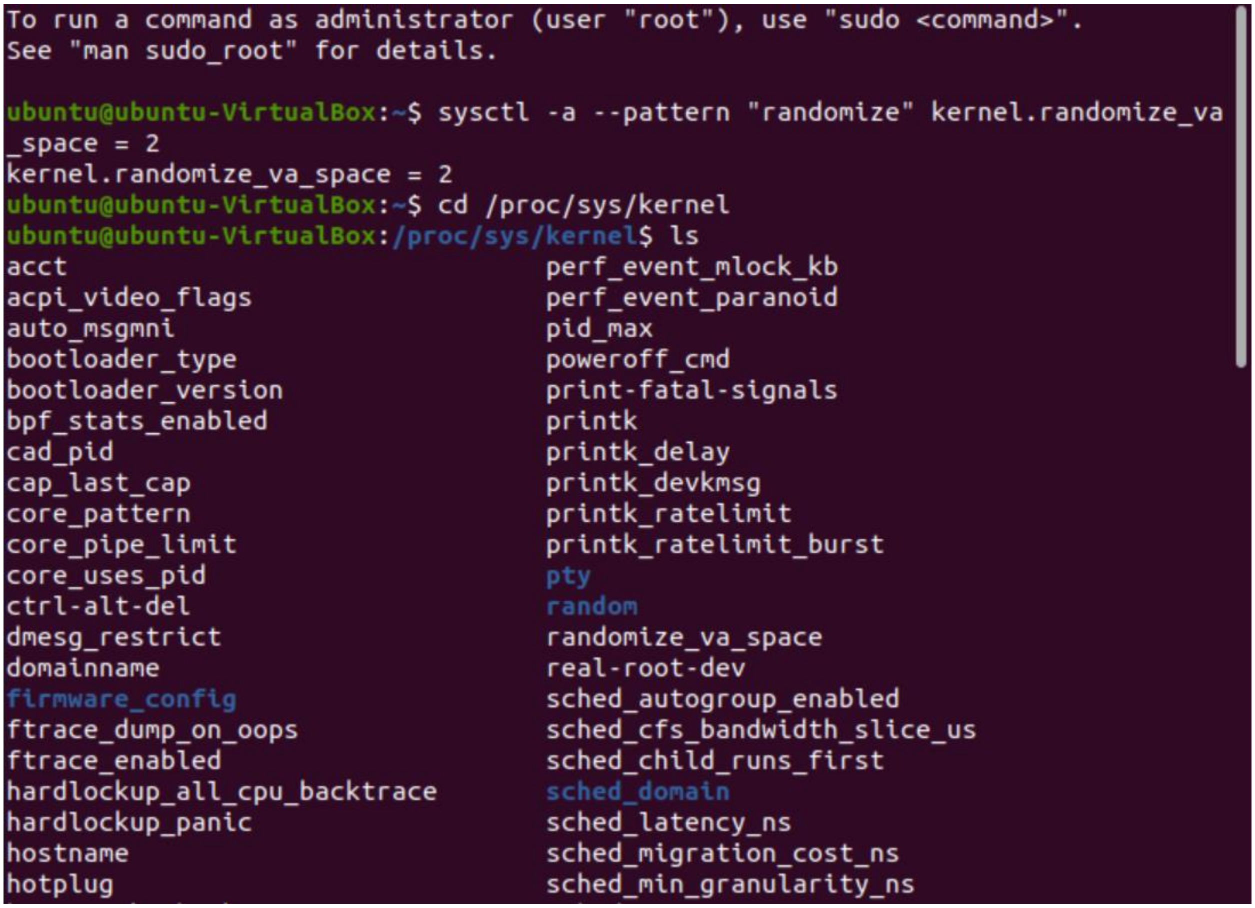
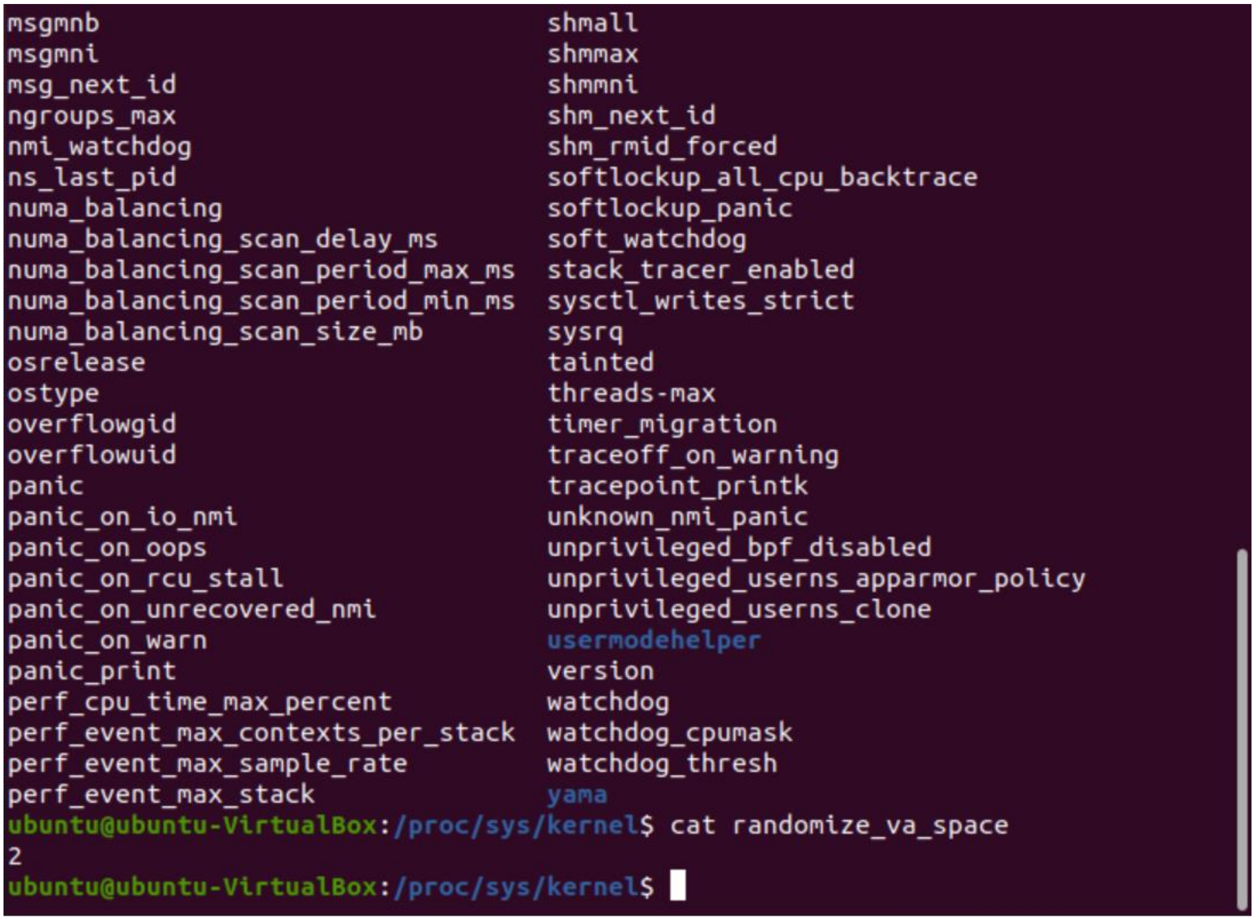
Alejandra Patricia Chaparro Matias



