

Binary JBU-CTF 2020

Jaehyeon Cho

INDEX

01.문제 소개

- SCP-RPG
- 플레이
- 개발

02.문제 풀이

- 예1) 메모리 변조
- 예2) 리버싱

1

문제 소개

SCP-RPG / 플레이 방법 / 개발

01 문제 소개

SCP-RPG



> SCP_RPG

분야 Binary - Reversing

분류 EXE(32bit)

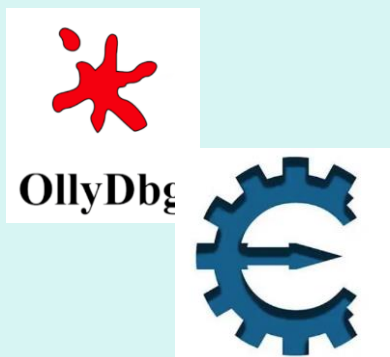
난이도 ★★★★★☆

재미 ★★★★★★

특징

- 텍스트형 RPG 게임
- 7개 스테이지 클리어하면 플래그 획득
- 일반적인 플레이로는 절대 못 갠
- 정말 다양한 방법으로 풀이가 가능할 것으로 예상

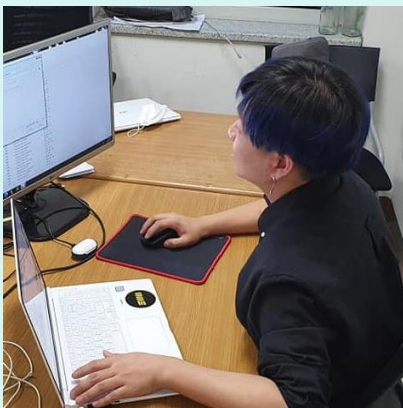
4가지의 출제 의도



툴 사용법 숙지

OllyDBG, X64dbg, CheatEngine...

다양한 툴 사용 가능



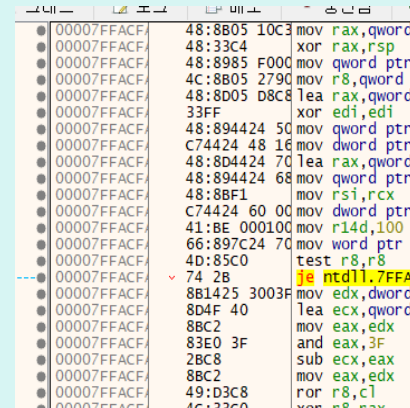
분석 능력 상승

깊은 분석을 통해
분석 능력 상승 유도



브레인 스토밍

생각치 못한 다양한 풀이 방법이
등장할 것으로 예상
(태현이, 다영이 사례)



리버싱 테크닉 단련

리버싱으로 풀고자 하면
소소한 테크닉이 요구될 수 있음

01 문제 소개

플레이

7개 스테이지, 클리어 시 플래그



Stage 1

체력 : 100
공격력 : 5



체력 : 100
공격력 : 10



승리 조건 : 상대의 체력을 0으로 만듦

01 문제 소개

플레이

2가지 선택 가능



Stage 1

체력 : 100
공격력 : 5



체력 : 100
공격력 : 10



공격? or 육성?

(1) 공격 선택 시



Stage 1

체력 : 100-10
공격력 : 5



체력 : 100-5
공격력 : 10



체력 = 체력 - 상대의 공격력

(2) 육성 선택 시



Stage 1

체력 : 90+1
공격력 : 5+1



체력 : 95
공격력 : 10

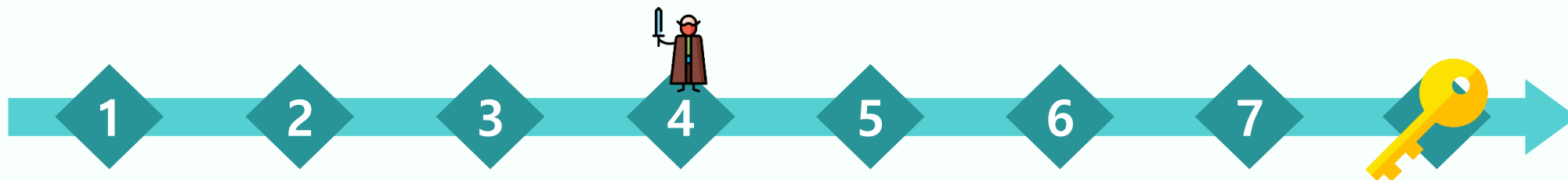


체력 +1, 공격력 +1(50번 제한)

