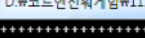


2013년 9월 12일 목요일
오후 2:49



D:\월드연원게임\111\W02.exe

```

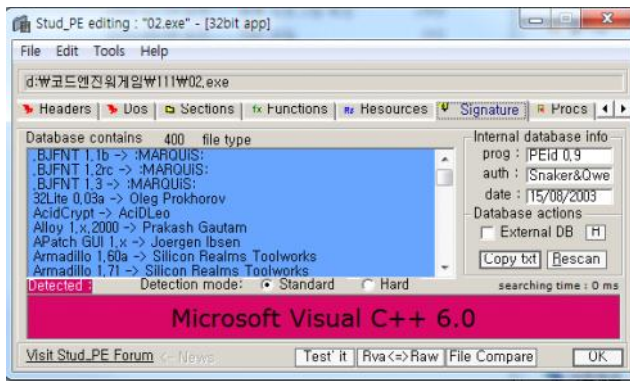
+++++ WHO CAN CRACK THE CRACKME!? +++++
+++++ CrackMe No2 , by Noble +++++
Enter Password:

```

문제의 의도는 프로그램에서 요구하는 특정 값을 찾는 것이다.

사용자가 입력한 값을 특정 값과 비교하기 때문에 문제 접근 방법은 다음과 같이 하였다.

1. 입력한 값이 어느 메모리에 있는 지 찾는다.
2. 입력한 값이 호출 되는 곳을 찾는다.
3. 호출되는 곳이 특정 값과 비교하는 로직 일 경우 답이 있을 것이다.



0040115C	PUSH	02.00414528	ASCII	"Kernel32.dll"
004011BC	PUSH	02.00414288	ASCII	"++++++*****"
004011E0	PUSH	02.0041425C	ASCII	"+++++ WHO CAN CRACK THE CRACKME!? +++++"
00401204	PUSH	02.00414288	ASCII	"++++++*****"
00401228	PUSH	02.00414244	ASCII	"CrackMe No2 , by Noble"
004012B5	PUSH	02.00414230	ASCII	"Enter Password: "
0040220E	PUSH	02.00414594	ASCII	"missing locale facet"
0040250C	PUSH	02.00414594	ASCII	"missing locale facet"
00403D09	MOV	ESI,02.004111E4	ASCII	"ios::badbit set"
00403D13	MOV	ESI,02.004111D0	ASCII	"ios::failbit set"
00403D1A	MOV	ESI,02.004111C0	ASCII	"ios::eofbit set"
00404093	MOV	ESI,02.00411220	ASCII	"string too long"
004042BF	MOV	ESI,02.00411250	ASCII	"invalid string position"
00406203	MOV	EAX,02.00411388	ASCII	"Unknown exception"

Address	Hex dump	ASCII	
0012F568	31 32 33 34 00 00 00 00 00 00 00 00 00 00 00 00	1234.....	0012F168 004184D0 02.004184D0
0012F578	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0012F16C 0012F568 ASCII "1234"
0012F588	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0012F170 00418440 02.00418440
			0012F174 00414230 ASCII "Enter Password: "

이는 처음 입력받은 값(12F568)을 호출하여 비교하는 것이 아닌, 루프를 통해 입력한 값을 다른 곳에 여러번 옮기고, 그 중에서 한 곳과 비교하기 때문에 종료되는 것이다.

0040134F	- 51	PUSH EAX	
0040135F	- RD424 ECHSHL EAX, EDI, DWORD PTR SS:[ESP+5EC]		
00401365	- FFD2	CALL EDI	
0040136C	- 83C4 08	ADD ESP, 8	입력값과 특정값(답)을 비교하는 함수
00401373	- EB 07E90000	CALL 02.0040FDDC	
0040137F	- 8B424 18	MOV EAX, DWORD PTR SS:[ESP+18]	
00401383	- 3BC7	CMP EAX, EDI	
00401385	- 74 1D	JE SHORT 02.004013F4	
00401387	- 8D48 FF	LEA ECK, DWORD PTR DS:[EAX-1]	
00401389	- 8D48 FF	MOV AL, BYTE PTR DS:[EAX-1]	
0040138B	- 84C0	TEST AL, AL	
0040138D	- 74 06	JE SHORT 02.004013E5	

Stack address=0012F75C
EDI=0000001F

복사된 곳 중, 실제 특정값(답)과 비교하는 값

Address	Hex dump	ASCII	0012F170	0012F17C
0177281C	F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D	???	0012F174	0177281C ASCII "1234"
0177281D	F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D	???	0012F178	00000000
0177281E	F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D	???	0012F17C	00000000
0177281F	F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D	???	0012F180	0012F888
01772820	F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D	???	0012F184	7FDD0000
01772821	F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D	???	0012F188	00000000
01772822	F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D	???	0012F18C	00000000
01772823	F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D	???	0012F190	0177281F ASCII "1234"
01772824	F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D	???	0012F194	00000000
01772825	F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D	???	0012F198	0000001F
01772826	F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D	???	0012F19C	75AD0C55
01772827	F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D	???	0012F1A0	kernel32.LoadI
01772828	F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D	???	0012F1A4	ntdll.RtlZerob

따라서 루프를 빠져 나온 후 Trace를 통해 조금만 진행해보면 위와 같이 입력 값을 특정 값과 비교하는 함수를 호출하는 곳을 볼 수 있다.

0012F768	8DBD 1CFFFFFF	LEA EDI,DWORD PTR SS:[EBP-E4]
0012F76E	B9 39000000	MOV ECX,39
0012F773	B8 CCCCCCCC	MOV EAX,CCCCCCCC
0012F778	F3:AB	REP STOS DWORD PTR ES:[EDI]
0012F77A	A1 08604000	MOV EAX,DWORD PTR DS:[406000]
0012F77F	33C5	XOR EAX,EBP
0012F781	8945 FC	MOV DWORD PTR SS:[EBP-4],EAX
0012F784	8B45 0C	MOV EAX,DWORD PTR SS:[EBP+C]
0012F787	0FBE08	MOVSX ECX,BYTE PTR DS:[EAX]
0012F78A	83F9 43	CMP ECX,43
0012F78D	0F85 F7000000	JNZ 0012F88A
0012F793	8B45 0C	MOV EAX,DWORD PTR SS:[EBP+C]
0012F796	0FBE48 01	MOVSX ECX,BYTE PTR DS:[EAX+1]
0012F79A	83F9 52	CMP ECX,52
0012F79D	0F85 E7000000	JNZ 0012F88A
0012F7A3	8B45 0C	MOV EAX,DWORD PTR SS:[EBP+C]
0012F7A6	0FBE48 02	MOVSX ECX,BYTE PTR DS:[EAX+2]
0012F7AA	83F9 41	CMP ECX,41
0012F7AD	0F85 D7000000	JNZ 0012F88A
0012F7B3	8B45 0C	MOV EAX,DWORD PTR SS:[EBP+C]
0012F7B6	0FBE48 03	MOVSX ECX,BYTE PTR DS:[EAX+3]

해당 함수를 들어가보면 입력 값을 특정 값(답)과 비교하며, 특정 값이 답임을 알 수 있다.

"4352414141434b454421" => "CRAAAKED!"