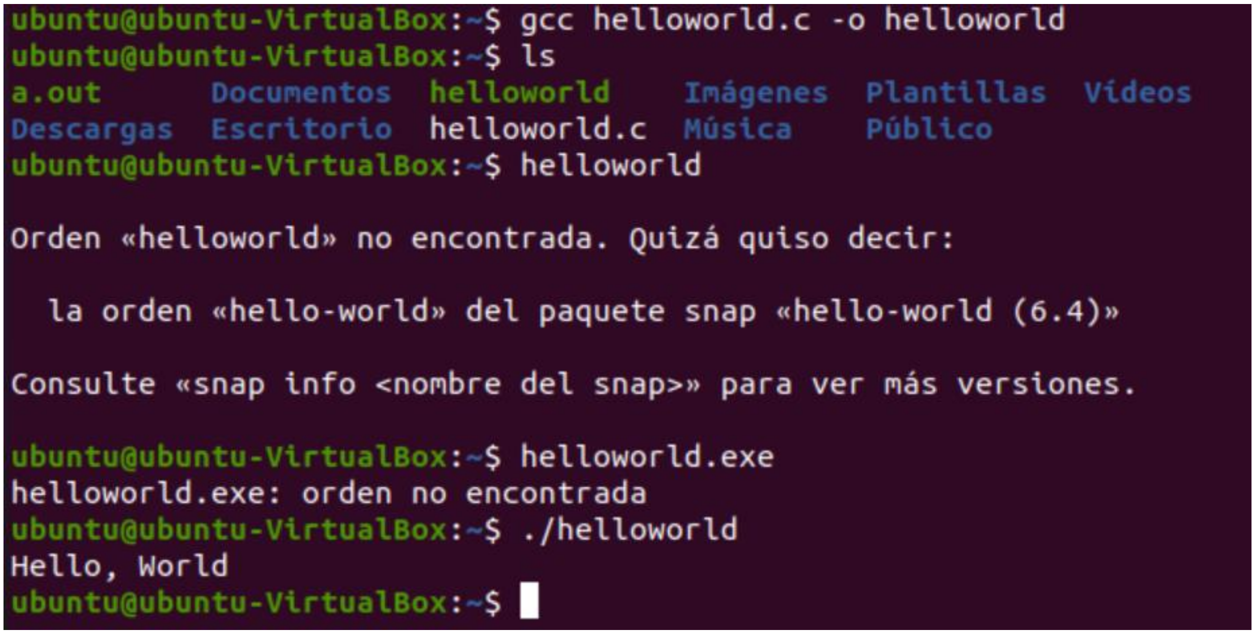
```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ubuntu-VirtualBox:~$ sysctl -a --pattern "randomize" kernel.randomize_va
_space = 2
kernel.randomize_va_space = 2
ubuntu@ubuntu-VirtualBox:~$ cd /proc/sys/kernel
ubuntu@ubuntu-VirtualBox:/proc/sys/kernel$ ls
acct                               perf_event_mlock_kb
acpi_video_flags                   perf_event_paranoid
auto_msgmni                        pid_max
bootloader_type                    poweroff_cmd
bootloader_version                 print-fatal-signals
bpf_stats_enabled                  printk
cad_pid                            printk_delay
cap_last_cap                       printk_devkmsg
core_pattern                       printk_ratelimit
core_pipe_limit                    printk_ratelimit_burst
core_uses_pid                      pty
ctrl-alt-del                       random
dmesg_restrict                     randomize_va_space
domainname                         real-root-dev
firmware_config                    sched_autogroup_enabled
ftrace_dump_on_oops                sched_cfs_bandwidth_slice_us
ftrace_enabled                     sched_child_runs_first
hardlockup_all_cpu_backtrace       sched_domain
hardlockup_panic                   sched_latency_ns
hostname                           sched_migration_cost_ns
hotplug                            sched_min_granularity_ns
```

Se creo el randomize_va_space con un igual a 2



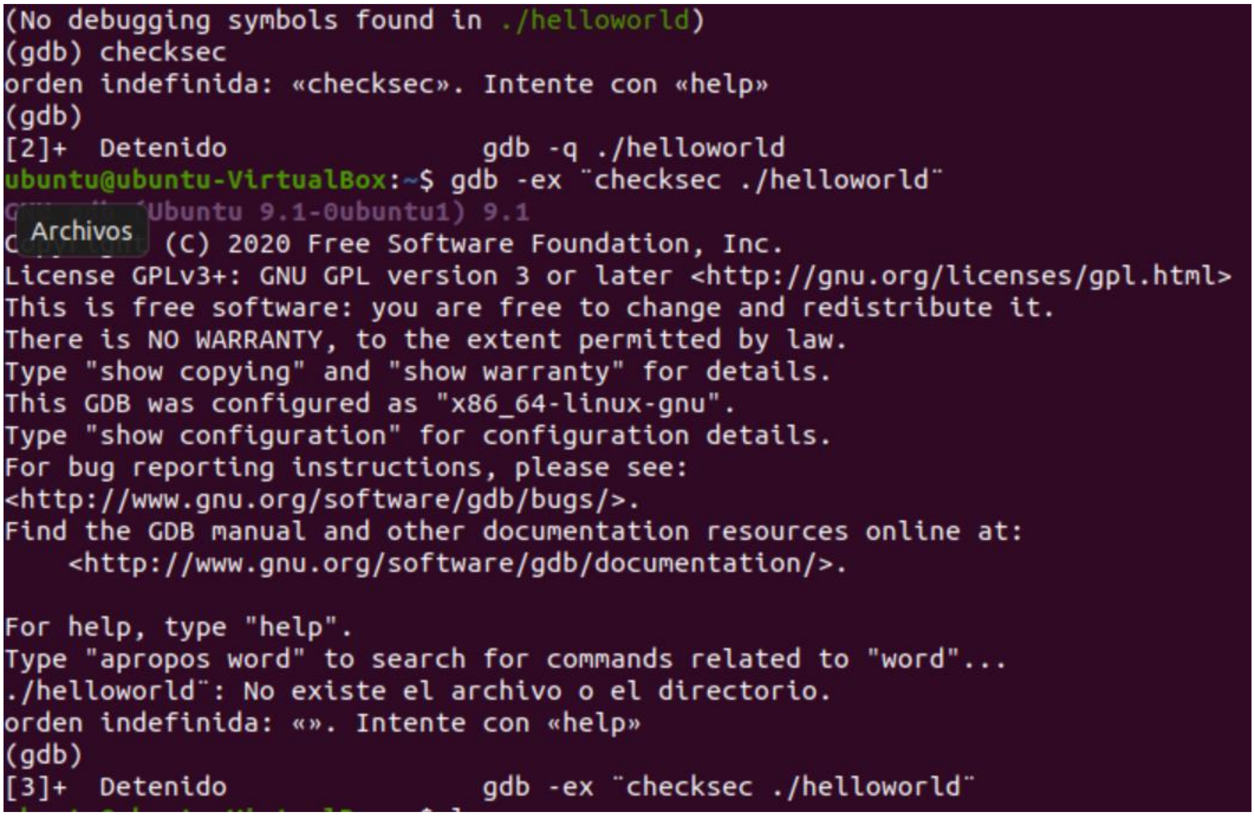
```
msgmnb                                  shmall
msgmni                                  shmmax
msg_next_id                             shmmni
ngroups_max                             shm_next_id
nmi_watchdog                            shm_rmid_forced
ns_last_pid                             softlockup_all_cpu_backtrace
numa_balancing                          softlockup_panic
numa_balancing_scan_delay_ms            soft_watchdog
numa_balancing_scan_period_max_ms       stack_tracer_enabled
numa_balancing_scan_period_min_ms       sysctl_writes_strict
numa_balancing_scan_size_mb             sysrq
osrelease                               tainted
ostype                                  threads-max
overflowgid                             timer_migration
overflowuid                             traceoff_on_warning
panic                                   tracepoint_printk
panic_on_io_nmi                         unknown_nmi_panic
panic_on_oops                           unprivileged_bpf_disabled
panic_on_rcu_stall                      unprivileged_userns_apparmor_policy
panic_on_unrecovered_nmi                unprivileged_userns_clone
panic_on_warn                           usermodehelper
panic_print                             version
perf_cpu_time_max_percent               watchdog
perf_event_max_contexts_per_stack       watchdog_cpumask
perf_event_max_sample_rate              watchdog_thresh
perf_event_max_stack                    yama
ubuntu@ubuntu-VirtualBox:/proc/sys/kernel$ cat randomize_va_space
2
ubuntu@ubuntu-VirtualBox:/proc/sys/kernel$ 
```

