1. Which of the following are forms of malicious attack?  
a) Theft of information  
b) Modification of data  
c) Wiping of information  
d) All of the mentioned

Answer: d  
Explanation: None.

2. What are the common security threats?  
a) File Shredding  
b) File sharing and permission  
c) File corrupting  
d) File integrity

Answer: b  
Explanation: Sharing and associated permissions are usual exploits which can compromise the system.

3. From the following, which is not a common file permission?  
a) Write  
b) Execute  
c) Stop  
d) Read

Answer: c  
Explanation: None.

4. Which of the following is a good practice?  
a) Give full permission for remote transferring  
b) Grant read only permission  
c) Grant limited permission to specified account  
d) Give both read and write permission but not execute

Answer: c  
Explanation: Limited access is a key method to circumvent unauthorized access and exploits.

5. What is not a good practice for user administration?  
a) Isolating a system after a compromise  
b) Perform random auditing procedures  
c) Granting privileges on a per host basis  
d) Using telnet and FTP for remote access

Answer: d  
Explanation: Telnet and FTP are not encrypted and can be compromised.

6. Which of the following is the least secure method of authentication?  
a) Key card  
b) fingerprint  
c) retina pattern  
d) Password

Answer: d  
Explanation: Passwords can be compromised more easily than to replicate a physical thing like key card, fingerprint or retina.

7. Which of the following is a strong password?  
a) 19thAugust88  
b) Delhi88  
c) P@assw0rd  
d) !augustdelhi

Answer: c  
Explanation: It has a combination of Alphabet both capital and small along with number and special character. Thus always use complex password with a combination of all these.

8. Why is one time password safe?  
a) It is easy to generated  
b) It cannot be shared  
c) It is different for every access  
d) It is a complex encrypted password

Answer: c  
Explanation: One time password is safe since it is generated per access and thus cannot be brute forced or deduced.

9. What forces the user to change password at first login?  
a) Default behavior of OS  
b) Part of AES encryption practice  
c) Devices being accessed forces the user  
d) Account administrator

Answer: d  
Explanation: Its administrator’s job to ensure that password of the user remains private and is known only to user. But while making a new user account he assigns a random general password to give it to user. Thus even administrator cannot access a particular users account.

10. What is not a best practice for password policy?  
a) Deciding maximum age of password  
b) Restriction on password reuse and history  
c) Password encryption  
d) Having change password every 2 years

Answer: d  
Explanation: Old passwords are more vulnerable to being misplaced or compromised. Passwords should be changed periodically to enhance security.