DUMPSBOSS.

CompTIA IT Fundamentals+ Certification Exam

CompTIA FC0-U61

Version Demo

Total Demo Questions: 45

Total Premium Questions: 454

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, IT Concepts and Terminology	50
Topic 2, Infrastructure	133
Topic 3, Applications and Software	36
Topic 4, Software Development	52
Topic 5, Database Fundamentals	66
Topic 6, Security	117
Total	454

QUESTION NO: 1

Which of the following BEST describes a LAN-hosted application? (Choose two.)

A. Internet access required

B. Services required

C. Network required

D. Files saved to the cloud

E. Internet access not required

F. Cloud availability

ANSWER: C E

Explanation:

A LAN-hosted application is made available from resources located within an organization's local area network rather than from a public cloud or Internet-based service. Therefore, **Network required** is correct: client devices must be connected to the local network to reach the application server or its shared resources. The connection may be wired Ethernet or Wi-Fi, but the application depends on LAN connectivity between the client and the internal host.

Internet access not required is also correct because the application and its supporting server can operate entirely inside the local network. Users can access an internally hosted file server, database application, intranet site, or line-of-business application while the organization has no external Internet connection, provided that the LAN and the required local server remain available. A LAN is specifically a network that connects devices over a limited geographic area, such as an office, school, or building. Hosting the application on that internal network distinguishes it from an Internet-hosted or cloud-hosted application. See the Cloudflare overview of local area networks and the CISA guidance on web application technologies.

QUESTION NO: 2

A network has been infected with a worm. Which of the following would be the BEST security measures to take? (Choose two.)

A. Update the IPS signatures.

B. Update the network firewall.

C. Update the malware definitions.

D. Quarantine the network.

E. Reset the network router.

F. Contact the ISP.

ANSWER: C D

Explanation:

Update the malware definitions. and **Quarantine the network.** are the best immediate measures following a worm infection. A worm is self-replicating malware that can spread rapidly across systems and network segments, often without requiring a user to open an infected file. Quarantining the affected network, hosts, or segments is a containment action: it limits communication with unaffected devices and prevents further propagation while responders investigate and remediate the incident. This containment step should occur promptly so that the organization can preserve the scope of the incident and reduce additional damage.

Updating malware definitions ensures endpoint security tools can recognize the currently identified worm and associated malicious components. Administrators can then run updated anti-malware scans, identify affected systems, remove or remediate the infection, and verify that systems are safe before returning them to normal network access. These actions

align with incident-response practice: contain the threat first, then use current detection capabilities to eradicate it and restore operations. The Cybersecurity and Infrastructure Security Agency describes containment, eradication, and recovery as core incident-response activities in its incident response guidance. Microsoft also explains the importance of maintaining current security intelligence for effective malware detection in Microsoft Defender Antivirus protection updates.

QUESTION NO: 3

Which of the following filesystems would a Linux computer MOST likely use?

A. HFS

B. NTFS

C. FAT32

D. ext4

ANSWER: D

Explanation:

ext4 is the filesystem a Linux computer would most likely use. The ext family of filesystems was designed for Linux, and ext4 is a mature, widely supported default choice across many Linux distributions. It provides core capabilities expected for a modern operating-system filesystem, including journaling to help preserve filesystem consistency following an unexpected shutdown, support for large files and volumes, extent-based allocation for efficient storage management, and improved reliability over earlier ext versions.

Although a Linux system can read or use several filesystem formats when compatibility is needed, its normal local system partitions are commonly formatted with a native Linux filesystem. ext4 is broadly available in Linux installers, kernels, administration tools, and boot environments, making it an appropriate general-purpose selection for Linux installations. The Linux kernel documentation describes ext4 as the “fourth extended filesystem,” and documents its supported features and behavior. The Ubuntu installation documentation also identifies ext4 as the standard filesystem format used for Linux partitions in typical installations.

References: Linux kernel documentation: ext4 filesystem and Ubuntu Community Help: Partitioning.

QUESTION NO: 4

A startup company has created a logo. The company wants to ensure no other entity can use the logo for any purpose. Which of the following should the company use to BEST protect the logo? (Select TWO).

A. Patent

B. Copyright

C. NDA

D. Trademark

E. EULA

ANSWER: B D

Explanation:

Copyright and **Trademark** provide complementary protection for a company logo. Copyright protection applies to an original logo as a creative visual work fixed in a tangible form. It gives the copyright owner exclusive rights to reproduce, distribute, display, and create derivative versions of that artwork. A startup obtains copyright protection automatically when the original logo is created, although registration provides important additional legal benefits, including a public record of the claim and stronger enforcement options.

Trademark protection applies to the logo when it identifies the source of the company's goods or services. Registering and using the logo as a trademark helps the company establish exclusive brand rights in the relevant marketplace and allows it to prevent uses that are likely to cause consumer confusion about the origin, sponsorship, or affiliation of products or services. Together, copyright protects the logo's artistic expression, while trademark protects its role as a distinctive business identifier. The U.S. Copyright Office discusses protection for visual artwork at copyright.gov, and the U.S. Patent and Trademark Office explains trademarks at uspto.gov.

QUESTION NO: 5

A regulation requires new applicants to provide a scan of their retinas in case of any future legal questions regarding who applied for the position. Which of the following concepts is this an example of?

A. Non-repudiation

B. Authentication

C. Integrity

D. Accounting

ANSWER: A

Explanation:

Non-repudiation is the correct concept because the retinal scan is being retained as evidence that can link a particular person to the act of submitting an application. The key detail is the stated purpose: resolving possible future legal questions about who applied. In this context, the biometric record provides strong identity evidence so that an applicant cannot credibly deny having been the individual associated with that application, and the organization can support its claim about the applicant's identity.

Non-repudiation is an assurance that an action or transaction can be attributed to an identified party and that the party cannot later reasonably deny it. Biometrics, including retinal characteristics, can contribute to that assurance when they are securely collected, associated with the relevant record, and protected against alteration. The U.S. National Institute of Standards and Technology defines non-repudiation as assurance that a party cannot deny the validity of an action or associated data. See the NIST Computer Security Resource Center definition of non-repudiation. NIST also discusses the role of biometric characteristics in identity proofing and authentication in NIST SP 800-63A.

