

Codeengn Challenges Advance RCE LEVEL6 풀이

Reverse2 L06 Start

Author : CodeEngn / Lee Kang-Seok

Korea :

남은 군생활은 몇일 인가

정답인증은 MD5 해쉬값(대문자) 변환 후 인증하시오

English :

How many more days to serve for the military

The solution is the MD5 hash of the answer

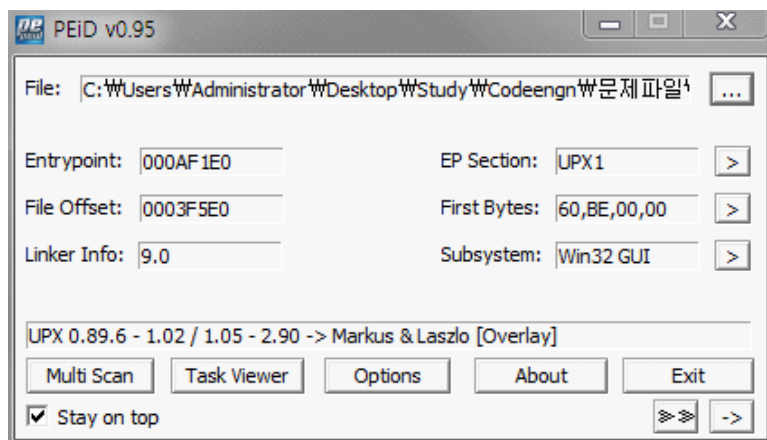
Down

실행해본 결과 메시지 창이 계속 뜨면서 표시되는 숫자가 증가한다 ,

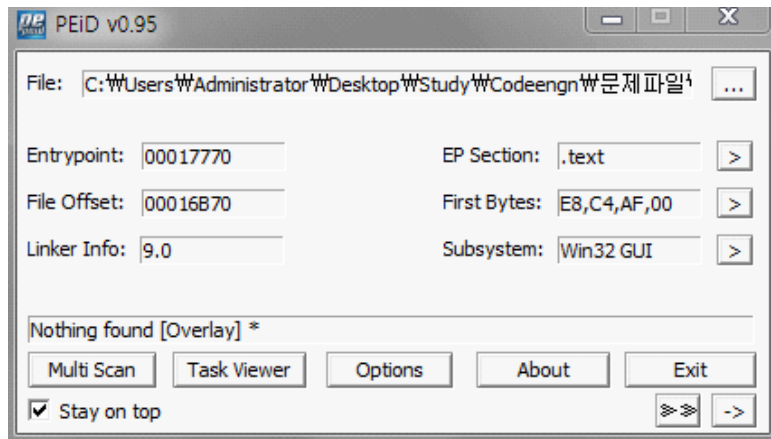
창이 귀찮게 계속 뜨길래 니가 이기나 내가 이기나 해보자는 식으로 확인란에 마우스 커서를 놓고 계속 엔터를 쭉 눌렀는데 790에서 메세지창이 끝났다.

분석 시작 전에 답을 알아버렸다.....ㅠ_ㅠ

아무튼 PEID로 PE를 확인해보았다.



UPX 패킹되어있어서 패킹을 풀어줬다.



OLLY로 열어 분석을 해보았다 .

Back to user 모드를 이용해 MessageBox함수를 call하는 부분을 찾았고 ,

```

0045E06D . 56      PUSH ESI
0045E06E . 51      PUSH ECX
0045E06F . 55      PUSH EBP
0045E070 . 53      PUSH EBX
0045E071 . FF15 9CD64701 CALL DWORD PTR DS:[<&USER32,MessageBoxW]
0045E073 . 8B7424 4C MOV ESI, DWORD PTR DS:[EBP+4C]

```

그리고 그 안으로 파고들어 MessageBoxTimeoutW라는 함수를 호출해 주는 부분을 찾았다.

MessageBoxTimeout 함수는 맨 마지막 인자로 종료될 시간을 밀리세컨트 단위로 받는데 -1로 되어있는걸 1로 바꿔주었다. 즉 1밀리 세컨드 후 자동적으로 메세지창이 소멸되게 만들어주었다.

그리고 계속 분석을해서 메세지창을 출력 하게 해주는 함수를 call하는 부분과 비교하는 함수를 call 하는 부분을 찾았다.

