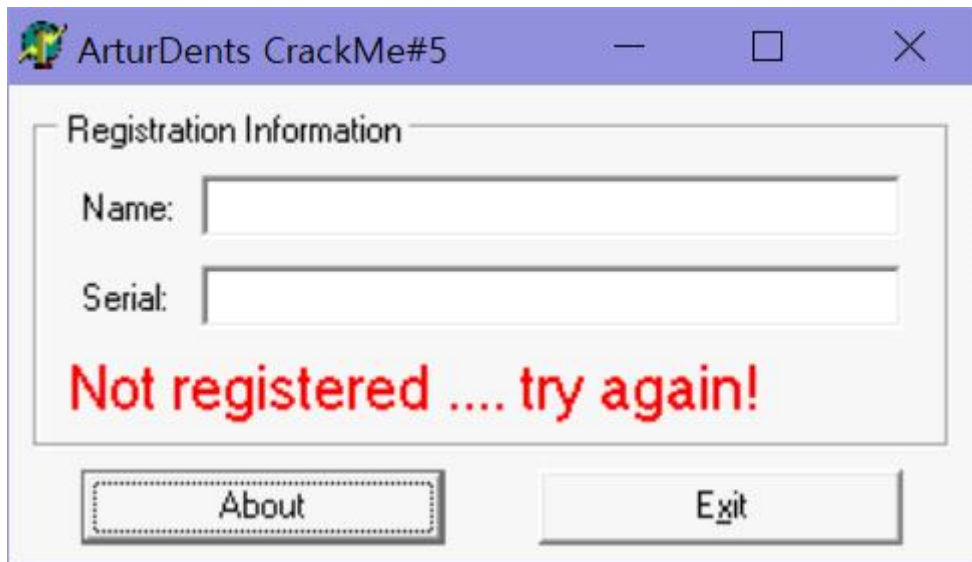


CodeEngn Basic RCE L10 Write up

:OEP를 구한 후 '등록성공' 으로 가는 분기점의 OPCODE를 구하시오.

정답인증은 OEP + OPCODE

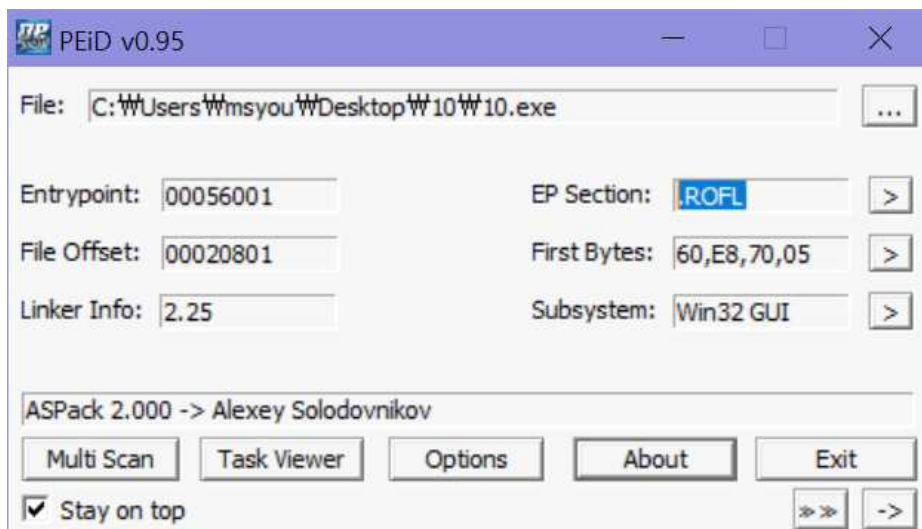
EX) 00400000EB03



10.EXE 실행 시 위와 같이 뜬다!

문제에서는 등록성공으로 가는 OPCODE를 찾으라 했으므로 NAME과 SERIAL입력시 등록성공을 띄우게 하는 코드를 찾아야 하는 것 같다.

1. PEiD로 구조 분석하기



이번에도 OEP 코드를 구하라 하길래 PEiD로 조회 시 UPX로 패킹 되어있을 것이라고 생각했는데 ASPack으로 패킹되어 있는 것을 알 수 있다.

2. OLLYDBG로 분석하기

키고 실행 몇번 눌러누면 바로 PUSHAD가 보인다.

Address	Disassembly
00456001	PUSHAD
00456335	POPAD
004564F1	POPAD
00456E7A	POPAD
00456E87	POPAD
00456E93	POPAD
00456EBC	POPAD
00456F08	POPAD
00456F17	POPAD
00456F25	POPAD
00456F35	POPAD
00456F4B	POPAD
00456F5A	POPAD
00456F68	POPAD
00456FAA	POPAD
00456FB5	POPAD
00456FBB	POPAD
004570A7	POPAD
004570AA	POPAD
004570B7	POPAD
004570C1	POPAD
004570C4	POPAD
00457158	POPAD
0045716B	POPAD
00457176	POPAD
00457179	POPAD
0045717E	POPAD
00457194	POPAD
004571A2	POPAD
004571C7	POPAD
004571D2	POPAD
004574DF	POPAD

POPAD를 찾기 위해 이번에도 SEARCH FOR로 검색하였다.