QUESTION NO: 6

The IT department has established a new password policy for employees. Specifically, the policy reads:

- Passwords must not contain common dictionary words
- Passwords must contain at least one special character.
- Passwords must be different from the las six passwords used. ▪ Passwords must use at least one capital letter or number.

Which of the following practices are being employed? (Choose two.)

A. Password lockout

B. Password complexity

C. Password expiration

D. Passwords history

E. Password length

F. Password age

ANSWER: B D

Explanation:

Password complexity is being employed because the policy requires passwords to include specific character types, including at least one special character and at least one capital letter or number. It also disallows common dictionary words. Together, these requirements restrict predictable password choices and require a password to meet defined composition rules. In a Windows-based environment, password-complexity policies can require a mix of character categories and can prevent users from selecting easily guessed credentials. Microsoft describes these types of settings in its password-policy guidance: Microsoft password policy guidance.

Password history is also being employed because users must choose a password different from the last six passwords they used. A password-history setting records a specified number of previous passwords and prevents their reuse, helping ensure that a user cannot simply cycle back to a recent credential after changing it. This supports stronger credential management by making password changes meaningful rather than allowing repeated use of familiar passwords. NIST likewise addresses preventing the reuse of recently used passwords in its digital identity guidance: NIST SP 800-63B.

QUESTION NO: 7

Which of the following are characteristics of a programming loop? (Choose two.)

A. Repeating code

B. Testing a condition

C. Declaring a variable

D. Adding a comment

E. Compiling source code

ANSWER: A B

Explanation:

A loop is a programming construct that repeats one or more instructions. **Repeating code** is therefore a defining characteristic of a loop. **Testing a condition** is also common because many loops continue or stop depending on whether a condition is true, such as whether a counter has reached a specified value.

Declaring a variable reserves a named location for data, while a comment documents code for people reading it. Compiling source code is a separate process that translates source code into another executable form. Python describes `for` and `while` statements in its control flow documentation.

QUESTION NO: 8

A technician is installing an MF

D.

After installation, all functions work except faxing. Which of the following interfaces is required to enable faxing functionality?

A. RJ11

B. RJ45

C. USB

D. Bluetooth

ANSWER: A

Explanation:

RJ11 is required because the fax feature of a multifunction device must connect to an analog telephone line in order to send and receive fax transmissions. An RJ11 connector is the common modular connector used for standard telephone service and is typically connected from the device's LINE or LINE IN port to a wall telephone jack. Once that physical telephone-line connection is present and the fax settings, such as dialing mode and fax number, are configured, the device can communicate with remote fax machines over the telephone network. This requirement is separate from the connection used for printing, scanning, or network access. In particular, a device may already be successfully connected to a computer or local network and still be unable to fax until its dedicated telephone-line port is connected. Manufacturers commonly document fax setup as connecting the supplied phone cord between the fax machine's line port and the telephone wall outlet. See HP's fax setup guidance and Brother's telephone line connection instructions.

QUESTION NO: 9

Which of the following are valid reasons to create regular backups of business data? (Choose two.)

A. Recover from accidental deletion.

B. Restore data after hardware failure.

C. Prevent all unauthorized logins.

D. Eliminate the need for software updates.

E. Prevent storage devices from failing.

ANSWER: A B

Explanation:

Recover from accidental deletion. and **Restore data after hardware failure.** are correct. A backup is a separate copy of data that can be used to restore information when the original files are unavailable, corrupted, deleted, or lost. Regular backups give an organization recovery points that can reduce the impact of common data-loss events.

Backups do not prevent hardware from failing, replace the need for access controls, or guarantee that malware cannot infect a system. However, properly protected backups can support recovery after a malware incident. The National Institute of Standards and Technology provides guidance on protecting and recovering data in NIST data backup guidance.

QUESTION NO: 10

Which of the following operating systems do not require extensions on files to execute a program? (Select

TWO).

A. Windows 7

B. Windows 8

C. UNIX

D. Windows Server 2012

E. Android

F. Linux

ANSWER: C F

Explanation:

UNIX and Linux use the executable permission associated with a file, rather than a filename extension, to control whether a user may execute it as a program. On these systems, permissions include read, write, and execute settings for the file owner, group, and other users. When the execute permission is set, the operating system can attempt to run the file. For a compiled executable, the system recognizes the file's binary format; for an interpreted script, a shebang line such as `#!/bin/sh` identifies the interpreter to use. Consequently, an executable can have no extension at all, or it can have an extension chosen simply for readability or convention.

This behavior is fundamental to UNIX-style operating systems and is why commands such as `ls`, `cat`, and many installed applications are commonly named without extensions. Administrators use commands such as `chmod +x` to grant execute permission. GNU's documentation describes the execute permission as the permission required to run a file, and the Linux `execve()` documentation describes how executable files and interpreter scripts are invoked. See the GNU Coreutils file-permission documentation and the Linux execve(2) manual page.

QUESTION NO: 11

Which of the following describes the ability to recover access to a specific account if a credential is forgotten?

A. Password manager

B. Password reuse

C. Password history

D. Password reset

ANSWER: D

Explanation:

Password reset is the process that enables a user to regain access to an individual account after forgetting a password or other credential. A properly designed reset process first verifies the requester's identity, often through a recovery email address, a verified phone number, multifactor authentication, recovery codes, or help-desk identity validation. After successful verification, the service permits the user to create a new password and restores access to that specific account. This is an important account-management and security capability because it provides a controlled recovery path without requiring the existing password to be known or disclosed. Organizations should ensure that password-reset workflows use secure, time-limited recovery links or codes and require appropriate identity proofing, since reset mechanisms are common targets for account takeover attempts. Microsoft describes self-service password reset as allowing users to reset or unlock their passwords without administrator or help-desk intervention, following verification methods configured by the organization. The NIST Digital Identity Guidelines also address secure account recovery and identity proofing considerations for authenticator recovery. See Microsoft Learn: How self-service password reset works and NIST SP 800-63B: Digital Identity Guidelines.

QUESTION NO: 12

A computer user is downloading software from the Internet and notices the following at the end of the install file: â€œâ€¦x86.exeâ€□. Which of the following statements BEST represents what the â€œâ€¦x86.exeâ€□ means in the installation file?

