Comptia Mobility+ Certification Exam

1. Which of the following is the BEST configuration for mission critical applications such as email that require load-balancing?

A. Active/Active

B. Active/Passive

C. Active

D. Passive/Passive

Answer(s): A

---

2. Which of the following frequencies fall under the unlicensed spectrum for WiFi network access? (Select TWO).

A. 5 GHz

B. 3 GHz

C. 2.4 GHz

D. 1 GHz

E. 3.5 GHz

Answer(s): A,C

---

3. A device that maliciously transmits on the same frequency as another device, which would prevent normal wireless communication, is an example of:

A. Sandboxing

B. Rooting

C. Spoofing

D. Jamming

Answer(s): D

---

4. If a user's device is compromised, it is best practice to FIRST:

A. Lock the device.

B. Capture the logs.

C. Document the incident.

D. Wipe the device.

Answer(s): B

---

5. Which of the following are considered security protocols? (Select THREE).

A. POP3

B. 3DES

C. TLS

D. SSL

E. SMTP

F. GCM

G. IMAP

Answer(s): B,C,D

---

6. Joe, a technician, is assigned to design a wireless network for a SOHO that has to be able to support video streaming with an acceptable throughput, have good coverage for the building, and be able to support multiple channels with a full duplex capability. Which of the following is the BEST device to choose to support these requirements?

A. Bluetooth PAN

B. 802.11g AP with omni-directional antennas

C. 802.11a AP with point-multipoint antennas

D. 802.11n AP with MIMO

Answer(s): D

---

7. Which of the following ports is used as alternate SMTP?

A. 443

B. 2175

C. 587

D. 25

Answer(s): C

---

8. Which of the following is considered a best practice when maintaining awareness of new technologies?

A. Applying all firmware patches released by vendors

B. Subscribing to operating system vendor sources only

C. Subscribing to multiple sources related to the technology in question

D. Continually testing the effects of all new risks and threats

Answer(s): C

---

9. An access point that is on a network without authorization would be defined as a(n):

A. Wireless access point.

B. Rogue access point.

C. Lightweight access point.

D. Autonomous access point.

Answer(s): B

---

10. In WiFi, loss of signal strength over distance is a result of which of the following?

A. Refraction

B. Absorption

C. Attenuation

D. Reflection

Answer(s): C

---

11. Company employees are reporting wireless network connectivity issues. Which of the following can cause interference for the company wireless network? (Select TWO).

A. Refrigerators

B. Bluetooth devices

C. Microwave ovens

D. Nearby cell phone towers

E. Vending machines

Answer(s): B,C

---

12. The proper order to configure a mobile device for use with an MDM system is:

A. sign in to server, install profiles, accept certificates, install client.

B. sign in to server, install profiles, install client, accept certificates.

C. install client, sign in to server, accept certificates, install profiles.

D. install profiles, install client, accept certificates, sign in to server.

Answer(s): C

---

13. A company replicates their MDM system to a geographically separate backup site. Which of the following is the BEST option to restore normal operations as soon as possible, in the event the main site goes down?

A. Warm site

B. Hot site

C. Cold site

D. Intermediate site

Answer(s): B

14. Which of the following is the definition of jailbreak?

A. Wiping personal data and returning the device to factory settings

B. Theft of a device and use by an unauthorized user

C. Locking down a device and disabling all applications

D. Bypassing OEM OS security controls

Answer(s): D

---

15. Joe, an employee, contacts the database administrator about an issue with a local database on his hard drive. Which of the following questions would be MOST helpful in determining the next step in troubleshooting?

A. Is there a connection to the Internet?

B. What is the password being used to access the database?

C. What is the state of the database service?

D. What is the error message being received?

Answer(s): D

---

16. An administrator is tasked with remotely wiping the Chief Information Officer's (CIO's) device after it is reported stolen. Which of the following should be reviewed to determine if authentication attempts have failed after the device was stolen?

A. Logon attempts on the MDM server

B. Review cellular logs

C. Location services on the device

D. Accounts lockout on the network ID

Answer(s): D

---

17. For a device that has corporate data segregated from personal data, if the device is destroyed and replaced, which of the following must be available to ensure the BEST end-user experience on the replacement device? (Select TWO).

A. Device PIN

B. Backup of full-disk encryption key

C. Backup of MDM enrollment certificate

D. Backup of corporate data

E. Backup of personal data

Answer(s): D,E

---

18. An administrator is tasked with implementing disk encryption for information stored on a mobile device with at least 128-bits of strength. Which of the following should be applied to meet this requirement?

A. SSL

B. AES

C. SHA-1

D. DES

Answer(s): B

---

19. Ann, a user, is concerned about her power class 3 Bluetooth device not having the distance she believes it should. Specifically, Ann reports that after moving more than 15 feet (4.6 meters)

away from the paired device the connection is lost. Which of the following is the MOST likely cause?

A. 15 feet (4.6 meters) is the maximum distance for power class 3 devices.

B. Bluetooth connectivity requires line of sight for connections.

C. Interference from other devices is disrupting the connection.

D. The device is not properly paired for maximum distance.

Answer(s): C

---

20. HTTP is run over which of the following ports? (Select TWO).

A. 443

B. 8080

C. 25

D. 110

E. 80

Answer(s): B,E