Leemos el archive y comprobamos que es igual a 2



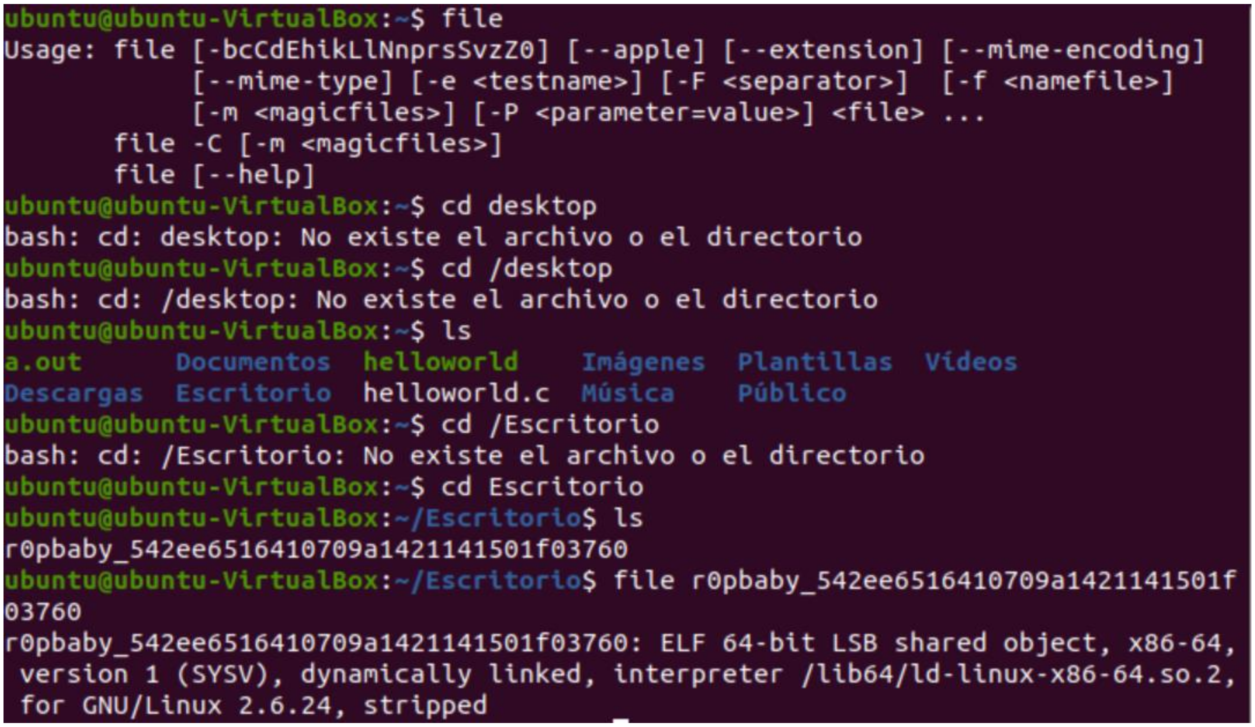
```
ubuntu@ubuntu-VirtualBox:~$ gcc helloworld.c -o helloworld
ubuntu@ubuntu-VirtualBox:~$ ls
a.out      Documentos  helloworld    Imágenes  Plantillas  Vídeos
Descargas  Escritorio  helloworld.c  Música    Público
ubuntu@ubuntu-VirtualBox:~$ helloworld

Orden «helloworld» no encontrada. Quizá quiso decir:

  la orden «hello-world» del paquete snap «hello-world (6.4)»

Consulte «snap info <nombre del snap>» para ver más versiones.

ubuntu@ubuntu-VirtualBox:~$ helloworld.exe
helloworld.exe: orden no encontrada
ubuntu@ubuntu-VirtualBox:~$ ./helloworld
Hello, World
ubuntu@ubuntu-VirtualBox:~$ 
```

Despues de crear el helloworld lo ejecutamos.



```
(No debugging symbols found in ./helloworld)
(gdb) checksec
orden indefinida: «checksec». Intente con «help»
(gdb)
[2]+  Detenido                gdb -q ./helloworld
ubuntu@ubuntu-VirtualBox:~$ gdb -ex ¨checksec ./helloworld¨
GNU gdb (Ubuntu 9.1-0ubuntu1) 9.1
Copyright (C) 2020 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/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 "x86_64-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"...
./helloworld¨: No existe el archivo o el directorio.
orden indefinida: «». Intente con «help»
(gdb)
[3]+  Detenido                gdb -ex ¨checksec ./helloworld¨
```

