Comptia Security+ Certification Exam

1. A security administrator is responsible for performing periodic reviews of user permission settings due to high turnover and internal transfers at a corporation. Which of the following BEST describes the procedure and security rationale for performing such reviews?

A. Ensure all users have adequate permissions and appropriate group memberships, so the volume of help desk calls is reduced.

B. Review the permissions of all transferred users to ensure new permissions are granted so the employee can work effectively.

C. Review all user permissions and group memberships to ensure only the minimum set of permissions required to perform a job is assigned.

D. Ensure former employee accounts have no permissions so that they cannot access any network file stores and resources.

Answer(s): C

---

2. Company employees are required to have workstation client certificates to access a bank website. These certificates were backed up as a precautionary step before the new computer upgrade. After the upgrade and restoration, users state they can access the bank's website, but not login. Which is the following is MOST likely the issue?

A. The IP addresses of the clients have change

B. The certificates have been installed on the CA

C. The client certificate passwords have expired on the server

D. The certificates have not been installed on the workstations

Answer(s): D

---

3. Which of the following should be done before resetting a user's password due to expiration?

A. Advise the user of new policies.

B. Verify the proper group membership.

C. Verify the user's domain membership.

D. Verify the user's identity.

Answer(s): D

---

4. A security administrator plans on replacing a critical business application in five years. Recently, there was a security flaw discovered in the application that will cause the IT department to manually re-enable user accounts each month at a cost of $2,000. Patching the application today would cost $140,000 and take two months to implement. Which of the following should the security administrator do in regards to the application?

A. Transfer the risk replacing the application now instead of in five years

B. Accept the risk and continue to enable the accounts each month saving money

C. Avoid the risk to the user base allowing them to re-enable their own accounts

D. Mitigate the risk by patching the application to increase security and saving money

Answer(s): B

---

5. A server with the IP address of 10.10.2.4 has been having intermittent connection issues. The logs show repeated connection attempts from the following IP:

A. DoS

B. DDoS

C. Xmas

D. XSS

Answer(s): A

---

6. Matt, the IT Manager, wants to create a new network available to virtual servers on the same hypervisor, and does not want this network to be routable to the firewall. How could this BEST be accomplished?

A. Create a virtual switch.

B. Create a VLAN without a default gateway.

C. Remove the network from the routing table.

D. Commission a stand-alone switch.

Answer(s): A

---

7. A supervisor in the human resources department has been given additional job duties in the accounting department. Part of their new duties will be to check the daily balance sheet calculations on spreadsheets that are restricted to the accounting group. In which of the following ways should the account be handled?

A. The supervisor should be removed from the human resources group and added to the accounting group.

B. The supervisor should be allowed to have access to the spreadsheet files, and their membership in the human resources group should be terminated.

C. The supervisor should be added to the accounting group while maintaining their membership in the human resources group.

D. The supervisor should only maintain membership in the human resources group.

Answer(s): C

---

8. Which of the following IP addresses would be hosts on the same subnet given the subnet mask 255.255.255.224? (Select TWO).

A. 10.4.4.199

B. 10.4.4.125

C. 10.4.4.158

D. 10.4.4.189

E. 10.4.4.165

Answer(s): D,E

---

9. Which of the following protocols is used to authenticate the client and server's digital certificate?

A. PEAP

B. ICMP

C. TLS

D. DNS

Answer(s): C

---

10. After running into the data center with a vehicle, attackers were able to enter through the hole in the building and steal several key servers in the ensuing chaos. Which of the following security measures can be put in place to mitigate the issue from occurring in the future?

A. Fencing

B. Video surveillance

C. Proximity readers

D. Bollards

Answer(s): D

---

11. Encryption of data at rest is important for sensitive information because of which of the following?

A. Facilitates tier 2 support, by preventing users from changing the OS

B. Prevents data from being accessed following theft of physical equipment

C. Renders the recovery of data harder in the event of user password loss

D. Allows the remote removal of data following eDiscovery requests

Answer(s): B

---

12. -- Exhibit -

A. Ping of Death

B. Smurf Attack

C. Spear Phishing

D. Replay

E. Blue Jacking

F. Xmas Attack

G. Man in the middle

H. Backdoor

Answer(s): B

---

13. Pete, a security engineer, is trying to inventory all servers in a rack. The engineer launches RDP sessions to five different PCs and notices that the hardware properties are similar. Additionally, the MAC addresses of all five servers appear on the same switch port. Which of the following is MOST likely the cause?

A. The system is using NAC.

B. The system is running 802.1x.

C. The system is in active-standby mode.

D. The system is virtualized.

Answer(s): D

---

14. Which of the following is described as an attack against an application using a malicious file?

A. Impersonation attack

B. Client side attack

C. Phishing attack

D. Spam

Answer(s): B

---

15. A hacker has discovered a simple way to disrupt business for the day in a small company which relies on staff working remotely. In a matter of minutes the hacker was able to deny remotely working staff access to company systems with a script. Which of the following security controls is the hacker exploiting?

A. DoS

B. Password recovery

C. Password complexity

D. Account lockout

Answer(s): D

---

16. To protect corporate data on removable media, a security policy should mandate that all removable devices use which of the following?

A. Application isolation

B. Data execution prevention

C. Digital rights management

D. Full disk encryption

Answer(s): D

---

17. Which of the following are Data Loss Prevention (DLP) strategies that address data in transit issues? (Select TWO).

A. Scanning copying of documents to USB.

B. Scanning of HTTP user traffic.

C. Scanning of shared drives.

D. Scanning of SharePoint document library.

E. Scanning printing of documents.

F. Scanning of outbound IM (Instance Messaging).

Answer(s): B,F

---

18. Which of the following is true about PKI? (Select TWO).

A. When encrypting a message with the private key, only the private key can decrypt it.

B. When encrypting a message with the public key, only the private key can decrypt it.

C. When encrypting a message with the private key, only the public key can decrypt it.

D. When encrypting a message with the public key, only the public key can decrypt it.

E. When encrypting a message with the public key, only the CA can decrypt it.

Answer(s): B,C

---

19. In the case of a major outage or business interruption, the security office has documented the expected loss of earnings, potential fines and potential consequence to customer service. Which of the following would include the MOST detail on these objectives?

A. Continuity of Operations

B. IT Contingency Plan

C. Disaster Recovery Plan

D. Business Impact Analysis

Answer(s): D

---

20. A security analyst has been informed that the development team has plans to develop an application which does not meet the company's password policy. Which of the following should be done NEXT?

A. Tell the application development manager to code the application to adhere to the company's password policy.

B. Inform the Chief Information Officer of non-adherence to the security policy so that the developers can be reprimanded.

C. Ask the application development manager to submit a risk acceptance memo so that the issue can be documented.

D. Contact the Chief Information Officer and ask them to change the company password policy so that the application is made compliant.

Answer(s): A