Aleksander Skjoelsvik

# CS210 PS2

## Problem 1

foo1 corresponds to choice 4
foo2 corresponds to choice 3
foo3 corresponds to choice 2
foo4 corresponds to choice 5
foo5 corresponds to choice 1
foo6 corresponds to choice 6

## Problem 2

A) The assembly code corresponds to function fun5
B) The assembly code corresponds to function fun4
C) The assembly code corresponds to function funA

## Problem 3

```
int bar(int x)
{
	int i;
	int val = 2x;

	for(i = 0, i < x, i++) {
		val += i + 7;
		val *= i + 5;
	}

	return val;
}
```

## Problem 4

| Address | Explanation | |
|---|---|---|
| **8048510** | initialize edx to emp_list | |
| **8048516** | Reset eax to 0 by xor itself | I Could've been used before, set to 0 |
| **8048518** | Push ebp (old framepointer) onto the stack | |
| **8048519** | Initialize new frame pointer | |
| **804851b** | Test to see if edx (pointer) is 0 | I Test if the object it's pointing to is empty |
| **804851d** | Jump to 804852a if zero flag set to 1 | I If it is, jump to 804852a (skip the loop) |
| **804851f** | NOP | |

| Address | Explanation | |
|---|---|---|
| **8048520** | eax = emp_list 0x58 (88/ salary) | I add the salary of current employee |
| **8048523** | Update edx to emp_list 0x5c (92/ next) | I Move the pointer to the next object |
| **8048526** | Test if edx is empty | I Test if there is another object (employee) |
| **8048528** | If zero flag != 0, jump to 8048520 | I If there is, jump to 8048520 (add another salary) |
| **804852a** | restore old frame pointer | |
| **804852b** | return | |

The ‘mystery’-function adds the salaries of the employees in emp_list

---

## Problem 5

a)

| Address | int hex value | Description |
|---|---|---|
| **0xffffd36c** | 0x08048433 | return address for call to foo |
| **0xffffd368** | 0xffffd378 | old frame pointer |
| **0xffffd364** | | |
| **0xffffd360** | 0x21646c72 | *buf* overflow causes char “rld!” to be here |
| **0xffffd35c** | 0x6f572064 | *int i* points to here. *buf* overflow causes char “o Wo” to be here |
| **0xffffd358** | 0x6c6c6548 | *buf* char “Hell” here |
| **0xffffd354** | | |
| **0xffffd350** | | |
| **0xffffd34c** | | |
| **0xffffd348** | | |
| **0xffffd344** | 0x8048504 | Pointer to char “Hello World!”, as part of parameters in call to *bar* |
| **0xffffd340** | 0xffffd354 | Pointer to *buf,* as part of parameters in call to *bar* |
| **0xffffd33c** | | |

b) Output:
0xffffd35c 0x6f572064

## Problem 6

```
typedef struct node {
        double x;
        (unsigned) short y;
        struct node *next;
        struct node *prev;
} node_t;

node_t n;

void func() {
        node_t *m;
        m = n;
        m->y /= 16;
        return;
}
```