00456335	61	POPAD
00456336	8B4E 04	MOV ECX,DWORD PTR DS:[ESI+4]
00456339	83E9 08	SUB ECX,8
0045633C	D1E9	SHR ECX,1
0045633E	8B3E	MOV EDI,DWORD PTR DS:[ESI]
00456340	03BD 04484400	ADD EDI,DWORD PTR SS:[EBP+444804]
00456346	83C6 08	ADD ESI,8
00456349	66:8B1E	MOV BX,WORD PTR DS:[ESI]
0045634C	C1EB 0C	SHR EBX,0C

그랬더니 정말 많은 POPAD가 나온다. 일단 PUSHAD와 제일 가까운 것부터 살펴보기로 하고 00456335 주소의 POPAD를 더블클릭하였다.

00456335	61	POPAD
00456336	8B4E 04	MOV ECX,DWORD PTR DS:[ESI+4]
00456339	83E9 08	SUB ECX,8
0045633C	D1E9	SHR ECX,1
0045633E	8B3E	MOV EDI,DWORD PTR DS:[ESI]
00456340	03BD 04484400	ADD EDI,DWORD PTR SS:[EBP+444804]
00456346	83C6 08	ADD ESI,8
00456349	66:8B1E	MOV BX,WORD PTR DS:[ESI]
0045634C	C1EB 0C	SHR EBX,0C

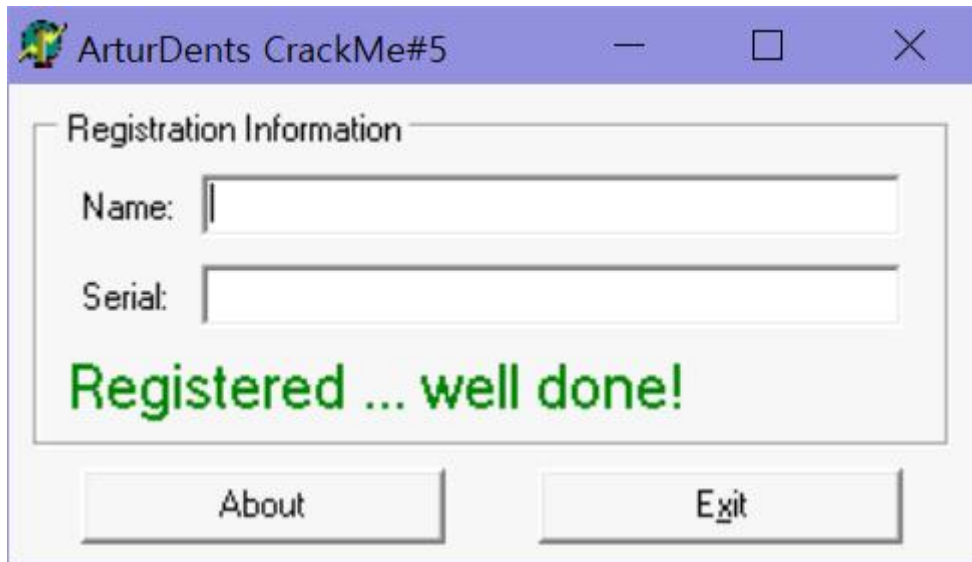
밑으로 이동시키는 명령어를 찾아보려 스크롤을 내렸는데 00456335 주소가 없어진다. 왜 이런건지는 모르겠지만 서치한 결과 이전 POPAD 검색 시 나왔던 목록에서 제외하고 살펴 보라고 나와있어서, 두번째 POPAD 주소, 004564F1로 이동해 보았다.

004564F1	61	POPAD
004564F2	75 08	JNZ SHORT 10.004564FC
004564F4	B8 01000000	MOV EAX,1
004564F9	C2 0C00	RETN 0C
004564FC	68 00000000	PUSH 0
00456501	C3	RETN

한줄씩 BP를 걸고 수행하면

004564F1	61	POPAD
004564F2	75 08	JNZ SHORT 10.004564FC
004564F4	B8 01000000	MOV EAX,1
004564F9	C2 0C00	RETN 0C
004564FC	68 34584400	PUSH 10.00445834
00456501	C3	RETN
00456502	8B85 08484400	MOV EAX,DWORD PTR SS:[EBP+444808]
00456508	8D8D 41484400	LEA ECX,DWORD PTR SS:[EBP+444841]
0045650E	51	PUSH ECX
0045650F	50	PUSH EAX
00456510	FF95 14494400	CALL DWORD PTR SS:[EBP+444914]
00456516	8985 ED394400	MOV DWORD PTR SS:[EBP+4439ED],EAX
0045651C	8D85 51484400	LEA EAX,DWORD PTR SS:[EBP+444851]

004564FC에서 PUSH되는 값이 00000000 -> 00445834로 바뀌고, 00456501 이후 프로그램이 실행되며, 아래와 같은 화면이 뜨게 되는 것을 알 수 있다.



