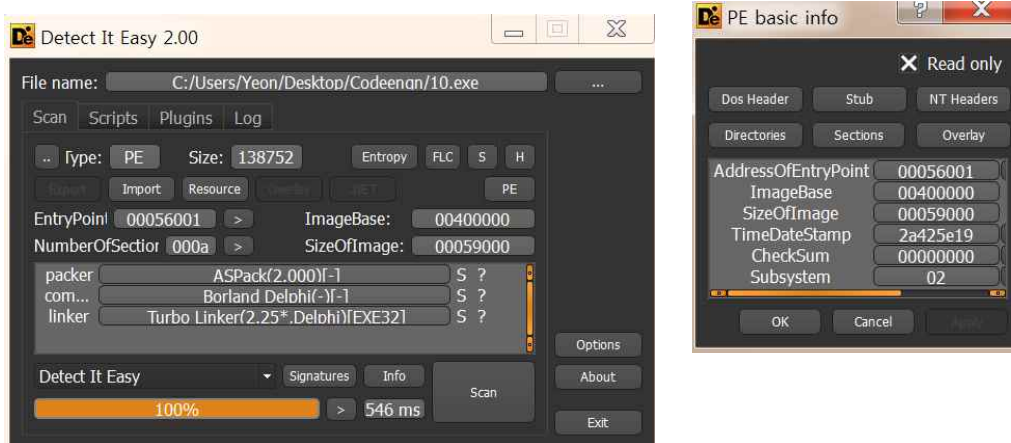


코드 엔진 Challenges: Basic 10

Author: CodeEngn

Korean: OEP를 구한 후 "등록성공"으로 가는 분기점의 OPCODE를 구하시오. 정답인증은 OEP+OPCODE
EX)00400000EB03

문제에서 OEP를 구하라고 하는 것을 보니 패킹되어 있는 프로그램을 언패킹해서 푸는 문제인 것 같다. 일단 언패킹을 위해 패킹에 관한 정보를 얻기위해 DE를 통해서 열어보자.



이 파일은 ASPack으로 패킹되어 있고 entrypoint는 00456001인 것을 알 수 있다.
문제에서 처음나왔으니 자동화툴이 아닌 레지스터를 이용해 언패킹하도록 해보자.

※레지스터를 이용한 언패킹을 하기위해서는 패킹의 원리에 대해 간단하게 알아볼 필요가 있다. 크게 보면 패킹은 아래와 같은 원리를 이용해서 풀리게된다.
-PUSHAD 명령어를 통해 레지스터를 스택에 쌓는다.
-정상코드 메모리에 복구한다.
-POPAD 명령어를 통해 레지스터 값들을 복구 OEP로 분기한다.

위의 원리를 따르면 PUSHAD로 레지스터값들을 스택에 저장해놓고 원본코드가 다 복구되면 메모리에 POPAD를 통해서 다시 레지터 값을 참조하게 될 것이다. 이 점을 이용해서 PUSHAD 후에 ESP값을 접근하는 지점(POPAD 명령어를 통한 접근)에 BP를 설정해 놓으면 OEP 분기점 전으로 이동할 수 있다.

먼저 PUSHAD에서 ESP 값을 구해야 되기 때문에 f8을 이용해서 ESP 값을 확인해보자.

00456000	90	NOP	
00456001	60	PUSHAD	
00456002	E8 70050000	CALL 10.00456577	
00456007	EB 4C	JMP SHORT 10.00456055	
00456009	0000	ADD BYTE PTR DS:[EAX],AL	
0045600B	0000	ADD BYTE PTR DS:[EAX],AL	
0045600D	0000	ADD BYTE PTR DS:[EAX],AL	
0045600F	0000	ADD BYTE PTR DS:[EAX],AL	
00456011	0000	ADD BYTE PTR DS:[EAX],AL	
00456013	0000	ADD BYTE PTR DS:[EAX],AL	
00456015	870B	XCHG EBX,EBX	
00456017	90	NOP	
0045601B	0000 44001000	ADD BYTE PTR DS:[EAX-00100044],AH	
0045601E	44	INC ESP	
0045601F	0000	ADD AL,DL	
00456021	74 44	JE SHORT 10.00456067	
00456023	0010	ADD BYTE PTR DS:[EAX],DL	
00456025	80 44	MOV AL,44	
00456027	0000	ADD BYTE PTR DS:[EAX],AL	
00456029	0000	ADD BYTE PTR DS:[EAX],AL	
0045602B	0000	ADD BYTE PTR DS:[EAX],AL	
0045602D	0000	ADD BYTE PTR DS:[EAX],AL	
0045602F	0000	ADD BYTE PTR DS:[EAX],AL	
00456031	0000 05	ADD BYTE PTR DS:[EAX-5],AH	
00456055	10.00456055		