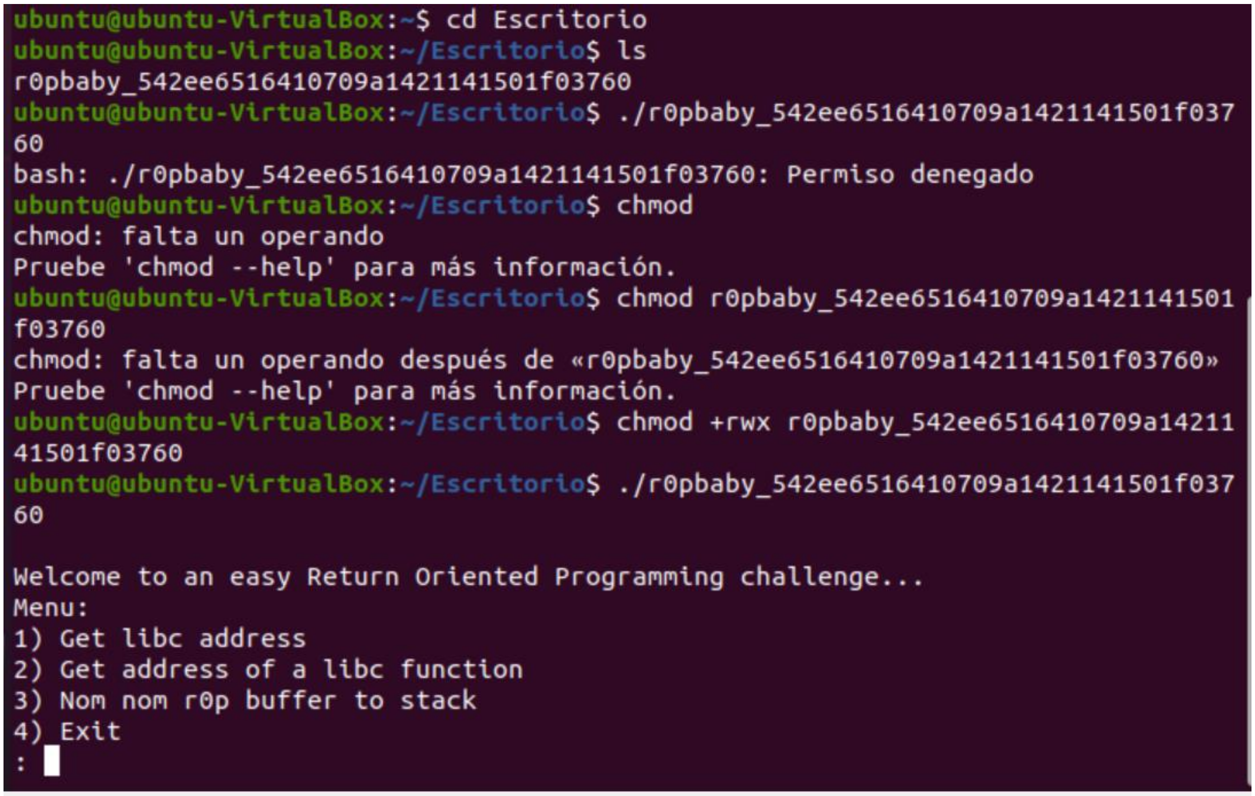
En este apartado se generan errores en el gdb en cuanto al checksec



```
ubuntu@ubuntu-VirtualBox:~$ file
Usage: file [-bcCdEhikLlNnprsSvzZ0] [--apple] [--extension] [--mime-encoding]
            [--mime-type] [-e <testname>] [-F <separator>]  [-f <namefile>]
            [-m <magicfiles>] [-P <parameter=value>] <file> ...
       file -C [-m <magicfiles>]
       file [--help]
ubuntu@ubuntu-VirtualBox:~$ cd desktop
bash: cd: desktop: No existe el archivo o el directorio
ubuntu@ubuntu-VirtualBox:~$ cd /desktop
bash: cd: /desktop: No existe el archivo o el directorio
ubuntu@ubuntu-VirtualBox:~$ ls
a.out      Documentos  helloworld    Imágenes  Plantillas  Vídeos
Descargas  Escritorio  helloworld.c  Música    Público
ubuntu@ubuntu-VirtualBox:~$ cd /Escritorio
bash: cd: /Escritorio: No existe el archivo o el directorio
ubuntu@ubuntu-VirtualBox:~$ cd Escritorio
ubuntu@ubuntu-VirtualBox:~/Escritorio$ ls
r0pbaby_542ee6516410709a1421141501f03760
ubuntu@ubuntu-VirtualBox:~/Escritorio$ file r0pbaby_542ee6516410709a1421141501f
03760
r0pbaby_542ee6516410709a1421141501f03760: ELF 64-bit LSB shared object, x86-64,
 version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2,
 for GNU/Linux 2.6.24, stripped
```

Por el momento se corre el r0pbaby para al fin generar la actividad.