A. x86 only supports an installation on a 32-bit CPU architecture.

B. x86 supports an installation on a 32-bit and a 64-bit CPU architecture.

C. x86 only supports an installation on a 64-bit CPU architecture.

D. x86 supports an installation on a 16-bit CPU architecture.

ANSWER: B

Explanation:

The statement “x86 supports an installation on a 32-bit and a 64-bit CPU architecture” is the best answer. In software download names, *x86* conventionally identifies a 32-bit build of an application, based on the Intel-compatible x86 instruction-set family. It is intended for a 32-bit operating-system environment, but it can also normally be installed and run on a compatible 64-bit version of Windows. This compatibility exists because 64-bit Windows includes the Windows-on-Windows 64 subsystem, commonly called WOW64, which provides the environment needed for many 32-bit applications to execute on 64-bit Windows systems. Therefore, the filename does not mean that the program is restricted to a physical 32-bit processor. Instead, it identifies the application binary as a 32-bit executable. The `.exe` extension indicates an executable program file for Windows. When selecting a download, users should match the package to the operating system and processor architecture; an x86 package is the appropriate choice for a 32-bit Windows installation and is generally usable on a 64-bit Windows installation as well. Microsoft documents WOW64 compatibility and execution support for 32-bit applications on 64-bit Windows in its WOW64 implementation documentation and guidance for running 32-bit applications.

QUESTION NO: 13

The IT department has established a new password policy for employees. Specifically, the policy reads:

Passwords must not contain common dictionary words

Passwords must contain at least one special character.

Passwords must be different from the las six passwords used.

Passwords must use at least one capital letter or number.

Which of the following practices are being employed? (Select TWO).

A. Password lockout

B. Password complexity

C. Password expiration

D. Password history

E. Password length

F. Password age

ANSWER: B D

Explanation:

Password complexity is being employed because the policy requires passwords to include varied character types, specifically at least one special character and at least one uppercase letter or number. It also disallows common dictionary words, helping ensure that passwords are less predictable and more resistant to guessing and dictionary-based password attacks. Complexity requirements define characteristics that a newly chosen password must satisfy rather than merely controlling when it can be used.

Password history is also being employed because employees must choose a password different from their previous six passwords. A password-history setting retains a defined number of prior password hashes and compares a proposed new password against them. This prevents rapid recycling of a small set of familiar passwords and ensures that a password change results in a meaningfully new credential. Together, these controls govern both the construction of a password and whether it has been used recently. Microsoft describes password-history enforcement in its Enforce password history policy documentation, and NIST discusses password-verifier considerations, including screening passwords against commonly used or compromised values, in SP 800-63B.

QUESTION NO: 14

A security administrator needs to set up multifactor authentication for a cloud application. Which of the following should the administrator use to establish an authentication process? (Choose two.)

A. Logs

B. Password

C. Receipt

D. Encryption

E. Database

F. Software token

ANSWER: B F

Explanation:

Multifactor authentication requires authentication evidence from at least two different factor categories. **Password** supplies a knowledge factor: information the user knows. A well-managed password is therefore an appropriate first component of the sign-in process. **Software token** supplies a possession factor because it is typically an authenticator application or credential held on and accessed through a user-controlled device. Such software tokens commonly generate time-based one-time passcodes or provide cryptographic approval for a login request.

Using a password together with a software token establishes the required combination of independent factors: something known and something possessed. This significantly improves account protection over password-only authentication because successful access requires both the password and access to the registered token or its device. NIST's digital identity guidance describes memorized secrets as knowledge-based authentication and recognizes cryptographic software authenticators as possession-based authenticators. For cloud applications, the administrator should also ensure that the token enrollment and recovery processes are protected, since those processes affect the strength of the overall authentication system. See NIST SP 800-63B: Digital Identity Guidelines and CISA guidance on turning on MFA.

QUESTION NO: 15

A network technician needs to ensure data on a network drive is fully backed up. Which of the following backups should the technician implement?

A. Database

B. Webserver

C. File

D. Operating system

ANSWER: C

Explanation:

File is the appropriate backup type for data stored on a network drive. Network drives commonly hold shared user documents, project folders, spreadsheets, media, and other individual files. A file backup protects this data by copying selected files and folders from the network location to a separate backup destination. The backup job can be configured to include the entire share, preserving the organization's data set for recovery if files are deleted, corrupted, encrypted by malware, or the source storage fails.

"Fully backed up" in this context means the technician should ensure that all required folders and files on the network drive are included in a complete backup scope. The technician may establish an initial full backup and then use scheduled incremental or differential backups to capture changes efficiently, while retaining restore points according to the organization's retention requirements. A sound implementation also verifies that backups complete successfully and periodically tests restoration of files to confirm that recovery will work when needed.

This matches CompTIA's IT Fundamentals focus on selecting storage and backup approaches appropriate to the data being protected. See CompTIA's IT Fundamentals certification overview and the National Institute of Standards and Technology guidance on protecting and recovering organizational data in NIST SP 800-34 Rev. 1.

QUESTION NO: 16

Which of the following are the primary functions of an operating system? (Choose two.)

A. Provide structure for file and data management.

B. Provide protection against malware and viruses.

C. Provide peer-to-peer networking capability.

D. Provide user data encryption.

E. Provide virtual desktop capability.

F. Provide system resources.

ANSWER: A F

Explanation:

An operating system has two foundational responsibilities: organizing stored information and managing the computer hardware that applications and users need. “Provide structure for file and data management.” is correct because the operating system supplies a file system that organizes data into files and folders, maintains file names and locations, and controls how programs store and retrieve information from storage devices. This consistent structure allows users and applications to locate, create, modify, and manage data reliably.

“Provide system resources.” is also correct because the operating system coordinates access to essential resources such as the processor, memory, storage, and input/output devices. It schedules processor time among running programs, allocates memory, and uses device drivers and related services to let software interact with hardware. Resource management enables multiple applications to run in an orderly manner while preventing one process from unnecessarily consuming resources needed by others. Microsoft describes the operating system as managing computer hardware and software resources, including memory, processes, and devices. See Microsoft Learn: System Information and IBM Documentation: Operating system overview.

QUESTION NO: 17

When a user types a web page name in an internet browser address field, this information is translated to an IP address behind the scenes. Which of the following is being used?

