Name: _____ Entry number: _____

Verify that your exam has pages 1 to 10. Please fill the name and entry number on *every page* front and back. Do this first before starting the exam.

● During the exam, you should not have any electronic equipment including laptop, mobile phone, calculator, tablets, etc.
● The exam is open notes, open book, open slides. You can keep the printouts with you during the exam.
● Please answer each question in the provided space. Rough space is available on Pages 2, 9, and 10.

Please sign below:
I will not give or receive aid in the examination. I accept that any act of mine that can be considered to be an *Honour Code* violation will invite disciplinary action.

_____

Q1. [2.5 marks] Compiling and running programs

Write which component is responsible for each of the following function:

A [0.5 marks] Takes C source code (ASCII text), expands #include, removes comments etc, produces C source code. _____
B [0.5 marks] Takes C source code (ASCII text), does compile-time optimizations, produces assembly program (also ASCII text) .c -> .s _____
C [0.5 marks] Takes assembly program (ASCII text), produces .o file (binary, relocatable object file) .s -> .o _____
D [0.5 marks] Takes multiple '.o's, does link-time optimizations, produces a single executable object a.out (binary) *.o -> a.out _____
E [0.5 marks] Copies the program image into memory at run-time and starts executing it. ./a.out _____

Q2. [5 marks] True/False

A [0.5 marks] After `movl %eax, (%ebx)` with `%eax = 0x11223344`, the byte at address `%ebx` is `0x44`. _____

Name: _____ Entry number: _____

B [0.5 marks] On x86-32 bit, when BIOS jumps to the bootloader, the CPU is in 32-bit protected mode.

_____

C [0.5 marks] After `xorl %eax, %eax`, the zero flag (`ZF`) is set.

_____

D [0.5 marks] IOAPIC registers are accessed using IN/OUT instructions.

_____

E [0.5 marks] With DMA, the CPU runs an `insl` loop to copy data from the disk controller into memory.

_____

F [0.5 marks] A ring 3 process can execute `lidt` if its data segment descriptor has DPL 3.

_____

G [0.5 marks] A write-back buffer cache can merge several writes to the same block into one disk write.

_____

H [0.5 marks] A process can access memory belonging to another process if it knows the physical address of that memory.

_____

I [0.5 marks] A process can access memory belonging to another process if it knows the physical address of that memory.

_____

J [0.5 marks] On x86, running the `CALL` instruction stores the function's return address in a CPU register.

_____

Intentionally left blank for rough work

Name: _____ Entry number: _____

Q3. [7.5 marks] x86 assembly

For the following problems, assume foo(3, 5) is called

```
foo:
    movl 4(%esp), %eax
    movl 8(%esp), %edx
    addl %edx, %eax
    pushl %eax
    call bar
    addl $4, %esp
    ret
bar:
    movl 4(%esp), %eax
    imull $2, %eax
    ret
```

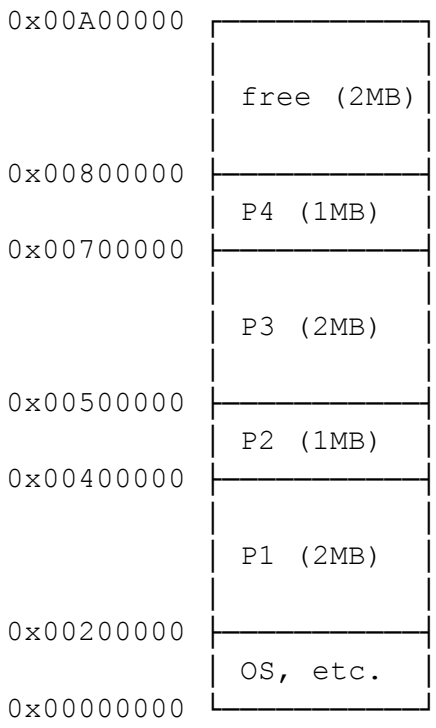
A [3 marks] Just after the `call bar` instruction, draw the stack. Highlight where `%esp` and `%eip` are pointing to.

B [1 mark] What are the values of `%eax` and `%edx` before the `call bar` instruction?

C [1 mark] What does `foo(3,5)` return?

D [2.5 marks] Rewrite `foo` to change `%edx` with `%ebx`.
HINT: ensure that `foo` adheres to the gcc calling convention.

Name: _____ Entry number: _____



Memory map

Idx	Type	Base	Size	DPL
0	null	–	–	–
1	kernel code	0x00000000	4GB	0
2	kernel data	0x00000000	4GB	0
3	P1 code	0x00200000	2MB	3
4	P1 data	0x00200000	2MB	3
5	P2 code	0x00400000	1MB	3
6	P2 data	0x00400000	1MB	3
7	P3 code			
8	P3 data			
9	P4 code			
10	P4 data			

Q4 [19 marks] Segmentation Hardware

Say our OS sets up the above Global Descriptor Table to realize the memory map shown on the right. Assume that the OS runs in Ring 0 and the processes run in ring 3. Assume that currently P3 is running. Assume that the total physical memory is only till `0x00A00000` as shown in the memory map, with the highest 2MB from `0x00800000` to `0x00A00000` free. Assume that the OS does all the allocations in multiples of 1MB.

A [3 marks] Fill the entries 7-10 in the Global Descriptor Table above.
B [2 marks] What are the values of `%cs` and `%ds`?
C [1 mark] What physical address does `%ds:0x1234` map to?

Name: _____ Entry number: _____

D [2 marks] P3 executes `movw $0x10, %ax; movw %ax, %ds` and then reads `0x1234`. Why does this not get it access to OS memory? (Recall that `movw` is an unprivileged instruction).

E [1 mark] Draw the OS' physical memory allocator's free list in the memory map above.

F [2 marks] Say P1 and P3 exit. What is the total free space available? What is the maximum size of an allocation request that can be satisfied without compaction?

G [2 marks] Say after P1 and P3 have exited, the OS wants to allocate a new process P5 with 3MB of memory. What is the minimum amount of memory that must be copied to allocate P5? Justify your answer.

H [2 marks] Why can a user level heap allocator that handles `malloc` and `free` cannot move memory in the same way that the OS could?

I [4 marks] Redraw the GDT and the free list with the changes above (P1 and P3 have exited, P5 has been allocated with 3MB of memory).

Q5 [9 marks] Protection

A [4.5 marks] Explain all the major steps that xv6 takes to stop a process from directly reading arbitrary blocks from the disk. Remember that our xv6 disk is port-mapped IO. Clearly highlight features provided by the x86 hardware and how it is leveraged by xv6.

Name: _____ Entry number: _____

B [4.5 marks] Explain all the major steps that a process needs to take to read from the disk. Clearly highlight features provided by the x86 hardware and how it is leveraged by xv6.

Q6 [7 marks] Crash consistency

Say the user deletes `/foo/bar` from an indexed file system. Assume that `/foo`'s inode is `#4`, `/foo/bar`'s inode is `#5`, `/foo`'s data block is `#23`, and `/foo/bar`'s data blocks are `#24` and `#25`.

A [3 marks] Identify all the blocks that must be written by the above deletion operation. Identify what is written on each of these blocks.

B [2 marks] Assume all disk writes are issued in parallel, identify a crash scenario which results into block leaks.

C [2 marks] Assume all disk writes are issued in parallel, identify a crash scenario which results in a situation worse than block leaks.

Intentionally left blank for rough work

Intentionally left blank for rough work