프로그램이 실행되면서 등록 성공이라는 메시지가 뜬다.

즉 PUSH명령어에서 주소를 스택에 넣고 그것을 리턴하면 등록성공이라는 메시지가 나오기 때문에, OEP주소는 00445834라는 것을 알 수 있다.

00445834	55	DB 55	CHAR 'U'
00445835	8B	DB 8B	
00445836	EC	DB EC	
00445837	83	DB 83	
00445838	C4	DB C4	
00445839	F4	DB F4	
0044583A	B8	DB B8	
0044583B	F4	DB F4	
0044583C	56	DB 56	CHAR 'U'
0044583D	44	DB 44	CHAR 'D'
0044583E	00	DB 00	
0044583F	E8	DB E8	
00445840	04	DB 04	
00445841	08	DB 08	
00445842	FC	DB FC	
00445843	FF	DB FF	
00445844	A1	DB A1	
00445845	6C	DB 6C	CHAR 'L'
00445846	6C	DB 6C	CHAR 'L'
00445847	44	DB 44	CHAR 'D'
00445848	00	DB 00	
00445849	8B	DB 8B	
0044584A	00	DB 00	
0044584B	E8	DB E8	
0044584C	F0	DB F0	
0044584D	CC	DB CC	
0044584E	FF	DB FF	
0044584F	FF	DB FF	
00445850	8B	DB 8B	
00445851	0D	DB 0D	
00445852	38	DB 38	CHAR '8'
00445853	6D	DB 6D	CHAR 'm'
00445854	44	DB 44	CHAR 'D'
00445855	00	DB 00	
00445856	A1	DB A1	
00445857	6C	DB 6C	CHAR 'L'
00445858	6C	DB 6C	CHAR 'L'
00445859	44	DB 44	CHAR 'D'

해당 OEP 주소로 들어가보면 아직 OEP인것을 인식하지 못한다고 한다. CTRL+A를 누르면 제대로 인식한다.

004454C1	. E8 3EE6FBFF	CALL 10.00403B04	
004454C6	. 8B85 F8DFFFF	MOV EAX, DWORD PTR SS:[EBP-208]	
004454CC	. 8B55 FC	MOV EDX, DWORD PTR SS:[EBP-4]	
004454CF	. E8 9CE7FBFF	CALL 10.00403C70	
004454D4	. 75 55	JNZ SHORT 10.0044552B	
004454D6	. 8085 F4DFFFF	LEA EAX, DWORD PTR SS:[EBP-20C]	
004454DC	. 8D95 17FEFFFF	LEA EDX, DWORD PTR SS:[EBP-1E9]	
004454E2	. E8 1DE6FBFF	CALL 10.00403B04	
004454E7	. 8B95 F4DFFFF	MOV EDX, DWORD PTR SS:[EBP-20C]	
004454ED	. 8B87 D4020000	MOV EAX, DWORD PTR DS:[EDI+2D4]	
004454F3	. E8 B4F5DFFF	CALL 10.00424AAC	
004454F8	. 8B87 D8020000	MOV EAX, DWORD PTR DS:[EDI+2D8]	
004454FE	. 8B55 FC	MOV EDX, DWORD PTR SS:[EBP-4]	
00445501	. E8 A6F5DFFF	CALL 10.00424AAC	
00445506	. 8B87 E8020000	MOV EAX, DWORD PTR DS:[EDI+2E8]	
0044550C	. BA 60564400	MOV EDX, 10.00445660	ASCII "Registered ... well done!"
00445511	. E8 96F5DFFF	CALL 10.00424AAC	
00445516	. 8B87 E8020000	MOV EAX, DWORD PTR DS:[EDI+2E8]	
0044551C	. 8B40 58	MOV EAX, DWORD PTR DS:[EAX+58]	
0044551F	. BA 00000000	MOV EDX, 0000	
00445524	. E8 BFF2FCFF	CALL 10.004147E8	
00445529	. EB 0A	JMP SHORT 10.00445535	
0044552B	> 33C0	XOR EAX, EAX	
0044552D	. 5A	POP EDX	
0044552E	. 59	POP ECX	
0044552F	. 59	POP ECX	
00445530	. 64:8910	MOV DWORD PTR FS:[EAX], EDX	
00445533	. EB 27	JMP SHORT 10.0044555C	
00445535	> 33C0	XOR EAX, EAX	
00445537	. 5A	POP EDX	
00445538	. 59	POP ECX	
00445539	. 59	POP ECX	

CTRL+A 를 누르고, SEARCH FOR -> STRING 찾기로 EXE파일의 "Registered ... well done!"을 찾을 수 있다. 문제에서 구하라고 했던 opcode는 주소와 어셈블리어 사이에 있는 기계어코드를 말하는데, 등록성공으로 가는 분기문의 OPCODE는 위쪽의 꺾새가 있는 75 55 를 말한다.

답은 004458347555이다.