Procdump脱PECompact1.4beta6 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/251/2021_2022_Procdump_E8_84_c101_251014.htm 1、如果你和我一样使用s3的早期显卡，那么你需要安装sdd v6.53或者 sdd v7.0 alpha3 2、运行天意的test程序，如果你的显卡支持的话，会生成一个Trackit.dat的文件！ 3、我们这次脱PE Compact 1.4 beta6的壳，用天意脱这个软件的壳， 用天意似乎比trw2000更快来到关键处！ 4、此篇文章由于我的水平有限无法涉及让他脱壳后跨平台运行的问题！ 不过在本机应该可以使用！主要是介绍天意为cracker们特设的suspend命令！ 好开始，首先用load载入pecompact.exe文件！ 来到如下程序段： 015F:00419800 JMP SHORT 00419808 中断与此，按f10继续 015F:00419802 PUSH DWORD 00019000 015F:00419807 RET 015F:00419808 PUSHF 按一下f10来到了这里，继续用f10单步执行！ 015F:00419809 PUSHA 015F:0041980A CALL 00419811 来到这里，不要用f10,改用f8,f10继续！ 015F:0041980F XOR EAX,EAX 015F:00419811 MOV EAX,ESP 015F:00419813 ADD EAX,BYTE 04 015F:00419816 XCHG EAX,EBX 015F:00419817 MOV ESP,EBX 015F:00419819 MOV EBX,[EBX-04] 015F:0041981C SUB EBX,0040A00F 015F:00419822 XCHG EBX,EBP 过不了多久就来到这里！ 015F:00419850 PUSH EBX 015F:00419851 PUSH EBX 015F:00419852 PUSH EBX 015F:00419853 PUSH EBX 015F:00419854 POP EAX 015F:00419855 SUB EAX,0040A070 015F:0041985A MOV [EBP 0040A071],EAX 015F:00419860 POP EDI 015F:00419861 LEA ESI,[EBP 0040A070] 015F:00419867 MOV

ECX,0447 015F:0041986C REP MOVSD 看见这条指令了吧！在天意里不管用f10或f8都是 要运行很长时间的（在trw2000里可以用f10带过） 其实，在这里，我们可以用天意的g命令跳过！ 马上会来到这里... 015F:0041B40B NOP 015F:0041B40C MOV ESI,[EBP 0040A5DC] 015F:0041B412 MOV EDI,[EBP 0040A5E0] 015F:0041B418 CALL 0041C0A4 015F:0041B41D POPA 015F:0041B41E POPF 015F:0041B41F PUSH EAX 015F:0041B420 PUSH DWORD 00419000 在41986c处，使用g命令后来到了这里 在按f10 015F:0041B425 RET 04 来到这里用f10带过，就来到程序脱壳的 关键处！ ..关键处代码： 015F:00419000 PUSHF 来到这里，用f10跑到419002处 015F:00419001 PUSHA 015F:00419002 CALL 00419009 来到这里就可以脱壳了，这里我们用 suspend命令回到windows环境，启动 procdump，然后在就可以脱壳了！ 在procdump里可以选种我们刚才准备脱壳文件的那个进程！点鼠标右键，选择 dump(full) 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com