系统安全知识系列之浅谈软件的脱壳 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/140/2021_2022__E7_B3_BB_E7_BB_9F_E5_AE_89_E5_c100_140761.htm 时下的软件加壳风盛行，而且一个比一个来的凶，如果不及时掌握脱壳的技巧，那么无论对于Cracker还是汉化人来讲都将很不利。小弟并不是什么高手，我也是刚刚学会脱壳，小弟在这将脱壳中总结出的一些经验写出来，希望能给和小弟一样刚学脱壳的朋友一定的帮助。请各位高手不要看了，那样只会浪费您宝贵的时间，如果小弟下面的内容有错漏的地方，请给小弟指正。 现在我们开始练习脱壳了，首先准备好 Trw2k 及 Prodump1.62，然后随便找一个EXE文件用Aspack2001压缩一次，我是用 speedcat2.1(以下简称sc) 。 启动Trw2k，将sc拖到TRW2K中，点击LOAD，如下： XXX:00431001 60 PUSHAD *注意这个入栈* XXX:00431002 E872050000 CALL 00431579 XXX:00431007 EB4C JMP 00431055 *跳到解压程序* 在这之后程序会在几个地方作循环，下 G 指令跳出这些循环以节省时间，然后小心按F10一直来到： XXX:004314F3 61 POPAD *注意这个出栈* XXX:004314F4 7508 JNZ 004314FE *程序入口* XXX:004314F6 B801000000 MOV EAX,00000001 XXX:004314FB C20C00 RET 000C XXX:004314FE 6864194000 PUSH 00401964 XXX:00431503 C3 RET 我们已经找到程序的入口，可以开始编辑 Prodump1.62 中的Script.ini文件脱壳了。但我还要加一点说明，留意 XXX:00431001 PUSHAD 和 XXX:004314F3 POPAD 这一对指令，汇编知识告诉我们它们缺一不可，我发现不管是Aspack还是Upx加壳的软件一开始都会停在 PUSHAD，然

后在 POPAD 指令后紧跟一个跳跃的指令，这个跳跃指令就是程序的入口。 我们现在开始编辑Script.ini文件。打开Script.ini文件，在[INDEX]最下面加上一行P??=Aspack2001(??是在[INDEX]中的行号)，然后在Script.ini文件最后完整地加上： [Aspack2001] L1=OBJR L2=LOOK EB,4C *跳到解压程序的代码* L3=JZ 5 L4=QUIT L5=BP L6=WALK L7=OBJR L8=LOOK 61,75 *程序入口的代码* L9=BP LA=STEP OPTL1=00000000 OPTL2=01010001 OPTL3=01010001 OPTL4=00030000 *这一行很重要，如果解压后的程序运行有问题，改成00010000 OPTL5=00000000 或00020000试试* 最后存盘。 现在还等什么?用Prodump32脱壳呀! 