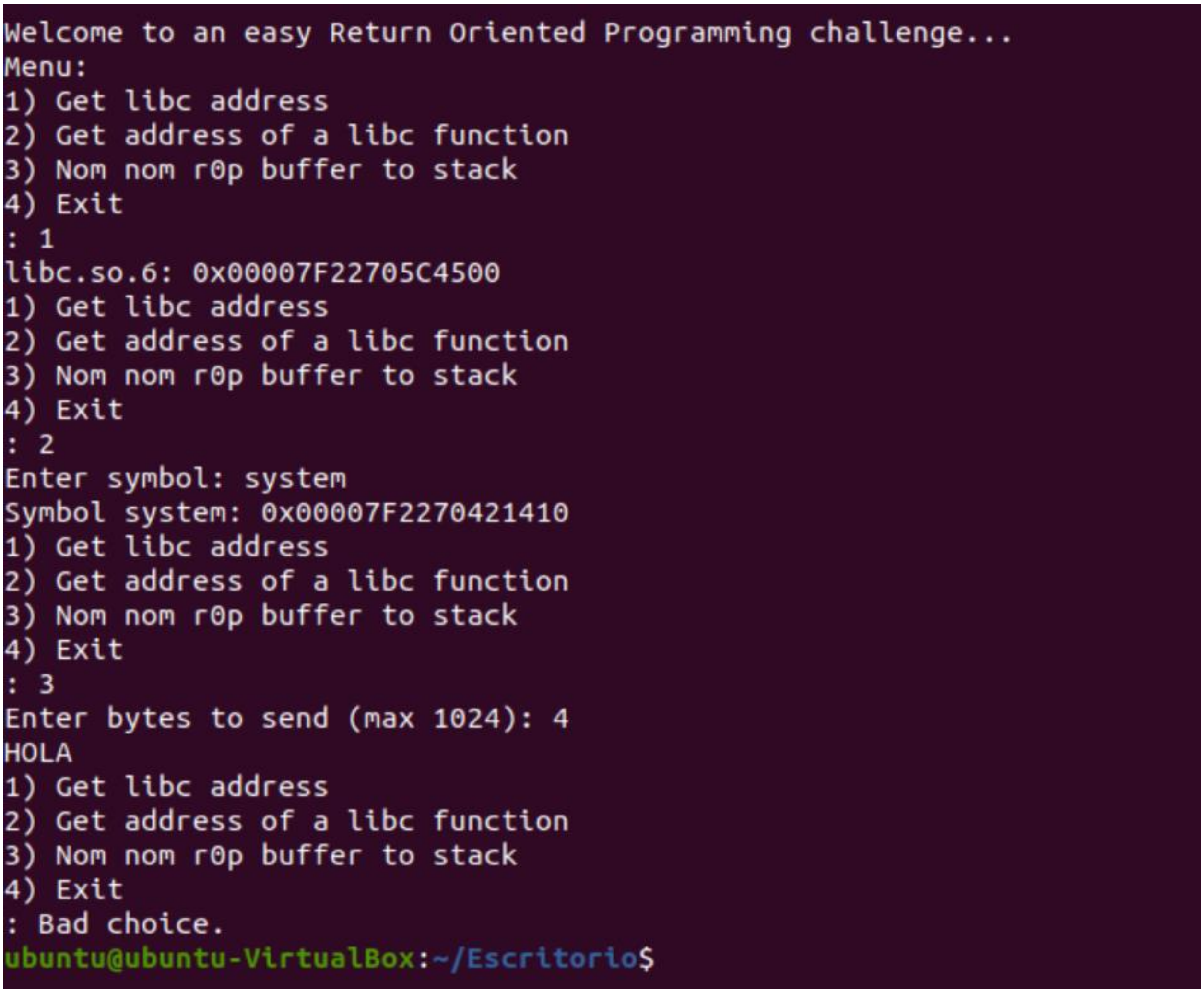
Alejandra Patricia Chaparro Matias



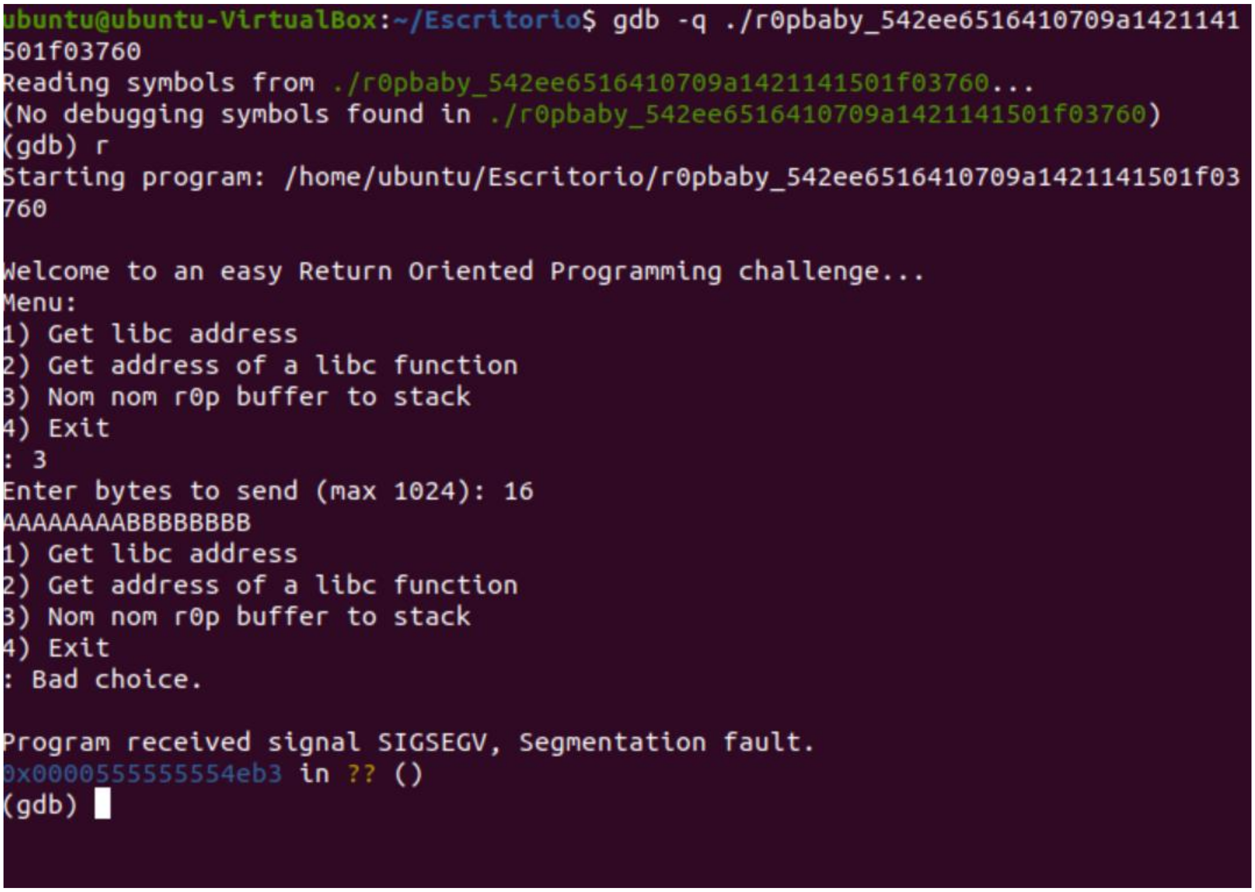
```
ubuntu@ubuntu-VirtualBox:~$ cd Escritorio
ubuntu@ubuntu-VirtualBox:~/Escritorio$ ls
r0pbaby_542ee6516410709a1421141501f03760
ubuntu@ubuntu-VirtualBox:~/Escritorio$ ./r0pbaby_542ee6516410709a1421141501f037
60
bash: ./r0pbaby_542ee6516410709a1421141501f03760: Permiso denegado
ubuntu@ubuntu-VirtualBox:~/Escritorio$ chmod
chmod: falta un operando
Pruebe 'chmod --help' para más información.
ubuntu@ubuntu-VirtualBox:~/Escritorio$ chmod r0pbaby_542ee6516410709a1421141501
f03760
chmod: falta un operando después de «r0pbaby_542ee6516410709a1421141501f03760»
Pruebe 'chmod --help' para más información.
ubuntu@ubuntu-VirtualBox:~/Escritorio$ chmod +rwx r0pbaby_542ee6516410709a14211
41501f03760
ubuntu@ubuntu-VirtualBox:~/Escritorio$ ./r0pbaby_542ee6516410709a1421141501f037
60

Welcome to an easy Return Oriented Programming challenge...
Menu:
1) Get libc address
2) Get address of a libc function
3) Nom nom r0p buffer to stack
4) Exit
: 
```