01 문제 소개

플레이

갈수록 강력해지는 보스

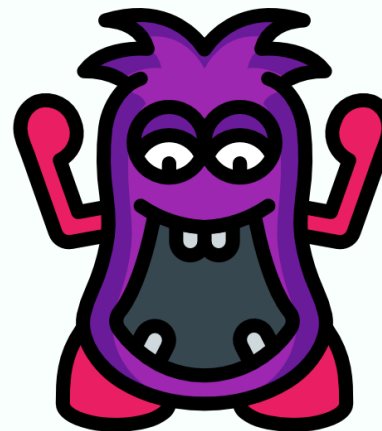


Stage 4

체력 : 100
공격력 : 5



체력 : 1000
공격력 : 50



갈수록 강력해지는 보스



Stage 7

체력 : 100
공격력 : 5



체력 : 50000
공격력 : 10000



01 문제 소개

개발

Stage1 ~ 7(){

1. 게임 구현

2. 이기면 복호화에 필요한 키가 2개씩 더해짐

}

Main(){

1. 스테이지 및 암호화된 키 관리

2. 7개 클리어 시 각스테이지에서 얻은 키로 복호화(플래그)

}

플래그는 AES-128 암호화해둔 상태로
선언/사용하여 사전에 키 노출 방지

2

문제 풀이

예1) 메모리 변조 / 예2) 리버싱

수백가지 풀이 법 존재 가능! 여기서 2가지만 다룰 예정

게임 핵 같이 메모리 변조

> 체력 변조, 공격력 변조 등

평소 문제 풀 듯 리버싱

> 육성 시 올라가는 값 변조, 무조건 clear 등

암호 문제 풀 듯

> 각 함수에서 키 값만 가져와서 복호화

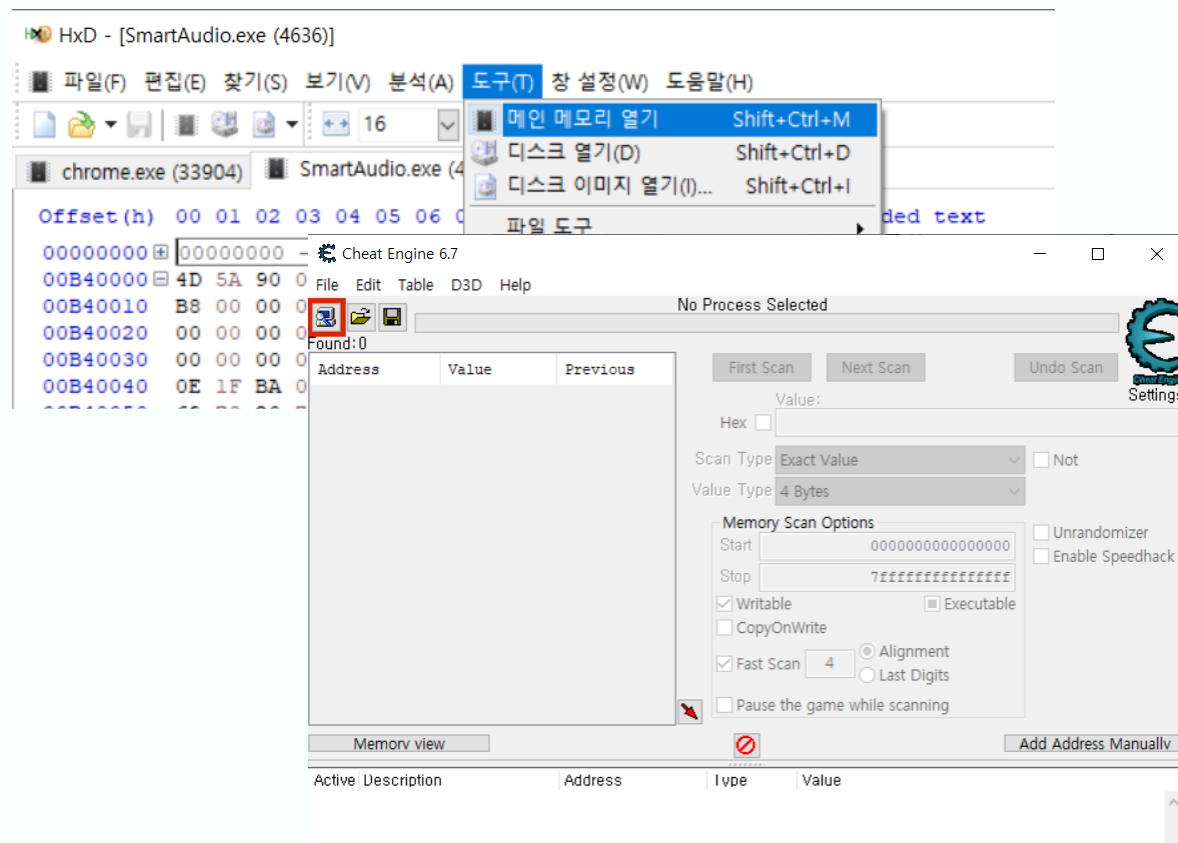
메모리 해킹, 그리고 치트엔진?

