CS 4910 Intro to Computer Security
Assignment 4

Number 1 – 5 are multiple choice questions. Chose the correct answer. 10 points for each. 50 points in total.

1. b
2. d
3. b
4. a
5. c

Number 6 -7 are short answer questions. Answer them shortly and concisely.

6. [40 points] Read the following code running on x86 system (32-bit) and answer questions.

```
1: int vulfoo()
2: {
3:   char buf[40];
4:   gets(buf);
5:   return 0;
6: }
7: int main(int argc, char *argv[])
8: {
9:   vulfoo();
10:  printf("I pity the fool!\n");
11:}
```

(i) [10 points]
The gets function does not check the size of the input, resulting in an out-of-bounds write onto the stack.

(ii) [10 points]
40 bytes buffer + 4 bytes saved ebp + 4 bytes RET = 48 bytes.

(iii) [10 points]
If the stack is executable, we can insert the shellcode into the 40-byte buffer or above the return address, and then redirect the return address to point to the stack where the shellcode is stored.

If the stack is non-executable, we can insert the shellcode into the system environment and then redirect the return address to point to the environment variable.

(iii) [10 points] How can we fix the problem of this piece of code? List three methods and simply explain them will be fine.

Base and bound check: Add size check to the local buffer.
DEP: Set the stack as non-executable.
Shado stack
Stack canary
ASLR

7. [10 points] Compare the traditional shadow stack with parallel shadow stack, including the strengths and weaknesses of each.

Performance overhead: TSS requires comparison when returns.
Code size overhead: TSS requires more instruction instrumentation than PSS.
Memory overhead: PSS requires more memory than TSS.