MIS5214 **Your Name _______________________**
Week 3 **Date _________**

1. Mark works as a Network Administrator for NetTech Inc. He wants users to access only those resources that are required for them. Which of the following access control models will he use?

   A. Policy Access Control
   B. Mandatory Access Control
   C. Discretionary Access Control
   D. Role-Based Access Control

   Answer: D

2. Which of the following types of attack can be used to break the best physical and logical security mechanism to gain access to a system?

   A. Social engineering attack
   B. Cross site scripting attack
   C. Mail bombing
   D. Password guessing attack

   Answer: A

3. You are the Security Consultant advising a company on security methods. This is a highly secure location that deals with sensitive national defense related data. They are very concerned about physical security as they had a breach last month. In that breach an individual had simply grabbed a laptop and ran out of the building. Which one of the following would have been most effective in preventing this?

   A. Not using laptops
   B. Keeping all doors locked with a guard
   C. Using a man-trap
   D. A sign in log

   Answer: C

3. Which of the following terms refers to a mechanism which proves that the sender really sent a particular message?

   A. Integrity
   B. Confidentiality
   C. Authentication
   D. Non-repudiation

   Answer: D

5. Adam works as a Security Analyst for Umbrella Inc. CEO of the company ordered him to implement two-factor authentication for the employees to access their networks. He has told him that he would like to use some type of hardware device in tandem with a security or identifying pin number. Which of the following types of hardware devices will Adam NOT use to implement two-factor authentication?

   A. Biometric device

B. One Time Password
C. Proximity cards
D. Security token

Answer: B

6. Which of the following protocols uses public-key cryptography to authenticate the remote computer?

A. SSH
B. Telnet
C. SCP
D. SSL

Answer: A

7. Which of the following cryptographic system services ensures that information will not be disclosed to any unauthorized person on a local network?

A. Authentication
B. Non-repudiation
C. Integrity
D. Confidentiality

Answer: D

8. Which of the following are the examples of technical controls? Each correct answer represents a complete solution. Choose two.

A. Auditing Procedures
B. Network architecture
C. System access control systems
D. Data backups

Answer: B,C

9. Which of the following tenets does the CIA triad NOT provide for which security practices are measured? Choose all that apply.

A. Integrity
B. Accountability
C. Availability
D. Confidentiality

Answer: B

10. Which of the following types of attacks cannot be prevented by technical measures only?

A. Social engineering
B. Brute force
C. Smurf DoS
D. Ping flood attack

Answer: A