메모리 해킹 >

RAM에 저장되는 데이터를 탈취/조작하는 기법

치트 엔진 >

시스템 메모리 변동을 읽어서
손쉽게 게임의 변수를 찾아내고 변조시킬 수 있는 툴
(실제 최근 게임 해킹에도 많이 쓰임)

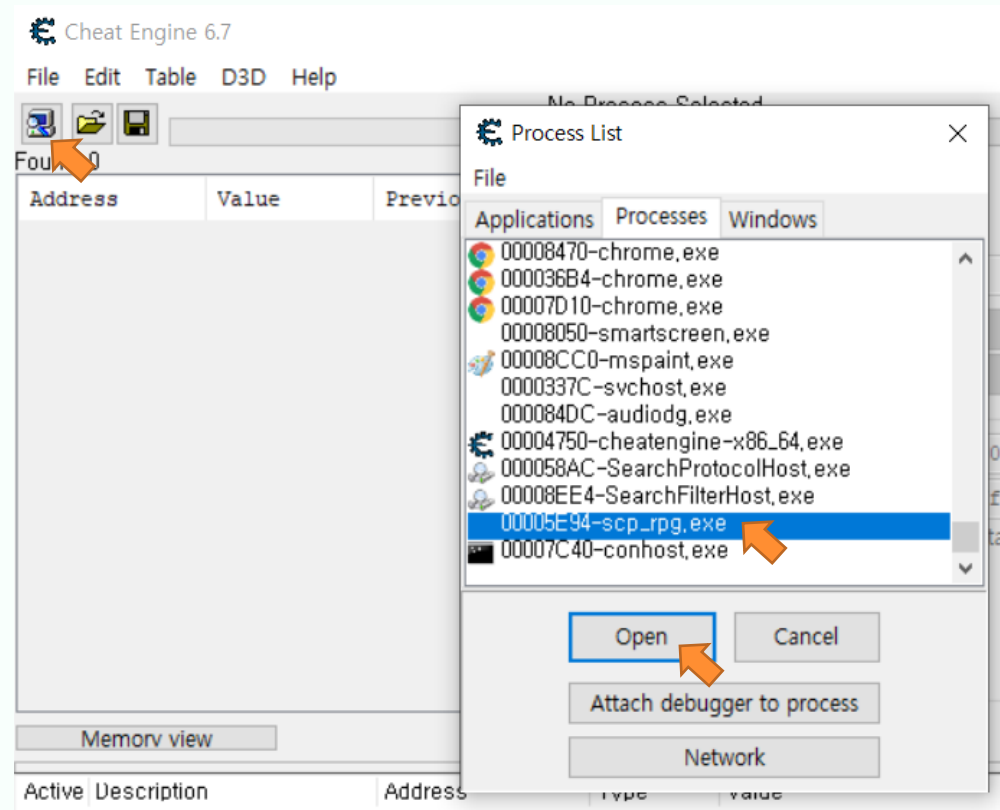


(1) 실행, 프로세스 붙임

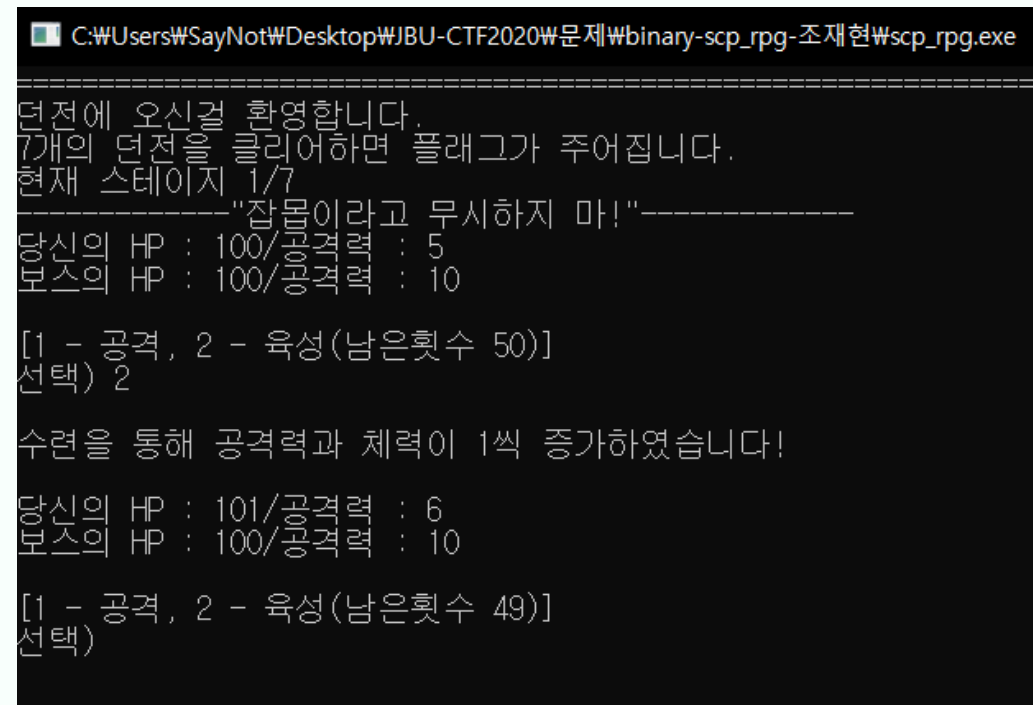
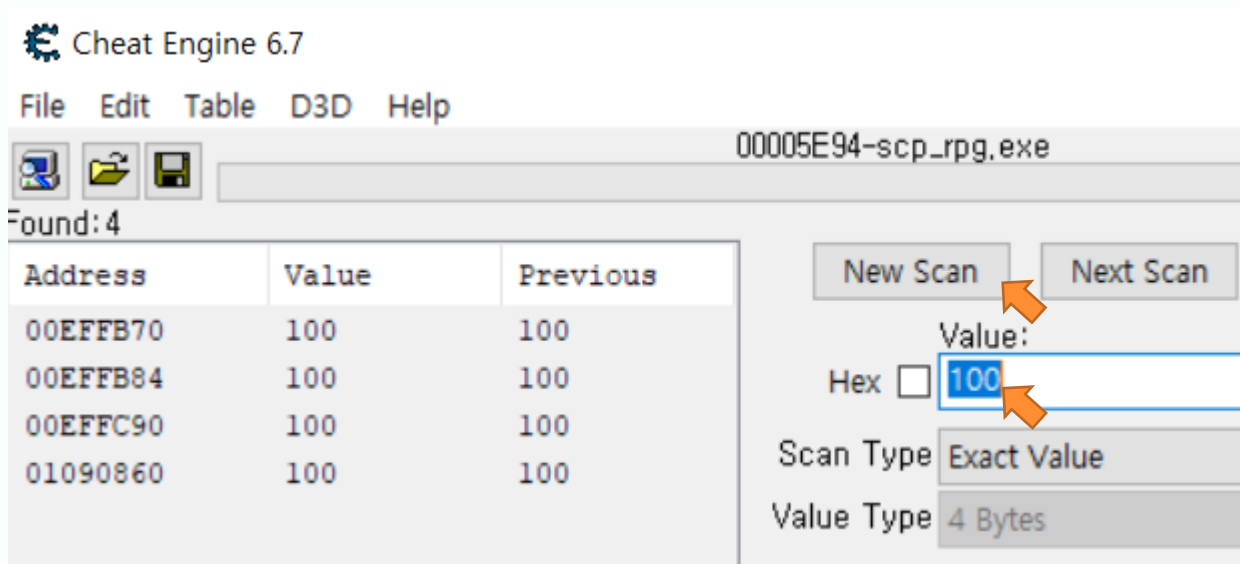
```
scp_rpg.exe 2020-09-29 오후 12:00 응용 프로그램
