1 GOT 表符号偏移

重定位结构体

typedef struct{

Elf32\_Addr r\_offset;

Elf32\_Word r\_info;

}Elf32\_Rel;

// 符号结构体

typedef struct{

Elf32\_Word st\_name;

Elf32\_Addr st\_value;

Elf32\_Word st\_size;

unsigned char st\_info;

unsinged char st\_other;

Elf32\_Half st\_shndx;

}Elf32\_Sym;

获取.rel.plt 每个重定位表所对应的符号的步骤：

1、使用ELF32\_R\_SYM宏（参数为.rel.plt的r\_info）获取符号在.dynsym中的偏移

2、找到对应的dynsym在获取.dynsym的st\_name字段，但这个字段不是字符串，也是一

个偏移，是.dynstr节的偏移

3、通过偏移可以获取到相应的符号

GOT表hook

字符串表 .dynstr

符号表 .dynsym

重定位表 .rel.plt

.got section

\_\_asm\_\_ \_\_volatile\_\_(

STMFD SP!,{R0-R12,LR}\n

);

myfunc();

\_\_asm\_\_ \_\_volatile\_\_(

“LDMFD SP!,{R0-R12}\n”

“LDR LR,=origin\_addr\n”

“LDR LR,[LR]\n”

“BLX LR\n”

“LDMFD SP!,{PC}\n”

);

全局偏移表和过程链接表