choose one: ☐ **Received no help** ☐ **Received help from:**
(or more) ☐ **Collaborated with:**_____

Homework: /SI110/The Cyber Battlefield/Information Assurance

1. What are the "five pillars of IA"?

10/8/6/0

2. A computer in an airtight-watertight vault would be **very** secure. Why is this level of security not attainable in any practical setting?

10/8/6/0

3. Suppose you went into a Starbucks (which offers wireless Internet access to its customers) and brought radio-jamming equipment so WiFi communication was impossible. Which of the five pillars of IA is attacked in this scenario?

10/8/6/0

4. Suppose you went into a Starbucks (which offers wireless Internet access to its customers) and used a WiFi snooping tool to discover someone's session key for their online bank login, and used it to login to their account, and …

a. … did nothing but look at the info there. Which one or more of the five pillars of IA would you have attacked? Explain!

10/8/6/0

b. … actually transferred money from their account into yours. Which additional pillar of IA would be attacked? Explain!

10/8/6/0

5. Note: This question refers to the fact that most systems have a file that stores usernames and some sort of encrypted form of users' passwords, from which "password cracking" programs can sometimes recover passwords. We will, in fact, cover this in some detail later. For this problem, you do not need to understand anything more than the above simple explanation.

Suppose a group of people all have an account on the same computer. The computer's administrator inadvertently made the file containing the password hashes readable by all users. A user named Ivan Trouble uses password cracking software on the file to figure out your password and deletes all the data you had stored in your account. Match the following:

___ Threat a. Loss of all your files

___ Exploit b. Ivan Trouble 10/8/6/0

___ Vulnerability c. Running cracking software on password hash file

___ Impact d. Open permissions on password hash file

6. Go and read carefully the sections of the notes that deal with the risk equation!

Suppose a small group of aid workers have a camp in a village in Afghanistan. They have set up a wireless network (using WEP) that they use to communicate their physical (gaurds & guns) security arrangements (using HTTP).

For each of the following actions, indicate (with ↑, ↓ or -) which of the risk equation factors go up, go down, or stay the same, where we are assessing the risk of someone breaking into their WiFi network and reading the packets as they are sent on the network.

	threat	vulnerability	likelihood	impact	risk	
a. Switch to using WPA2 instead of WEP.	____	____	____	____	____	10/8/6/0
b. Use propaganda (pamplets, radio broadcasts, etc.) to convince the villagers that the aid workers are there to help.	____	____	____	____	____	10/8/6/0
c. Switch to HTTPS instead of HTTP	____	____	____	____	____	10/8/6/0
d. Reduce the broadcasting power of their base station so that the signal is not easily picked up outside of the camp.	____	____	____	____	____	10/8/6/0