A. SMTP

B. DHCP

C. WPA

D. DNS

E. WEP

ANSWER: D

Explanation:

DNS is the service used to translate a human-readable web name, such as `www.example.com`, into the numerical IP address that network devices use to locate the destination server. When the user enters a URL or domain name in the browser’s address bar, the device typically checks locally cached DNS information first. If no valid record is available, it sends a DNS query to a configured resolver, which obtains or returns the matching address record. The browser can then establish a network connection to that IP address and request the web page. This name-resolution process makes internet navigation practical because people can use memorable domain names instead of needing to remember numerical IPv4 or IPv6 addresses. DNS is therefore a foundational network service for accessing websites and many other named network resources. The Internet Engineering Task Force describes DNS concepts and operation in RFC 1034. For an accessible overview of how DNS converts domain names to IP addresses, see Cloudflare’s DNS explanation.

QUESTION NO: 18

A computer technician is assigned a ticket to install a laptop for a new employee. Due to the arrangement of the workspace, the employee requests that the laptop be installed with the cover closed. Which of the following would be required to satisfy this request? (Choose two.)

A. Printer

B. Mouse

C. Webcam

D. External hard drive

E. Speakers

F. Display

ANSWER: B F

Explanation:

Mouse and **Display** are required for a practical closed-lid laptop workstation. Closing the laptop lid makes its integrated screen unavailable, so an external display provides the visual workspace needed to sign in, run applications, view documents, and otherwise use the computer. The laptop must be configured to remain awake while connected to power and operating with its lid closed, commonly called clamshell or closed-display mode.

Because the laptop's built-in keyboard and touchpad are inaccessible with the cover shut, a mouse provides a usable pointing device for navigating the operating system and applications. In a fully equipped workstation, an external keyboard would also normally be connected for text entry, but it is not one of the available selections. The specified mouse and display therefore provide the listed devices essential to operating the laptop with its cover closed. Microsoft documents the settings used to control what happens when a laptop lid is closed in Windows power options guidance. Apple likewise describes using an external display and input devices with a closed portable Mac in closed-display mode guidance.

QUESTION NO: 19

A startup company has created a logo. The company wants to ensure no other entity can use the logo for any purpose. Which of the following should the company use to BEST protect the logo? (Choose two.)

A. Patent

B. Copyright

C. NDA

D. Trademark

E. EULA

ANSWER: B D

Explanation:

Copyright and **Trademark** provide complementary protection for a company logo. Copyright protects the logo's original artistic expression as a creative work. Once an original logo is fixed in a tangible form, such as a digital design file or printed image, copyright protection generally exists automatically. Copyright registration can provide important enforcement benefits, including a public record of ownership and eligibility to bring an infringement action in U.S. federal court. The U.S. Copyright Office specifically recognizes that logos with sufficient original authorship may qualify for copyright protection.

Trademark protection addresses the logo's commercial role as an identifier of the company's goods or services. Using and registering the logo as a trademark helps establish the company's rights to prevent confusingly similar use by other businesses in connection with related products or services. Federal registration with the U.S. Patent and Trademark Office provides broader legal advantages, including a nationwide presumption of ownership for the listed goods or services.

Together, copyright protects the logo as artwork, while trademark protects its brand-identifying use. See the U.S. Copyright Office guidance on works not protected by copyright and the USPTO trademark basics.

QUESTION NO: 20

Which of the following are examples of physical security controls? (Choose two.)

A. Locked doors

B. Antivirus software

C. Security cameras

D. Firewall rules

E. Encryption

ANSWER: A C

Explanation:

Locked doors and **security cameras** are physical security controls because they help protect facilities, equipment, and people from unauthorized physical access. Locked doors restrict entry to authorized individuals, while security cameras can monitor activity and provide evidence of events occurring in a protected area.

Antivirus software, firewalls, and encryption are technical controls. They protect systems and data through software or configuration rather than by securing the physical environment. NIST describes physical and environmental protection controls in NIST SP 800-53.

QUESTION NO: 21

Which of the following is an example of a compiled computer language?

A. Perl

B. HTML

C. Java

D. Python

ANSWER: C

Explanation:

Java is an example of a compiled programming language because Java source files, normally written with the `.java` extension, are processed by the Java compiler (`javac`) before they are run. Compilation translates the human-readable source code into platform-independent Java bytecode, typically stored in `.class` files. That bytecode is then executed by the Java Virtual Machine (JVM), which may interpret it and/or use just-in-time compilation to convert frequently used bytecode into native machine instructions for the host processor.

This compile-then-run workflow is the key point: Java programs are not executed directly from their original source text. A developer must first compile the source successfully, which also allows the compiler to detect syntax and type-related issues before the application is deployed or run. Java's use of bytecode and the JVM supports its "write once, run anywhere" design, since the same compiled bytecode can run on systems that provide a compatible JVM. Oracle's Java documentation describes `javac` as the compiler that reads source files and produces class files, and the Java Virtual Machine Specification defines the class-file and bytecode execution model. See Oracle's javac documentation and The Java Virtual Machine Specification.

QUESTION NO: 22

Which of the following are benefits of a security awareness training program9 (Select two).

A. Enhances overall security

B. Provides information on how to avoid phishing

C. Lowers the incidence of hardware failures

D. Increases the availability of computers

E. Advances end users' technical skills

F. Creates IT security opportunities for end users

ANSWER: A B

Explanation:

“Enhances overall security” is a benefit because people are an essential part of an organization’s security posture. A security awareness program helps users understand their responsibilities for protecting devices, accounts, data, and organizational resources. Training reinforces safe everyday practices, such as using strong, unique passwords, protecting sensitive information, recognizing suspicious activity, and promptly reporting potential security incidents. These behaviors reduce the likelihood that routine user actions will expose the organization to avoidable security risk. NIST describes awareness and training as measures intended to ensure that personnel understand security responsibilities and are prepared to fulfill them, supporting the organization’s overall information-security program.

“Provides information on how to avoid phishing” is also a direct benefit. Phishing is a common social-engineering technique that attempts to persuade a recipient to disclose credentials or sensitive information, open a malicious attachment, or follow a harmful link. Awareness training teaches users to inspect unexpected messages carefully, recognize warning signs, verify requests using trusted channels, and report suspected phishing attempts. This knowledge supports safer decisions before an attack succeeds. See NIST SP 800-50, Building an Information Technology Security Awareness and Training Program and CISA guidance on recognizing and reporting phishing.

