

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМ. І. СІКОРСЬКОГО»
ФАКУЛЬТЕТ ІНФОРМАТИКИ І ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ
КАФЕДРА ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ

Лабораторна робота №6
з курсу «ДПКС»

Виконав:
Студент 5-го курсу ФІОТ
Групи ІВ-91мп
Захарчук Д. В.

Київ – 2020

Завдання:

Ознайомитися з можливостями дебагу модуля.

Хід виконання Basic 1:

Модифікуємо файли, експортуємо необхідні параметри та виконуємо збирання модулю. Створюємо архів CPIO для rootfs. Запускаємо емулятор.

```
dmitriy@dmitriy:~/repos/busybox/_install$ mkdir lab6
dmitriy@dmitriy:~/repos/busybox/_install$ cd lab6
dmitriy@dmitriy:~/repos/busybox/_install/lab6$ ls -l
total 12
-rw-rw-rw- 1 dmitriy dmitriy 2200 чеп  3 01:29 hello.c
-rw-rw-rw- 1 dmitriy dmitriy  44 чеп  3 01:29 Kbuild
-rw-rw-rw- 1 dmitriy dmitriy 136 чеп  3 01:29 Makefile
dmitriy@dmitriy:~/repos/busybox/_install/lab6$ mv hello.c module6.c
dmitriy@dmitriy:~/repos/busybox/_install/lab6$ nano module6.c
dmitriy@dmitriy:~/repos/busybox/_install/lab6$ export PATH=/opt/gcc-arm-8.3-2019.03-x86_64-arm-eabi/bin:$PATH
dmitriy@dmitriy:~/repos/busybox/_install/lab6$ export CROSS_COMPILE='ccache arm-eabi-'
dmitriy@dmitriy:~/repos/busybox/_install/lab6$ export ARCH=arm
dmitriy@dmitriy:~/repos/busybox/_install/lab6$ export KDIR=/home/dmitriy/repos/linux-stable/
```

```
dmitriy@dmitriy:~/repos/busybox/_install/lab6$ make
make -C /home/dmitriy/repos/linux-stable/ M=$PWD
make[1]: Entering directory '/home/dmitriy/repos/linux-stable'
CC [M] /home/dmitriy/repos/busybox/_install/lab6/module6.o
/home/dmitriy/repos/busybox/_install/lab6/module6.c: In function 'module6_init':
/home/dmitriy/repos/busybox/_install/lab6/module6.c:44:2: error: expected ';' before 'if'
    if (repeats >= 5 && repeats <= 10)
    ^~
scripts/Makefile.build:309: recipe for target '/home/dmitriy/repos/busybox/_install/lab6/module6.o' failed
make[2]: *** [/home/dmitriy/repos/busybox/_install/lab6/module6.o] Error 1
Makefile:1522: recipe for target '_module_/home/dmitriy/repos/busybox/_install/lab6' failed
make[1]: *** [_module_/home/dmitriy/repos/busybox/_install/lab6] Error 2
make[1]: Leaving directory '/home/dmitriy/repos/linux-stable'
Makefile:6: recipe for target 'default' failed
make: *** [default] Error 2
dmitriy@dmitriy:~/repos/busybox/_install/lab6$ nano module6.c
Use "fg" to return to nano.

[7]+ Stopped nano module6.c
dmitriy@dmitriy:~/repos/busybox/_install/lab6$ nano module6.c
dmitriy@dmitriy:~/repos/busybox/_install/lab6$ make
make -C /home/dmitriy/repos/linux-stable/ M=$PWD
make[1]: Entering directory '/home/dmitriy/repos/linux-stable'
CC [M] /home/dmitriy/repos/busybox/_install/lab6/module6.o
Building modules, stage 2.
MODPOST 1 modules
CC /home/dmitriy/repos/busybox/_install/lab6/module6.mod.o
LD [M] /home/dmitriy/repos/busybox/_install/lab6/module6.ko
make[1]: Leaving directory '/home/dmitriy/repos/linux-stable'
dmitriy@dmitriy:~/repos/busybox/_install/lab6$ cd ..
dmitriy@dmitriy:~/repos/busybox/_install$ find . | cpio -o -H newc | gzip > ../rootfs.cpio.gz
119205 blocks
dmitriy@dmitriy:~/repos/busybox/_install$ cd ..
dmitriy@dmitriy:~/repos/busybox$ qemu-system-arm -kernel _install/boot/zImage -initrd rootfs.cpio.gz -machine virt -nographic -m 512 --append "root=/dev/ram0 rw console=ttyAMA0,115200 mem=512M"
[ 0.000000] Booting Linux on physical CPU 0x0
[ 0.000000] Linux version 4.19.116 (dmitriy@dmitriy) (gcc version 8.3.0 (GNU Toolchain for the A-profile Architecture 8.3-2019.03 (arm-rel-8.36))) #1 SMP Wed Apr 22 00:03:26 EEST 2020
[ 0.000000] CPU: ARMv7 Processor [412fc0f1] revision 1 (ARMv7), cr=10c5387d
[ 0.000000] CPU: div instructions available: patching division code
[ 0.000000] CPU: RPI2 / VPI2: populating data cache, RPI2 instruction cache
```

