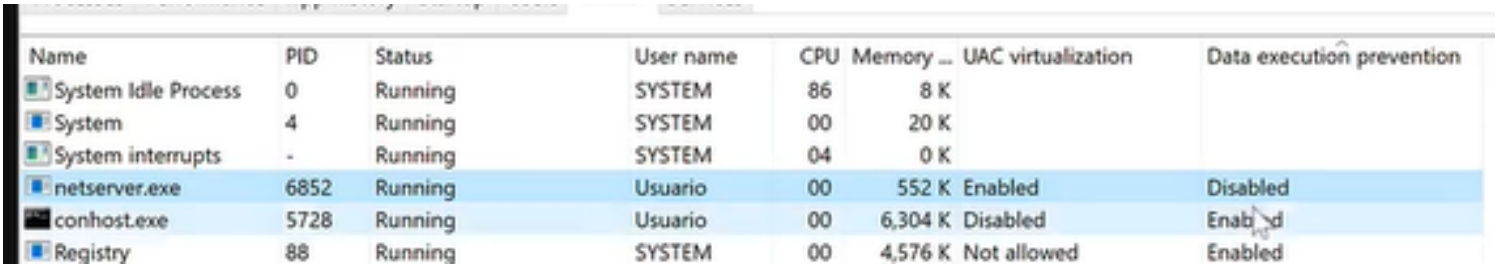
→ A opção de baixo seria a mais segura
→ Para ver quais programas tem o DEP ativado:
Canto inferior (rodapé) da tela do notebook → botão direito do mouse →
task manager (ou gerenciador de tarefas) → Detalhes



Em detalhes: Botão direito do mouse → selecionar colunas→ seleciona a do DEP → OK

