

Unpack을 한 후 Serial을 찾으시오.

정답인증은 OEP + Serial

Ex) 00400000PASSWORD

OEP는, POPAD를 한 직후 점프해서 간 복원된EP다.

PUSHAD를 실행하고 스택창0012ff6c에서 EDI값을 찾았다. dump창 0012ff6c주소로 가서 hardware bp를 걸어주고 실행하면

00429A36	. 57	PUSH EDI
00429A37	. FFD5	CALL EBP
00429A39	. 58	POP EAX
00429A3A	. 61	POPAD
00429A3B	. 8D4424 80	LEA EAX,DWORD PTR SS:[ES
00429A3F	> 6A 00	PUSH 0
00429A41	. 39C4	CMP ESP,EAX
00429A43	. ^ 75 FA	JNZ SHORT 06.00429A3F
00429A45	. 83EC 80	SUB ESP,-80
00429A48	.- E9 1379FDFF	JMP 06.00401360
00429A4D	00	DB 00
00429A4E	00	DB 00
00429A4F	00	DB 00
00429A50	00	DB 00
00429A51	00	DB 00
00429A52	00	DB 00
-----	--	-- --

POPAD로 보내진다. 이제 압축공간을 원래대로 늘려줬으니 jmp를 따라가면 oep가 나오게 된다. OEP=00401360.

진행하다보면 아래 그림의 코드가 나오는데

00401110	55	PUSH EBP	
00401111	8BEC	MOV EBP,ESP	
00401113	83EC 44	SUB ESP,44	
00401116	53	PUSH EBX	
00401117	56	PUSH ESI	
00401118	57	PUSH EDI	
00401119	8D7D BC	LEA EDI,DWORD PTR SS:[EBP-44]	
0040111C	B9 11000000	MOV ECX,11	
00401121	B8 CCCCCCCC	MOV EAX,CCCCCCCC	
00401126	F3:AB	REP STOS DWORD PTR ES:[EDI]	
00401128	8BF4	MOV ESI,ESP	
0040112A	6A 00	PUSH 0	
0040112C	68 0A104000	PUSH 06.0040100A	
00401131	6A 00	PUSH 0	
00401133	6A 65	PUSH 65	
00401135	8B45 08	MOV EAX,DWORD PTR SS:[EBP+8]	
00401138	50	PUSH EAX	
00401139	FF15 A8524200	CALL DWORD PTR DS:[4252A8]	USER32.DialogBoxParamA
0040113F	3BF4	CMP ESI,ESP	
00401141	E8 DA010000	CALL 06.00401320	

파라미터가 5개다. 다이얼로그창을 만드는듯.

F8로 진행하다보면 같은구간을 계속 도는데

75F237B2	8B86 B4000000	MOV EAX,DWORD PTR DS:[ESI+B4]
75F237B8	33C9	XOR ECX,ECX
75F237BA	3BC1	CMP EAX,ECX
75F237BC	74 7E	JE SHORT USER32.75F2383C
75F237BE	F640 14 01	TEST BYTE PTR DS:[EAX+14],1
75F237C2	75 78	JNZ SHORT USER32.75F2383C
75F237C4	6A 01	PUSH 1
75F237C6	51	PUSH ECX
75F237C7	51	PUSH ECX
75F237C8	51	PUSH ECX
75F237C9	8D45 E0	LEA EAX,DWORD PTR SS:[EBP-20]
75F237CC	50	PUSH EAX
75F237CD	E8 782BFEFF	CALL USER32.PeekMessageW
75F237D2	85C0	TEST EAX,EAX
75F237D4	0F85 C3000000	JNZ USER32.75F2389D
75F237DA	85FF	TEST EDI,EDI
75F237DC	0F84 0CFFFFFF	JE USER32.75F236EE
75F237E2	837D 0C 00	CMP DWORD PTR SS:[EBP+C],0
75F237E6	74 24	JE SHORT USER32.75F2380C
75F237E8	FF75 0C	PUSH DWORD PTR SS:[EBP+C]
75F237EB	E8 CA1BFEFF	CALL USER32.IsWindow
75F237F0	85C0	TEST EAX,EAX
75F237F2	0F84 64A90000	JE USER32.75F2E15C
75F237F8	837D 0C 00	CMP DWORD PTR SS:[EBP+C],0
75F237FC	74 0E	JE SHORT USER32.75F2380C
75F237FE	85DB	TEST EBX,EBX
75F23800	74 0A	JE SHORT USER32.75F2380C
75F23802	837D FC 00	CMP DWORD PTR SS:[EBP-4],0
75F23806	0F84 DCC7FFFF	JE USER32.75F1FFE8
75F2380C	8B4D 08	MOV ECX,DWORD PTR SS:[EBP+8]
75F2380F	B2 01	MOV DL,1
75F23811	E8 097DFDFF	CALL USER32.75EFB51F
75F23816	85C0	TEST EAX,EAX
75F23818	74 22	JE SHORT USER32.75F2383C
75F2381A	B8 00C00000	MOV EAX,0C000
75F2381F	66:8546 2A	TEST WORD PTR DS:[ESI+2A],AX
75F23823	75 17	JNZ SHORT USER32.75F2383C
75F23825	E8 932EFEFF	CALL USER32.WaitMessage
75F2382A	8B4D 08	MOV ECX,DWORD PTR SS:[EBP+8]
75F2382D	B2 01	MOV DL,1
75F2382F	E8 EB7CFDFF	CALL USER32.75EFB51F
75F23834	85C0	TEST EAX,EAX
75F23836	0F85 76FFFFFF	JNZ USER32.75F237B2
75F23838	6A 00	PUSH 0

메시지 창, 윈도우창을 만들고 입력을 기다리면서 루프를 계속 돈다.