Модифікуємо Kbuild файл

```
dmitriy@dmitriy:~/repos/busybox/_install$ cd lab6/  
dmitriy@dmitriy:~/repos/busybox/_install/lab6$ cat Kbuild  
  
# kbuild part of makefile  
ccflags-y += -g  
obj-m := module6.o  
dmitriy@dmitriy:~/repos/busybox/_install/lab6$
```

Лістинг коду модуля.

```
#define DEBUG  
  
#include <linux/init.h>  
#include <linux/module.h>  
#include <linux/printk.h>  
  
#include <linux/ktime.h>  
#include <linux/slab.h>  
  
static LIST_HEAD(lab_list_head);  
  
struct time_keeper {  
    ktime_t time_before;  
    ktime_t time_after;  
    struct list_head time_list;  
};  
  
static void print_text(unsigned int repeats)  
{  
    unsigned int repeat;  
    struct time_keeper *ptr;  
  
    for (repeat = 0; repeat < repeats; repeat++) {  
        if (repeat == 2)  
            ptr = 0; <- Навмисно створюємо помилку  
        else  
            ptr = kmalloc(sizeof(*ptr), GFP_KERNEL);  
        ptr->time_before = ktime_get();  
        pr_info("Hello there!\n");  
        ptr->time_after = ktime_get();  
        list_add(&ptr->time_list, &lab_list_head);  
    }  
}  
  
static unsigned int repeats = 1;  
  
module_param(repeats, uint, 0444);  
MODULE_PARM_DESC(repeats, "How many times to print hello");  
  
static int __init module6_init(void)
```

```

{
    BUG_ON(repeats > 10); <- Виклик BUG_ON

    if (repeats >= 5 && repeats <= 10)
        pr_warn("Repeatition from 5 to 10 times\n");

    if (repeats == 0)
        pr_warn("No repeatition\n");

    print_text(repeats);
    return 0;
}

static void __exit module6_exit(void)
{
    struct list_head *p;
    struct list_head *n;
    struct time_keeper *curr;

    pr_info("Module 5 exit\n");

    list_for_each_safe(p, n, &lab_list_head) {
        curr = list_entry(p, struct time_keeper, time_list);
        pr_info("Time needed for printing is: %lld(ns).\n",
                curr->time_after - curr->time_before);
        list_del(p);
        kfree(curr);
    }
}

module_init(module6_init);
module_exit(module6_exit);

MODULE_AUTHOR("Dmytro Zakharchuk");
MODULE_DESCRIPTION("Test work with debug");
MODULE_LICENSE("Dual BSD/GPL");

```

Результат виконання:

Введемо параметер який буде більше 10

```
/home/dmitriy/repos/busybox/_install/lab6/module6.c:42!  
[ 54.243322] module6: loading out-of-tree module taints kernel.  
[ 54.244714] -----[ cut here ]-----  
[ 54.245254] kernel BUG at /home/dmitriy/repos/busybox/_install/lab6/module6.c:42!  
[ 54.245307] Internal error: Oops - BUG: 0 [#1] SMP ARM  
Rhythmbox  
[ 54.247232] CPU: 0 PID: 62 Comm: insmod Tainted: G          0      4.19.116 #1  
[ 54.247994] Hardware name: Generic DT based system  
[ 54.249179] PC is at module6_init+0x18/0x1000 [module6]  
[ 54.249595] LR is at do_one_initcall+0x54/0x208  
[ 54.250572] pc : [<bf005018>]   lr : [<c0302d4c>]   psr: 200f0013  
[ 54.251242] sp : c8b4fdb0   ip : c8bbb540   fp : 00000000  
[ 54.251714] r10: bf002040   r9 : c1604c48   r8 : 00000000  
[ 54.252149] r7 : bf005000   r6 : fffffe00   r5 : c1604c48   r4 : bf002000  
[ 54.252760] r3 : 00000014   r2 : 6dc64406   r1 : 00003b4d   r0 : 00000000  
[ 54.253314] Flags: nzCv IRQs on FIQs on Mode SVC_32 ISA ARM Segment none  
[ 54.254032] Control: 10c5387d Table: 48bb406a DAC: 00000051  
[ 54.254598] Process insmod (pid: 62, stack limit = 0x(ptrval))  
[ 54.255130] Stack: (0xc8b4fdb0 to 0xc8b50000)  
[ 54.255770] fda0:                                c1788000 c1604c48 fffffe00 bf005000  
[ 54.256670] fdc0: 00000000 c1604c48 bf002040 c0302d4c 00000000 c035c13c 00210d00 00000000  
[ 54.257612] fde0: c1604c48 c8b92900 c8b4fde4 6dc64406 00000000 e0c93fff ffe00000 fffff000  
[ 54.258389] fe00: 8040003f c8b92840 dbcf0560 6dc64406 dbcf0560 c8b92900 bf002040 6dc64406  
[ 54.259173] fe20: bf002040 00000002 c8bbb4c0 00000002 c8bbb400 c03d2400 00000001 c03d474c  
[ 54.259942] fe40: c8b4ff30 c8b4ff30 00000002 c8bbb3c0 00000002 c03d4768 bf00204c 00007fff  
[ 54.260655] fe60: bf002040 c03d1658 00000001 c03d0f6c bf002088 bf001110 bf00222c bf002170  
[ 54.261940] fe80: c0f089cc c13566d4 c121dbfc c121dc08 c121dc60 c1604c48 c1608ec4 c8b99180  
[ 54.262782] fea0: fffffff0 e0800000 c8b99180 c8b92900 00000000 00000000 00000000 00000000  
[ 54.263684] fec0: 00000000 00000000 6e72656b 00006c65 00000000 00000000 00000000 00000000  
[ 54.264515] fee0: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000  
[ 54.265405] ff00: 00000000 6dc64406 00000080 00001b30 00000000 e0c92b30 0012cd88 c1604c48  
[ 54.266252] ff20: 0011b1f8 fffffe00 00000051 c03d4bac e0c812b6 e0c813c0 e0c81000 00011b30  
[ 54.267427] ff40: e0c92b30 e0c921e4 e0c8e770 00003000 00003040 00000000 00000000 00000000  
[ 54.268222] ff60: 000016f4 0000002d 0000002e 00000018 00000000 00000010 00000000 6dc64406  
[ 54.268994] ff80: 000f411f 0011b1f8 b6fc7950 00011b30 00000080 c0301204 c8b4e000 00000080  
[ 54.269749] ffa0: 000f411f c0301000 0011b1f8 b6fc7950 0011b258 00011b30 0011b1f8 00000000  
[ 54.270536] ffc0: 0011b1f8 b6fc7950 00011b30 00000080 00000001 be9dde80 001086c5 000f411f  
[ 54.271325] ffe0: be9ddb38 be9ddb28 0003b270 b6e811b0 600f0010 0011b258 00000000 00000000  
[ 54.272877] [<bf005018>] (module6_init [module6]) from [<c0302d4c>] (do_one_initcall+0x54/0x208)  
[ 54.273812] [<c0302d4c>] (do_one_initcall) from [<c03d2400>] (do_init_module+0x64/0x214)  
[ 54.274386] [<c03d2400>] (do_init_module) from [<c03d4768>] (load_module+0x2150/0x243c)  
[ 54.275116] [<c03d4768>] (load_module) from [<c03d4bac>] (sys_init_module+0x158/0x18c)  
[ 54.275987] [<c03d4bac>] (sys_init_module) from [<c0301000>] (ret_fast_syscall+0x0/0x54)  
[ 54.276566] Exception stack(0xc8b4ffa8 to 0xc8b4ffff)  
[ 54.277076] ffa0:                                0011b1f8 b6fc7950 0011b258 00011b30 0011b1f8 00000000  
[ 54.277914] ffc0: 0011b1f8 b6fc7950 00011b30 00000080 00000001 be9dde80 001086c5 000f411f  
[ 54.278590] ffe0: be9ddb38 be9ddb28 0003b270 b6e811b0  
[ 54.279491] Code: e34b4f00 e5943000 e353000a 9a000000 (e7f001f2)  
[ 54.280580] ---[ end trace 9b81b3f9bfd75018 ]---  
Segmentation fault  
/lab6 #
```

