Comptia A+ Certification Exam (902)

1. A technician is dispatched to work on a computer that belonged to a recently terminated employee. The technician determines the system is hosting illegal software.

A. Immediately notify the local authorities or corporate security

B. Secure the computer to establish chain of custody

C. Back up the computer data to an IT share

D. Reimage the computer for future use

Answer(s): A

---

2. Ann, an end user, receives a call from someone claiming to be from the help desk and asking for her username and password to prevent her email box from being deleted immediately. Which of the following BEST describes this type of attack?

A. Shoulder surfing

B. Man-in-the-middle

C. Social engineering

D. Ransomware

Answer(s): C

---

3. A user's smartphone is experiencing limited bandwidth when at home. The user reports to a technician that the device functions properly when at work or in the car. Which of the following troubleshooting steps should the technician take NEXT?

A. Run any pending application or OS updates

B. Verify the SSID with which the device is associated

C. Reset the device's network settings

D. Check the data usage statistics on the device

Answer(s): C

---

4. When securing a mobile device with a screen lock, which of the following lock types use the "something you know" type of security factor? (Select TWO)

A. Swipe

B. Password

C. Face

D. Pattern

E. Fingerprint

Answer(s): B,D

---

5. A technician is working on a corporate computer and discovers illegal software in the system as well as key generators. Which of the following should the technician do NEXT?

A. Document the event for future reference

B. Contact local law enforcement

C. Delete the illegal software and files

D. Inform the technician's immediate supervisor.

Answer(s): D

---

6. A user's smartphone keeps connecting to WiFi connections. This is a security issue, and the user wants to connect to known wireless networks only. The user does not want the phone to connect to any wireless networks automatically, especially public open networks.

A. Put the phone in airplane mode

B. Use the cellular network only for data.

C. Disable the Bluetooth in phone settings.

D. Adjust the settings to prompt for WiFi networks

E. Disable WiFi when it is not needed.

Answer(s): E

---

7. A company has just experienced a data breach that affected all mobile devices. Which of the following would BEST secure access to users' mobile devices? (Choose two.)

A. OS security updates

B. SSO authentication

C. Remote backup application

D. Device profiles update

E. Biometric authentication

F. Full device encryption

Answer(s): A,E

---

8. A user receives a call from someone who claims to be part of the IT department. The IT caller instructs the user to provide the IP address of the user's computer.

A. Provide the caller with the information requested

B. Contact the IT department for conformation

C. Assume a social engineering attack and disconnect

D. Receive advice from a coworker on the situation

Answer(s): B

---

9. Which of the following features is being used when a smartphone is used to purchase a product at a retail kiosk?

A. Virtual assistant

B. NFC

C. Bluetooth

D. SDK

Answer(s): B

---

10. A technician has decided to upgrade all users' iPhones to the latest model. Which of the following is the FIRST thing the technician should advise the users to do with the old phones before turning them in?

A. Go into the device settings to remove personal customizations.

B. Enable remote wipe to clear all personal and corporate data.

C. Factory reset the old phones to ensure the data is no longer on the device.

D. Back up the mobile data with a cloud backup service.

Answer(s): D

---

11. A technician is setting up a computer that will have a hypervisor installed. The technician checks the specifications of the available computer.

A. External storage

B. Second NIC installed

C. Amount of RAM

D. Size of HDD

E. Speed of NIC

F. Graphic resolution

Answer(s): C,D

---

12. A mobile phone has started to respond slowly and erratically. The user has done a soft reset and the problem still exists. Which of the following is the BEST step the user can take to fix this problem?

A. Close running apps

B. Upgrade to a larger battery

C. Perform a force stop

D. Reset to factory default

Answer(s): D

---

13. All of the workstations in the human resources department contain sensitive employee information. Which of the following policies should the department follow while the data is still being processed?

A. Open source licensing

B. Data sanitization policy

C. PI data storage policy

D. Incident response plan

Answer(s): C

---

14. A technician is called into the office during a thunderstorm. Users are reporting that machines are intermittently powering off. Which of the following will BEST prevent user data loss?

A. A surge protector

B. A UPS

C. Auto save

D. An ESD mat

Answer(s): B

---

15. A user has an installed application that is not working properly after an update. Which of the following could help resolve the issue? (Select TWO.)

A. Use Regsvr32 to reregister the application.

B. Delete the application folder and reinstall it

C. Select the repair option under Program and Features

D. Use the application's uninstall feature, reboot, and reinstall

E. Reinstall the application, and then run SFC to verify any changes

Answer(s): C,E

---

16. A technician is working on a computer when the PC suddenly experiences a blue screen and restarts before the technician can note the error message. The computer boots up normally, and the technician now wants to know which error message was displayed. Which of the following should the technician use to help troubleshoot the issue?

A. msconfig

B. msinfo32

C. eventvwr

D. sfc

E. regedit32

Answer(s): C

---

17. A user needs access to files within a shared folder on a Linux server. The user is mapped to the folder but cannot access the files. Which of the following tools should the technician use to give the user access to these files? (Select two.)

A. netshare

B. groups

C. chmod

D. apt-get

E. passwd

F. chown

Answer(s): C,F

---

18. Which of the following statements is true regarding the differences between a 32-bit and 64-bit OS?

A. A 32-bit version of the OS requires twice the number of CPU clock cycles to write the same amount of data as a 64-bit OS.

B. A 32-bit version of the OS will not run on 64-bit hardware, but a 64-bit OS will run on 32-bit hardware.

C. A 64-bit version of the OS will write data to disk in block sizes of eight octets

D. A 64-bit version of the OS will address memory in eight octets.

Answer(s): D

---

19. Which of the following is a risk of implementing a BYOD policy?

A. Higher risk of phishing attacks

B. Different encryption technology

C. DHCP may fail due to incompatibility

D. Introducing malware onto the network

Answer(s): D

---

20. The network administrator is investigating latency on a WiFi network. The administrator discovers a number of unidentified devices connected and wishes to limit access to only authorized users. Which of the following will BEST meet the requirement?

A. Enable MAC filtering

B. Assign static IP addresses

C. Disable SSID broadcast

D. Limit the DHCP scope

Answer(s): A