CompTIA A+ Core 2 (220-1202) - Free 30-Question Sample

Unofficial practice material. Not affiliated with or endorsed by CompTIA.

S1. A technician needs to see which processes are using the most CPU and memory on a Windows PC. Which tool should be opened?
A) Task Manager
B) Disk Management
C) Device Manager
D) Event Viewer
Correct answer: A
Explanation: Task Manager displays running processes along with their CPU, memory, disk, and network usage in real time. Disk Management handles partitions, Device Manager handles hardware drivers, and Event Viewer shows system logs - none of them show live resource usage per process.
S2. A company requires strong passwords. Which of the following is the strongest password?
A) P@ssw0rd123
B) Tr0ub4dor&3
C) $vBn4#zL9@qW7!
D) Summer2026!Fall2026
Correct answer: C
Explanation: The long, randomly generated passphrase is strongest because length combined with unpredictability is the dominant factor in password strength. The other options are short, use predictable substitutions, or contain dictionary words with simple patterns that password-cracking tools guess quickly.
S3. A smartphone app crashes every time it is opened, but the rest of the phone works normally. What is the best first troubleshooting step?
A) Perform an immediate full factory reset of the phone
B) Replace the phone with a new one
C) Restart the phone and reinstall the crashing app
D) Root or jailbreak the phone to fix it
Correct answer: C
Explanation: Restarting the phone clears the app's bad state, and reinstalling replaces its corrupted files - the standard fix for a single misbehaving app. A factory reset wipes all data unnecessarily, replacing the phone is extreme, and rooting voids warranties while adding risk.
S4. A technician shrinks the C: volume to make room for a new partition, but the "Extend Volume" option is grayed out for the new partition. What is the most likely reason?
A) The disk is using the MBR partition style instead of GPT
B) The volume is encrypted with BitLocker Drive Encryption

C) The disk is a dynamic disk rather than a basic disk
D) There is no unallocated space directly after the volume
Correct answer: D
Explanation: On basic disks using either the MBR or GPT partition style, Windows Disk Management can only extend a volume into unallocated space directly adjacent to it on the right - so a gap or another partition in between grays out the option. Dynamic disks use volumes that can span non-contiguous space and extend more flexibly, so this contiguous-space requirement applies specifically to basic disks. BitLocker encryption would present a different error rather than graying out the option.
S5. A user needs to encrypt a single folder of sensitive documents on a Windows laptop rather than the entire drive. Which feature should be used?
A) Windows Defender Firewall with Advanced Security
B) Disk Cleanup to remove temporary files
C) Encrypting File System (EFS)
D) Storage Spaces to pool multiple drives together
Correct answer: C
Explanation: EFS encrypts individual files and folders at the NTFS level, which fits the requirement precisely. The firewall filters network traffic, Disk Cleanup removes temporary files, and Storage Spaces pools disks - none of them encrypt selected folders.
S6. A printer outputs pages full of garbled characters and symbols, while other printers work fine from the same PC. What is the most likely cause?
A) A corrupted print spooler queue on the PC
B) A loose or damaged printer cable connection
C) The wrong or corrupted printer driver
D) Low toner or a nearly empty toner cartridge
Correct answer: C
Explanation: Garbled "garbage" printouts are the classic symptom of a wrong or corrupted driver misrendering the print job. A damaged cable usually causes missing output rather than random characters, and low toner causes fading rather than garbled text.
S7. A company adopts a SaaS email platform and asks who is responsible for securing the physical servers and patching the email application itself. Which answer reflects the shared-responsibility model?
A) The customer handles everything, including the servers
B) Responsibility is split exactly evenly down the middle for every task
C) The customer patches the application while the provider secures the physical building
D) The provider manages the app and infrastructure; the customer manages data
Correct answer: D
Explanation: In the SaaS model the provider owns the entire stack up to the application, while the customer remains responsible for its own data, identities, and who can access what. The customer does not manage servers or patch the SaaS app, and there is no arbitrary fifty-fifty split of duties.
S8. An administrator wants to stop employees from copying sensitive files onto personal USB flash drives on company workstations. Which control enforces this?
A) Disabling the USB ports in the BIOS on each workstation
B) A Group Policy blocking USB removable storage devices
C) Encrypting workstation drives with BitLocker
D) Uninstalling the USB controller drivers in Device Manager
Correct answer: B
Explanation: Group Policy can disable USB mass storage across domain workstations, technically

