

# codeengn-basic-L08 풀이


리버싱 문제풀이 / Wonlf / 2022. 3. 21. 23:35

Basic RCE L08

OEP를 구하시오 Ex) 00400000

— Author: Rekenmachine

— File Password: codeengn



문제는 OEP를 원하고 있다.

OEP는 codeengn-basic-L06 문제를 풀 때 다뤘었다.

아래를 참고하기 바란다.

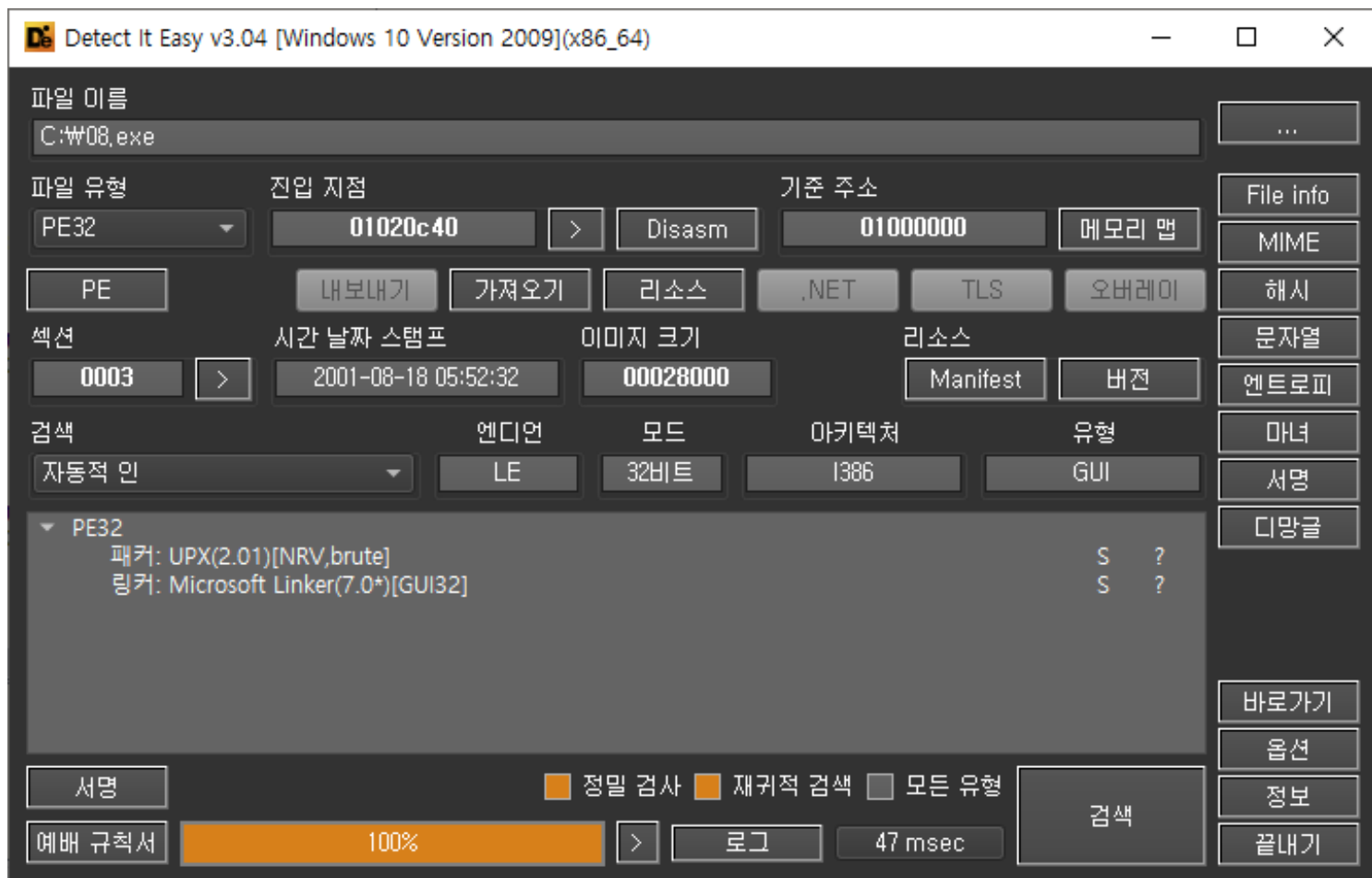
[2022.03.13 - \[리버스 엔지니어링\] - codeengn-basic-L06 풀이](#)

```
!6.4235D4  
!6.422A30  
!6.401290  
p,8  
!ax, eax  
!4010A3  
!1, esp  
0  
!6.420048  
!06.sub_420038>  
!x, dword ptr ds:[423638]  
!CX  
!word ptr ds:[!&Message]
```