C:\Users\SayNot\Desktop\JBU-CTF2020\문제\binary-scp_rpg-조재현\scp_rpg.exe

=====
던전에 오신걸 환영합니다.
7개의 던전을 클리어하면 플래그가 주어집니다.
현재 스테이지 1/7
-----"잡몹이라고 무시하지 마!"-----
당신의 HP : 100/공격력 : 5
보스의 HP : 100/공격력 : 10

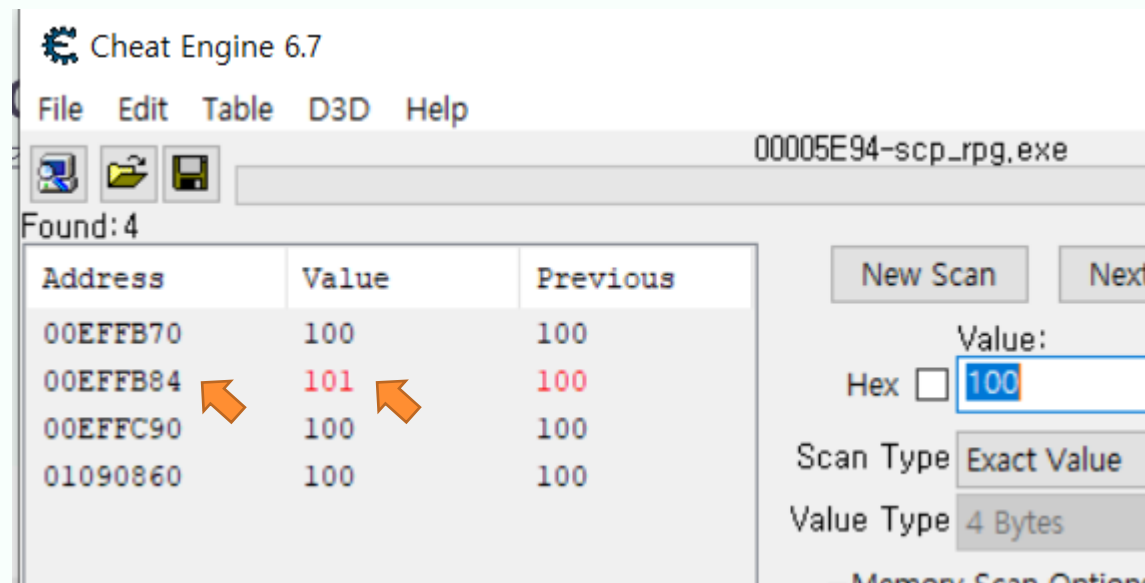
[1 - 공격, 2 - 육성(남은횟수 50)]
선택)
```