preventing the copy operation. BIOS changes and driver removals are per-machine workarounds that updates or users can undo, and BitLocker protects data at rest rather than blocking copies.
S9. After a phone OS update, the battery drains in half the time it used to, even when the phone sits idle. What should the user check first?
A) The battery usage screen to identify the draining app
B) The list of apps allowed to keep running in the background
C) Whether battery saver mode is turned off
D) The screen brightness and screen timeout settings
Correct answer: A
Explanation: The battery usage screen breaks down consumption by app, quickly revealing a misbehaving app stuck running after the update. Background restrictions, battery saver, and brightness are secondary checks after identifying the culprit.
S10. A Linux administrator needs to create a new local user account named "support". Which command creates the account?
A) newuser support
B) useradd support
C) mkuser support
D) adduser --delete support
Correct answer: B
Explanation: The useradd command is the standard tool for creating local user accounts on Linux. "newuser" and "mkuser" are not standard Linux commands, and "adduser --delete" would attempt to remove an account rather than create one.
S11. Before receiving network credentials, every new hire must sign a document agreeing not to install personal software or visit malicious sites on company equipment. What is this document called?
A) A signed software license agreement
B) An equipment packing slip
C) An acceptable use policy (AUP)
D) A team meeting agenda
Correct answer: C
Explanation: An acceptable use policy defines the permitted and prohibited uses of company systems, and employees acknowledge it before gaining access. A license key activates software, a packing slip lists shipped items, and a meeting agenda organizes a meeting - none of them govern user behavior.
S12. A Remote Desktop connection to a Windows Pro PC fails, although ping to the PC succeeds. What should be verified on the target PC?
A) That File Explorer is open on the target PC
B) RDP is enabled and allowed through the firewall
C) That the Recycle Bin on the target PC has been emptied
D) That the target PC's screensaver is disabled
Correct answer: B
Explanation: RDP requires both the Remote Desktop feature to be enabled and a firewall exception permitting inbound RDP traffic - ping only proves basic network reachability. File Explorer, the Recycle Bin, and the screensaver do not affect Remote Desktop connectivity.

Operational Procedures

S13. After installing a new web browser, clicking links in other programs still opens the old browser. Where in Windows 11 Settings is the default browser changed?
A) Apps > Default apps

B) Personalization > Background
C) System > Sound
D) Network & internet > Wi-Fi
Correct answer: A
Explanation: The Apps > Default apps page assigns which program opens each link and file type. Personalization controls appearance, System > Sound controls audio, and Network settings manage connectivity - none of them set default applications.
S14. A company has stored customers' credit card numbers indefinitely "just in case." Which practice best reduces the damage if a breach occurs?
A) Keep the data forever since storage is cheap
B) Keep data only as long as needed, then destroy it
C) Copy the data to every workstation for redundancy
D) Encrypt it but keep it on the shared drive forever
Correct answer: B
Explanation: Data minimization - keeping sensitive data only while needed and then destroying it securely - shrinks the amount of valuable data a breach can expose. Indefinite retention, workstation copies, and permanent shared storage all maximize the attacker's potential haul.
S15. A technician inherits a server rack full of unlabeled cables and cannot trace any connection. Which practice prevents this problem going forward?
A) Memorizing every cable run
B) Using only one cable color
C) Labeling both ends of every cable
D) Never touching any of the cables again
Correct answer: C
Explanation: Labels on both ends plus up-to-date documentation make every connection traceable by anyone, not just the original installer. Memory is unreliable, a single color identifies nothing, and avoiding the rack is not a workable practice.
S16. A technician builds a reference Windows 11 PC and wants to capture its image for deployment to 40 identical office PCs. What must be run before capturing the image?
A) Run sysprep /generalize to remove the PC's unique security identifier
B) Run chkdsk /f to mark the disk as clean so the cloning tool will accept it
C) Run diskpart clean to wipe the recovery partition and keep the image small
D) Run sfc /scannow to lock the system files in their current state
Correct answer: A
Explanation: Sysprep /generalize strips machine-specific data like the SID so each deployed PC generates its own unique identity, preventing domain and WSUS conflicts. Chkdsk, diskpart clean, and sfc do not generalize an image, and capturing without sysprep duplicates the SID across all 40 machines.
S17. A user belongs to the Sales group, which is granted Modify on a folder, and the Temps group, which is explicitly denied Write on the same folder. What is the user's effective access?
A) Full Control, because group memberships combine to the highest level
B) Modify, because the Sales permission is more recently assigned
C) Read only, because conflicting permissions cancel down to the lowest level
D) Modify minus Write, because an explicit Deny always overrides an Allow
Correct answer: D
Explanation: In NTFS, an explicit Deny takes precedence over any Allow, so the user keeps Modify except for the denied Write capability. Permissions do not merge up to Full Control, recency does not

