

```
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
msgmni
msg_next_id
ngroups_max
nmi_watchdog
ns_last_pid
numa_balancing
numa_balancing_scan_delay_ms
numa_balancing_scan_period_max_ms
numa_balancing_scan_period_min_ms
numa_balancing_scan_size_mb
osrelease
ostype
overflowgid
overflowuid
panic
panic_on_io_nmi
panic_on_oops
panic_on_rcu_stall
panic_on_unrecovered_nmi
panic_on_warn
panic_print
perf_cpu_time_max_percent
perf_event_max_contexts_per_stack
perf_event_max_sample_rate
perf_event_max_stack
shmall
shmmax
shmmni
shm_next_id
shm_rmid_forced
softlockup_all_cpu_backtrace
softlockup_panic
soft_watchdog
stack_tracer_enabled
sysctl_writes_strict
sysrq
tainted
threads-max
timer_migration
traceoff_on_warning
tracepoint_printk
unknown_nmi_panic
unprivileged_bpf_disabled
unprivileged_usersns_apparmor_policy
unprivileged_usersns_clone
usermodehelper
version
watchdog
watchdog_cpumask
watchdog_thresh
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  Videos
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_542ee6516410709a1421141501f03760
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.