(2) 체력 값인 100 스캔, 육성하기

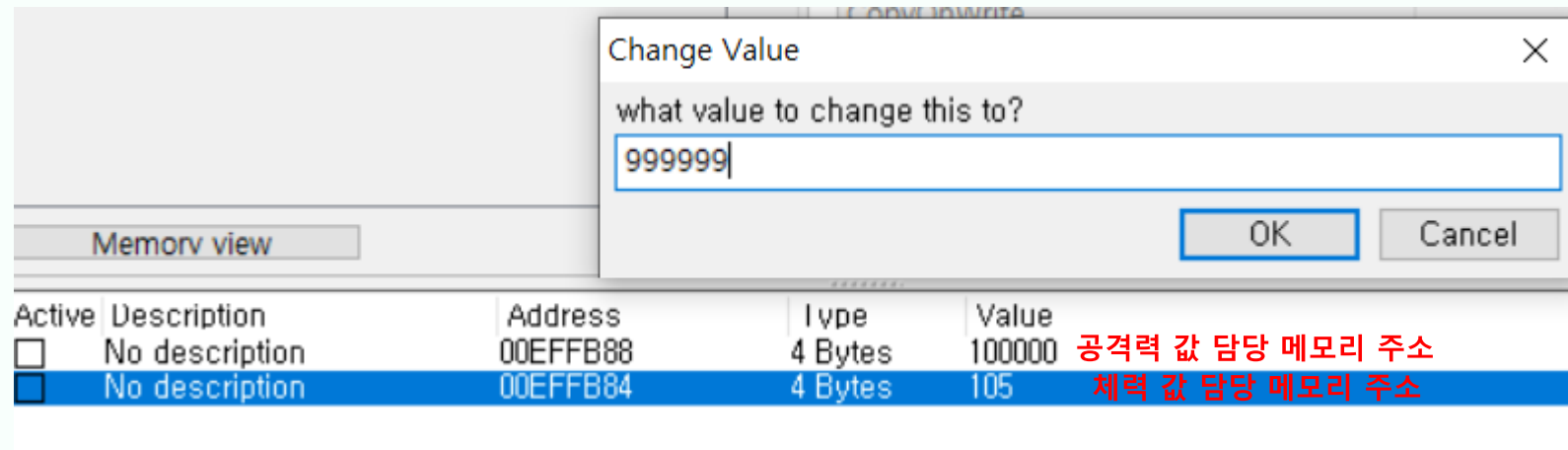


- (3) 바뀐 값의 주소가 체력 값을 나타냄, 저장
- (4) 공격력도 똑같이 진행(6 검색, 육성, 저장)



Memory view					Add Address Manually	
Active	Description	Address	Type	Value		
<input type="checkbox"/>	No description	00EFFB88	4 Bytes	10	공격력 값 담당 메모리 주소	
<input type="checkbox"/>	No description	00EFFB84	4 Bytes	105	체력 값 담당 메모리 주소	

(5) 체력, 공격력 value 수정



(6) 공격하면 바로 게임 클리어

당신의 HP : 105/공격력 : 10
보스의 HP : 100/공격력 : 10

[1 - 공격, 2 - 육성(남은횟수 45)]
선택) 1

플레이어와 보스가 서로 공격을 주고받았습니다!

