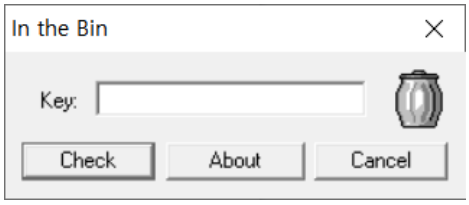
CodeEngn Basic RCE

12. Level 12

Basic RCE L12

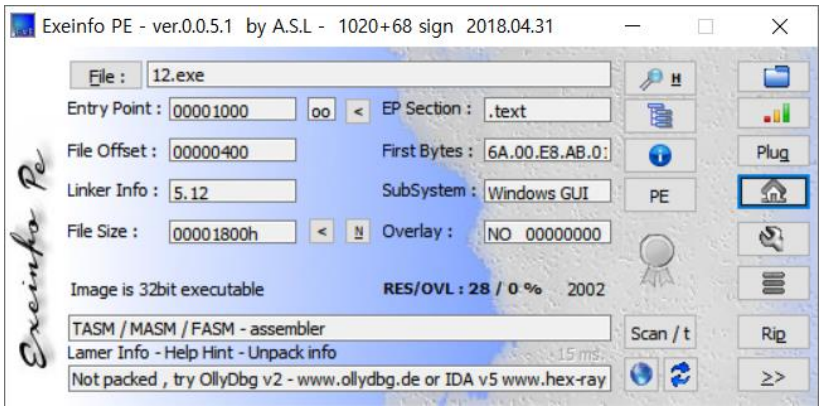
Key를 구한 후 입력하게 되면 성공메시지를 볼 수 있다
이때 성공메시지 대신 Key 값이 MessageBox에 출력 되도록 하려면 파일을 HexEdit로 오픈 한 다음 0x???? ~ 0x???? 영역에 Key 값을 overwrite 하면 된다.
문제 : Key값과 + 주소영역을 찾으시오
Ex) 7777777????????



프로그램 실행 화면이다.

key값을 구한 후 입력하게 되면 성공메시지를 볼 수 있다고 한다.

먼저 exeinfo로 패킹여부를 확인해보자.

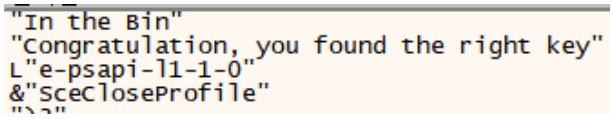


Not packed.

x64dbg로 12.exe 파일을 까보자.

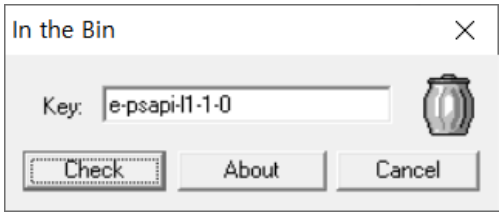
먼저 key값을 찾아야 할 것 같다.

다음을 찾기 > 모든 모듈 > 문자열 참조



"e-psapi-l1-1-0"

key 값처럼 보이는 문자열이 보인다. 한 번 입력해보자.



아닌 것 같다.

그러면 key 값이 정확했을 때 출력되는 문자열을 x64dbg로 자세히 봐보자.

cmp 함수로 eax값과 7A2896BF를 비교한 후 같지않다면 jne 함수로 인해 401098로 점프한다.

jne : jump if not equal 두 값이 같지 않다면 점프하라.

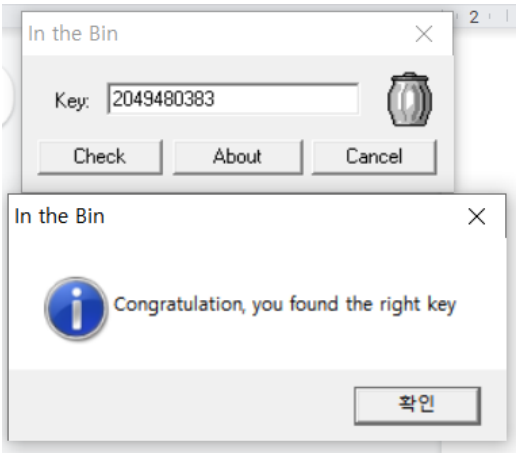
그러면 eax값이 7A2896BF와 같아야한다. 즉, eax-7A2896BF=0.

eax값은 내가 입력하는 값일 것이다.

7A2896BF를 입력하면 성공 문자열이 뜨지않는 것을 보니 10진수로 바꿔줘야하는 것 같다.

7A2896BF(16진수) => 2049480383(10진수)

프로그램 key값에 넣어보자.



성공 메시지 박스가 출력된다.

하지만 문제에서는 성공 메시지 출력 대신 key값을 출력하라고 한다.

HxD를 열어 성공 문자열을 찾아보자.

"Congratulation, you found the right key"

```
00000D30  49 6E 20 74 68 65 20 42 69 6E 00 43 6F 6E 67 72  In the Bin.Congr
00000D40  61 74 75 6C 61 74 69 6F 6E 2C 20 79 6F 75 20 66  atulation, you f
00000D50  6F 75 6E 64 20 74 68 65 20 72 69 67 68 74 20 6B  ound the right k
00000D60  65 79 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ey..............
```

이 부분을 2049480383으로 바꾸면 될 것 같다.

수정할 때는 16진수 ASCII 코드로 수정해야한다.

2 => 32

0 => 30

4 => 34

9 => 39

4 => 34

8 => 38

0 => 30

3 => 33

8 => 38

3 => 33

```
00000D30  49 6E 20 74 68 65 20 42 69 6E 00 32 30 34 39 34  In the Bin.20494
00000D40  38 30 33 38 33 00 00 00 00 00 00 00 00 00 00 00  80383...........
```

바꾼 주소 영역은 0D3B~0D45이다.

key값은 20494803830D3B0D45.