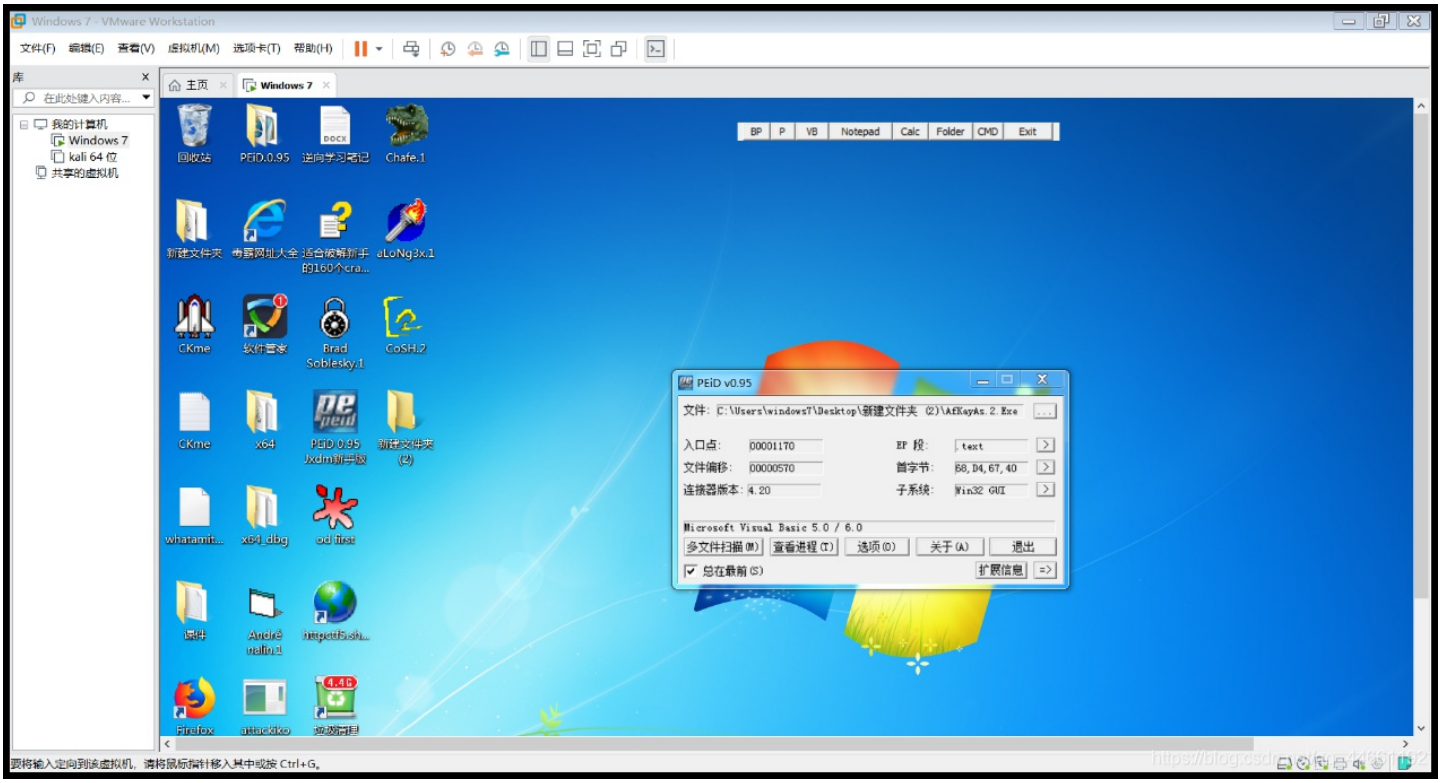
crackme160 003 writeup

原创

Aaaapply 于 2019-04-14 09:58:05 发布 112 收藏

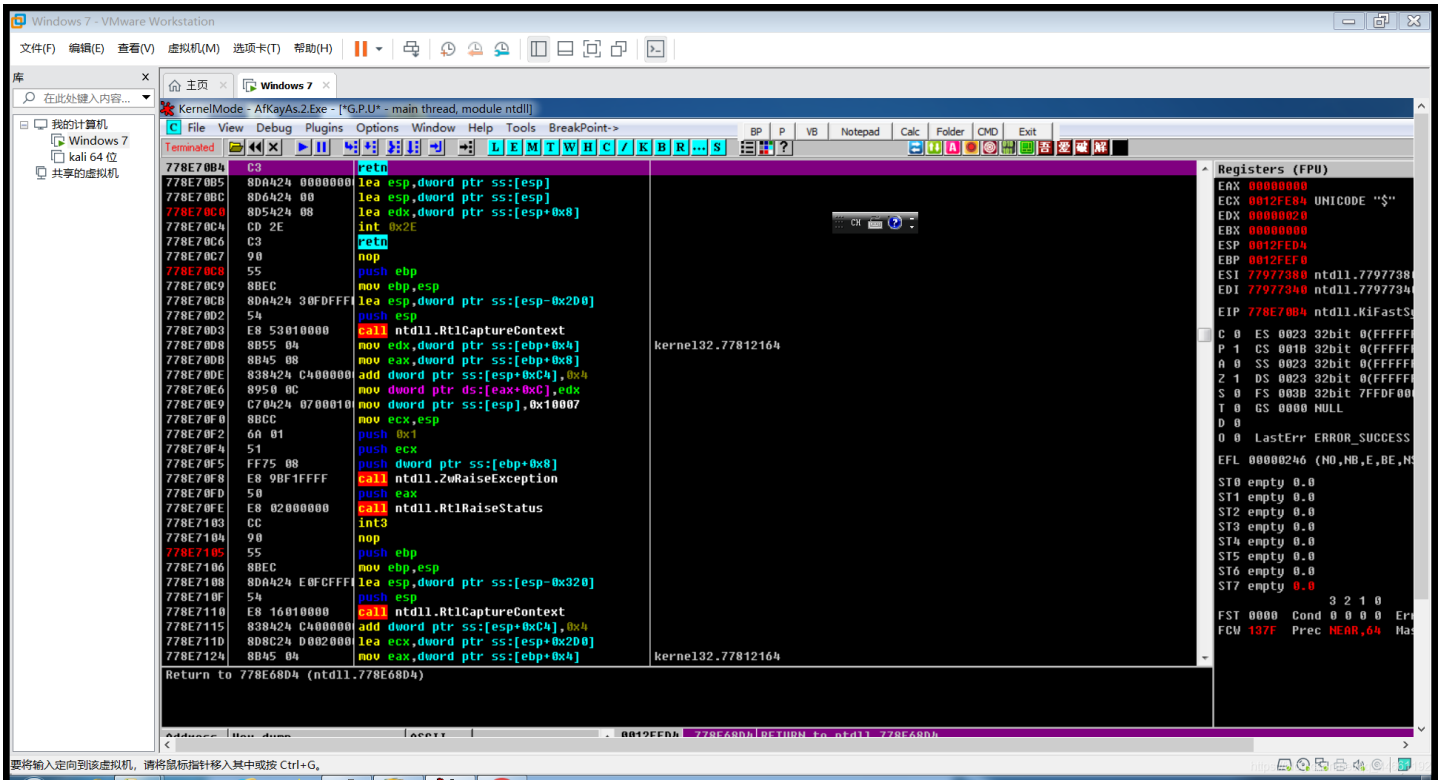
分类专栏： 安全 文章标签： crackme 逆向 二进制

查壳 无壳



用od载入 运行

输入假码



运行结束后 输入假码点击关闭

Address	Stack	Procedure / arguments	Called from	Frame
0012ED90	77D19418	Includes ntdll.KiFastSystemCallRet	user32.77D19416	0012EDC4
0012ED94	77D2770A	user32.WaitMessage	user32.77D27705	0012EDC4
0012EDC8	77D249C4	user32.77D2757B	user32.77D249BF	0012EDC4
0012EDF0	77D3A956	user32.77D2490E	user32.77D3A951	0012EDEC
0012F0B0	77D3A2BC	user32.SoftModalMessageBox	user32.77D3A2B7	0012F0AC
0012F200	77D3A10B	user32.77D3A147	user32.77D3A106	0012F1FC
0012F26C	740CEE19	user32.MessageBoxIndirectA	msvbvm50.740CEE13	0012F268
0012F270	0012F278	pMsgBoxParams = 0012F278		
0012F2A4	740CEC81	Includes msvbvm50.740CEE19	msvbvm50.740CEC7E	0012F2A0
0012F2C8	740CEFAF	msvbvm50.740CEB58	msvbvm50.740CEFAA	0012F2C4
0012F2F8	740C6394	msvbvm50.740CEF19	msvbvm50.740C638F	0012F2F4
0012F364	740F414D	msvbvm50.740C60F3	msvbvm50.740F4148	0012F360
0012F3D8	00408722	msvbvm50.rtcMsgBox	AfKayAs_.00408718	0012F3D4

出现堆栈窗口 点击最后一个 msgbox 是对话框messagebox函数

右键showcall跟入

发现附近代码出有je跳转 应该也是书迷用户名密码如果正确运行 不正确的话会跳转

直接用nop爆破填充

右键二进制 用nop填充

运行成功