Registers (FPU)	
EAX	76F83C33 kernel32.BaseThreadInitThunk
ECX	00000000
EDX	00456001 OFFSET 10.<ModuleEntryPoint>
EBX	7FFD5000
ESP	0012FF6C
EBP	0001265C
ESI	00000000
EDI	00000000
EIP	00456007 10.00456007
C 0	ES 0023 32bit 0(FFFFFFFF)
P 1	CS 001B 32bit 0(FFFFFFFF)
A 1	SS 0023 32bit 0(FFFFFFFF)
Z 0	DS 0023 32bit 0(FFFFFFFF)
S 0	FS 003B 32bit 7FDF000(FFF)
T 0	GS 0000 NULL
D 0	
O 0	LastErr ERROR_SUCCESS (00000000)
EFL	00000216 (NO,NB,NE,A,NS,PE,GE,G)
ST0	empty 0.0
ST1	empty 0.0
ST2	empty 0.0
ST3	empty 0.0
ST4	empty 0.0
ST5	empty 0.0

확인 결과 ESP 주소는 0012FF6C 라는 것을 알 수 있다. 이제 여기에 BP를 걸고 실행하면 OEP 분기 전으로 이동할 수 있을 것이다. (왼쪽 아래의 ESP 관련주소가 안나오고 다른주소가 나온다면 오른쪽 상단의 레지스터 영역에서 ESP 의 오른쪽 마우스 클릭 후 Follow in Dump를 해주자.)

BP->Hardware On Access -> Dword를 통해서 스택에 저장된 4Byte 값에 BP를 설정하도록 하자. 설정후에 F9을 이용해서 실행시키면 아래와 같이 004564F2 주소에서 멈추는 것을 확인할 수 있다.

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]	
00456522	50	PUSH EAX	
00456523	FF95 1C494400	CALL DWORD PTR SS:[EBP+44491C]	
00456529	8985 4D484400	MOV DWORD PTR SS:[EBP+44484D],EAX	
0045652F	8D8D 5C484400	LEA ECX,DWORD PTR SS:[EBP+44485C]	
00456535	51	PUSH ECX	
00456536	50	PUSH EAX	
00456537	FF95 14494400	CALL DWORD PTR SS:[EBP+444914]	
0045653D	8985 F1394400	MOV DWORD PTR SS:[EBP+4439F1],EAX	
00456543	8B85 4D484400	MOV EAX,DWORD PTR SS:[EBP+44484D]	
00456549	8D8D 68484400	LEA ECX,DWORD PTR SS:[EBP+444868]	
0045654F	51	PUSH ECX	
00456550	50	PUSH EAX	

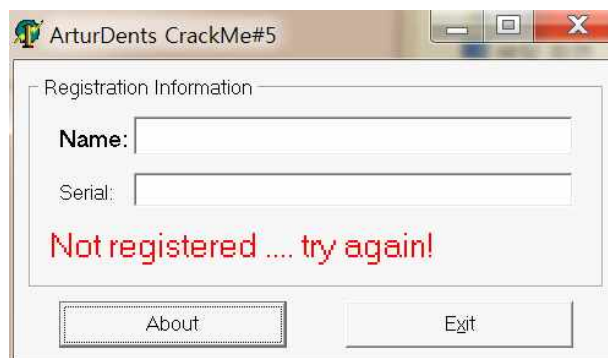
위의 그림을 보면 알 수 있듯이 JNZ 구문에 의해 분기가 일어난 후 특정주소 (00445834)를 PUSH하는 것을 알 수 있다. 이렇게 JNZ이후에 특정주소를 PUSH 하는 경우 JMP 구문과 동일하게 스택에 저장된 주소로 이동하게 된다 . 위의 같은경우에 00445834(OEP)로 이동하게 된다.

