CTF Report: Rock Scissor Paper

2017313008 Kim TaeEun

```
~/rock-scissor-paper gdb rock-scissor-paper
```

First, open gdb to debug the rock-scissor-paper program.

```
gef➤  disas main
Dump of assembler code for function main:
   0x0804936c <+0>:     endbr32
   0x08049370 <+4>:     lea    ecx,[esp+0x4]
   0x08049374 <+8>:     and    esp,0xfffffff0
   0x08049377 <+11>:    push   DWORD PTR [ecx-0x4]
   0x0804937a <+14>:    push   ebp
   0x0804937b <+15>:    mov    ebp,esp
   0x0804937d <+17>:    push   ecx
   0x0804937e <+18>:    sub    esp,0x24
   0x08049381 <+21>:    mov    DWORD PTR [ebp-0x10],0x0
   0x08049388 <+28>:    sub    esp,0xc
   0x0804938b <+31>:    push   0x5
   0x0804938d <+33>:    call   0x8049890 <ctf_init>
   0x08049392 <+38>:    add    esp,0x10
   0x08049395 <+41>:    sub    esp,0xc
   0x08049398 <+44>:    push   0x7e3
   0x0804939d <+49>:    call   0x80490a0 <srand@plt>
   0x080493a2 <+54>:    add    esp,0x10
   0x080493a5 <+57>:    sub    esp,0xc
   0x080493a8 <+60>:    push   0x804a148
   0x080493ad <+65>:    call   0x8049130 <puts@plt>
```

You can see that the seed at random generation is a fixed value (0x7e3).

If the seed is fixed, the same sequence random number is always generated.

```python
from pwn import *
from ctypes import *

target='./rock-scissor-paper'
c=CDLL("/lib/x86_64-linux-gnu/libc.so.6")
p=process(target)
io=p

count=0
seed=0x7e3
c.srand(seed)

print(io.recv())

# 0: rock, 1: scissor, 2: paper
while count<1000:

    select=c.rand()%3

    if select==0:  # rock
        io.sendline("p")
    elif select==1:  # scissor
        io.sendline("r")
    else:  # paper
        io.sendline("s")

    count+=1


io.interactive()
```

Exploit code in Python

Therefore, use the pwntool, ctypes module to generate the random number with the fixed seed (0x7e3).

At this time, in the order of rock-scissor-paper, if random number is 0, it is rock,

if 1, scissor, and if 2, paper.

Therefore, sends a value that can beat this value to the program.

If you repeat 1000 times, the flag is displayed after 1000 victories.

```
You WON!!! 1000/1000 wins so far
MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMWX0kdc:;;;;:cdk0XWMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
M
MMMMMMMMMMMMMMMMMMMMMMMMMMMMWWX0koc:;;;;;;;;;;;;:cok0XWMMMMMMMMMMMMMMMMMMMMMMM
M
MMMMMMMMMMMMMMMMMMMMMMMMMMWWX0xoc;;;;;lxO0KKKK0Oxl;;;;:cox0XWWMMMMMMMMMMMMMMMM
M
MMMMMMMMMMMMMMMMMMMMMMWWXOxoc;;;;;;;;l0WMMMMMMMMW0l;;;;;;;;cox0XWMMMMMMMMMMMMM
M
MMMMMMMMMMMMMMMMWNKOxoc;;;;;;;;;;;;;:lxO0KKKK0Oxl:;;;;;;;;;;;;coxOKNWMMMMMMMMM
M
MMMMMMMMMMWNKOxoc;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;coxOKNWMMMMM
M
```

```
M
MMMMMMMMMMMMMMMMMMMMMWX0kdl:;;;;;;;;;;cOWWOc;;;;;;;
M
MMMMMMMMMMMMMMMMMMMMMMMMWN0kdl:;;;;;;cOWWOc;;;;;;;
M
MMMMMMMMMMMMMMMMMMMMMMMMMMMWNKkdl:;;cOWWOc;;:ldk0
M
MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMWXko:l0WW0l:oOXWWM
M

------------------------------------------------
Your Flag: YCe3BOW7zp2wybybsKYd7PI9rpQbYOvY
------------------------------------------------
```

flag: YCe3BOW7zp2wybybsKYd7PI9rpQbYOvY