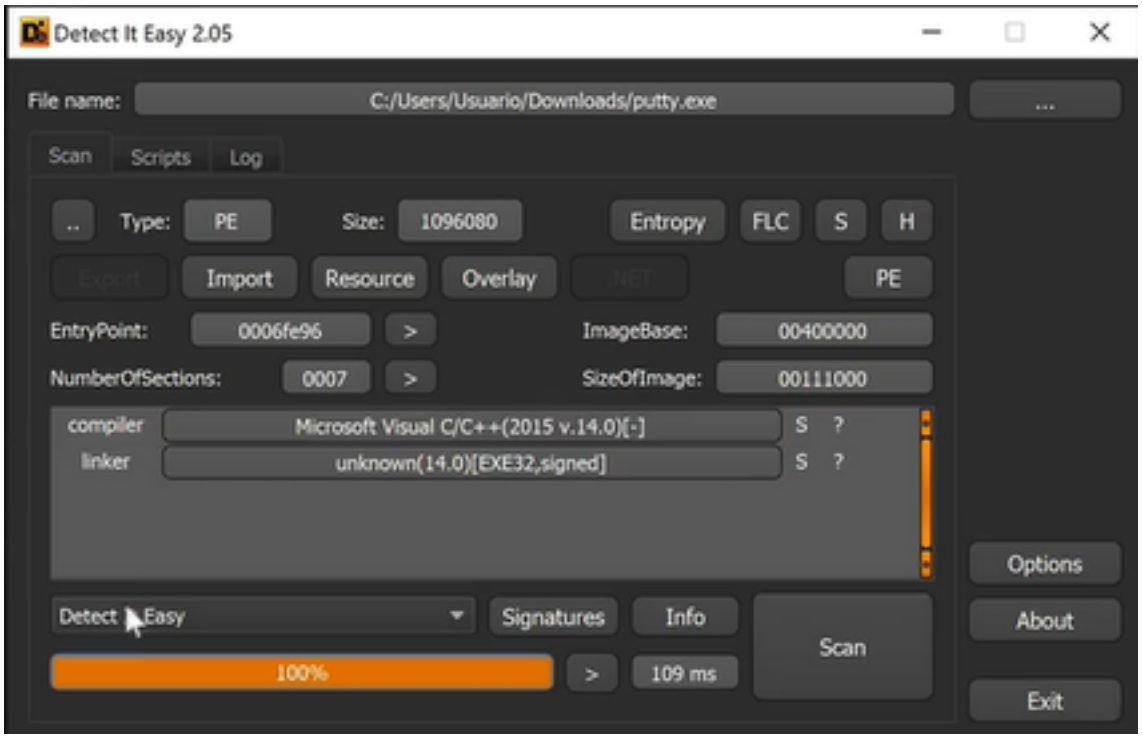


→ Ao executarmos o netserver.exe, veremos que o DEP está desabilitado para ele

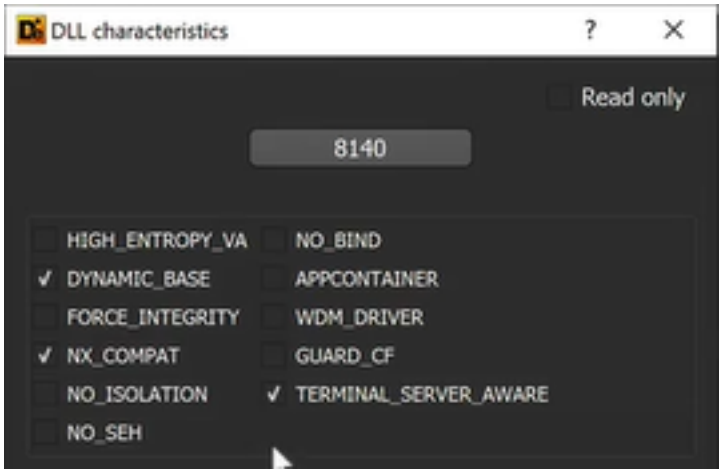


Name	PID	Status	User name	CPU	Memory ...	UAC virtualization	Data execution prevention
System Idle Process	0	Running	SYSTEM	86	8 K		
System	4	Running	SYSTEM	00	20 K		
System interrupts	-	Running	SYSTEM	04	0 K		
netserver.exe	6852	Running	Usuario	00	552 K	Enabled	Disabled
conhost.exe	5728	Running	Usuario	00	6,304 K	Disabled	Enabled
Registry	88	Running	SYSTEM	00	4,576 K	Not allowed	Enabled

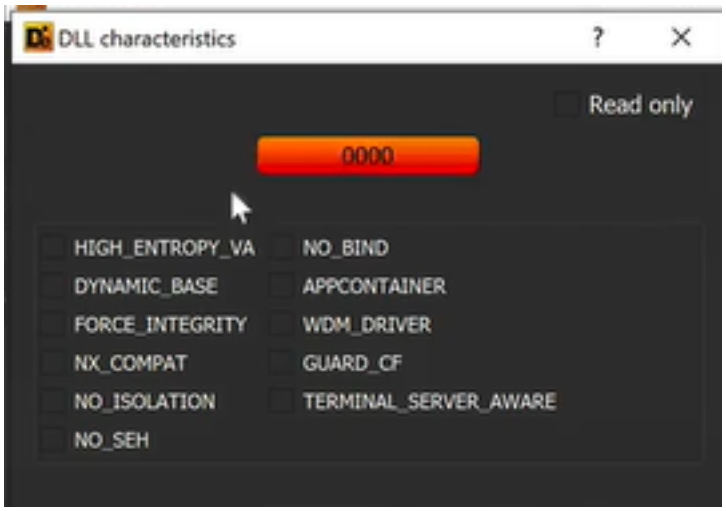
→ O objetivo agora é entender como o windows olha pra esses programas e determina se vai ou não ligar o DEP
→ O windows sabe se o executável aceita ou não o DEP se ele tiver suporte. Pra saber se ele tem suporte, ele analisa o executável
→ Para visualizar informações do executável, vamos usar um software chamado DIE [2.05]



→ PE → NT Header → Optimal Header → Characteristics → ... → Read Only

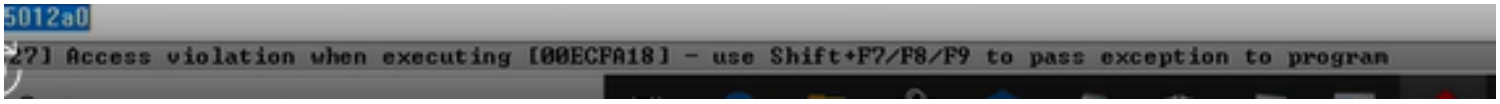


→ As flags setadas indicam que há suporte para ASLR e DEP (análise do Putty)
→ Para o Netserver:



→ essas são as configurações do netserver.exe
→ Podemos habilitar o NC_COMPAT no .exe e na .dll pra que seja habilitado o DEP em ambos. O resultado final é que o DEP será ativado para o Netserver

→ Quando o DEP está ativo e tentamos sobrescrever uma área de memória, ele encerra o programa
→ No Immunity Debugger, vemos que ao executar o nosso payload preparado para o netserver, obteremos agora um access violation como resposta



→ Dessa forma, a configuração mais segura do windows é a que força a configuração do DEP para todos os programas