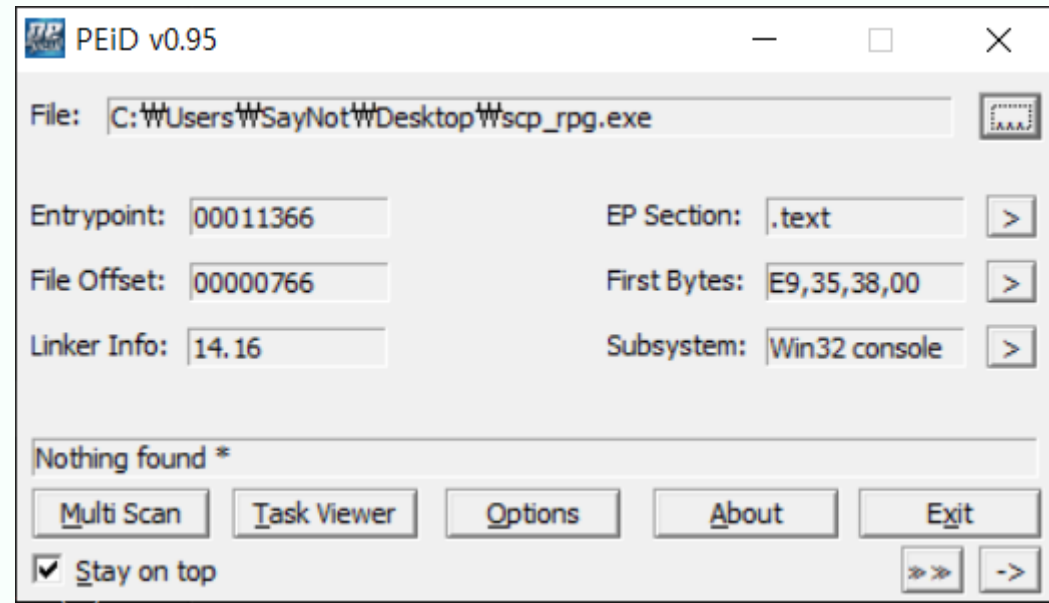
=====

던전에 오신걸 환영합니다.
7개의 던전을 클리어하면 플래그가 주어집니다.
현재 스테이지 2/7
-----"운동 좀 했다고!"-----

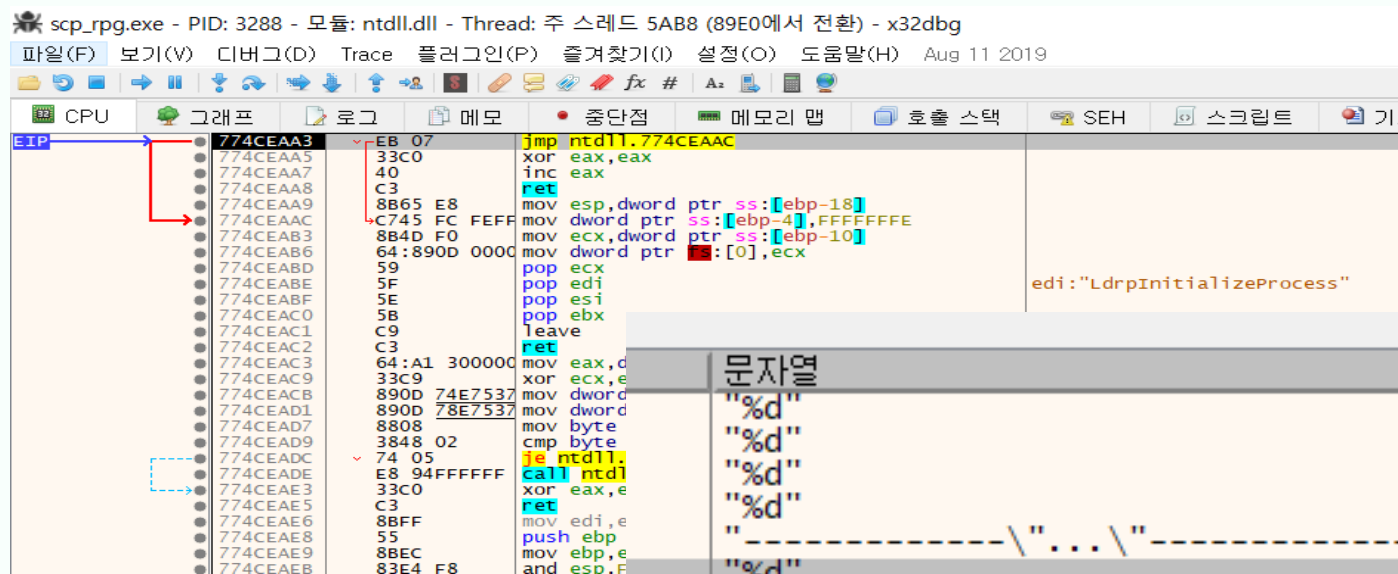
당신의 HP : 100/공격력 : 5
보스의 HP : 300/공격력 : 15

[1 - 공격, 2 - 육성(남은횟수 50)]
선택)

(1) 정보 확인(패킹여부, 문자열 등)



(2) x32dbg 열기, 분석 시작



문자열

"%d"

"%d"

"%d"

"%d"

"-----\"...\"-----\n"

"%d"

"\n\"...\" \n\n"

"%d"

"===== \n"

"'%s' \n"

"===== \n"

"Stack area around _alloca memory reserved by this function is corru"

