Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»
Факультет інформатики та обчислювальної техніки

Кафедра обчислювальної техніки

Архітектура комп'ютерів 2. Процесори

Лабораторна робота №5

«Розроблення модулів Linux Kernel (3)»

Виконав:
студент групи ІО-14
Пономарчук Євгеній
Перевірив:
Гайдай А. Р.

Київ - 2023 р.

Тема: Розроблення модулів Linux Kernel (частина 3)

Виконання лабораторної роботи:

Завдання 1:

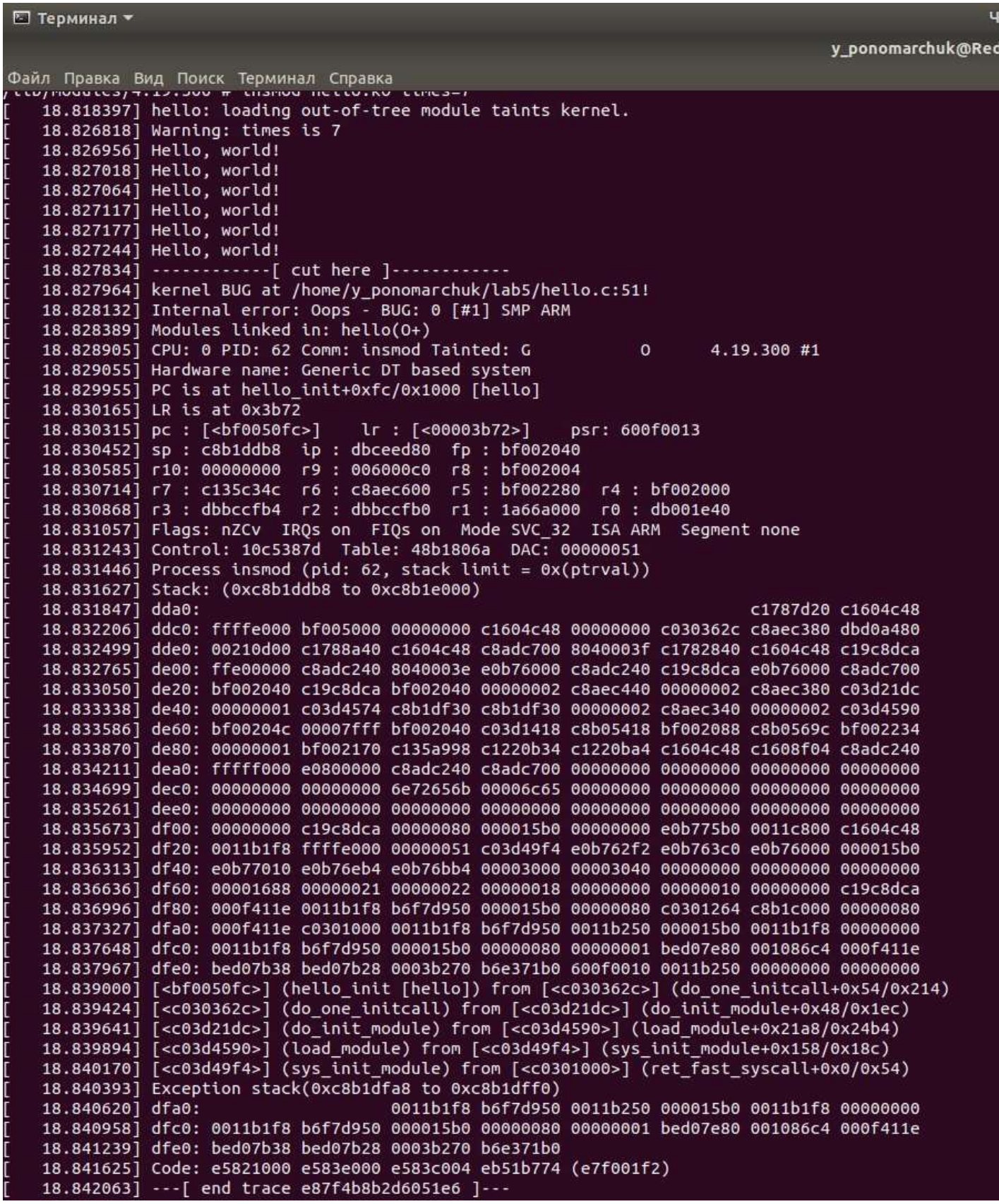
I. Додайте BUG_ON() замість друку повідомлення та повернення - EINVAL для неприпустимого значення параметра.
II. Додайте примусове внесення помилки "начебто kmalloc() повернув 0" під час формування елемента списку для якогось повідомлення (останнього із серії, 5-го, ... — на ваш вибір).
III. Модифікуйте Makefile аналогічно *appendix1*.
IV. Отримайте обидва повідомлення, роздивіться їх та для одного з них виконайте пошук місця аварії аналогічно *appendix1*.
    A. Зауважте, що при виконанні BUG_ON() модуль буде "зайнятий", і ви не зможете виконати rmmod.