QUESTION NO: 23

Which of the following network protocols will MOST likely be used when sending and receiving Internet email?

(Select TWO.)

A. SMTP

B. POP3

C. SNMP

D. DHCP

E. ICMP

F. SFTP

ANSWER: A B

Explanation:

SMTP and **POP3** are the appropriate protocols for the usual send-and-receive email workflow. Simple Mail Transfer Protocol is the standard application-layer protocol used to submit outgoing messages from an email client to a mail server and to relay messages between mail servers. An email client commonly uses SMTP submission with authentication and transport encryption, typically on port 587.

Post Office Protocol version 3 is an email-access protocol used by a client to retrieve messages that have arrived at a mailbox on a mail server. POP3 is designed primarily for downloading messages to the receiving client, often for local storage and offline reading. Secure deployments commonly protect POP3 with TLS, either through POP3S or STARTTLS. Together, SMTP handles message submission and delivery, while POP3 provides mailbox retrieval, matching the two directions described in the question. The Internet Engineering Task Force defines SMTP in RFC 5321 and POP3 in RFC 1939.

QUESTION NO: 24

Which of the following actions would help protect a computer from malware? (Choose two.)

A. Install security updates.

B. Use anti-malware software.

C. Disable the firewall.

D. Share administrator credentials.

E. Open unexpected email attachments.

ANSWER: A B

Explanation:

Install security updates. and **Use anti-malware software.** are correct. Security updates correct known vulnerabilities in operating systems and applications that malware could exploit. Applying updates promptly reduces the number of weaknesses available to attackers.

Anti-malware software helps detect, block, quarantine, and remove known malicious software. Its effectiveness depends on keeping the application and its security intelligence current. Disabling the firewall or using an account with unnecessary administrative privileges would increase security risk rather than protect the computer. See CISA guidance on updating software and CISA security guidance.

QUESTION NO: 25

The broadcast signal from a recently installed wireless access point is not as strong as expected. Which of the following actions would BEST improve the signal strength?

A. Update from 802.11b to 802.11g.

B. Ensure sources of EMI are removed.

C. Enable WPA2-Enterprise.

D. Use WiFi Protected Setup.

ANSWER: B

Explanation:

Ensure sources of EMI are removed is correct because electromagnetic interference can reduce the effective performance and apparent strength of a wireless LAN signal. Wireless access points use radio-frequency transmissions, and nearby devices or equipment that emit energy in overlapping or adjacent frequency ranges can introduce noise. This lowers the signal-to-noise ratio at wireless clients, making a normally adequate access-point transmission seem weak, unreliable, or intermittent. Common environmental sources include microwave ovens, cordless devices, Bluetooth equipment, poorly shielded electrical equipment, and some industrial electronics, particularly when Wi-Fi is using the 2.4 GHz band. Removing, relocating, shielding, or otherwise mitigating the interfering source helps the client receive a cleaner radio signal and can improve usable coverage without changing authentication settings or wireless configuration standards. Cisco's wireless troubleshooting guidance describes radio-frequency interference as a factor that affects wireless client connectivity and performance: Cisco RF Interference Troubleshooting. The Federal Communications Commission also explains that

unlicensed devices operating in shared spectrum must tolerate interference, an important consideration for Wi-Fi deployments: FCC Equipment Authorization.

QUESTION NO: 26

Which of the following network protocols will MOST likely be used when sending and receiving Internet email? (Choose two.)

A. SMTP

B. POP3

C. SNMP

D. DHCP

E. ICMP

F. SFTP

ANSWER: A B

Explanation:

SMTP and POP3 are commonly used protocols for Internet email. SMTP, or Simple Mail Transfer Protocol, is the standard protocol used to submit outgoing messages from an email client to a mail server and to relay messages between mail servers. When a user sends an email, the client typically connects to an SMTP service, often using authenticated and encrypted submission settings.

POP3, or Post Office Protocol version 3, is a mail-retrieval protocol. It enables an email client to connect to the recipient's mail server, download received messages, and make them available locally to the user. POP3 is therefore associated with receiving email, while SMTP is associated with sending it. Together, these protocols represent a traditional client-server email workflow. Although modern email systems may instead use IMAP for mailbox synchronization, POP3 remains a recognized protocol for receiving Internet email. For protocol details, see RFC 5321: Simple Mail Transfer Protocol and RFC 1939: Post Office Protocol Version 3.

QUESTION NO: 27

Which of the following is an advantage of using locally saved files?

A. Readily shareable with others

B. No reliance on local backups

C. Immediately accessible by others on the cloud

D. No dependence on network connection

ANSWER: D

Explanation:

No dependence on network connection is an advantage of locally saved files because those files reside on storage physically attached to, or installed in, the user's device, such as an internal SSD, hard drive, or local external drive. The operating system can open and save the data directly through the local file system, so routine access does not require an internet connection, Wi-Fi, a cloud-service login, or availability of a remote server. This is especially valuable when working while traveling, during an internet outage, or in locations with unreliable connectivity. It can also provide predictable access and performance because opening a file does not depend on network bandwidth or latency. Local storage does not eliminate the need for sound data-management practices: important files should still be backed up, ideally following a strategy that maintains separate copies on different media or locations. However, the ability to continue accessing and editing files offline is the defining practical benefit addressed by this question. Microsoft's overview of offline files describes how locally

available files can be accessed when a network location is unavailable, illustrating the core offline-access concept: Microsoft Learn: Offline Files. For general guidance on maintaining protected copies of local data, see CISA: Back Up Data.

QUESTION NO: 28

A technician is troubleshooting a problem. The technician tests the theory and determines the theory is

confirmed. Which of the following should be the technicianâ€™s NEXT step?

A. Implement the solution.

B. Document lessons learned.

C. Establish a plan of action.

D. Verify full system functionality.

ANSWER: C

Explanation:

Establish a plan of action. is the next step in the CompTIA troubleshooting methodology after a technician has tested a theory and confirmed that it identifies the problem's cause. At this point, the technician has sufficient evidence to move from diagnosis to remediation planning. The plan should define the appropriate corrective action, required tools or resources, any needed backups or rollback measures, and the likely effect of the change on the device, users, services, or related systems.

