


Angstrom CTF 2021

Jailbreak

 *Challenge's description:* Clam was arguing with kmh about whether including 20 pyjails in a ctf is really a good idea, and kmh got fed up and locked clam in a jail with a python! [Can you help clam escape?](#)
Source file được tìm thấy tại [đây](#) nếu server down

Phân tích src và workflow của challenge

Hiểu tổng quát về chương trình

```
1  angstromCTF_2021:/>$../jailbreak
2
3  Welcome to clam's daring jailbreak! Please keep your hands and feet inside
4  What would you like to do?
```

- Thử running chương trình, ta sẽ thấy một dòng thông báo thể hiện ý tưởng của tác giả cho challenge: chúng ta phải làm gì đó để giải cứu cho clam đang bị kmh nhốt vào tù :<
- Thực hiện phân tích file ELF bằng IDA, dưới đây là một đoạn code được cắt từ cửa sổ decompile của IDA Pro ver:

```
1  int main()
2  {
3
4  //...[REDACTED]..
5
6  sub_1620(1LL);
7  while ( 1 )
8  {
9      v10 = sub_15A0(0);
10     puts(v10);
```

```

11     free(v10);
12     if ( !fgets(v31, 256, stdin) )
13         goto LABEL_24;
14     v31[strcspn(v31, "\n")] = 0;
15     if ( v5 )
16         break;
17     v6 = sub_15A0(2);
18     v7 = strcmp(v31, v6);
19     free(v6);
20     if ( v7 )
21     {
22         v17 = sub_15A0(6);
23         v18 = strcmp(v31, v17);
24         free(v17);
25         if ( !v18 )
26         {
27             sub_1620(7LL);
28 LABEL_24:
29             sub_1620(5LL);
30             goto LABEL_25;
31         }
32
33     //...[REDACTED]..
34
35 }

```

- Chúng ta sẽ thấy một vài điểm khá thú vị:
 - 2 hàm **sub_15A0()** và **sub_1620()** được gọi lặp đi lặp lại nhiều lần trong main
 - ngoài ra **sub_1620()** thật chất là sự kết hợp của **put()** và **sub_15A0()**, trong đó **sub_15A0()** là hàm nhận vào một số nguyên và trả về một chuỗi:

Phân tích hàm sub_15A0()


```

v1 = dword_4080[a1];
v2 = dword_4080[a1 + 1] - v1;
v3 = malloc(v2 + 1);
v3[v2] = 0;
v4 = v3;
if ( v2 > 0 )
{
    v5 = a1;
    v6 = 0LL;
    do
    {
        v7 = v5 ^ byte_4100[v1 + v6];
        v4[v6++] = v7;
        v5 = v5 * v7 + 17 * a1;
    }
    while ( v2 != v6 );
}
return v4;

```

pseudo code ban đầu của hàm sub_15A0

- Sau khi phân tích hàm này, ta sẽ thấy:
 - có 2 mảng **dword_4080** và **byte_4100**, dễ thấy **dword_4080** sẽ chứa index đầu tiên (**v1**) của tham số **a1** trong mảng lớn **byte_4100** và **v2** là index cuối
 - Sử dụng IDA Python để trích xuất dữ liệu 2 mảng trên từ file thực thi và sau đó re-implement lại hàm **sub15A0(int a1)**, ta sẽ sinh ra tất cả các chuỗi được trả về với tham số a1 tương ứng

 Chúng ta có thể xác định được các giá trị của tham số a1, vì $0 \leq a1 < \text{size}(\text{mảng } \text{dword_4080}) - 1$ (vì có $v2 = \text{dword_4080}[a1 + 1] - v1$)

- IDAPython Script ở [đây](#)
- Output từ IDA:

```

1  0 What would you like to do?
2  1 Welcome to clam's daring jailbreak! Please keep your hands and feet insi
3  2 look around
4  3 You look around your cell and you see an old bed along with a snake. Out
5  4 You're speaking nonsense. Cut that out.
6  5 It seems that clam won't be escaping today.
7  6 sleep
8  7 You lie down on the bed and close your eyes. You then get bitten by the
9  8 You look around your cell and you see an old bed along with a snake. Out
10 9 knock on the wall
11 10 You here a muffled voice from the other side saying "I shouldn't have b
12 11 pry the bars open
13 12 You start prying the prison bars open. Realizing this is unintended, km
14 13 You start prying the prison bars open. A wide gap opens and you slip th
15 14 throw the snake at kmh
16 15 pick the snake up
17 16 You pick the snake up.
18 17 You throw the snake at kmh and watch as he runs in fear.
19 18 You look around and see that kmh has already made the jail contrived! T
20 19 press the red button
21 20 press the green button
22 21 You pressed the red button. Nothing changed.
23 22 You pressed the green button. Nothing changed.
24 23 bananarama
25 24 For some reason, a flag popped out of the wall, and you walk closer to
26 25 flag.txt
27 26 r
28 27 Couldn't find flag file.
29 28 Attached to the flag is a key to the front door. It looks like clam is
30 29
31 30


```

Passing this challenge

- Sau khi đã có các chuỗi trả về từ hàm **sub15A0** với các tham số tương ứng, ta sẽ dễ dàng hiểu chương trình hơn.
- Tóm tắt workflow:
 - Thực hiện hành động thích hợp để giải cứu **clam**
 - Ngoài hành động cuối cùng "**bananarama**" là, còn phải set một số bằng 1337(bằng cách thực hiện hành động "press the red button", "press the green button" số

lần thích hợp) thì mới mở được flag.

```
1  Thứ tự các hành động như sau:  
2  
3  pick the snake up  
4  throw the snake at kmh  
5  pry the bars open  
6  press the red button  
7  press the green button  
8  press the red button  
9  press the red button  
10 press the green button  
11 press the green button  
12 press the green button  
13 press the red button  
14 press the red button  
15 press the green button  
16 bananarama
```

 Vì flag challenge này trên server, vì vậy để test có thể tạo file flag.txt ở local để test.