

Hand in a stapled, printed copy with your answers.

Homework: /SI110/Models and Tools/Information Assurance

1. A web server that is literally plugged into the Internet for only 5 minutes each day and then disconnected would be **very** secure. Why is this level of security not practical?

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

3. Suppose you went into a Starbucks (which offers wireless Internet access to its customers) and brought radio-jamming equipment so nobody could connect to their WiFi. Which of the five pillars of IA is attacked in this

scenario?

4. Suppose afterwards, while you were still in Starbucks, you then decided to use a WiFi snooping tool to obtain someone's session key for their online bank login and then used it to login to their account. If you...

a. did nothing but simply looked at their personal info on the bank website. Which of the five pillars of IA would you have attacked? Explain!

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

Hand in a stapled, printed copy with your answers.

5. 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 recover passwords. 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 Kevin Mitnick 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. Running cracking software on password hash file |
| ___ Exploit | b. Open permissions on password hash file |
| ___ Vulnerability | c. Loss of all your files |
| ___ Impact | d. Kevin Mitnick |

6. We discussed that WEP is "weak" in terms of security; WEP passwords can actually be obtained in a matter of minutes by even a novice hacker. Recall **Risk = Likelihood * Impact**. If the local Starbucks has wireless Internet for its customers and..

a. is using WEP to encrypt their wireless network, is using WEP riskier for the Starbucks or user J. Q. Public who likes to access his government email account while sipping a latte? Explain in terms of the risk formula.

b. Which part(s) of the Risk equation go down if a stronger form of encryption is used?