

**9628-07 Level 3 Award in Mobile and Operating Systems (for the
Level 3 Infrastructure Technician Apprenticeship)**
9628-807 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 one 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?
- Analyse the test execution and agree a new test plan.
 - Review the test plan and identify elements for change.
 - Review the results and create a new testing methodology.
 - Analyse results and agree appropriate corrective action.
- 11 Which one of the following **best** describes the purpose of a command line interface (CLI)?
- It allows user interaction with the OS via a typewritten interface.
 - It is a graphical user interface (GUI).
 - It is only used to run system backups.
 - It stops malware and Trojans from infecting the computer system.
- 12 What are accessibility tools used for?
- Adapting the system time based on local time zone.
 - Adjusting the firewall access settings for online gaming.
 - Adapting the system for vision impaired individuals.
 - Adjusting the language settings for non-English readers.
- 13 What is a built-in editor be used to for?
- Editing images.
 - Editing system settings and script files.
 - Collecting error messages via syslog.
 - Parsing and sorting large data sets.
- 14 Which one of the following is the correct definition of cryptographic hashing?
- A form of symmetric encryption.
 - A function that is one way and cannot be reversed.
 - A function that generates public and private keys.
 - 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?
- Users can only be a member of a single group on any computer system.
 - Users can override their group rights based on their sudo rights.
 - Some groups can be merged to form superusers on some systems.
 - 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?
- Anti-virus software.
 - Anti-spyware software.
 - Software firewall.
 - Encryption software.
- 17 Which one of the following **best** describes the use of 'authentication policy enforcement'?
- The authentication process is the same for all users.
 - The password is not the same for different users.
 - All users are regularly audited.
 - All users authenticate periodically.
- 18 Which one of the following statements is **not** correct regarding anti-malware?
- It focuses on newer threats than anti-virus software.
 - It removes all non-essential programmes and utilities.
 - It protects users from the latest threats.
 - It updates rules faster than anti-virus software.
- 19 Which one of the following cable types supports communication over 150 metres?
- Cat 5.
 - Cat 5e.
 - Cat 6.
 - Fibre.

- 20 Which one of the following is a tool used to deploy software to remote mobile devices?
- Mobile Device Management (MDM).
 - User configuration tools.
 - Mobile operating system updates.
 - Push notifications.
- 21 Which protocol uses a RADIUS server for authentication?
- WAP.
 - WEP.
 - WPA2 Personal.
 - WPA2 Enterprise.
- 22 Which one of the following **best** describes an authentication method?
- It is a technology that can establish a user's identity.
 - It is a technology that provides access permissions to users.
 - It is technology that enables access via secure means.
 - It is technology that provides users with passwords.
- 23 Which one of the following is the **main** security vulnerability when authenticating a user during remote support?
- Two factor authentication.
 - AES encryption.
 - Asymmetric encryption.
 - The individual delivering the support.
- 24 Which one of the following is the **main** security consideration when a user requires access to a secure database?
- Ensuring that they are able to gain access.
 - Ensuring that they have the correct authorisation.
 - Having a 24/7 help desk to resolve access issues.
 - Having a set of personal questions to authenticate the user.
- 25 Which one of the following is the **most** likely reason to remotely wipe a secure mobile device?
- It has been left in a secure office.
 - It has been left at the user's home.
 - It has been lost on public transport.
 - It has been handed to the police as lost property.
- 26 What must be considered **before** commencing remote desktop support service to a customer who has agreed to subscribe to this?
- Customer's staff concerns about privacy issues.
 - IP addressing conflicts and potential duplication.
 - Local host software licencing and copyright issues.
 - Compatibility with existing systems.
- 27 Which one of the following is **not** a valid reason for BYOD management?
- The device is being used in a secure environment.
 - The device is being used in an insecure environment.
 - The device may not be PIN protected.
 - The company software can only be used in specific locations.
- 28 What are the **most** important security factors for providing remote access to business data on a mobile device?
- Authentication and bandwidth.
 - Monitoring and performance.
 - Performance and encryption.
 - Authentication and encryption.
- 29 Which one of the following should **not** be included in an organisational disaster recovery plan?
- Contact information.
 - Guidelines on use.
 - Step-by-step recovery procedures.
 - 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?