Creating the plan before making changes supports controlled, repeatable troubleshooting and reduces the risk that a repair will introduce an unexpected outage or data loss. A sound plan also identifies whether authorization, maintenance scheduling, documentation, or testing procedures are needed before the fix is applied. Once the action plan has been established, the technician can implement the solution, verify that the system operates normally, and document the outcome as later stages of the process.

This sequence reflects CompTIA's published troubleshooting-process expectations for IT support professionals. See CompTIA's exam objectives resource page and its overview of troubleshooting best practices.

QUESTION NO: 29

Which of the following commands can be used to remove a database permanently?

A. DENY

B. DROP

C. ALTER

D. DUMP

ANSWER: B

Explanation:

DROP is the SQL Data Definition Language command used to permanently delete an entire database. In typical SQL implementations, the command is written as `DROP DATABASE database_name;`. Executing it removes the database definition and its contents, including the objects stored in it, such as tables and their data. Because this action is destructive, administrators should verify that the intended database is selected and confirm that appropriate backups exist before issuing the command. The exact behavior and prerequisites can vary by database platform; for example, a database may need to have no active connections before it can be dropped, and the user must have sufficient administrative privileges. The core purpose remains the same: permanently remove the database from the database management system. This aligns with SQL's definition-language operations, which create, modify, and delete database structures. Microsoft's SQL Server documentation describes `DROP DATABASE` as removing one or more user databases or database snapshots, while MySQL

documents `DROP DATABASE` as dropping all tables in the database and deleting the database. See Microsoft Learn: DROP DATABASE and MySQL Reference Manual: DROP DATABASE.

QUESTION NO: 30

Which of the following is an example of PI I? (Select two).

A. Full name

B. Date of birth

C. Employment status

D. School attended

E. Social media username

F. City of residence

ANSWER: A B

Explanation:

Personally identifiable information (PII) is information that can identify a specific individual, either on its own or when combined with other data. **Full name** is a direct identifier because it names a person and is commonly used to distinguish that person in business, government, education, and online records. **Date of birth** is also treated as PII because it is a personal attribute that can help identify or verify an individual, particularly when it is used with other identifying details. Organizations commonly protect dates of birth in the same manner as other sensitive personal data because they are frequently used in identity-verification processes and can contribute to identity theft if exposed alongside related records. The U.S. National Institute of Standards and Technology defines PII broadly as information that can distinguish or trace an individual's identity, including information that may be linked with a person. This classification supports applying appropriate privacy and security safeguards to names and birth-date information in stored records, forms, and systems. See NIST's definition of personally identifiable information and FTC privacy and data-security guidance.

QUESTION NO: 31

A technician needs to install and configure a wireless SOHO network. Which of the following should the technician configure to reduce Wi-Fi interference from other household appliances?

A. 2.4GHz

B. 5GHz

C. 802.11b

D. 802.11g

ANSWER: B

Explanation:

5GHz is the appropriate configuration because it moves the wireless network away from the heavily used 2.4 GHz radio spectrum. Many common household devices—including microwave ovens, some cordless phones, Bluetooth devices, and certain wireless peripherals—use or can generate noise in the 2.4 GHz range. Selecting 5 GHz therefore reduces the likelihood that these devices will disrupt Wi-Fi transmissions in a small office/home office environment.

The 5 GHz Wi-Fi band also provides substantially more available channels, including more channels that do not overlap. This gives a technician greater flexibility to select a clean channel when neighboring networks are present. In practical terms, clients operating on 5 GHz can often experience a more stable connection and better throughput in an interference-prone home environment. The technician should still consider coverage requirements: higher-frequency 5 GHz signals generally have less range and penetrate walls less effectively than 2.4 GHz signals. For the stated goal of reducing interference from

household appliances, however, configuring 5GHz directly addresses the primary source of radio-frequency contention. See Cisco's overview of Wi-Fi frequency bands and the FCC's information on wireless devices and radio-frequency operation.

QUESTION NO: 32

A technician is upgrading a company ' s Wi-Fi from 802.11a to support a range of 115ft (35m) indoors and a speed of 700Mbps. Which of the following should the technician select for the upgrade?

A. 802.11ac

B. 802.11b

C. 802.11g

D. 802.11n

ANSWER: A

Explanation:

802.11ac is the appropriate upgrade because it was designed to deliver substantially higher wireless throughput than 802.11a while operating in the 5 GHz band. It supports wider channels, multiple-input multiple-output antenna technology, and higher-order modulation, allowing real-world deployments to target throughput requirements such as 700 Mbps when compatible access points, client adapters, channel widths, signal conditions, and network configuration are used. The stated indoor distance of 115 feet (35 meters) is also a reasonable planning estimate for a 5 GHz wireless deployment, although actual coverage always depends on walls, interference, antenna placement, transmit power, and client capability. In certification questions, the requested combination of approximately 700 Mbps and this indoor range maps to 802.11ac, commonly known as Wi-Fi 5. An upgrade from 802.11a to 802.11ac also maintains the move to the less-congested 5 GHz spectrum while adding major capacity and performance enhancements. IEEE 802.11 working-group resources describe the family of wireless LAN standards at IEEE 802.11. The Wi-Fi Alliance's overview of Wi-Fi generations provides additional context for Wi-Fi 5 and newer technologies at Wi-Fi Alliance.

QUESTION NO: 33

Which of the following filesystems is most commonly found on a computer running macOS?

A. ext4

B. FAT32

C. HFS

D. NTFS

E. APFS

ANSWER: E

Explanation:

APFS is the correct answer because Apple File System is the modern default filesystem for Macs running current versions of macOS. Apple introduced APFS with macOS High Sierra and designed it specifically for modern Apple storage hardware, especially solid-state drives. It provides features important to macOS, including strong encryption support, space sharing between volumes in the same container, snapshots that support system updates and recovery, cloning of files and directories, and improved reliability for flash storage. When a current Mac's internal startup disk is formatted or macOS is installed normally, APFS is ordinarily used for the system and data volumes. This makes APFS the most accurate answer for a question referring generally to a computer running macOS today. HFS, more precisely Mac OS Extended (HFS Plus), was the standard macOS filesystem before APFS and may still be encountered on older Macs or legacy external disks, but it is not the usual default for modern installations. Apple documents APFS as the filesystem used by macOS and describes its

volume and container architecture in its Disk Utility file-system format guide. Additional technical details are available in Apple's Apple File System Programming Guide.

