0x01 시작하며

역시나 이번에도 어김없이 돌아온 Semtax입니다..
오늘은 앞에 글에 이어 CodeEngn Reverse L02문제를
풀이 하려합니다.. 잘 봐주시기 바랍니다..

0x02 풀이 과정

자.. 역시나 문제를 먼저 보아야 겠지요?

Korea :
패스워드로 인증하는 실행파일이 손상되어 실행이 안되는 문제가 생겼다. 패스워드가 무엇인지 분석하시오

English :
The program that verifies the password got messed up and ceases to execute. Find out what the password is.

음? 문제에 실행파일이 손상 되었다고 나왔네요..
혹시 모르니 한번 실행해 봅시다..


<fig 1>
...어라? 정말로 실행이 되지않습니다.

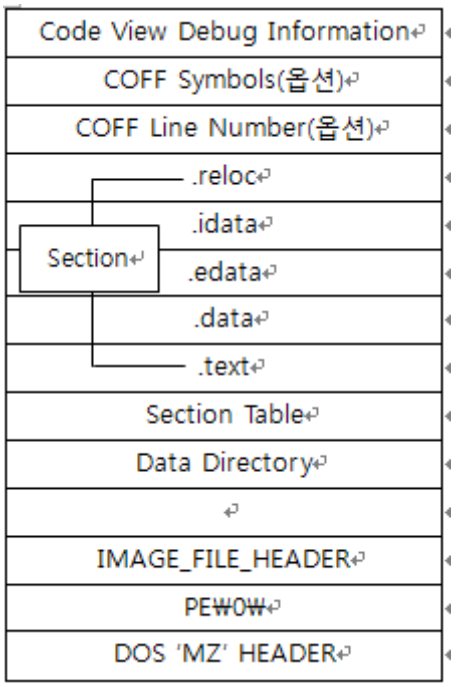
그렇다면 왜 실행이 되지 않는 것 일까요?
그 이유는 Window나 Linux같은 운영체제에는 일정한 규칙을 이루고 있는 실행파일 구조를 가지고 있습니다...
대표적으로 Windows에서는 PE라는 파일 구조를 가지고 있고 Linux에서는 ELF(엘프와는 다르다 엘프와는!)라는
파일구조를 가지고 있습니다.

이러한 파일의 특정부분이 바뀌게 되면 실행이 되지않는데 이러한 경우를 흔히 '파일이 손

상되었다'라고 하는 것 입니다.

흠.. 그렇다면 어떻게 Password를 분석할까요?

우선 Password를 분석하기 전에 PE구조를 '간단히' 보도록 하겠습니다..
PE구조는 아래 그림과 같이 되어있습니다..




<fig 2>

위 그림을 보면 .data나 .text라는 부분을 볼수 있습니다
참고로 .xxx라고 되어있는 부분을 Section이라고 부르는데 일종의 저장공간입니다..
또한 .data 와 .text는 각각 프로그램에 쓰이는 데이터 와 코드 등을 저장 하는 곳입니다.

여기서 우리는 .data영역에 Password가 저장 되어있다는 사실을 유추 해낼 수 있습니다.
그렇다면 저 .data영역을 어떻게 확인 할까요?

컴퓨터에서 쓰이는 NotePad같은 Editor 중에서는 HexEditor라고 하는 편집기가 있습니다.
HexEditor는 일반 Editor와는 다르게 Exe파일을 열으면은 16진수로 표현된 데이터와 옆에 문자(ASCII)로
표현된 데이터가 각각 표시되어 나오는것이 특징입니다.

자, 그렇다면 HexEditor로 열어보면 Password를 알 수 있겠죠?

열어 봅시다.

C.exe | 023C27FA.exe | 023C27FA.exe

| Offset | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00000000 | 4D | 5A | 90 | 00 | 03 | 00 | 00 | 00 | 04 | 00 | 00 | 00 | FF | FF | 00 | 00 |
| 00000010 | B8 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 40 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000020 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000030 | 00 | 0A | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 10 | 00 | 00 | 00 | 10 | 00 | 00 |
| 00000040 | 00 | 20 | 00 | 00 | 00 | 00 | 40 | 00 | 00 | 10 | 00 | 00 | 00 | 02 | 00 | 00 |
| 00000050 | 04 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 04 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000060 | 00 | 50 | 00 | 00 | 00 | 04 | 00 | 00 | 00 | 00 | 00 | 00 | 02 | 00 | 00 | 00 |
| 00000070 | 00 | 00 | 10 | 00 | 00 | 10 | 00 | 00 | 00 | 00 | 10 | 00 | 00 | 10 | 00 | 00 |
| 00000080 | 00 | 00 | 00 | 00 | 10 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000090 | 2C | 20 | 00 | 00 | 3C | 00 | 00 | 00 | 00 | 40 | 00 | 00 | 18 | 03 | 00 | 00 |
| 000000A0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 000000B0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 000000C0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 000000D0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 000000E0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 20 | 00 | 00 | 2C | 00 | 00 | 00 |
| 000000F0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000100 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 2E | 74 | 65 | 78 | 74 | 00 | 00 | 00 |
| 00000110 | 52 | 01 | 00 | 00 | 00 | 10 | 00 | 00 | 00 | 02 | 00 | 00 | 00 | 04 | 00 | 00 |
| 00000120 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 20 | 00 | 00 | 60 |
| 00000130 | 2E | 72 | 64 | 61 | 74 | 61 | 00 | 00 | 38 | 01 | 00 | 00 | 00 | 20 | 00 | 00 |
| 00000140 | 00 | 02 | 00 | 00 | 00 | 06 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000150 | 00 | 00 | 00 | 00 | 40 | 00 | 00 | 40 | 2E | 64 | 61 | 74 | 61 | 00 | 00 | 00 |
| 00000160 | 5C | 02 | 00 | 00 | 00 | 30 | 00 | 00 | 00 | 02 | 00 | 00 | 00 | 08 | 00 | 00 |
| 00000170 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 40 | 00 | 00 | C0 |
| 00000180 | 2E | 72 | 73 | 72 | 63 | 00 | 00 | 00 | 18 | 03 | 00 | 00 | 00 | 40 | 00 | 00 |
| 00000190 | 00 | 04 | 00 | 00 | 00 | 0A | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 000001A0 | 00 | 00 | 00 | 00 | 40 | 00 | 00 | C0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 000001B0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 000001C0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 000001D0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 000001E0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 000001F0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000200 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000210 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |

<fig 3>

쭉~ 확인 하다 보면은 Password로 추정 되는 부분을 확인 할 수 있습니다.

```
00000750  41 44 44 69 61 6C 6F 67  00 41 72 74 75 72 44 65  ADDialog ArturDe
00000760  6E 74 73 20 43 72 61 63  6B 4D 65 23 31 00 00 00  nts CrackMe#1
00000770  00 00 00 00 00 4E 6F 70  65 2C 20 74 72 79 20 61       Nope, try a
00000780  67 61 69 6E 21 00 59 65  61 68 2C 20 79 6F 75 20  gain! Yeah, you
00000790  64 69 64 20 69 74 21 00  43 72 61 63 6B 6D 65 20  did it! Crackme
000007A0  23 31 00 4A 4B 33 46 4A  5A 68 00 00 00 00 00 00  #1 JK3FJZh
```

<fig 4>

Password를 찾으셨겠죠?

0x03 마치며
휴.. 힘들군요..

실행파일 구조에 대한 자세한 내용은 추후에 포스팅 하도록 하겠습니다..