chmod – Da permiso al archivo

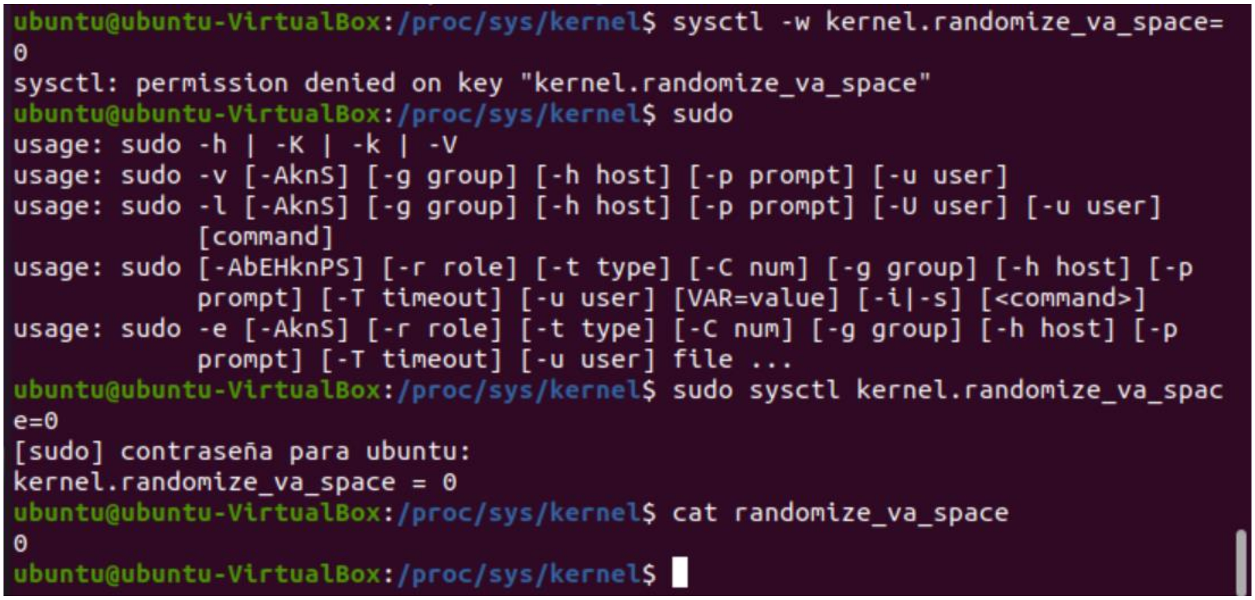
Alejandra Patricia Chaparro Matias



```
Welcome to an easy Return Oriented Programming challenge...
Menu:
1) Get libc address
2) Get address of a libc function
3) Nom nom r0p buffer to stack
4) Exit
: 1
libc.so.6: 0x00007F22705C4500
1) Get libc address
2) Get address of a libc function
3) Nom nom r0p buffer to stack
4) Exit
: 2
Enter symbol: system
Symbol system: 0x00007F2270421410
1) Get libc address
2) Get address of a libc function
3) Nom nom r0p buffer to stack
4) Exit
: 3
Enter bytes to send (max 1024): 4
HOLA
1) Get libc address
2) Get address of a libc function
3) Nom nom r0p buffer to stack
4) Exit
: Bad choice.
ubuntu@ubuntu-VirtualBox:~/Escritorio$
```



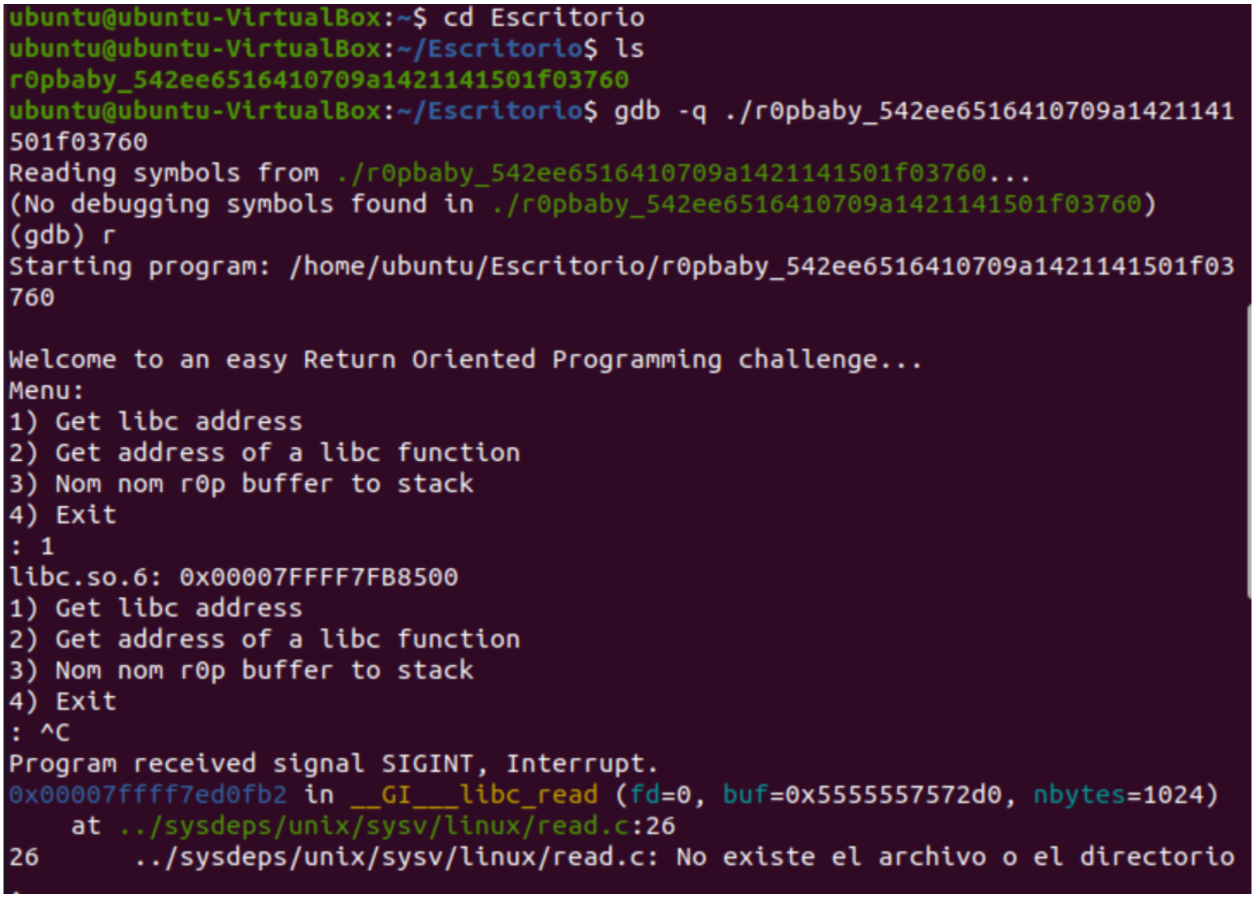
```
ubuntu@ubuntu-VirtualBox:~/Escritorio$ gdb -q ./r0pbaby_542ee6516410709a1421141
501f03760
Reading symbols from ./r0pbaby_542ee6516410709a1421141501f03760...
(No debugging symbols found in ./r0pbaby_542ee6516410709a1421141501f03760)
(gdb) r
Starting program: /home/ubuntu/Escritorio/r0pbaby_542ee6516410709a1421141501f03
760

Welcome to an easy Return Oriented Programming challenge...
Menu:
1) Get libc address
2) Get address of a libc function
3) Nom nom r0p buffer to stack
4) Exit
: 3
Enter bytes to send (max 1024): 16
AAAAAAAABBBBBBBB
1) Get libc address
2) Get address of a libc function
3) Nom nom r0p buffer to stack
4) Exit
: Bad choice.

Program received signal SIGSEGV, Segmentation fault.
0x0000555555554eb3 in ?? ()
(gdb) 
```



```
ubuntu@ubuntu-VirtualBox:/proc/sys/kernel$ sysctl -w kernel.randomize_va_space=
0
sysctl: permission denied on key "kernel.randomize_va_space"
ubuntu@ubuntu-VirtualBox:/proc/sys/kernel$ sudo
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user]
            [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p
            prompt] [-T timeout] [-u user] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p
            prompt] [-T timeout] [-u user] file ...
ubuntu@ubuntu-VirtualBox:/proc/sys/kernel$ sudo sysctl kernel.randomize_va_spac
e=0
[sudo] contraseña para ubuntu:
kernel.randomize_va_space = 0
ubuntu@ubuntu-VirtualBox:/proc/sys/kernel$ cat randomize_va_space
0
ubuntu@ubuntu-VirtualBox:/proc/sys/kernel$ 
```