Запустимо objdump та побачимо що значення PC та рядку ідентичні.

```
dmitriy@dmitriy:~/repos/busybox$ cd _install/lab6/
dmitriy@dmitriy:~/repos/busybox/_install/lab6$ arm-eabi-objdump -dS module6.ko

module6.ko:      file format elf32-littlearm

Disassembly of section .init.text:

00000000 <init_module>:

module_param(repeats, uint, 0444);
MODULE_PARM_DESC(repeats, "How many times to print hello");

static int __init module6_init(void)
{
    0: e92d47f0    push    {r4, r5, r6, r7, r8, r9, sl, lr}
      BUG_ON(repeats > 10);
    4: e3004000    movw    r4, #0
    8: e3404000    movt    r4, #0
   c: e5943000    ldr     r3, [r4]
  10: e353000a    cmp     r3, #10
  14: 0-00000000    bls     1c <init_module+0x1c>
  18: e7f001f2    .word   0xe7f001f2

      if (repeats >= 5 && repeats <= 10)
  1c: e2433005    sub     r3, r3, #5
  20: e3530005    cmp     r3, #5
  24: 8a000002    bhi     34 <init_module+0x34>
      pr_warn("Repeation from 5 to 10 times\n");
  28: e3000000    movw    r0, #0
  2c: e3400000    movt    r0, #0
  30: ebf0ffff    bl      0 <printk>

      if (repeats == 0)
  34: e5943000    ldr     r3, [r4]
  38: e3530000    cmp     r3, #0
  3c: 1a000002    bne     4c <init_module+0x4c>
      pr_warn("No repeation\n");
  40: e3000000    movw    r0, #0
```


Введемо значення від 5 до 10.

```
Please press Enter to activate this console.
/ # cd lab6
/lab6 # insmod module6.ko repeats=9
[ 37.207838] module6: loading out-of-tree module taints kernel.
[ 37.218414] Repeattion from 5 to 10 times
[ 37.218851] Hello there!
[ 37.219372] Hello there!
[ 37.219397] Unhandled fault: page domain fault (0x81b) at 0x00000000
[ 37.219992] pgd = (ptrval)
[ 37.220173] [00000000] *pgd=48ba7835, *pte=00000000, *ppte=00000000
[ 37.222121] Internal error: : 81b [#1] SMP ARM
[ 37.222819] Modules linked in: module6(0+)
[ 37.223709] CPU: 0 PID: 62 Comm: insmod Tainted: G      0      4.19.116 #1
[ 37.224213] Hardware name: Generic DT-based system
[ 37.225372] PC is at module6_init+0x9c/0x1000 [module6]
[ 37.225372] LR is at 0x17
[ 37.226150] pc : [<bf00509c>]   lr : [<00000017>]   psr: 900f0013
[ 37.226816] sp : c8b4fdb0 ip : 80000000 fp : 00000000
[ 37.227282] r10: 00000009 r9 : 006000c0 r8 : c135834c
[ 37.227685] r7 : bf0010c0 r6 : 00000003 r5 : 00000000 r4 : bf002000
[ 37.228129] r3 : 00000008 r2 : b0000000 r1 : 00000008 r0 : a771deb0
[ 37.228655] Flags: NzCv IRQs on FIQs on Mode SVC_32 ISA ARM Segment none
[ 37.229144] Control: 10c5387d Table: 48c0806a DAC: 00000051
[ 37.229607] Process insmod (pid: 62, stack limit = 0x(ptrval))
[ 37.230054] Stack: (0xc8b4fdb0 to 0xc8b50000)
[ 37.230664] fda0: c1788000 c1604c48 fffffe00 bf005000
[ 37.231525] fdc0: 00000000 c1604c48 bf002040 c0302d4c 00000000 c035c13c 00210d00 00000000
[ 37.232309] fde0: c1604c48 c8b915c0 c8b4fde4 6dc64406 00000000 e0c93fff ffe00000 fffff000
[ 37.233085] fe00: 8040003f c8b91840 dbcf1200 6dc64406 dbcf1200 c8b915c0 bf002040 6dc64406
[ 37.233868] fe20: bf002040 00000002 c8ba34c0 00000002 c8ba3400 c03d2400 00000001 c03d474c
[ 37.234626] fe40: c8b4ff30 c8b4ff30 00000002 c8ba33c0 00000002 c03d4768 bf00204c 00007fff
[ 37.235258] fe60: bf002040 c03d1658 00000001 c03d0f6c bf002088 bf001110 bf00222c bf002170
[ 37.235925] fe80: c0f089cc c13566d4 c121dbfc c121dc08 c121dc60 c1604c48 c1608ec4 c8b98180
[ 37.237348] fea0: fffff000 e0800000 c8b98180 c8b915c0 00000000 00000000 00000000 00000000
[ 37.237960] fec0: 00000000 00000000 6e7265b6 00006c65 00000000 00000000 00000000 00000000
[ 37.238704] fee0: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
[ 37.239299] ff00: 00000000 6dc64406 00000080 00001b30 00000000 e0c92b30 0012cd88 c1604c48
[ 37.239889] ff20: 0011b1f8 fffffe00 00000051 c03d4bac e0c812b6 e0c813c0 e0c81000 00011b30
[ 37.240524] ff40: e0c92b30 e0c921e4 e0c8e770 00003000 00003040 00000000 00000000 00000000
[ 37.241239] ff60: 000016f4 0000002d 0000002e 00000018 00000000 00000010 00000000 6dc64406
[ 37.241853] ff80: 000f411f 0011b1f8 b6f10950 00011b30 00000080 c0301204 c8b4e000 00000080
[ 37.242494] ffa0: 000f411f c0301000 0011b1f8 b6f10950 0011b258 00011b30 0011b1f8 00000000
[ 37.243148]ffc0: 0011b1f8 b6f10950 00011b30 00000080 00000001 bed06e80 001086c5 000f411f
[ 37.243893]ffe0: bed06b38 bed06b28 0003b270 b6dca1b0 600f0010 0011b258 00000000 00000000
[ 37.245669] [<bf00509c>] (module6_init [module6]) from [<c0302d4c>] (do_one_initcall+0x54/0x208)
[ 37.246553] [<c0302d4c>] (do_one_initcall) from [<c03d2400>] (do_init_module+0x64/0x214)
[ 37.247098] [<c03d2400>] (do_init_module) from [<c03d4768>] (load_module+0x2150/0x243c)
[ 37.247724] [<c03d4768>] (load_module) from [<c03d4bac>] (sys_init_module+0x158/0x18c)
[ 37.248288] [<c03d4bac>] (sys_init_module) from [<c0301000>] (ret_fast_syscall+0x0/0x54)
[ 37.248806] Exception stack(0xc8b4ffa8 to 0xc8b4fff0)
[ 37.249274] ffa0: 0011b1f8 b6f10950 0011b258 00011b30 0011b1f8 00000000
[ 37.249972]ffc0: 0011b1f8 b6f10950 00011b30 00000080 00000001 bed06e80 001086c5 000f411f
[ 37.250595]ffe0: bed06b38 bed06b28 0003b270 b6dca1b0
[ 37.251345] Code: eb51b020 e1a05000 eb4ed047 e2866000 (e1c500f0)
[ 37.252258] ---[ end trace 8d9b7c3c7d5a6fd8 ]---
Segmentation fault
/lab6 #
```