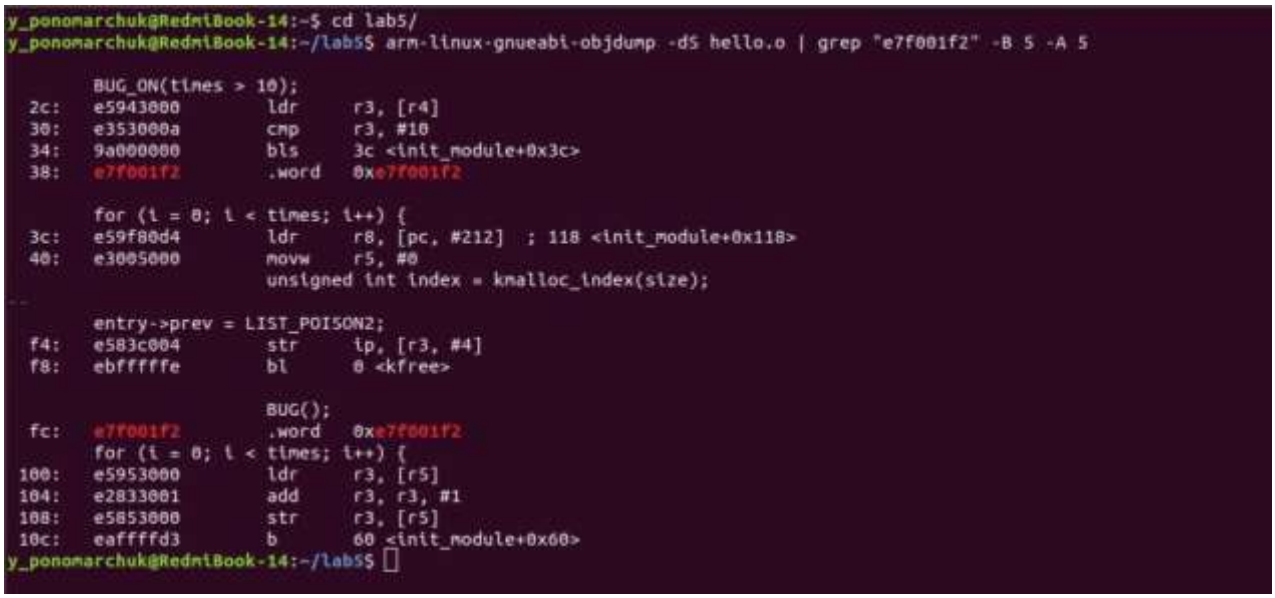
Посилання на github:

