Root-me

ELF_FAKE_INSTRUCTION Write Up

Author : hideroot(M.O.K)

Data : 2017/11/20

이번 문제는 푸는데 조금 빡쳤다. ~~더러운 UTF-8~~

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  void *dest; // ST20_4@4
  int result; // eax@4
  int v5; // edx@4
  const char **v6; // [sp+10h] [bp-9Ch]@1
  char v7; // [sp+1Eh] [bp-8Eh]@4
  char v8; // [sp+82h] [bp-2Ah]@4
  int v9; // [sp+A0h] [bp-Ch]@1
  int *v10; // [sp+A8h] [bp-4h]@1

  v10 = &argc;
  v6 = argv;
  v9 = *MK_FP(__GS__, 20);
  if ( argc != 2 )
  {
    printf("(*) -Syntaxe: %s [password] Wn", *argv);
    exit(0);
  }
  dest = malloc(0x1Du);
  memcpy(dest, "_0cGj35m9V5T3쵈8CJ09H95h3xdh", 31u);
  memset(&v7, 0, 0x64u);
  memcpy(&v7, "_Celebration", 0xDu);
  *((_BYTE *)dest + 5) = 99;
  *((_BYTE *)dest + 22) = 0;
  function_ptr_2175 = (int (__cdecl *)(_DWORD, _DWORD))WPA;
  strcpy(&v8, v6[1]);
  *((_BYTE *)dest + 8) = 95;
  *((_BYTE *)dest + 9) = 46;
  result = function_ptr_2175(&v8, dest);
  v5 = *MK_FP(__GS__, 20) ^ v9;
  return result;
}
```

먼저 문제를 받은 후에 뜯어보자. 문제명이 fake-instruction 이니까 왠지 함정이 있을 것 같은 느낌을 갖고 들어가보자. 메인 에서 바로 딱 보이는건 Syntaxe(usage)가 보인다. 그 밑으로 동적할당을 받고 이상한 문자열들을 카피하고 세팅하고 Celebration을 다시 카피하고 이상한짓을 하는것이 보일 것이다. 그리고 그밑에 ptr_2175라고 해서 함수 포인터가 들어가 있다 옆에 이름은 WPA로 되어 있다. 일단 _Celebration을 넣어보자. 당연히 안된다. 자 그럼 저 이상한 문자열은 도저히 모르겠으니까 의심가는 WPA로 들어가보자

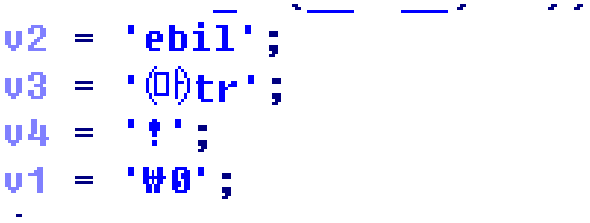
```
void __cdecl __noreturn WPA(char *s1, char *s2)
{
  s2[11] = 13;
  s2[12] = 10;
  puts("V챕rification de votre mot de passe..");
  if ( !strcmp(s1, s2) )
    blowfish();
  RS4();
}
```

WPA로 들어가면 strcmp로 문자열 비교를 한다. 지금 까지 계속 crack문제를 풀다보면 느낌이 온다. 이부분을 분석하면 답이 나온다. 일단 blowfish(이것에 대해서 좀 설명하자면 DES 암호를 대체하려고 내놓은 알고리즘 중에 하나다.) 함수를 들어가보자.

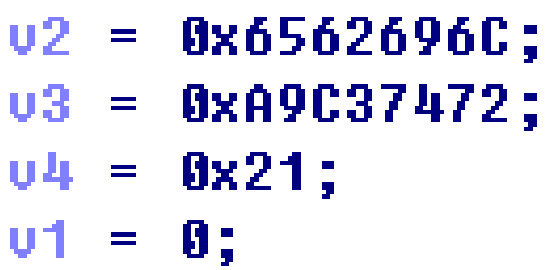
```
void __noreturn blowfish()
{
  char *v0; // ST14_4@3
  unsigned int v1; // [sp+Ch] [bp-4Ch]@1
  int v2; // [sp+18h] [bp-40h]@1
  int v3; // [sp+1Ch] [bp-3Ch]@1
  int v4; // [sp+20h] [bp-38h]@1
  char v5[23]; // [sp+24h] [bp-34h]@2
  int v6; // [sp+3Bh] [bp-1Dh]@3
  int v7; // [sp+3Fh] [bp-19h]@3
  int v8; // [sp+43h] [bp-15h]@3
  int v9; // [sp+47h] [bp-11h]@3
  int v10; // [sp+4Bh] [bp-Dh]@3
  int v11; // [sp+4Fh] [bp-9h]@3
  char v12; // [sp+53h] [bp-5h]@3
  int v13; // [sp+54h] [bp-4h]@1

  v13 = *MK_FP(__GS__, 20);
  v2 = 1700948332;
  v3 = -1446808462;
  v4 = 33;
  v1 = 0;
  do
  {
    *(_DWORD *)&v5[v1] = 0;
    v1 += 4;
  }
  while ( v1 < 0x14 );
  v0 = &v5[v1];
  *(_WORD *)v0 = 0;
  v0[2] = 0;
  v6 = 1197682783;
  v7 = 1832215402;
  v8 = 1412771423;
  v9 = 948421427;
  v10 = -1020245437;
  v11 = 961034624;
  v12 = 0;
  printf("'+) Authentification r챕ussie...Wn U'r root! WnWn sh 3.0 # password: %sWnWr", &v2);
  exit(0);
}
```

함수에 들어가보면 printf로 password: %s 가 보인다. 아 이부분만 알아내면 동적분석 안해도 패스워드를 알 수 있겠다는 생각이 든다. 그래서 v2를 살펴보았다.

```
v12 = 0;
printf("'+) Authentification r챕ussie...Wn U'r root! WnWn sh 3.0 # password: %sWnWr", &v2);
exit(0);
```



문자열로 바꿔보니 libert??가 나온다. 아무래도 UTF-8느낌이 난다. 나는 여기서 20분을 삽질을 했다. ~~(출제자 국적이 짜증나기는 이번이 처음)~~



다시 16진수로 바꿔서 보니 ₩xc3₩a9 이라는 문자열인데.. ASCII에서는 이딴 문자는 존재하지 않는다. 그래서 UTF-8로 찾아보았다.

U+00E9	é	₩xc3₩xa9	&#xE9;	é	LATIN SMALL LETTER E WITH ACUTE

후... 이거 찾아보고 진짜 빡쳤다. e첨자(?)인데 이게 입력이 계속 안돼서 엄청 애먹었다.

답은 liberté! 로 넣어야 성공한다.