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 'V'
0044583D	44	DB 44	CHAR 'D'
0044583E	00	DB 00	
0044583F	E8	DB E8	

이동해보니 디버거가 OPCODE를 인식하지 못하고 있다. 위와 같은 경우는 덤프를 해주면 정상적으로 인식한다. 올림덤프를 이용해서 프로그램을 열어보면 정상적으로 인식하는 것을 확인할 수 있다.

00445834	\$ 55	PUSH EBP	
00445835	. 8BEC	MOV EBP,ESP	
00445837	. 83C4 F4	ADD ESP,-0C	
0044583A	. B8 F4564400	MOV EAX,10_dump.004456F4	
0044583F	. E8 0408FCFF	CALL 10_dump.00406048	
00445844	. A1 6C6C4400	MOV EAX,DWORD PTR DS:[446C6C]	
00445849	. 8B00	MOV EAX,DWORD PTR DS:[EAX]	
0044584B	. E8 F0CCFFFF	CALL 10_dump.00442540	
00445850	. 8B0D 386D4400	MOV ECX,DWORD PTR DS:[446D38]	10_dump.0044784C
00445856	. A1 6C6C4400	MOV EAX,DWORD PTR DS:[446C6C]	
0044585B	. 8B00	MOV EAX,DWORD PTR DS:[EAX]	
0044585D	. 8B15 88514400	MOV EDX,DWORD PTR DS:[445188]	10_dump.004451D4
00445863	. E8 F0CCFFFF	CALL 10_dump.00442558	
00445868	. 8B0D 586D4400	MOV ECX,DWORD PTR DS:[446D58]	10_dump.00447844
0044586E	. A1 6C6C4400	MOV EAX,DWORD PTR DS:[446C6C]	
00445873	. 8B00	MOV EAX,DWORD PTR DS:[EAX]	
00445875	. 8B15 104F4400	MOV EDX,DWORD PTR DS:[444F10]	10_dump.00444F5C
0044587B	. E8 D8CCFFFF	CALL 10_dump.00442558	

이제 OEP 주소를 찾았으니 등록 성공으로 가는 분기점을 찾아보도록 하자.



파일을 실행해보니 어떠한 것도 입력되지 않는다.

Address	Disassembly	Text string
00445354	ASCII "Button2Click"	
00445361	ASCII "IForm1"	
00445382	ASCII "IForm1"	
00445393	ASCII "Unit1"	
004453D5	MOV EDX,10_dump.004455A0	ASCII "159357852645875692311335664857125469857213526859478212124"
004453ED	MOV EDX,10_dump.0044561C	ASCII "cm5.dat"
00445472	MOV EAX,10_dump.0044562C	ASCII "Name must be at least 5 characters long!"
0044550C	MOV EDX,10_dump.00445660	ASCII "Registered ... well done!"
004455A0	ASCII "1593578526458756"	
004455B0	ASCII "9231133566485712"	
004455C0	ASCII "5469857213526859"	
004455D0	ASCII "4782121245693486"	
004455E0	ASCII "4795123216572876"	
004455F0	ASCII "1953213754495421"	
00445600	ASCII "3756785431267218"	

문자열 찾기를 보니 "Registered ~"라는 문자열이 눈에 들어온다. 이 주소로 이동해 살펴보도록 하자.

004454D4	75 55	JNZ SHORT 10_dump.0044552B	
004454D6	. 8D85 F4FDFFFF	LEQ EAX,DWORD PTR SS:[EBP-20C]	
004454DC	. 8D95 17FEFFFF	LEQ EDX,DWORD PTR SS:[EBP-1E9]	
004454E2	. E8 1DE6FBFF	CALL 10_dump.00403B04	
004454E7	. 8B95 F4FDFFFF	MOV EDX,DWORD PTR SS:[EBP-20C]	
004454ED	. 8B87 D4020000	MOV EAX,DWORD PTR DS:[EDI+2D4]	
004454F3	. E8 B4F5FDFF	CALL 10_dump.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_dump.00424AAC	
00445506	. 8B87 E8020000	MOV EAX,DWORD PTR DS:[EDI+2E8]	
0044550C	. BA 60564400	MOV EDX,10_dump.00445660	ASCII "Registered ... well done!"
00445511	. E8 26F5DFFF	CALL 10_dump.00424AAC	

이 주소로 이동해서 살펴보면 위에 조건 분기점을 확인할 수 있다. 즉 분기점의 OPCODE는 75 55이다.

답은 004458347555 이다.