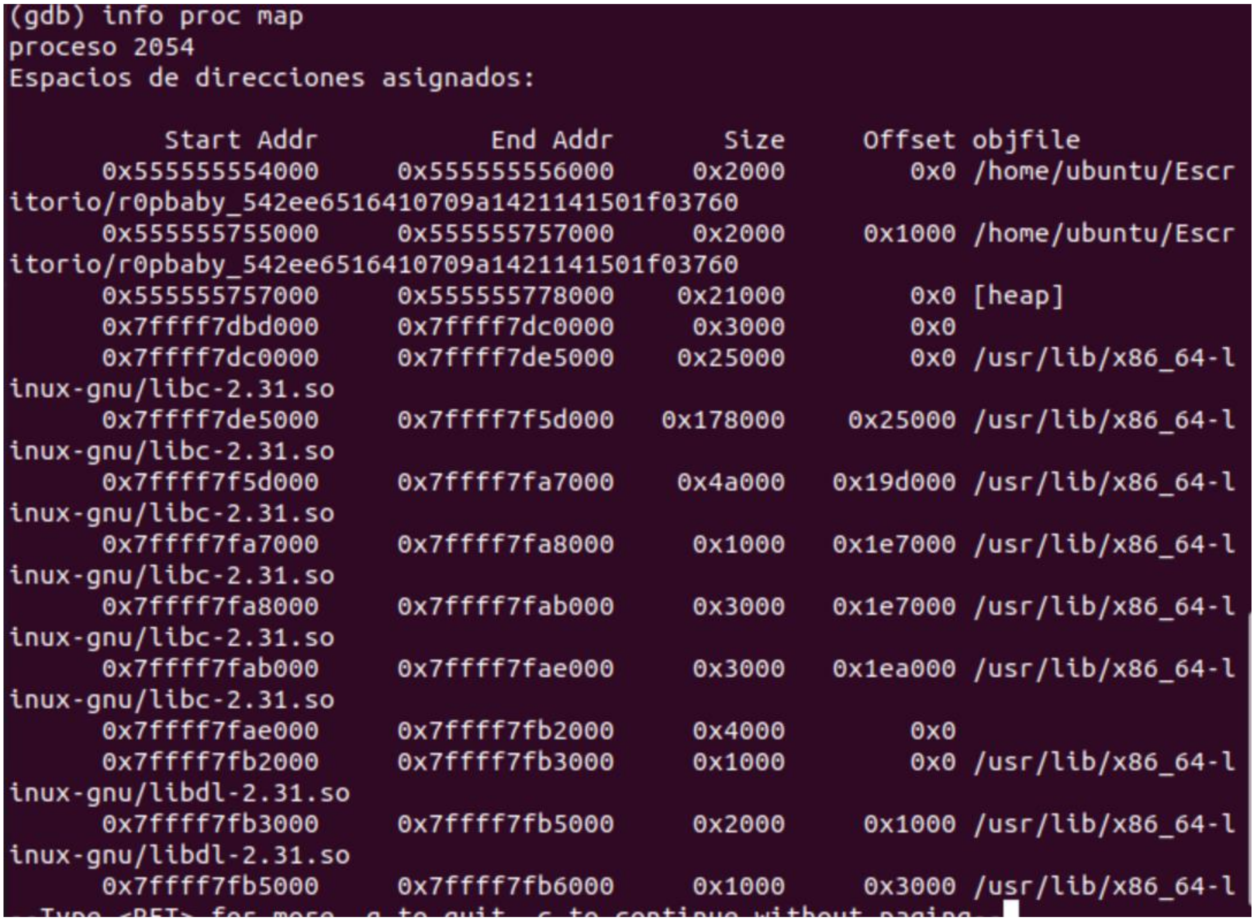
Convertí el ASLR en no random, igualándolo a 0

