做题的过程中突然发现了一个点 记录一下：

程序加载之后 在gdb中 print函数的地址 就是函数首地址。

text：

```
#include<stdio.h>
void main()
{
 puts("hello world!\n");
}
```

然后gdb调试运行

print puts的地址：

```
gdb-peda$ print puts
$1 = {<text variable, no debug info>} 0xb7e797e0 <_IO_puts>
gdb-peda$
```

可以看到puts的函数地址为：`0xb7e797e0`

然后我们看一下 puts函数的汇编代码 可以看到puts函数的起始地址：

```
gdb-peda$ disassemble puts
Dump of assembler code for function _IO_puts:
   0xb7e797e0 <+0>:     push   ebp
   0xb7e797e1 <+1>:     push   edi
   0xb7e797e2 <+2>:     push   esi
   0xb7e797e3 <+3>:     push   ebx
   0xb7e797e4 <+4>:     sub    esp,0x1c
   0xb7e797e7 <+7>:     call   0xb7f3cc6b <__x86.get_pc_thunk.bx>
   0xb7e797ec <+12>:    add    ebx,0x147814
   0xb7e797f2 <+18>:    mov    eax,DWORD PTR [esp+0x30]
   0xb7e797f6 <+22>:    mov    DWORD PTR [esp],eax
   0xb7e797f9 <+25>:    call   0xb7e8efd0 <__strlen_ia32>
   0xb7e797fe <+30>:    mov    edx,DWORD PTR [ebx+0xd80]
   0xb7e79804 <+36>:    mov    edi,edx
   0xb7e79806 <+38>:    mov    esi,eax
```

也是`0xb7e797e0`