https://github.com/Djekichoid/AK

Результат:

```
                                                                    y_ponomarchu
Файл  Правка  Вид  Поиск  Терминал  Справка
Please press Enter to activate this console.
/ # cd lib/modules/4.19.300/
/lib/modules/4.19.300 # modinfo hello.ko
filename:       hello.ko
author:         Ponomarchuk Yevhenii
description:    Lab5
license:        Dual BSD/GPL
parm:           times:Times to print Hello, World!
depends:
vermagic:       4.19.300 SMP mod_unload ARMv7 p2v8
/lib/modules/4.19.300 # insmod hello.ko
[   42.989507] hello: loading out-of-tree module taints kernel.
/lib/modules/4.19.300 # rmmod hello.ko
[   53.786912] CHao!, Bambino)
/lib/modules/4.19.300 # insmod hello.ko times=0
[   71.320307] Warning: times is 0
/lib/modules/4.19.300 # rmmod hello.ko
[   73.890991] CHao!, Bambino)
/lib/modules/4.19.300 # insmod hello.ko times=20
[   80.206091] ------------[ cut here ]------------
[   80.206259] kernel BUG at /home/y_ponomarchuk/lab5/hello.c:33!
[   80.206414] Internal error: Oops - BUG: 0 [#1] SMP ARM
[   80.206611] Modules linked in: hello(O+) [last unloaded: hello]
[   80.207096] CPU: 0 PID: 72 Comm: insmod Tainted: G           O      4.19.300 #1
[   80.207283] Hardware name: Generic DT based system
[   80.207925] PC is at hello_init+0x38/0x1000 [hello]
[   80.208221] LR is at do_one_initcall+0x54/0x214
[   80.208317] pc : [<bf015038>]    lr : [<c030362c>]    psr: 200f0013
[   80.208452] sp : c8ae7db8  ip : c8b47280  fp : bf012040
[   80.208619] r10: 00000000  r9 : c1604c48  r8 : 00000000
[   80.208766] r7 : bf015000  r6 : ffffe000  r5 : c1604c48  r4 : bf012000
[   80.208952] r3 : 00000014  r2 : a52587b1  r1 : 00000014  r0 : 00000000
[   80.209216] Flags: nzCv  IRQs on  FIQs on  Mode SVC_32  ISA ARM  Segment none
[   80.209486] Control: 10c5387d  Table: 48b4c06a  DAC: 00000051
[   80.209798] Process insmod (pid: 72, stack limit = 0x(ptrval))
[   80.210138] Stack: (0xc8ae7db8 to 0xc8ae8000)
[   80.210366] 7da0:                                                   c1787d20 c1604c48
[   80.210665] 7dc0: ffffe000 bf015000 00000000 c1604c48 00000000 c030362c c8b472c0 c04f1df8
[   80.210942] 7de0: 00000000 00000002 00000000 00000000 c8b47ee4 c04f27d4 00000000 e0b7efff
[   80.211213] 7e00: ffe00000 fffff000 c0f12218 c8b478c0 dbceed80 dbbd9000 dbceed80 00000001
[   80.211484] 7e20: bf012040 a52587b1 bf012040 00000002 c8b47000 00000002 c8b47f00 c03d21dc
[   80.211756] 7e40: c8b47f00 c04633e0 c8ae7f30 c8ae7f30 00000002 c8b47ec0 00000002 c03d4590
[   80.212028] 7e60: bf01204c 00007fff bf012040 c03d1418 c8b05418 bf012088 c8b0569c bf012234
[   80.212300] 7e80: 00000001 bf012170 c135a998 c1220b34 c1220ba4 c1604c48 c1608f04 c8b47280
[   80.212568] 7ea0: fffff000 e0800000 c8b47280 c8b47000 00000000 00000000 00000000 00000000
[   80.212839] 7ec0: 00000000 00000000 6e72656b 00006c65 00000000 00000000 00000000 00000000
[   80.213110] 7ee0: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
[   80.213381] 7f00: 00000000 a52587b1 00000080 000015b0 00000000 e0b7d5b0 0011c800 c1604c48
[   80.213652] 7f20: 0011b1f8 ffffe000 00000051 c03d49f4 e0b7c2f2 e0b7c3c0 e0b7c000 000015b0
[   80.213913] 7f40: e0b7d010 e0b7ceb4 e0b7cbb4 00003000 00003040 00000000 00000000 00000000
[   80.214151] 7f60: 00001688 00000021 00000022 00000018 00000000 00000010 00000000 a52587b1
[   80.214432] 7f80: 000f411e 0011b1f8 b6f6b950 000015b0 00000080 c0301264 c8ae6000 00000080
[   80.214702] 7fa0: 000f411e c0301000 0011b1f8 b6f6b950 0011b250 000015b0 0011b1f8 00000000
[   80.214971] 7fc0: 0011b1f8 b6f6b950 000015b0 00000080 00000001 beaa0e80 001086c4 000f411e
[   80.215240] 7fe0: beaa0b38 beaa0b28 0003b270 b6e251b0 600f0010 0011b250 00000000 00000000
[   80.215913] [<bf015038>] (hello_init [hello]) from [<c030362c>] (do_one_initcall+0x54/0x214)
[   80.216217] [<c030362c>] (do_one_initcall) from [<c03d21dc>] (do_init_module+0x48/0x1ec)
```