Alejandra Patricia Chaparro Matias

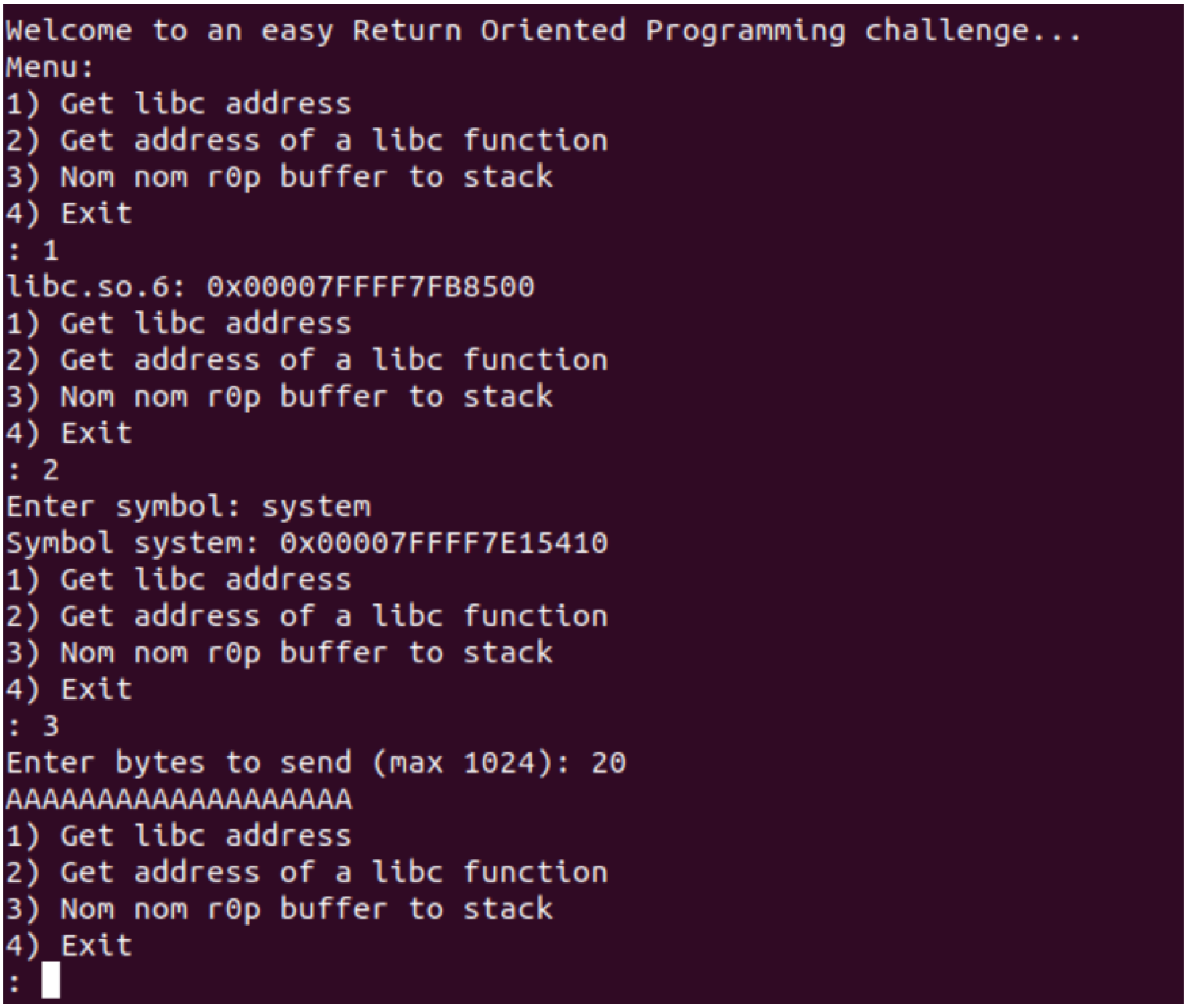


```
ubuntu@ubuntu-VirtualBox:~$ cd Escritorio
ubuntu@ubuntu-VirtualBox:~/Escritorio$ ls
r0pbaby_542ee6516410709a1421141501f03760
ubuntu@ubuntu-VirtualBox:~/Escritorio$ gdb -q ./r0pbaby_542ee6516410709a1421141
501f03760
Reading symbols from ./r0pbaby_542ee6516410709a1421141501f03760...
(No debugging symbols found in ./r0pbaby_542ee6516410709a1421141501f03760)
(gdb) r
Starting program: /home/ubuntu/Escritorio/r0pbaby_542ee6516410709a1421141501f03
760

Welcome to an easy Return Oriented Programming challenge...
Menu:
1) Get libc address
2) Get address of a libc function
3) Nom nom r0p buffer to stack
4) Exit
: 1
libc.so.6: 0x00007FFFF7FB8500
1) Get libc address
2) Get address of a libc function
3) Nom nom r0p buffer to stack
4) Exit
: ^C
Program received signal SIGINT, Interrupt.
0x00007ffff7ed0fb2 in __GI___libc_read (fd=0, buf=0x5555557572d0, nbytes=1024)
    at ../sysdeps/unix/sysv/linux/read.c:26
26      ../sysdeps/unix/sysv/linux/read.c: No existe el archivo o el directorio
```

Alejandra Patricia Chaparro Matias



```
(gdb) info proc map
proceso 2054
Espacios de direcciones asignados:

          Start Addr           End Addr       Size     Offset objfile
      0x555555554000     0x555555556000     0x2000        0x0 /home/ubuntu/Escr
itorio/r0pbaby_542ee6516410709a1421141501f03760
      0x555555755000     0x555555757000     0x2000     0x1000 /home/ubuntu/Escr
itorio/r0pbaby_542ee6516410709a1421141501f03760
      0x555555757000     0x555555778000    0x21000        0x0 [heap]
      0x7ffff7dbd000     0x7ffff7dc0000     0x3000        0x0
      0x7ffff7dc0000     0x7ffff7de5000    0x25000        0x0 /usr/lib/x86_64-l
inux-gnu/libc-2.31.so
      0x7ffff7de5000     0x7ffff7f5d000   0x178000    0x25000 /usr/lib/x86_64-l
inux-gnu/libc-2.31.so
      0x7ffff7f5d000     0x7ffff7fa7000    0x4a000   0x19d000 /usr/lib/x86_64-l
inux-gnu/libc-2.31.so
      0x7ffff7fa7000     0x7ffff7fa8000     0x1000   0x1e7000 /usr/lib/x86_64-l
inux-gnu/libc-2.31.so
      0x7ffff7fa8000     0x7ffff7fab000     0x3000   0x1e7000 /usr/lib/x86_64-l
inux-gnu/libc-2.31.so
      0x7ffff7fab000     0x7ffff7fae000     0x3000   0x1ea000 /usr/lib/x86_64-l
inux-gnu/libc-2.31.so
      0x7ffff7fae000     0x7ffff7fb2000     0x4000        0x0
      0x7ffff7fb2000     0x7ffff7fb3000     0x1000        0x0 /usr/lib/x86_64-l
inux-gnu/libdl-2.31.so
      0x7ffff7fb3000     0x7ffff7fb5000     0x2000     0x1000 /usr/lib/x86_64-l
inux-gnu/libdl-2.31.so
      0x7ffff7fb5000     0x7ffff7fb6000     0x1000     0x3000 /usr/lib/x86_64-l
--Type <RET> for more, q to quit, c to continue without paging--
```



```
Welcome to an easy Return Oriented Programming challenge...
Menu:
1) Get libc address
2) Get address of a libc function
3) Nom nom r0p buffer to stack
4) Exit
: 1
libc.so.6: 0x00007FFFF7FB8500
1) Get libc address
2) Get address of a libc function
3) Nom nom r0p buffer to stack
4) Exit
: 2
Enter symbol: system
Symbol system: 0x00007FFFF7E15410
1) Get libc address
2) Get address of a libc function
3) Nom nom r0p buffer to stack
4) Exit
: 3
Enter bytes to send (max 1024): 20
AAAAAAAAAAAAAAAAAAA
1) Get libc address
2) Get address of a libc function
3) Nom nom r0p buffer to stack
4) Exit
: 
```

Me quedo en este apartado, me nació la duda de si al convertir el randomize_va_space a 0 manda los apuntadores reales. Por el momento se seguirá trabajando en ello, ya que incluso el checksec en el gdb no se encuentra.