Запустимо objdump.

```

pr_warn("No repetition\n");
40: e3000000 movw r0, #0
44: e3400000 movt r0, #0
48: ebfffffe bl 0 <prntk>

print_text(repeats);
4c: e594a000 ldr sl, [r4]
      unsigned int index = kcalloc_index(size);

      if (!index)
          return ZERO_SIZE_PTR;

      return kmem_cache_alloc_trace(kmalloc_caches[index],
50: e3008000 movw r8, #0
54: e3a090c0 mov r9, #192 ; 0xc0
pr_info("Hello there!\n");
58: e3007000 movw r7, #0
5c: e3408000 movt r8, #0
60: e3409060 movt r9, #96 ; 0x60
64: e3407000 movt r7, #0
for (repeat = 0; repeat < repeats; repeat++) {
68: e3a06000 mov r6, #0
6c: e15a0006 cmp sl, r6
70: 0a000016 beq d0 <init_module+0xd0>
if (repeat == 2)
74: e3560002 cmp r6, #2
ptr = 0;
78: 03a05000 moveq r5, #0
if (repeat == 2)
7c: 0a000004 beq 94 <init_module+0x94>
80: e3a02018 mov r2, #24
84: e1a01009 mov r1, r9
88: e5980018 ldr r0, [r8, #24]
8c: ebfffffe bl 0 <kmem_cache_alloc_trace>
90: e1a05000 mov r5, r0
ptr->time_before = ktime_get();
94: ebfffffe bl 0 <ktime_get>
for (repeat = 0; repeat < repeats; repeat++) {
98: e2866001 add r6, r6, #1
ptr->time_before = ktime_get();
9c: e1c500f0 strd r0, [r5]
pr_info("Hello there!\n");
a0: e1a00007 mov r0, r7
a4: ebfffffe bl 0 <prntk>
ptr->time_after = ktime_get();
a8: ebfffffe bl 0 <ktime_get>
*/
static inline void list_add(struct list_head *new, struct list_head *head)

```