Терминал
y_ponomarchuk@Rec
Файл Правка Вид Поиск Терминал Справка
[18.818397] hello: loading out-of-tree module taints kernel.
[18.826818] Warning: times is 7
[18.826956] Hello, world!
[18.827018] Hello, world!
[18.827064] Hello, world!
[18.827117] Hello, world!
[18.827177] Hello, world!
[18.827244] Hello, world!
[18.827834] ------------[cut here]------------
[18.827964] kernel BUG at /home/y_ponomarchuk/lab5/hello.c:51!
[18.828132] Internal error: Oops - BUG: 0 [#1] SMP ARM
[18.828389] Modules linked in: hello(O+)
[18.828905] CPU: 0 PID: 62 Comm: insmod Tainted: G O 4.19.300 #1
[18.829055] Hardware name: Generic DT based system
[18.829955] PC is at hello_init+0xfc/0x1000 [hello]
[18.830165] LR is at 0x3b72
[18.830315] pc : [<bf0050fc>] lr : [<00003b72>] psr: 600f0013
[18.830452] sp : c8b1ddb8 ip : dbceed80 fp : bf002040
[18.830585] r10: 00000000 r9 : 006000c0 r8 : bf002004
[18.830714] r7 : c135c34c r6 : c8aec600 r5 : bf002280 r4 : bf002000
[18.830868] r3 : dbbccfb4 r2 : dbbccfb0 r1 : 1a66a000 r0 : db001e40
[18.831057] Flags: nZCv IRQs on FIQs on Mode SVC_32 ISA ARM Segment none
[18.831243] Control: 10c5387d Table: 48b1806a DAC: 00000051
[18.831446] Process insmod (pid: 62, stack limit = 0x(ptrval))
[18.831627] Stack: (0xc8b1ddb8 to 0xc8b1e000)
[18.831847] dda0: c1787d20 c1604c48
[18.832206] ddc0: ffffe000 bf005000 00000000 c1604c48 00000000 c030362c c8aec380 dbd0a480
[18.832499] dde0: 00210d00 c1788a40 c1604c48 c8adc700 8040003f c1782840 c1604c48 c19c8dca
[18.832765] de00: ffe00000 c8adc240 8040003e e0b76000 c8adc240 c19c8dca e0b76000 c8adc700
[18.833050] de20: bf002040 c19c8dca bf002040 00000002 c8aec440 00000002 c8aec380 c03d21dc
[18.833338] de40: 00000001 c03d4574 c8b1df30 c8b1df30 00000002 c8aec340 00000002 c03d4590
[18.833586] de60: bf00204c 00007fff bf002040 c03d1418 c8b05418 bf002088 c8b0569c bf002234
[18.833870] de80: 00000001 bf002170 c135a998 c1220b34 c1220ba4 c1604c48 c1608f04 c8adc240
[18.834211] dea0: fffff000 e0800000 c8adc240 c8adc700 00000000 00000000 00000000 00000000
[18.834699] dec0: 00000000 00000000 6e72656b 00006c65 00000000 00000000 00000000 00000000
[18.835261] dee0: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
[18.835673] df00: 00000000 c19c8dca 00000080 000015b0 00000000 e0b775b0 0011c800 c1604c48
[18.835952] df20: 0011b1f8 ffffe000 00000051 c03d49f4 e0b762f2 e0b763c0 e0b76000 000015b0
[18.836313] df40: e0b77010 e0b76eb4 e0b76bb4 00003000 00003040 00000000 00000000 00000000
[18.836636] df60: 00001688 00000021 00000022 00000018 00000000 00000010 00000000 c19c8dca
[18.836996] df80: 000f411e 0011b1f8 b6f7d950 000015b0 00000080 c0301264 c8b1c000 00000080
[18.837327] dfa0: 000f411e c0301000 0011b1f8 b6f7d950 0011b250 000015b0 0011b1f8 00000000
[18.837648] dfc0: 0011b1f8 b6f7d950 000015b0 00000080 00000001 bed07e80 001086c4 000f411e
[18.837967] dfe0: bed07b38 bed07b28 0003b270 b6e371b0 600f0010 0011b250 00000000 00000000
[18.839000] [<bf0050fc>] (hello_init [hello]) from [<c030362c>] (do_one_initcall+0x54/0x214)
[18.839424] [<c030362c>] (do_one_initcall) from [<c03d21dc>] (do_init_module+0x48/0x1ec)
[18.839641] [<c03d21dc>] (do_init_module) from [<c03d4590>] (load_module+0x21a8/0x24b4)
[18.839894] [<c03d4590>] (load_module) from [<c03d49f4>] (sys_init_module+0x158/0x18c)
[18.840170] [<c03d49f4>] (sys_init_module) from [<c0301000>] (ret_fast_syscall+0x0/0x54)
[18.840393] Exception stack(0xc8b1dfa8 to 0xc8b1dff0)
[18.840620] dfa0: 0011b1f8 b6f7d950 0011b250 000015b0 0011b1f8 00000000
[18.840958] dfc0: 0011b1f8 b6f7d950 000015b0 00000080 00000001 bed07e80 001086c4 000f411e
[18.841239] dfe0: bed07b38 bed07b28 0003b270 b6e371b0
[18.841625] Code: e5821000 e583e000 e583c004 eb51b774 (e7f001f2)
[18.842063] ---[end trace e87f4b8b2d6051e6]---



Висновок:

Модифіковано модуль з третьої лабораторної роботи для ядра Linux, зібрано та протестовано його в середовищі програмного емулятора Qemu для архітектури процесорів ARM. При збиранні ядра та виконанні команди make помилок не виникло. При виконанні insmod/rmmod можна побачити, що драйвер працює правильно відповідно до умови завдання. Тобто BUG_ON() генерує помилку виконання, що призводить до аварійного завершення роботи ядра, це унеможливлюся виконання команди rmmod.