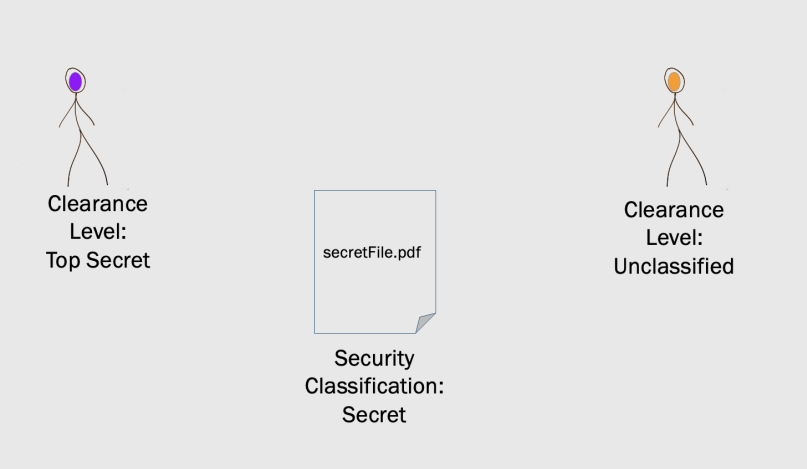
COMP435 Written Assignment 4 Name: _____

Question 1: Heartbleed The heartbleed vulnerability could have been mitigated by (check all that apply):

- ◯ Using a canary on the stack
- ◯ Correctly zeroing out freed memory
- ◯ Using W-xor-W page permissions
- ◯ Checking the length of received stringstyle



Question 2: Mandatory Access Control Models 2.1. In the above figure, Purple has a Top Secret clearance level, Orange has an Unclassified clearance level, and the file has a security classification of Secret. Under the Biba mandatory access control model, who is allowed to read the secret file?

2.2. Using the same figure, under the Bell-LaPadula mandatory access control model, who is allowed to write the secret file?

Question 3: More Mandatory Access Control Mandatory Access control models make use of which security principles?

- ◯ Defense in depth and type checking
- ◯ Separate date and control channels and fail-safe defaults
- ◯ Principle of least privilege and complete mediation
- ◯ Sepration of privilege and open design

Question 4: Integer Overflow The code in the following figure is excerpted from OpenSSH 3.3 cwe.mitre.org/data/definitions/190.html. The code has an integer overflow vulnerability

```
1 int nresp = packet_get_size();
2 if (nresp > 0) {
3   response = malloc(nresp * sizeof(char *));
4   for (i = 0; i < nresp; i++) {
5     response[i] = packet_get_char();
6   }
7 }
```

4.1. Explain the vulnerability and how it might be exploited to cause harm. Use line numbers to refer to points in the code.

4.2. Suggest a fix. If you need to add code, use the line numbers to indicate where the new code will go. If you need to delete code, use the line numbers to indicate which code gets deleted.

Question 5: Confused Deputy Attack The code in the following listing runs with root privileges (the executable has the setuid bit set) and is vulnerable to a confused deputy attack.

```
1 FILE *fp1, *fp1;
2 // open argv[2] for writing
3 fp1 = fopen(argv[2], "w");
4
5 // open fstab file to append
6 fp2 = fopen("/etc/fstab", "a");
7
8 /* update the /etc/fstab file, write any error messages
9 to the user-provided file, and exit */
```

5.1. Identify the line of code that is vulnerable.

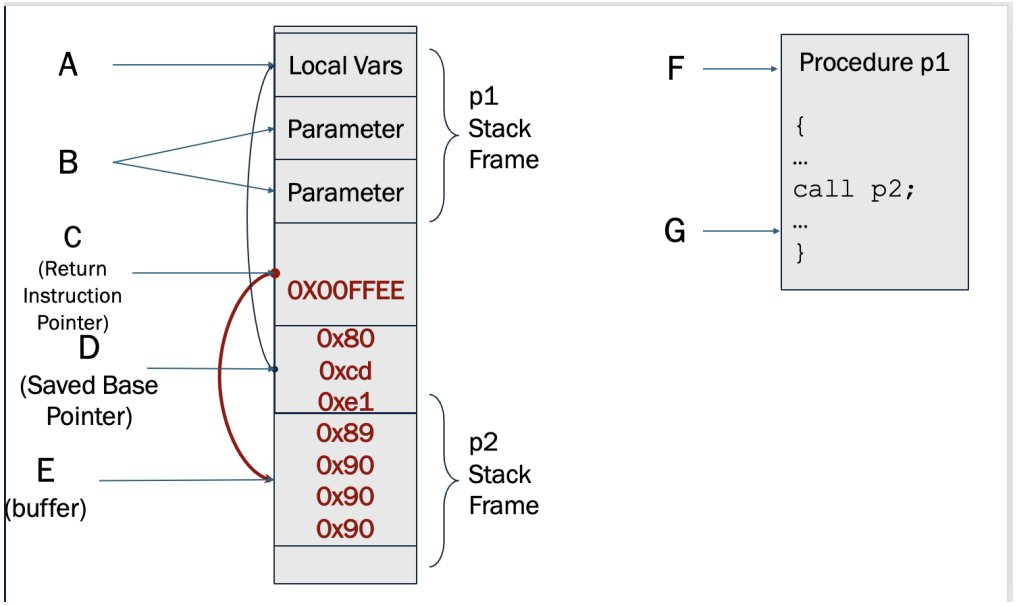
5.2. Explain the vulnerabilitiy.

5.3. What is the mechanism for making authorization decisions that is designed to stop confused deputy attacks like this one?

Question 6: Discretionary Access Control Below we have an access control matrix for a shared instructional computer, which uses a discretionary access control policy. Alice is an instructor for the course and should have read and write access to the exam and the syllabus. Bob is a TA for the course and should have only read access to the exam, and read and write access to the syllabus. Carol is a student in the course and should have no access to the exam and only read access to syllabus. Everyone can print to the attached printer. The access control matrix shown in the figure enforces this policy. Describe one way in which the spirit of the policy could be violated, despite the correct enforcement of the access control matrix

	exam.txt	printer	syllabus.txt
Instructor Alice	RW	W	RW
TA Bob	R	W	RW
Student Carol	--	W	R

Question 7: Stack / 211 Review! Consider this diagram from our discussion of buffer overflow attacks. I recommend reviewing that worksheet in preparation for the quiz!



What role does the saved base pointer (D) play in stack frame management, and how does overwriting it differ from overwriting the return address (C)?