QUESTION NO: 34

A computer user is downloading software from the Internet and notices the following at the end of the install file: "…x86.exe". Which of the following statements BEST represents what the "…x86.exe" means in the installation file?

A. x86 only supports an installation on a 32-bit CPU architecture.

B. x86 supports an installation on a 32-bit and a 64-bit CPU architecture.

C. x86 only supports an installation on a 64-bit CPU architecture.

D. x86 supports an installation on a 16-bit CPU architecture.

ANSWER: B

Explanation:

x86 supports an installation on a 32-bit and a 64-bit CPU architecture. The x86 designation conventionally identifies a 32-bit version of software, built for the 32-bit x86 instruction set. It is appropriate for 32-bit Windows installations and, in typical modern Windows environments, can also be installed and run on 64-bit Windows. This is possible because 64-bit versions of Windows provide the WOW64 compatibility subsystem, which enables many 32-bit applications to execute on 64-bit systems. The ".exe" portion simply identifies the file as a Windows executable file; the "x86" portion distinguishes the installer from a native 64-bit version, often labeled x64 or AMD64. Therefore, when choosing between an x86 installer and an x64 installer, x86 is the broadly compatible 32-bit package for supported 32-bit and 64-bit Windows environments, while x64 is intended for 64-bit Windows only. Microsoft documents the WOW64 subsystem and its role in running 32-bit applications on 64-bit Windows at WOW64 Implementation Details. Additional guidance on 32-bit and 64-bit application considerations is available in Microsoft's Overview of 64-bit Windows.

QUESTION NO: 35

Which of the following practices support the principle of least privilege? (Choose two.)

A. Assign permissions required for a job role.

B. Give all users administrator privileges.

C. Remove access when it is no longer needed.

D. Share one account among multiple employees.

E. Grant access to all network shares by default.

ANSWER: A C

Explanation:

Assign permissions required for a job role. and **Remove access when it is no longer needed.** are correct. Least privilege means granting users, applications, and processes only the minimum permissions necessary to perform authorized tasks. Limiting permissions reduces the potential impact of an account compromise or accidental action.

Giving every employee administrator privileges or sharing accounts makes it difficult to control access and determine who performed an action. Retaining access after an employee changes roles also violates least privilege. NIST describes least privilege as restricting access to the minimum necessary for authorized functions in its least privilege glossary entry.

QUESTION NO: 36

Which of the following are examples of personal identifying information (PII)? (Choose two.)

A. Social Security number

B. Computer model number

C. Date of birth

D. Operating system version

E. Office building address

ANSWER: A C

Explanation:

Social Security number and **Date of birth** are examples of personally identifiable information because they can identify or help distinguish an individual when used alone or with other information. Organizations should collect, store, and share PII only when necessary and should protect it through appropriate access controls and safeguards.

A computer model number, office building address, and operating system version may be useful organizational information, but they do not normally identify a specific individual. NIST defines PII as information that can be used to distinguish or trace an individual's identity in its PII glossary entry.

QUESTION NO: 37

Which of the following BEST describes a technology that allows multiple users to create and edit reports at the same time?

A. Text file on a shared drive

B. Managed relational database

C. Informational intranet page

D. Locally installed productivity software

E. Cloud-based collaborative productivity software

ANSWER: E

Explanation:

Cloud-based collaborative productivity software is the best description because it is specifically designed to let several people work on the same report or document concurrently. These platforms store the shared file centrally in a cloud service and synchronize each contributor’s changes, allowing users to see updates in near real time. They commonly provide coauthoring features such as simultaneous editing, presence indicators that show who is working in the file, comments, version history, and controlled sharing permissions. This supports a team preparing a report without needing to pass separate copies between users or manually combine edits later.

For example, Microsoft 365 supports real-time coauthoring when a file is stored in OneDrive or SharePoint; collaborators can work in the same document and view one another’s changes as they occur. Microsoft describes the requirements and behavior for this feature in its real-time coauthoring documentation. Google Workspace similarly supports simultaneous editing and collaboration in Google Docs, as documented in its sharing and collaboration guide.

QUESTION NO: 38

When following the troubleshooting methodology, which of the following should be performed when establishing a theory of probable cause?

A. Question the obvious.

B. Identify the symptoms.

C. Duplicate the problem.

D. Determine if anything has changed.

ANSWER: A

Explanation:

“Question the obvious.” is performed while establishing a theory of probable cause. After the issue has been identified and relevant information has been gathered, the technician develops a likely explanation for the symptoms. Beginning with obvious, simple, and common potential causes helps create a practical theory that can be tested efficiently. This means checking fundamental conditions that could account for the reported behavior before pursuing more complex possibilities. The objective at this stage is not yet to implement a repair; it is to form a logical, evidence-based hypothesis that explains the problem and can be validated in the next troubleshooting step. CompTIA’s troubleshooting process emphasizes using a structured method so that technicians move from problem identification to a probable-cause theory, test that theory, and then implement and verify a solution. Reviewing the published exam objectives is useful for understanding the intended sequencing and terminology of this methodology. See CompTIA Exam Objectives and the CompTIA IT Fundamentals certification page.

QUESTION NO: 39

A technician has verified full system functionality. Which of the following actions should the technician take next?

A. Question the users.

B. Determine if anything has changed.

C. Document the findings.

D. Gather Information.

ANSWER: C

Explanation:

Document the findings is the appropriate next action once the technician has verified that the system is fully functional. In the standard CompTIA troubleshooting methodology, verification confirms that the implemented solution resolved the reported issue and that normal operation has been restored. The final step is to document the findings, actions, and outcomes. Useful documentation includes the symptoms reported, the identified cause, the solution applied, any configuration or component changes made, validation results, and recommendations that could prevent recurrence. This creates a reliable support record for future technicians, helps identify recurring incidents or trends, and provides a knowledge-base resource that can reduce resolution time for similar issues. Documentation also supports consistent service management by preserving an accurate history of work performed on systems. CompTIA’s troubleshooting process explicitly places documentation after solution implementation and verification of full system functionality. See the CompTIA exam objectives resources and the CompTIA troubleshooting methodology guide for an overview of the final documentation step.

