

Challenges : Basic 02

(Code Engn)

Writer : Ho Yeul Lee

Date : 2017.10.27

Challenges : Basic 02

Author : ArturDents

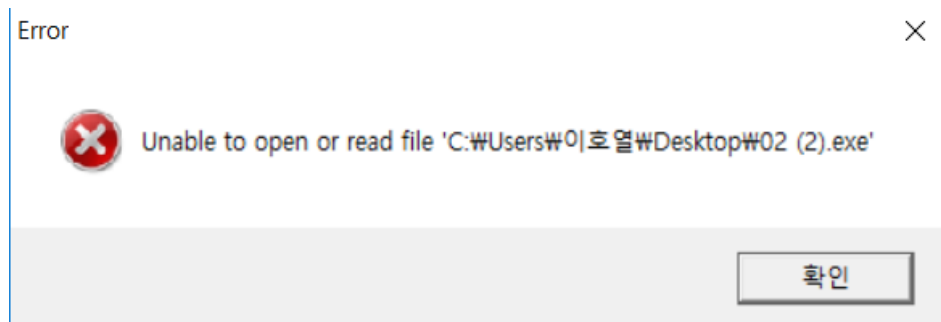
Korean :

패스워드로 인증하는 실행파일이 손상되어 실행이 안되는 문제가 생겼다. 패스워드가 무엇인지 분석하시오

English :

The program that verifies the password got messed up and ceases to execute. Find out what the password is.

문제는 실행파일이 손상되어 실행이 안되는 문제가 생겼다고 하여 일단 실행을 시켜 보았습니다.



실행결과 파일을 열수 없다는 말이 나오면서 종료가 됩니다.

리버싱을 처음 해보는 저로서 여기서 무슨 문제가 발생한지 몰랐기 때문에 열심히 찾아본 결과 PE 헤더가 손상되어서 이런 문제가 발생한다고 하였고 이를 확인하기 위해 PViewer 을 사용해야 한다고 했습니다.

PEview - C:\Users\W이호열\Desktop\W02 (2).exe

File View Go Help

	pFile	Raw Data	Value
02 (2).exe			
IMAGE_DOS_HEADER	000005D0	A6 20 00 00 D2 20 00 00 94 20 00 00 E0 20 00 00
	000005E0	00 00 00 00 92 00 44 69 61 6C 6F 67 42 6F 78 50DialogBoxP
	000005F0	61 72 61 6D 41 00 B8 00 45 6E 64 44 69 61 6C 6F	aramA...EndDialo
	00000600	67 00 00 01 47 65 74 44 6C 67 49 74 65 6D 00 00	g...GetDlgItem..
	00000610	02 01 47 65 74 44 6C 67 49 74 65 6D 54 65 78 74	..GetDlgItemText
	00000620	41 00 BB 01 4D 65 73 73 61 67 65 42 6F 78 41 00	A...MessageBoxA..
	00000630	10 02 53 65 6E 64 4D 65 73 73 61 67 65 41 00 00	..SendMessageA..
	00000640	2B 02 53 65 74 46 6F 63 75 73 00 00 55 53 45 52	+.SetFocus..USER
	00000650	33 32 2E 64 6C 6C 00 00 75 00 45 78 69 74 50 72	32.dll..u.ExitPr
	00000660	6F 63 65 73 73 00 11 01 47 65 74 4D 6F 64 75 6C	rocess...GetModul
	00000670	65 48 61 6E 64 6C 65 41 00 00 4B 45 52 4E 45 4C	eHandleA..KERNEL
	00000680	33 32 2E 64 6C 6C 00 00 00 00 00 00 00 00 00 00	32.dll.....
	00000690	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	000006A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	000006B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	000006C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	000006D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	000006E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	000006F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	00000700	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	00000710	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	00000720	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	00000730	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	00000740	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	00000750	41 44 44 69 61 6C 6F 67 00 41 72 74 75 72 44 65	ADDialog.ArturDe
	00000760	6E 74 73 20 43 72 61 63 6B 4D 65 23 31 00 00 00	nts CrackMe#1...
	00000770	00 00 00 00 00 4E 6F 70 65 2C 20 74 72 79 20 61Nope, try a
	00000780	67 61 69 6E 21 00 59 65 61 68 2C 20 79 6F 75 20	gain!.Yeah, you
	00000790	64 69 64 20 69 74 21 00 43 72 61 63 6B 6D 65 20	did it!.Crackme
	000007A0	23 31 00 4A 4B 33 46 4A 5A 68 00 00 00 00 00 00	#1.JK3FJZh.....
	000007B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

PE vier 사용결과 바로 ... 정답이 나오네요...

이 문제가 출제된 이유는 실행파일을 열 수 없는 상황이 왔을 때 어떻게 처리를 할 것이냐가 가장 중요 했던 부분인 것 같습니다.

이 문제에서는 PE 헤더에 대해 알 필요 없이 정답을 확인 할 수 있었지만, 조금 응용 한 문제가 나오면 못 풀었을 것 같습니다.

그래서 읽고있는 방독면 책에서 1 장 어셈블리 쪽을 끝내고 바로 뒤에 나오는 PE 파일 구조 부분을 읽고 2 장을 읽어볼 생각입니다~