0040B187	E8 B4DAFFFF	CALL _reverse.00408C40	
0040B18C	EB C0	JMP SHORT _reverse.0040B14E	
0040B18E	> 897C24 58	MOV DWORD PTR SS:[ESP+58],EDI	Case 1 of switch 0040B0A5
0040B192	C74424 60 01	MOV DWORD PTR SS:[ESP+60],1	
0040B19A	897C24 64	MOV DWORD PTR SS:[ESP+64],EDI	
0040B19E	C74424 38 78	MOV DWORD PTR SS:[ESP+38],_reverse.00408C40	ASCII "GyF"
0040B1A6	897C24 3C	MOV DWORD PTR SS:[ESP+3C],EDI	
0040B1AA	897C24 40	MOV DWORD PTR SS:[ESP+40],EDI	
0040B1AE	897C24 44	MOV DWORD PTR SS:[ESP+44],EDI	
0040B1B2	8B01	MOV EAX,DWORD PTR DS:[ECX]	
0040B1B4	8B08	MOV ECX,DWORD PTR DS:[EAX]	
0040B1B6	0FBF50 0A	MOVZX EDX,WORD PTR DS:[EAX+A]	
0040B1BA	894C24 18	MOV DWORD PTR SS:[ESP+18],ECX	
0040B1BE	8D4424 7C	LEA EAX,DWORD PTR SS:[ESP+7C]	
0040B1C2	50	PUSH EAX	
0040B1C3	8D4C24 20	LEA ECX,DWORD PTR SS:[ESP+20]	
0040B1C7	51	PUSH ECX	
0040B1C8	895424 28	MOV DWORD PTR SS:[ESP+28],EDX	
0040B1CC	56	PUSH ESI	
0040B1CD	8D5424 44	LEA EDX,DWORD PTR SS:[ESP+44]	
0040B1D1	52	PUSH EDX	
0040B1D2	8BCB	MOV ECX,EBX	
0040B1D4	E8 77CEFFFF	CALL _reverse.00408050	
0040B1D9	85C0	TEST EAX,EAX	
0040B1DB	0F85 D6560200	JNZ _reverse.004308B7	
0040B1E1	8B4424 18	MOV EAX,DWORD PTR SS:[ESP+18]	
0040B1E5	8B8B DC010000	MOV ECX,DWORD PTR DS:[EBX+1DC]	
0040B1EB	8D0440	LEA EAX,DWORD PTR DS:[EAX+EAX*2]	
0040B1EE	C1E0 04	SHL EAX,4	
0040B1F1	03C1	ADD EAX,ECX	
0040B1F3	8B4C24 7C	MOV ECX,DWORD PTR SS:[ESP+7C]	
0040B1F7	3B48 20	CMP ECX,DWORD PTR DS:[EAX+20]	
0040B1FA	0F8C AA560200	JL _reverse.004308AA	
0040B200	3B48 24	CMP ECX,DWORD PTR DS:[EAX+24]	
0040B203	0F8F A1560200	JG _reverse.004308AA	
0040B209	8B4C24 18	MOV ECX,DWORD PTR SS:[ESP+18]	
0040B20D	8D5424 58	LEA EDX,DWORD PTR SS:[ESP+58]	
0040B211	52	PUSH EDX	
0040B212	8D4424 3C	LEA EAX,DWORD PTR SS:[ESP+3C]	
0040B216	50	PUSH EAX	
0040B217	51	PUSH ECX	
0040B218	8BCB	MOV ECX,EBX	
0040B21A	E8 510A0000	CALL _reverse.0040BC70	

주소 부분이 빨간 저 두부분이 위에서 부터 비교 , 출력 하는 함수인데 비교하는 함수를 파헤치다보면 다음과 같은 비교문을 볼 수가있다.

00408F11	> 8B06	MOV EAX,DWORD PTR DS:[ESI]	
00408F13	> 3BE8	CMP EBP,EAX	
00408F15	> 7C 7E	JL SHORT _reverse.00408F95	
00408F17	> 8B47 04	MOV EAX,DWORD PTR DS:[EDI+4]	
00408F1A	8B4C24 44	MOV ECX,DWORD PTR SS:[ESP+44]	
00408F1E	40	INC EAX	
00408F1F	8901	MOV DWORD PTR DS:[ECX],EAX	
00408F21	> 8B4424 34	MOV EAX,DWORD PTR SS:[ESP+34]	
00408F25	85C0	TEST EAX,EAX	
00408F27	0F85 46690200	JNZ _reverse.0042F873	
00408F2D	83FB 08	CMP EBX,8	
00408F30	0F84 54690200	JE _reverse.0042F88A	
00408F36	83FB 0A	CMP EBX,0A	
00408F39	0F84 70690200	JE _reverse.0042F8AF	
00408F3F	83FB 05	CMP EBX,5	
00408F42	0F84 7E690200	JE _reverse.0042F8C6	
00408F48	83FB 0B	CMP EBX,0B	
00408F4B	0F84 83690200	JE _reverse.0042F8D4	
00408F51	83FB 0C	CMP EBX,0C	
00408F54	0F85 97FEFFFF	JNZ _reverse.00408DF1	
00408F5A	E9 97690200	JMP _reverse.0042F8F6	
00408F5F	> 83E9 02	SUB ECX,2	
00408F62	83F9 07	CMP ECX,7	
00408F65	77 B0	JA SHORT _reverse.00408F17	
00408F67	FF248D 909290	JMP DWORD PTR DS:[ECX+4+409290]	
00408F6E	> 83F8 03	CMP EAX,3	
00408F71	0F85 25660200	JNZ _reverse.0042F59C	
00408F77	DD45 00	FLD QWORD PTR SS:[EBP]	

EAX=00000014
EBP=00000316

14와 316을 비교해주는데 316을 10진수로 바꿔주면 790이 된다.
이전에 내가 우연히 노가다로 알아낸 답과 같다! :D