Київський національний університет імені Тараса Шевченка
радіофізичний факультет

лабораторна робота № 4

Роботу виконав
студент 3 курсу
Комп’ютерна Інженерія
Качмарський Олекса

Київ 2019

Хід роботи

1. Створення makefile для автоматизації збірки

```
[okachm@g04-s09 ~]$ cat makefile
ASFLAGS=-O0 -s --64 --gdwarf-2
LDFLAGS=-static

.PHONY: all clean exec


all:
        make chxid

chxid:
        as $(ASFLAGS) chxid_asm.s -o chxid.o
        ld $(LDFLAGS) chxid.o -o Chxid

clean:
        rm -f *.o Chxid

exec:
        chmod +x Chxid
```

2. Асемблювання програми-заготовки та зв'язування

```
[okachm@g04-s09 ~]$ as -o chxid.o -c chxid_asm.s
[okachm@g04-s09 ~]$ ld -static -o chxid chxid.o
[okachm@g04-s09 ~]$ make chxid
make: `chxid' is up to date.
[okachm@g04-s09 ~]$
```

3. Код програми

```
[okachm@g04-s09 ~]$ cat chxid_asm.s
.include "defs.h"

NULL = 0
SIZEOF_STRUCT_SOCKADDR = 16
ACCEPTED_CONNECTIONS = 1
CHXID_PORT_HTONS = 0x7527

.text
.bss
.align 16
.type   sock_address, @object
.size   sock_address, 16

sock_address:
        .zero   16
        .comm   sock,4,4
        .comm   sock_fd,4,4
        .globl  bash
        .section        .rodata

.bash_str_data:
        .string "/bin/bash"
        .data
        .align 8
        .type   bash, @object
        .size   bash, 8

bash:
        .quad   .bash_str_data
        .text
        .globl  main
        .type   main, @function

.section .text

.global _start
_start:
        movq    $SYS_SOCKET, %rax
        movl    $AF_INET, %edi
        movl    $SOCK_STREAM, %esi
        movl    $IPPROTO_TCP, %edx
        syscall
        movl    %eax, sock(%rip)
```

```
  movq    $SYS_BIND, %rax
  movw    $AF_INET, sock_address(%rip)
  movw    $CHXID_PORT_HTONS, sock_address+2(%rip)
  movl    sock(%rip), %edi
  movl    $SIZEOF_STRUCT_SOCKADDR, %edx
  movl    $sock_address, %esi
  syscall

  movq    $SYS_LISTEN, %rax
  movl    sock(%rip), %edi
  movl    $ACCEPTED_CONNECTIONS, %esi
  syscall

  movq    $SYS_ACCEPT, %rax
  movl    sock(%rip), %edi
  movl    $NULL, %edx
  movl    $NULL, %esi
  syscall
  movl    %eax, sock_fd(%rip)

  movq    $SYS_DUP2, %rax
  movl    sock_fd(%rip), %edi
  movl    $STDIN, %esi
  syscall

  movq    $SYS_DUP2, %rax
  movl    sock_fd(%rip), %edi
  movl    $STDOUT, %esi
  syscall

  movq    $SYS_DUP2, %rax
  movl    sock_fd(%rip), %edi
  movl    $STDERR, %esi
  syscall

  movq    $SYS_EXECVE, %rax
  movq    bash(%rip), %rdi
  movq    $NULL, %rsi
  movq    $NULL, %rdx
  syscall

  movq $SYS_EXIT, %rax
  movq $0, %rdi
  syscall
```

4. Результати роботи програми

Програма запущена:

```
[okachm@g04-s09 ~]$ ./chxid
```

Результат:

```
[okachm@g04-s09 ~]$ telnet 127.0.0.1 10101
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
echo qwqewqew
qwqewqew
echo this works
this works
```

Посилання на github репозиторій: https://github.com/skantorp/CompSystems/tree/master/Lab4

Висновок: У ході виконання лабораторної роботи я отримав навички створення файлів для автоматичної збірки, та базові знання мови асемблер.