分析：

打开 DEP，关掉 ASLR.

利用 rop 攻击关掉对栈的 DEP 保护，进而执行栈中的 shellcode(打开 shell)，shellcode 可以更换。系统调用 mprotect()　changes protection for the calling process's memory page(s)。利用 rop 链执行此系统调用关掉对栈的 DEP 保护。

int mprotect(void *addr, size_t len, int prot);

containing any part of the address range in the interval [addr, addr+len-1]. addr must be aligned to a page boundary.

prot is either PROT_NONE or a bitwise-or of the other values in the following list:

PROT_NONE　The memory cannot be accessed at all.

PROT_READ　The memory can be read.

PROT_WRITE The memory can be modified.

PROT_EXEC　The memory can be executed.

ROP Gadget:

Pop rdi; ret

Pop rdx; pop rsi; ret

Pop rax; ret

Syscall; ret

栈：

Payload 在栈中的情况

a ...offset...
Ret1
Page address in stack
Ret2
7
3 * pagesize
Ret3
0xa mprotect syscall num
Ret4
Shellcode address

/bin/sh address
0x3b ececv syscall num
0
0
shellcode