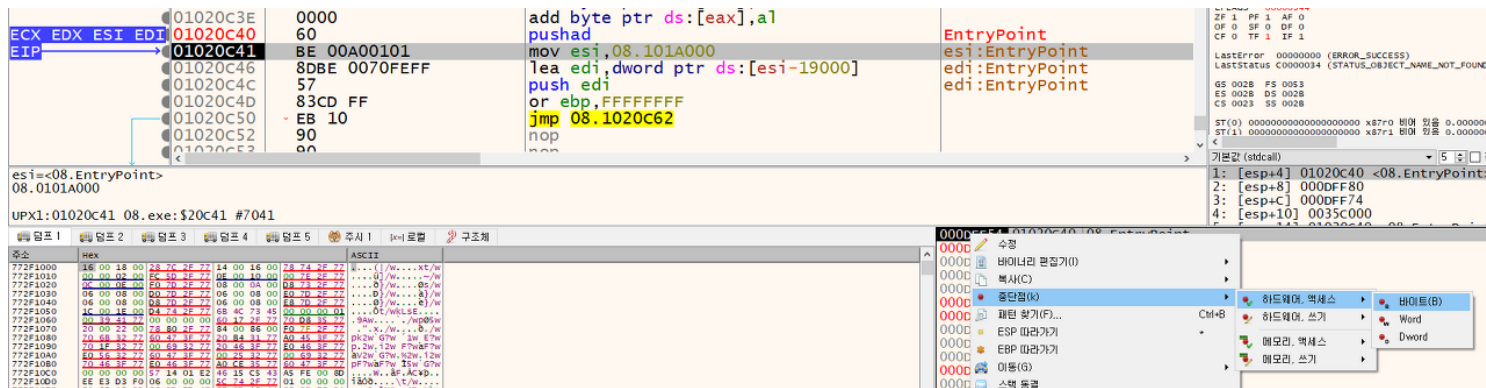
codeengn-basic-L06 풀이

wonlf.tistory.com

먼저 Die를 통해 프로그램의 정보를 얻어보았다.



UPX로 패킹이 되어 있다. 6번 문제를 풀 때처럼 OEP를 찾아보겠다.



pushad 구문을 실행하고 스택에 하드웨어 브레이크 포인트를 걸어준다.

그리고 F9로 여러번 전체 실행을 시키면...

	01020DB9	57	push edi	
	01020DBA	FFD5	call ebp	
	01020DBC	58	pop eax	
	01020DBD	61	popad	
EIP →	01020DBE	8D4424 80	lea eax,dword ptr ss:[esp-80]	
	01020DC2	6A 00	push 0	
	01020DC4	39C4	cmp esp,eax	
	01020DC6	75 FA	jne 08.1020DC2	
	01020DC8	83EC 80	sub esp,FFFFFF80	
	01020DCB	E9 A516FFFF	jmp 08.1012475	
	01020DD0	0000	add byte ptr ds:[eax],a	

이런식으로 popad구문에 멈추게 되고 jmp에 써있는 주소인 1012475가 OEP로 되게 된다.

문제는 OEP를 원했으니 "1012475"