Київський національний університет імені Тараса Шевченка
Факультет радіофізики, електроніки та комп’ютерних систем
Навчальна дисципліна «Комп’ютерні системи»

Звіт з лабораторної роботи №4

на тему ««Assember»»

Роботу виконав
Студент 3 курсу
КІ, група СА
Кравченко В’ячеслав
Васильович

Київ 2019

Хід роботи

1. Makefile для автоматизації збірки

root@g00-s00:~/lab4

```
OBJ = envp.asm

wildcards := *.s *.as *.asm

SRCS := $(basename$(wildcard$(wildcards)))
OBJS := $(SRCS:.*=.o)

ASFLAGS = -c -g --gdwarf-2
LDFLAGS = -static

lab: $(OBJ)
        nasm -f elf64 $(OBJ)
        ld $(LDFLAGS) -o lab $(OBJ).0

all: $(SRCS)

$(SRCS): $(OBJS)
        as $(ASFLAGS) -o $(OBJS) -c $(SRCS)
        ld $(LDFLAGS) -o lab $(OBJS)

.PHONY: all clean help

clean:
        rm -f $(SRCS) $(OBJS)

help:
        @echo 'make lab        build $(OBJ)'
        @echo 'make <code>     build targeted code.s|as'
        @echo 'make all        build all sources'
        @echo 'make clean      remove all binaries'
        @echo 'make help       show this help'
```

Демонстрація:

```
[root@g00-s00 lab4]# ls
envp.asm  Makefile
[root@g00-s00 lab4]# make lab
nasm -felf64 envp.asm
ld -static -o lab envp.o
[root@g00-s00 lab4]#
[root@g00-s00 lab4]# ls
envp.asm  envp.o  lab  Makefile
[root@g00-s00 lab4]# make clean
rm envp.o lab
[root@g00-s00 lab4]# ls
envp.asm  Makefile
```

2. Навички відлагоджування:

- Точки зупинки

```
[root@g00-s00 lab4]# gdb lab
GNU gdb (GDB) Red Hat Enterpris
Copyright (C) 2013 Free Softwar
License GPLv3+: GNU GPL versior
This is free software: you are
There is NO WARRANTY, to the ex
and "show warranty" for details
This GDB was configured as "x86
For bug reporting instructions,
<http://www.gnu.org/software/gc
Reading symbols from /root/lab4
(gdb) b _start
Breakpoint 1 at 0x4000b0
(gdb) b loop
Breakpoint 2 at 0x4000dc
(gdb) b string_count
Breakpoint 3 at 0x4000ed
(gdb) b output
Breakpoint 4 at 0x4000fa
(gdb) b end
Breakpoint 5 at 0x400145
```

```
(gdb) c output
Will ignore next 4194553 crossings of breakpoint 1.  Continuing.
This is env command via assembler:

Breakpoint 2, 0x00000000004000dc in loop ()
(gdb) i r
rax            0x25     37
rbx            0x1      1
rcx            0x7fffffffe5a8   140737488348584
rdx            0x25     37
rsi            0x60016e 6291822
rdi            0x1      1
rbp            0x0      0x0
rsp            0x7fffffffe590   0x7fffffffe590
r8             0x0      0
r9             0x0      0
r10            0x0      0
r11            0x202    514
r12            0x0      0
r13            0x0      0
r14            0x0      0
r15            0x0      0
rip            0x4000dc 0x4000dc <loop>
eflags         0x202    [ IF ]
cs             0x33     51
ss             0x2b     43
ds             0x0      0
es             0x0      0
fs             0x0      0
gs             0x0      0
(gdb) n
Single stepping until exit from function loop,
which has no line number information.
```

- Перехід до точок або покроково. Відображення регістрів

```
(gdb) n
Single stepping until exit from function loop,
which has no line number information.

Breakpoint 3, 0x00000000004000ed in string_count ()
(gdb) i r
rax            0x25     37
rbx            0x1      1
rcx            0x7fffffffe5a8   140737488348584
rdx            0x0      0
rsi            0x7fffffffe80a   140737488349194
rdi            0x7fffffffe80a   140737488349194
rbp            0x0      0x0
rsp            0x7fffffffe590   0x7fffffffe590
r8             0x0      0
r9             0x0      0
r10            0x0      0
r11            0x202    514
r12            0x0      0
r13            0x0      0
r14            0x0      0
r15            0x0      0
rip            0x4000ed 0x4000ed <string_count>
eflags         0x246    [ PF ZF IF ]
cs             0x33     51
ss             0x2b     43
ds             0x0      0
es             0x0      0
fs             0x0      0
gs             0x0      0
```

3. Індивідуальне завдання «Правда про своє оточення»