루프 아래에 bp를 걸고 실행시키자 입력란이 나왔다. 아무거나 적고 확인을 눌렀더니 틀렸다는 창이 뜬다. 창을닫고 free구문을 지나면

00401056	A1 38364200	MOV EAX,DWORD PTR DS:[423638]	
00401058	50	PUSH EAX	
0040105C	FF15 B0524200	CALL DWORD PTR DS:[4252B0]	USER32.GetDlgItemTextA
00401062	3BF4	CMP ESI,ESP	
00401064	E8 B7020000	CALL 06.00401320	
00401069	68 D4354200	PUSH 06.004235D4	
0040106E	68 302A4200	PUSH 06.00422A30	ASCII "AD46DFS547"
00401073	E8 18020000	CALL 06.00401290	
00401078	83C4 08	ADD ESP,8	
0040107B	85C0	TEST EAX,EAX	
0040107D	75 24	JNZ SHORT 06.004010A3	
0040107F	8BF4	MOV ESI,ESP	
00401081	6A 40	PUSH 40	
00401083	68 48004200	PUSH 06.00420048	ASCII "Good Job!"
00401088	68 38004200	PUSH 06.00420038	ASCII "You got it ;)"
0040108D	8B0D 38364200	MOV ECX,DWORD PTR DS:[423638]	
00401093	51	PUSH ECX	
00401094	FF15 B4524200	CALL DWORD PTR DS:[4252B4]	USER32.MessageBoxA
0040109A	3BF4	CMP ESI,ESP	
0040109C	E8 7F020000	CALL 06.00401320	
004010A1	EB 22	JMP SHORT 06.004010C5	
004010A3	8BF4	MOV ESI,ESP	
004010A5	6A 10	PUSH 10	
004010A7	68 30004200	PUSH 06.00420030	ASCII "ERROR"
004010AC	68 1C004200	PUSH 06.0042001C	ASCII "Wrong serial!!!"
004010B1	8B15 38364200	MOV EDX,DWORD PTR DS:[423638]	
004010B7	52	PUSH EDX	
004010B8	FF15 B4524200	CALL DWORD PTR DS:[4252B4]	USER32.MessageBoxA
004010BE	3BF4	CMP ESI,ESP	
004010C0	E8 5B020000	CALL 06.00401320	

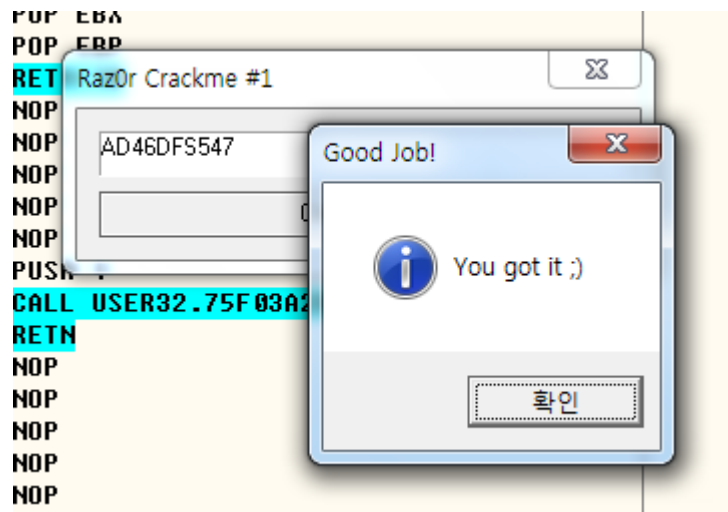
요렇게 digltemTextA라는 함수로 뭔가 받고 수상해보이는 AD46DFS547를 인자로 받는 함수가 있다. 또한 TEST EAX,EAX로 EAX값이 0이 아니면 틀린창이 뜨는 구간으로 점프한다. 일단 답은 AD46DFS547인걸 알았다만 저기에 실행흐름이 들어가지 못했으므로 좀더 분석해보겠다.

분석해보니

0040120C	8945 F8	MOV DWORD PTR SS:[EBP-8],EAX	
0040120F	817D F8 E90300	CMP DWORD PTR SS:[EBP-8],3E9	
00401216	74 02	JE SHORT 06.0040121A	
00401218	EB 0C	JMP SHORT 06.00401226	
0040121A	E8 E6FDFFFF	CALL 06.00401005	str cmp function (ref)
0040121F	B8 01000000	MOV EAX,1	
00401224	EB 02	JMP SHORT 06.00401228	
00401226	33C0	XOR EAX,EAX	
00401228	5F	POP EDI	

00401005	E9 26000000	JMP 06.00401030
0040100A	E9 91010000	JMP 06.004011A0
0040100F	E9 FC000000	JMP 06.00401110
00401014	CC	INT3
00401015	CC	INT3

이렇게 입력이 시작되기 전에 간접적인 call로 교묘하게 비교하는 구간으로 넘겨주는 것을 볼 수 있다. 그래서 처음 시작할 때 못 찾고 한번 틀리고서야 찾을 수 있던것이다.



여튼..AD46DFS547을 넣으니 clear.