Basic RCE L02

Korea :

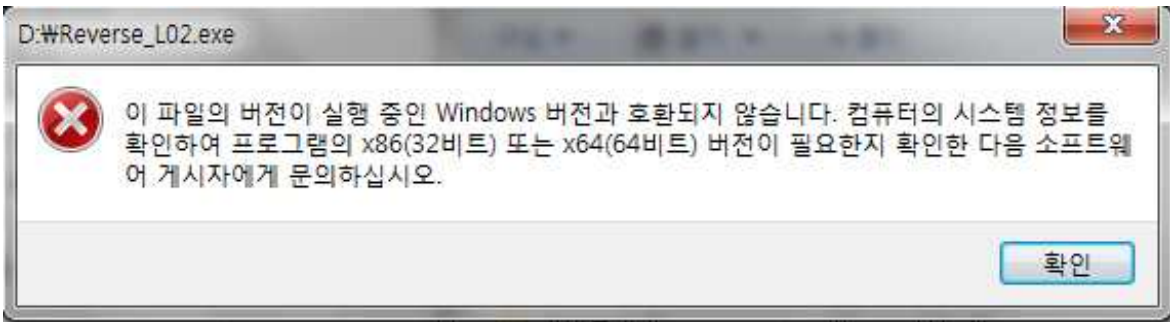
패스워드로 인증하는 실행파일이 손상되어 실행이 안되는 문제가 생겼다. 패스워드가 무엇인지 분석하시오.

English :

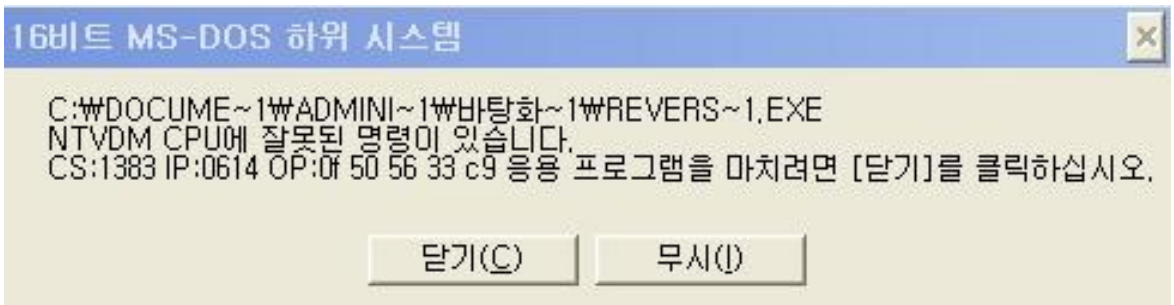
The Program that verifies the password got messed up and ceases to execute. Find out whatthe password is.

일단 프로그램을 실행시켜보자.

Windows7 64bit 환경에서 실행시켰더니 이런 메시지가 떴다.



혹시나 해서 Windows XP sp3 32bit에서도 실행시켰더니
역시나 이런메시지가 뜨고 실행이 안됐다.



프로그램을 실행시키지 않아도 프로그램 내부의 데이터같은걸 볼 수 있는 방법이 있는데 바로 그 파일의 PE구조를 보는 것이다. 모든 실행 가능한 파일은 PE구조라는 어떠한 규칙으로 이뤄진 16진수의 값들로 채워져 있는데 그걸 분석하면은 문자열 같은 것을 볼 수 있다.
파일의 PE구조를 보기위해서는 WinHex라는 프로그램이 필요하다.

WinHex를 통해서 프로그램을 열어보면

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ ÿÿ
00000016	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	¸ @
00000032	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000048	00	0A	00	00	00	00	00	00	00	10	00	00	00	10	00	00	
00000064	00	20	00	00	00	00	40	00	00	10	00	00	00	02	00	00	@
00000080	04	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00	
00000096	00	50	00	00	00	04	00	00	00	00	00	00	02	00	00	00	P
00000112	00	00	10	00	00	10	00	00	00	00	10	00	00	10	00	00	
00000128	00	00	00	00	10	00	00	00	00	00	00	00	00	00	00	00	
00000144	2C	20	00	00	3C	00	00	00	00	40	00	00	18	03	00	00	, < @
00000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000176	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000192	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000208	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000224	00	00	00	00	00	00	00	00	00	20	00	00	2C	00	00	00	,
00000240	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000256	00	00	00	00	00	00	00	00	2E	74	65	78	74	00	00	00	.text
00000272	52	01	00	00	00	10	00	00	00	02	00	00	00	04	00	00	R `
00000288	00	00	00	00	00	00	00	00	00	00	00	00	20	00	00	60	
00000304	2E	72	64	61	74	61	00	00	38	01	00	00	00	20	00	00	.rdata 8
00000320	00	02	00	00	00	06	00	00	00	00	00	00	00	00	00	00	
00000336	00	00	00	00	40	00	00	40	2E	64	61	74	61	00	00	00	@ @.data
00000352	5C	02	00	00	00	30	00	00	00	02	00	00	00	08	00	00	\ 0
00000368	00	00	00	00	00	00	00	00	00	00	00	00	40	00	00	C0	@ À
00000384	2E	72	73	72	63	00	00	00	18	03	00	00	00	40	00	00	.rsrc @
00000400	00	04	00	00	00	0A	00	00	00	00	00	00	00	00	00	00	
00000416	00	00	00	00	40	00	00	C0	00	00	00	00	00	00	00	00	@ À
00000432	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000448	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000464	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000480	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

이렇게 뜬다. 여기서 조금 더 밑으로 내려보면

이 부분을 볼 수 있을 것이다.

00001872	41	44	44	69	61	6C	6F	67	00	41	72	74	75	72	44	65	ADDialog ArturDe
00001888	6E	74	73	20	43	72	61	63	6B	4D	65	23	31	00	00	00	nts CrackMe#1
00001904	00	00	00	00	00	4E	6F	70	65	2C	20	74	72	79	20	61	Nope, try a
00001920	67	61	69	6E	21	00	59	65	61	68	2C	20	79	6F	75	20	gain! Yeah, you
00001936	64	69	64	20	69	74	21	00	43	72	61	63	6B	6D	65	20	did it! Crackme
00001952	23	31	00	4A	4B	33	46	4A	5A	68	00	00	00	00	00	00	#1 JK3FJZh
00001968	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

딱 봐도 실패했을때의 메시지인 "Nope,try again!"과, 성공했을때의 메시지인 “Yeah, you did it!"이 있고 Crackme 1번이라는 의미의 문자열들이 있는 것 같다.
그렇다면 마지막의 JK3FJZh 가 패스워드일 것이다. JK3FJZh를 입력 해 보자. 성공이다.

2011.08.16

Made by hypen1117
hypen1117@daum.net
http://hypen1117.tistory.com

리버싱을 그렇게 잘하지 못해 구체적이지 못하고 잘못 될 수 있습니다.
잘못되거나 부족한 부분 지적해 주시길 바랍니다.