QUESTION NO: 40

A user is attempting to print a document to a wireless printer and receives an error stating the operation could not be completed. Which of the following should the user do to correct this issue?

A. Ensure both devices are connected to the LAN.

B. Enable task scheduling.

C. Reset the proxy settings to their default values.

D. Review the fault tolerance configurations.

ANSWER: A

Explanation:

Ensure both devices are connected to the LAN. A wireless print job depends on a working network path between the computer or mobile device submitting the document and the wireless printer receiving it. The user should first confirm that the device and printer are joined to the same local network, such as the same wireless router and appropriate network segment. They should also verify that the printer is powered on, connected to Wi-Fi, and visible or reachable from the user's device. Once both endpoints have valid connectivity on the local network, the operating system can discover or communicate with the printer and send the job through its configured print queue. This is an appropriate first troubleshooting step because the stated error occurs during a network-dependent operation and can result when either endpoint has lost its wireless connection or joined a different network. CompTIA's networking guidance describes a local area network as connecting devices within a limited area so they can communicate and share resources such as printers. See CompTIA's overview of local area networks and CompTIA's wireless-networking guide.

QUESTION NO: 41

Which of the following operating systems do not require extensions on files to execute a program? (Choose two.)

A. Windows 7

B. Windows 8

C. UNIX

D. Windows Server 2012

E. Android

F. Linux

ANSWER: C F

Explanation:

UNIX and Linux do not require a filename extension in order to identify a file as executable. On these systems, executability is primarily controlled by file permissions: a user can grant execute permission with a command such as `chmod +x filename`. When a user invokes the file, the operating system determines how to run it from its contents rather than from a required suffix in its name. For example, a compiled executable is recognized through its executable format, while a script can specify its interpreter in a `#!` (shebang) line, such as `#!/bin/sh` or `#!/usr/bin/env python3`. Extensions such as `.sh`, `.py`, or `.bin` may still be used as helpful naming conventions, but they are not required for execution. This behavior reflects the shared UNIX design model used by Linux systems. The GNU Coreutils documentation describes changing file modes, including execute permissions, with `chmod`: GNU Coreutils chmod invocation. The Linux `execve` manual also describes executing programs and interpreter scripts: Linux execve(2) manual page.

QUESTION NO: 42

Ann, a user, wants to ensure that if her credentials are compromised, they cannot be used to access all of her logins or accounts. Which of the following best practices should she implement?

A. Password history

B. Password length

C. Avoid password reuse

D. Password complexity

ANSWER: C

Explanation:

Ann should avoid password reuse by using a different, strong password for every login or account. Unique passwords limit the impact of a credential compromise: if one site suffers a breach or one password is captured through phishing, that credential pair will not also authenticate Ann to her email, financial, work, shopping, or other accounts. This practice is often called password compartmentalization because it prevents a single exposed password from becoming a master key to many services. A password manager is a practical way to follow this practice, since it can generate and securely store long, random, distinct passwords without requiring Ann to memorize each one. Where available, Ann should also enable multifactor authentication to provide an additional verification factor if a password is exposed. CISA specifically recommends using a password manager to create and maintain unique passwords for all accounts, helping reduce the risk of credential-stuffing attacks. See CISA: Use Strong Passwords and NIST SP 800-63B Digital Identity Guidelines.

QUESTION NO: 43

A technician has established a plan of action. Which of the following should the technician do next?

A. Verify system functionality.

B. Identify preventive measures.

C. Document the findings.

D. Implement a solution.

ANSWER: D

Explanation:

Implement a solution. is correct because, in CompTIA's standard troubleshooting methodology, establishing a plan of action is immediately followed by executing that plan to resolve the issue. A plan identifies the appropriate remediation approach, required resources, potential impacts, and any necessary escalation or authorization. Once the plan is in place, the technician carries out the selected corrective action, such as changing a configuration, replacing a failed component, installing an update, or restoring a service.

Implementation should be performed carefully and in accordance with organizational procedures, including change-control requirements where applicable. The technician should use the plan as a guide so the work is deliberate, repeatable, and appropriately scoped rather than relying on unplanned changes. Following implementation, the next stages of the methodology involve confirming that the system works fully and that the issue has been resolved, applying preventive measures when appropriate, and documenting findings, actions, and outcomes. This ordered process helps technicians resolve incidents consistently while maintaining an accurate record of support work. CompTIA describes troubleshooting as a structured process in its guide to troubleshooting IT issues; related operational change practices are covered by the NIST asset-management guidance.

QUESTION NO: 44

Which of the following actions help protect a mobile device that is used for company email? (Choose two.)

A. Enable a screen lock

B. Share the device passcode

C. Install operating system updates

D. Disable device encryption

E. Connect to unknown wireless networks

ANSWER: A C

Explanation:

Enabling a screen lock and **installing operating system updates** help protect a mobile device. A screen lock prevents an unauthorized person from easily accessing the device if it is lost or left unattended. Operating system updates correct known security vulnerabilities and improve the device's resistance to threats.

Disabling encryption reduces protection for data stored on the device. Sharing a device passcode and connecting to unknown wireless networks can expose company information to unauthorized access. CISA provides mobile-device security recommendations in its mobile device cybersecurity checklist.

QUESTION NO: 45

Which of the following should be used to store a list of strings?

A. Array

B. Constant

C. Variable

D. Branch

ANSWER: A

Explanation:

Array is correct because an array is a data structure designed to hold multiple related values under one identifier. In this case, each element of the array can contain a string, such as a name, filename, or item description. The program can then access an individual string by its position, commonly called an index, and can process the complete collection with iteration. For example, an array could hold the strings “red,” “green,” and “blue,” allowing a program to retrieve or work through those values in an organized sequence.

This use of an array is a core programming concept: selecting a collection data structure when a program needs to retain multiple values of the same general type. Arrays make it practical to store, retrieve, and manipulate a set of strings without creating a separate named storage location for every value. JavaScript documentation describes arrays as list-like objects whose elements can be accessed by index, while Microsoft’s introductory programming material similarly explains arrays as collections that store multiple values. See MDN Web Docs: Array and Microsoft Learn: Arrays.