Створіть програму, яка виводить вміст змінних оточення власного процесу на стандартний потік виведення.

```
;macro for printing text. example: 'print info, info_length'
    %macro print 2
mov rax, SYS_WRITE
mov rdi, STDOUT
mov rsi, %1     ;first argument (info)
mov rdx, %2     ;second argument {info_length)
syscall
    %endmacro

    section .data
;defined Linux System Calls for x64
%define SYS_WRITE 1
%define STDOUT 1
%define SYS_EXIT 60

newline db 10, 0    ;newline implementation in NASM
nl_len: equ $-newline   ;length of new line

msg db "This is env command via assembler: ", 10, 0    ;message with new line
msg_len: equ $-msg  ;calculated length of message

    section .bss
envp: resq 1    ;variable for strings of env command

    section .text
global _start
_start:
print msg, msg_len

mov rbx, qword [rsp]    ; argc = *(%rsp)
lea rcx, [rsp + rbx*8 + 16] ;needed offset of cmd args ;rcx = %rsp +8 * (argc + 2)
mov qword [envp], rcx   ; **envp = rcx

loop:   ;while (envp != NULL)
mov rcx, [envp]     ;temp var for transfering value
mov rsi, qword [rcx]    ;p = *envp
mov rdi, rsi        ;temp for output
xor rdx, rdx        ;len = 0

;loop to count length of each row of environmnet array
string_count:       ;while (*p != '\0')
cmp byte [rdi], 0   ;check of LSB
je output
inc rdi         ;p++
inc rdx         ;len++
jmp string_count

output: ;printing string (%rdi is p, %rdx is length)
mov rax, SYS_WRITE
mov rdi, STDOUT
syscall

add qword [envp], 8 ;offset to next element of env
mov r8, [envp]      ;temp var for check
cmp qword [r8], 0
je end
cmp qword [envp], 0
je end

print newline, nl_len
jmp loop

end: ;exit from program
print newline, nl_len
mov rax, SYS_EXIT
xor rdi, rdi
syscall
```

```
[root@g00-s00 lab4]# ./lab
This is env command via assembler:
XDG_SESSION_ID=47
HOSTNAME=g00-s00
SELINUX_ROLE_REQUESTED=
TERM=xterm
SHELL=/bin/bash
HISTSIZE=1000
SSH_CLIENT=192.168.136.1 58579 22
SELINUX_USE_CURRENT_RANGE=
SSH_TTY=/dev/pts/0
USER=root
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=
40;31;01:mi=01;05;37;41:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=
01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.l
zma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.d
z=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.bz2=01;31:*.bz=01;31:*.tbz
=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.
sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:
*.cab=01;31:*.jpg=01;35:*.jpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01
;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.png=01;35:*.svg=01;35:*.sv
gz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35
:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=0
1;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.fl
v=01;35:*.gl=01;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.a
xv=01;35:*.anx=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=01;36:*.au=01;36:*.flac=01;36:*.mid=01;36:
*.midi=01;36:*.mka=01;36:*.mp3=01;36:*.mpc=01;36:*.ogg=01;36:*.ra=01;36:*.wav=01;36:*.axa=01;
36:*.oga=01;36:*.spx=01;36:*.xspf=01;36:
MAIL=/var/spool/mail/root
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/root/bin
PWD=/root/lab4/Kravhchenko/lab4
LANG=en_US.UTF-8
SELINUX_LEVEL_REQUESTED=
HISTCONTROL=ignoredups
SHLVL=1
HOME=/root
LOGNAME=root
SSH_CONNECTION=192.168.136.1 58579 192.168.136.146 22
LESSOPEN=||/usr/bin/lesspipe.sh %s
XDG_RUNTIME_DIR=/run/user/0
_=./lab
OLDPWD=/root/lab4
```

- Порівняйте результат виконання із результатом команди env.

```
[root@g00-s00 lab4]# env
XDG_SESSION_ID=47
HOSTNAME=g00-s00
SELINUX_ROLE_REQUESTED=
TERM=xterm
SHELL=/bin/bash
HISTSIZE=1000
SSH_CLIENT=192.168.136.1 58579 22
SELINUX_USE_CURRENT_RANGE=
SSH_TTY=/dev/pts/0
USER=root
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=
40;31;01:mi=01;05;37;41:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=
01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.l
zma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.d
z=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.bz2=01;31:*.bz=01;31:*.tbz
=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.
sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:
*.cab=01;31:*.jpg=01;35:*.jpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01
;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.png=01;35:*.svg=01;35:*.sv
gz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35
:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=0
1;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.fl
v=01;35:*.gl=01;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.a
xv=01;35:*.anx=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=01;36:*.au=01;36:*.flac=01;36:*.mid=01;36:
*.midi=01;36:*.mka=01;36:*.mp3=01;36:*.mpc=01;36:*.ogg=01;36:*.ra=01;36:*.wav=01;36:*.axa=01;
36:*.oga=01;36:*.spx=01;36:*.xspf=01;36:
MAIL=/var/spool/mail/root
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/root/bin
PWD=/root/lab4/Kravhchenko/lab4
LANG=en_US.UTF-8
SELINUX_LEVEL_REQUESTED=
HISTCONTROL=ignoredups
SHLVL=1
HOME=/root
LOGNAME=root
SSH_CONNECTION=192.168.136.1 58579 192.168.136.146 22
LESSOPEN=||/usr/bin/lesspipe.sh %s
XDG_RUNTIME_DIR=/run/user/0
_=/usr/bin/env
OLDPWD=/root/lab4
```

Отже, згідно скірншотів – вивід ідентичний, тому програма працює правильно.

ВИСНОВОК

У ході виконаня лабораторної роботи я отримав навички:

- створення файлів для автоматизації збірки
- дебагу програм (мовою ассемблер
- написання програм мовою асемблер (у синтаксисі Інтел для 64-розрядної архітектури)

Код програм та звіт містяться у репозиторії за цим посиланням (натисніть мене).