STRTAB=0x8048278 SYMTAB = OX80481d8 pre-resolve = 0x8048380 8. 200 延时野定 read 0X800 "binlsh" 0x 80ta 040 system  $\rightarrow e(f32 - sym - struct)$ = fake\_start > elf32 - rel\_struct align\*'a' oxlo > [pre\_resolve] push -- @ jmp --\_dl\_runtime\_resolve (link\_map, rel\_offset) [·got+4] > 0xf7ffd918 ? 所有以数此参数都一样

JMPREL = 0x8048330

