1. a) In this example, integrity is violated. The definition of integrity is the ability of a system to ensure that an asset is modified only by authorized parties. Mallory is not authorized by me to change all of the images to be of puppies. Thus, integrity is violated.

   b) In this example, confidentiality is violated. The definition of integrity of confidentiality is the ability of a system to ensure that an asset is viewed only by authorized parties. Clearly, I expect the airport WiFi network to be secured, and "I" do not expect a third party to know my password and username. "I" do not authorize this third party to have my information. Thus, confidentiality is violated.

   c) In this example, privacy violated. I do not authorize the online store to share or sell my personal information to a third party, and I do not authorize any other parties to have my information. Thus, privacy is violated.

   d) The May 2017 WannaCry attacks violated availability. During the attack, data were locked and many Microsoft Windows users have to pay to decrypt their data. While the users were trying to access the data, the data was not available for them. Thus, this example violates availability.

2. a) This example violates integrity, and this is an example of fabrication. Since Mallory slip a letter into the bag, she inserts a spurious transaction to an asset. Thus, this is an example of fabrication.

   b) This example violates confidentiality, and this is an example of interception. Since Mallory secretly acquires the letter Alice send to Bob, the courier is unaware of her action, and so this action is unauthorized. Thus, this is an example of interception.

   c) This example violates integrity, and this is an example of modification. Mallory tampers the content of the letter Alice send to Bob. Thus, this is an example of modification.

   d) this example violates availability, and this is an example of interruption. After Mallory steals the letter, the courier will not have the letter in his bag anymore, so the letter is unavailable for Bob to pick up. Thus, this is an example of interruption.

   In the digital world, there is network interception attack, called replay attack, in which a data transmission between sender and receiver is maliciously or fraudulently repeated or delayed. It could be caused by the sender who sends malicious data, or it could be caused by the adversary who intercepts the data and re-transmits it.

3. a) I deter threats in this example. Since I enclose data servers in a "fire-proof" room, it is harder for hackers to attack the servers.

b) I detect threats in this example. Since sensors are installed in the server room, I would notice a flood immediately if water has entered the room.

c) I can recover from threats in this example. Since all data on the servers are backed up twice a day, if the servers break down, I could recover all data and will not suffer from losing my assets.

d) I deflect threats in this example. Since the less secure server is always left open, it is more attractive to attackers, and it makes the main servers less attractive to attackers.

4. Hash function is one-way, but encryption function is two-ways. Encrypted data can be decrypted with the right data, but hash function cannot be decrypted.

Programming question

Sploit3: In the function usage, line 176 has a format string vulnerability. This function uses **printf(output)**. In my sploit3, I make output to be filled with some spaces, an address which points to NOP, NOPs and shellcode. Once printf tries to print output, the program will eventually execute shellcode, and I get root privilege. In order to fix this problem, we can write printf("%s", output.)

Sploit4: in function the show_files, it calls the function run_cmd("ls", "-la", …). If we create a file named "ls" in the current directory, and writes shellcode into the "ls" file, the function run_cmd will read this "ls" file. Since the shellcode is in the "ls" file, the program will spawn shell, and then we get the root privilege.

User	Sploit#	Type	Flag
Alice			
Bob	4	Incomplete mediation	
Carol	2	Buffer overflow vulnerability	
David	1	Buffer overflow vulnerability	23879165ae355e02730cb36cb3f9f17b46a28e9f2ebb260972c5e0ae06cded3a –
Eve	3	Format string vulnerability	