이 과정이 시간 오래 걸림

(3) 분석으로 스테이지 함수 찾기

00EC7910	55	push ebp	main.cpp:5
00EC7911	8BEC	mov ebp,esp	
00EC7913	81EC 0001000	sub esp,100	
00EC7919	53	push ebx	
00EC791A	56	push esi	
00EC791B	57	push edi	
00EC791C	8DBD 00FFFFFF	lea edi,dword ptr ss:[ebp-100]	
00EC7922	B9 40000000	mov ecx,40	40: '@'
00EC7927	B8 CCCCCCCC	mov eax,CCCCCCCC	
00EC792C	F3:AB	rep stosd	
00EC792E	A1 04C0EC00	mov eax,dword ptr ds:[<security_cookie>]	
00EC7933	33C5	xor eax,ebp	
00EC7935	8945 FC	mov dword ptr ss:[ebp-4],eax	
00EC7938	B9 0DE0EC00	mov ecx,scp_rpg.ECE00D	main.cpp:15732480
00EC793D	E8 F898FFFF	call scp_rpg.EC123A	
00EC7942	C745 F4 6400	mov dword ptr ss:[ebp-C],64	main.cpp:6, 64: 'd'
00EC7949	C745 E8 0A00	mov dword ptr ss:[ebp-18],A	main.cpp:7, A: '\n'
00EC7950	C745 DC 0000	mov dword ptr ss:[ebp-24],0	main.cpp:8
00EC7957	C745 D0 3200	mov dword ptr ss:[ebp-30],32	main.cpp:9, 32: '2'
00EC795E	68 AC9DEC00	push scp_rpg.EC9DAC	main.cpp:10
00EC7963	E8 ED96FFFF	call scp_rpg.EC1055	
00EC7968	83C4 04	add esp,4	
00EC796B	837D 08 00	cmp dword ptr ss:[ebp+8],0	main.cpp:11
00EC796F	7F 0A	jg scp_rpg.EC797B	
00EC7971	837D F4 00	cmp dword ptr ss:[ebp-C],0	
00EC7975	0F8E 9201000	jle scp_rpg.EC7B0D	
00EC797B	8B45 0C	mov eax,dword ptr ss:[ebp+C]	main.cpp:12
00EC797E	50	push eax	
00EC797F	8B4D 08	mov ecx,dword ptr ss:[ebp+8]	
00EC7982	51	push ecx	
00EC7983	68 EC9DEC00	push scp_rpg.EC9DEC	
00EC7988	E8 C896FFFF	call scp_rpg.EC1055	
00EC798D	83C4 0C	add esp,C	
00EC7990	8B45 E8	mov eax,dword ptr ss:[ebp-18]	main.cpp:13
00EC7993	50	push eax	
00EC7994	8B4D F4	mov ecx,dword ptr ss:[ebp-C]	

(4) 육성 누르고, F8로 한 줄씩 실행

레지스터 `eax`에 1을 더하고 있다!

```

C:\Users\SayNot\Desktop\scp_rpg.exe
=====
던전에 오신걸 환영합니다.
7개의 던전을 클리어하면 플래그가 주어집니다.
현재 스테이지 1/7
-----"잡몹이라고 무시하지 마!"-----
당신의 HP : 100/공격력 : 5
보스의 HP : 100/공격력 : 10

[1 - 공격, 2 - 육성(남은횟수 50)]
선택) 2
  
```

00EC7A6B	83C0 01	add eax,1
00EC7A6E	8945 08	mov dword ptr ss:[ebp+8],eax
00EC7A71	8B45 0C	mov eax,dword ptr ss:[ebp+C]
00EC7A74	83C0 01	add eax,1
00EC7A77	8945 0C	mov dword ptr ss:[ebp+C],eax
00EC7A7A	8B45 D0	mov eax,dword ptr ss:[ebp-30]
00EC7A7D	83E8 01	sub eax,1
00EC7A80	8945 D0	mov dword ptr ss:[ebp-30],eax
00EC7A83	EB 11	jmp scp_rpg.EC7A96
00EC7A85	68 D89EEC00	push scp_rpg.EC9ED8
00EC7A8A	E8 C695FFFF	call scp_rpg.EC1055

(5) value 변경

1을 2로 바꿔보자.

● 00EC7A68	8B45 08	mov eax, dword ptr ss:[ebp+
● 00EC7A6B	83C0 02	add eax, 2
● 00EC7A6E	8945 08	mov dword ptr ss:[ebp+8], e
● 00EC7A71	8B45 0C	mov eax, dword ptr ss:[ebp+
● 00EC7A74	83C0 02	add eax, 2
● 00EC7A77	8945 0C	mov dword ptr ss:[ebp+8], e
● 00EC7A7A	8B45 D0	mov eax, dword ptr ss:[ebp+
● 00EC7A7D	83E8 01	sub eax, 1
● 00EC7A80	8945 D0	mov dword ptr ss:[ebp+8], e
● 00EC7A83	EB 11	jmp scp_rpg
● 00EC7A85	68 D89EEC00	push scp_rpg

add eax, 0x2

(6) 7마리 보스 때려잡기.

