CS 395

G01167216

Nghi Vi

Final Project Writeup

Nihaal's Revenge CD validator

I. Reconnaissance

The way to solve this binary is through giving it the right CD key. Opening the binary in Ghidra, we rename variables in main function to better understand the inner working of CD key generation algorithm.

```
1
2  undefined8 main(int argc,char *argv)
3
4  {
5    int num1;
6    int num2;
7    char *string;
8
9    puts("Enter your CD key to play \"Nihaal\'s Revenge\"(tm):");
10   if (argc != 4) {
11     puts("invalid key format");
12     puts("usage: ./[this binary] XXX XXXX XXX");
13                     /* WARNING: Subroutine does not return */
14     exit(1);
15   }
16   num1 = atoi(*(char **)(argv + 8));
17   string = *(char **)(argv + 0x10);
18   num2 = atoi(*(char **)(argv + 0x18));
19   if (num1 - num2 / 3 != 0x17c) {
20     printf("%d\n",(ulong)(uint)(num1 + -(num2 / 3)),(ulong)(uint)-(num2 / 3));
21     fail();
22   }
23   puts("Validation progress: 33%");
24   num1 = strncmp(string,"GM3R",4);
25   if (num1 != 0) {
26     fail();
27   }
28   puts("Validation progress: 66%\n");
29   if (99 < num2) {
30     if (num2 % 3 == 1) goto LAB_00101309;
31   }
```

dereference

From the order of dereferencing algorithm with offsets 0x8,0x10, and 0x18 of pointer array argv, we know that the variables stored on the stack must be in format : 'sss iiii xxx' where iiii is a string, sss = num1 and xxx = num2 are a numbers

LAB_00101309 is the goto statement that will jump to the code section that calls win functions. Only the right key would let the program go to that stage.

Constraints we can see are:

- Num1 – (Num2 / 3) == 0x17c = 380
- Num2 > 99
- Num2 mod 3 = 1
- String = GM3R

Note, divide operation of num2 / 3, num2 doesn't need to be divisible by 3.

II. Crafting Exploit

Put all these constraints into z3 solver

```
#!/usr/bin/python3
from z3 import *

num1 = Int('num1')
num2 = Int('num2')

zfinal_key = String('generated CD key')
string = String('string')

s = Solver()

# Program Hashing Algorithm
s.add(string == 'GM3R')
s.add( (num1 - (num2/3)) == 380)
s.add( num2 > 99)
s.add( (num2 % 3) == 1)
s.add(zfinal_key == (str(num1) + " " + string + " " + str(num2)))

#show answer
print(s.check())
print(s.model())
```

```
┌──(cs395㉿kali)-[~/Desktop/CS395_Final_Challenges/Nihaal's_Revenge]
└─$ python3 CS395_vnghi_NihaalsRevenge.py
sat
[string = "GM3R",
 generated CD key = "num1 GM3R num2",
 num1 = 413,
 num2 = 100]
```

III. Result

Using answer from solver: 413 GM3R 100

```
┌──(cs395㉿kali)-[~/Desktop/CS395_Final_Challenges/Nihaal's_Revenge]
└─$ ./cd_validator 413 GM3R 100
Enter your CD key to play "Nihaal's Revenge"(tm):
Validation progress: 33%
Validation progress: 66%

Congratulations! You may now play "Nihaal's Revenge!"
https://www.coolmathgames.com/
```