9628-07 Level 3 Award in Mobile and Operating Systems (for the Level 3 Infrastructure Technician Apprenticeship)
9628-307 Mobile and Operating Systems

Sample question paper

Duration: 45 minutes

Candidate's name:

Candidate's enrolment number:

Centre name:

Centre number:

Date:

1 What is the function of a hardware server?

a. A mobile device for personal use.
b. A computer that is dedicated to sharing data and resources.
c. A laptop computer for personal use.
d. A computer that runs multiple virtualised operating systems.

2 Which one of the following would be **best** for storing confidential data?

a. A virtual server accessed using the internet.
b. A standalone computer with no networking connections.
c. A laptop computer.
d. A mobile device.

3 Which one of the following would be **best** for a travelling sales representative who needs to have access to both MS Windows and Mac OS?

a. A desktop and laptop computer running different systems.
b. A laptop computer.
c. A laptop computer that has been virtualised.
d. A mobile device.

4 What is an **essential** feature of Firmware?

a. It can be reprogrammed when needed.
b. It is coded into system hardware.
c. It requires regular system updates.
d. It can be applied to different systems.

5 Which of the following are tasks performed by Operating Systems?

a. Editing videos.
b. Word processing.
c. Requesting downloads and displaying web pages from the internet.
d. Controlling computer hardware and organising the running of software.

6 Which one of the following is a command line program?

a. An application that has a rich Graphical User Interface (GUI).
b. An internet web browser.
c. A program that only accepts typed instructions.
d. A desktop publishing application.

7 Which one of the following methods of disposal meets Waste Electrical and Electronic Equipment recycling regulations?

a. Computer equipment can be put in with normal waste.
b. Computer equipment must have all data erased.
c. Electrical equipment must be incinerated.
d. Electrical batteries must be recycled professionally.

8 Which one of the following **must** be included in an end-to-end test plan?

a. Pass and fail criteria for later evaluation.
b. A record of each test result.
c. The cause of any test failure.
d. Corrective action in the event of a pass.

9 Which one of the following is a **key** part of an end-to-end test execution?

a. Define an approach on how to carry out the test plan.
b. Carry out a test as documented in the test plan.
c. Select what will be tested.
d. Define the scope of the test.

10 Following an end-to-end test, which one of the following would be the **most** appropriate action to take if a newly installed system is not working correctly?

a. Analyse the test execution and agree a new test plan.
b. Review the test plan and identify elements for change.
c. Review the results and create a new testing methodology.
d. Analyse results and agree appropriate corrective action.

11 Which one of the following **best** describes the purpose of a command line interface (CLI)?

a. It allows user interaction with the OS via a typewritten interface.
b. It is a graphical user interface (GUI).
c. It is only used to run system backups.
d. It stops malware and Trojans from infecting the computer system.

12 What are accessibility tools used for?

a. Adapting the system time based on local time zone.
b. Adjusting the firewall access settings for online gaming.
c. Adapting the system for vision impaired individuals.
d. Adjusting the language settings for non-English readers.

13 What is a built-in editor used for?

a. Editing images.
b. Editing system settings and script files.
c. Collecting error messages via syslog.
d. Parsing and sorting large data sets.

14 Which one of the following is the correct definition of cryptographic hashing?

a. A form of symmetric encryption.
b. A function that is one way and cannot be reversed.
c. A function that generates public and private keys.
d. A form of asymmetric decryption.

15 Which one of the following **best** describes the role of 'groups' when setting member permissions to use a system resource?

a. Users can only be a member of a single group on any computer system.
b. Users can override their group rights based on their sudo rights.
c. Some groups can be merged to form superusers on some systems.
d. They are a collection of users with the same inherited rights.

16 Which anti-malware tool is **primarily** used to protect against information being passed on without authorisation?

a. Anti-virus software.
b. Anti-spyware software.
c. Software firewall.
d. Encryption software.

17 Which one of the following **best** describes the use of 'authentication policy enforcement'?

a. The authentication process is the same for all users.
b. The password is not the same for different users.
c. All users are regularly audited.
d. All users authenticate periodically.

18 Which one of the following statements is **not** correct regarding anti-malware?

a. It focuses on newer threats than anti-virus software.
b. It removes all non-essential programmes and utilities.
c. It protects users from the latest threats.
d. It updates rules faster than anti-virus software.

19 Which one of the following cable types supports communication over 150 metres?

a. Cat 5.
b. Cat 5e.
c. Cat 6.
d. Fibre.

20 Which one of the following is a tool used to deploy software to remote mobile devices?

a. Mobile Device Management (MDM).
b. User configuration tools.
c. Mobile operating system updates.
d. Push notifications.

21 What are the **most** important security factors for providing remote access to business data on a mobile device?

a. Authentication and bandwidth.
b. Monitoring and performance.
c. Performance and encryption.
d. Authentication and encryption.

22 Which protocol uses a RADIUS server for authentication?

a. WAP.
b. WEP.
c. WPA2 Personal.
d. WPA2 Enterprise.

23 Which one of the following **best** describes an authentication method?

a. It is a technology that can establish a user's identity.
b. It is a technology that provides access permissions to users.
c. It is technology that enables access via secure means.
d. It is technology that provides users with passwords.

24 Which one of the following is the **main** security vulnerability when authenticating a user during remote support?

a. Two factor authentication.
b. AES encryption.
c. Asymmetric encryption.
d. The individual delivering the support.

25 Which one of the following is the **main** security consideration when a user requires access to a secure database?

a. Ensuring that they are able to gain access.
b. Ensuring that they have the correct authorisation.
c. Having a 24/7 help desk to resolve access issues.
d. Having a set of personal questions to authenticate the user.

26 Which one of the following is the **most** likely reason to remotely wipe a secure mobile device?

a. It has been left in a secure office.
b. It has been left at the user's home.
c. It has been lost on public transport.
d. It has been handed to the police as lost property.

27 What must be considered **before** commencing remote desktop support service to a customer who has agreed to subscribe to this?

a. Customer's staff concerns about privacy issues.
b. IP addressing conflicts and potential duplication.
c. Local host software licensing and copyright issues.
d. Compatibility with existing systems.

28 Which one of the following is **not** a valid reason for BYOD management?

a. The device is being used in a secure environment.
b. The device is being used in an insecure environment.
c. The device may not be PIN protected.
d. The company software can only be used in specific locations.

29 Which one of the following should **not** be included in an organisational disaster recovery plan?

a. Contact information.
b. Guidelines on use.
c. Step-by-step recovery procedures.
d. How to respond to data protection requests.

30 Which one of the following is a **key** element of an acceptable use policy?

a. PIN protection is not required on mobile devices.
b. Passwords are the responsibility of the organisation to manage.
c. Users should be guided on the types of network they can connect to.
d. Employees are not responsible for the safety of unattended equipment.

NOW GO BACK AND CHECK YOUR WORK

- IMPORTANT -
  Are the details at the top of the answer sheet correct?

See next page