당신의 HP : 101/공격력 : 6
보스의 HP : 100/공격력 : 10

[1 - 공격, 2 - 육성(남은횟수 49)]
선택) 2

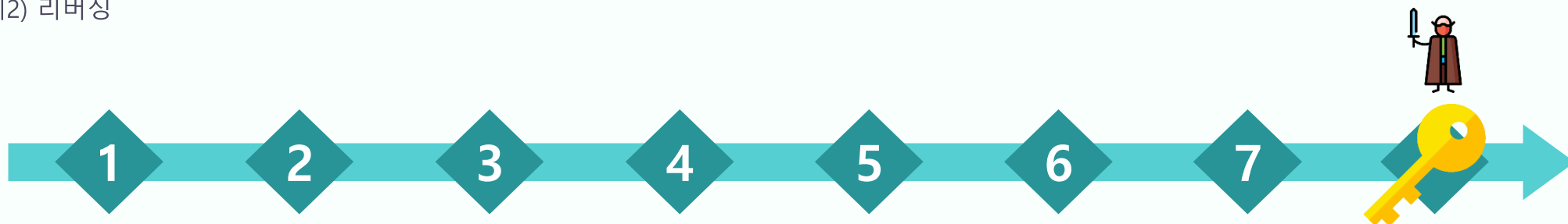
수련을 통해 공격력과 체력이 1씩 증가하였습니다!

당신의 HP : 103/공격력 : 8 **스탯이 2씩 증가했다!!!!**
보스의 HP : 100/공격력 : 10

[1 - 공격, 2 - 육성(남은횟수 48)]
선택)

02 문제 풀이

예2) 리버싱



```
=====
던전에 오신걸 환영합니다.
7개의 던전을 클리어하면 플래그가 주어집니다.
현재 스테이지 7/7
-----"돌아갈 시간이다."-----
당신의 HP : 100000/공격력 : 50000
보스의 HP : 50000/공격력 : 10000

[1 - 공격, 2 - 육성(남은횟수 50)]
선택) 1

플레이어와 보스가 서로 공격을 주고받았습니다!

축하합니다. 모든 던전을 클리어하셨습니다.
'scpCTF{f1na1ly_gam3_ov3r}'
```



+ 추가 문제 두쪽 요약

Challenge

0 Solves

×


producer

500

SCP_조재현

...
압축 파일의 비밀번호가 기억이 나질 않습니다!
...

잠깐, 모니터 옆에 포스트잇이 눈에 들어오네요.
[id : smith/pw : scp292912]
[id : tmaltm/pw : scp825392]
[project_edm.zip/pw : scp175234]

 project.zip

scpCTF{...}

Submit

> producer

분야

Forensic – Brute Force

분류

ZIP File

난이도

★★★★☆

재미

★★★★☆

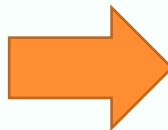
특징

- 비밀번호 걸려있는 압축파일 던져 줌. 풀면 플래그.
- 문제에 포스트잇 힌트로 알 수 있는 PW 사용 패턴
- 브루트포스 쓰는 문제

+ 추가 문제 두쪽 요약

PW: scp??????

project_music.zip



```
import zipfile
from itertools import product

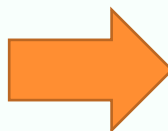
zip_file = "project_music.zip"
zip_file = zipfile.ZipFile(zip_file)
ints = '0123456789'

to_attempt = product(ints, repeat=6)

for attempt in to_attempt:
    brute = 'scp'+''.join(attempt)
    print(brute)
    try:
        zip_file.extractall(pwd=brute)
    except:
        continue
    else:
        print("Password Found: ", brute)
        exit(0)
```



```
scp771997
scp771998
scp771999
scp772000
scp772001
scp772002
scp772003
scp772004
scp772005
scp772006
scp772007
scp772008
scp772009
scp772010
scp772011
scp772012
scp772013
scp772014
scp772015
scp772016
scp772017
scp772018
scp772019
scp772020
('Password Found: ', 'scp772020')
```



```
drwxr-xr-x 2 root root 4096 Oct 2 20:05 project_music
-rw-r--r-- 1 root root 1284 Oct 2 20:02 project_music.zip
```

```
root@kali:~/ctf/project_music# ls -l
total 4
-rw-r--r-- 1 root root 0 Oct 2 20:05 bass.mp3
-rw-r--r-- 1 root root 78 Oct 2 20:05 code.txt
-rw-r--r-- 1 root root 0 Oct 2 20:05 guitar.mp3
-rw-r--r-- 1 root root 0 Oct 2 20:05 kick.mp3
-rw-r--r-- 1 root root 0 Oct 2 20:05 snare.mp3
-rw-r--r-- 1 root root 0 Oct 2 20:05 vocal.mp3
root@kali:~/ctf/project_music# cat code.txt
A G Am E
A G Am E
A G Am E
A G Am E

Umm..
Song name is..
"scpCTF{A_G_Am_E}"
```

You Win.
감사합니다.