decide conflicts, and the result is not reduced all the way to Read.

S18. After using su and sudo multiple times during a maintenance session, a Linux technician wants to confirm which user account is currently active. Which command answers this?

A) whoami

B) hostname

C) uname -a

D) ps

Correct answer: A

Explanation: The whoami command prints the effective username of the current session. hostname shows the computer's name, uname -a displays kernel and system information, and ps lists running processes - none of them identify the current user.

S19. A small business left Remote Desktop exposed directly to the internet with a weak administrator password. On Monday morning every PC is encrypted with a ransom note. What would have best prevented this attack?

A) Moving RDP from port 3389 to a non-standard port purely for obscurity

B) Requiring a 14-character password on the internet-facing RDP

C) Keep RDP off the internet - behind a VPN with strong authentication

D) Disabling antivirus so that scans run faster

Correct answer: C

Explanation: Internet-facing RDP with weak credentials is one of the most common ransomware entry points because attackers brute-force it around the clock; placing RDP behind a VPN with restricted access removes that exposure entirely. Changing the port only obscures the service without removing the exposure, a strong password alone still leaves RDP brute-forcible, and disabling antivirus removes a layer of defense rather than adding one.

S20. A victim's phone suddenly loses all cellular service, and within hours the attacker - who ported the victim's number to their own SIM - intercepts SMS two-factor codes and drains the victim's accounts. What happened, and what is the lesson?

A) An evil twin attack captured the victim's Wi-Fi traffic at a public hotspot

B) Juice jacking malware infected the phone through a compromised public charger

C) A SIM swap hijacked the number - SMS is the weakest second factor

D) A Bluetooth attack paired with the victim's phone remotely

Correct answer: C

Explanation: In a SIM swap the attacker convinces the carrier to move the victim's number to their SIM, instantly receiving all calls and SMS codes; app-based and hardware second factors stay on the victim's device and are unaffected. An evil twin impersonates Wi-Fi hotspots rather than porting numbers, juice jacking needs a physical USB connection, and Bluetooth pairing does not transfer a phone number.

S21. A company retires a fleet of laptops equipped with self-encrypting drives (SEDs), where all data was always encrypted at rest by keys held in the drive controller. What is the fastest compliant way to render the data unrecoverable before disposal?

A) Cryptographic erase - destroy the drive's encryption keys

B) Delete all partitions and reinstall the operating system on each laptop

C) Run the retired drives through a magnetic degausser

D) Overwrite each drive with a single zero-fill pass before disposal

Correct answer: A

Explanation: On a self-encrypting drive the stored data is only ciphertext without its keys, so destroying the keys renders everything unrecoverable in seconds - the essence of cryptographic erase. Deleting

partitions leaves the data recoverable, degaussers have no effect on flash chips, and a manual overwrite pass is slower and unnecessary when crypto-erase exists.

S22. An older desktop with a traditional hard drive takes a long time to open large files, and it has never had maintenance performed. Which built-in maintenance task addresses fragmented files?

A) Disk Cleanup
B) Error checking with chkdsk /r
C) Optimize Drives (defrag)
D) Storage Sense

Correct answer: C

Explanation: Optimize Drives defragments HDDs, consolidating fragmented files for faster access. Disk Cleanup and Storage Sense free space rather than reorganizing files, and chkdsk repairs file-system errors. Note: never defragment an SSD - SSDs use TRIM instead.

S23. The same email server issue has been "fixed" three times this quarter and keeps returning. Each individual incident ticket restored service temporarily. What should be created now?

A) Another identical incident ticket to restore service again
B) A new user training manual to prevent user errors
C) A problem ticket to perform root-cause analysis
D) A purchase order for a replacement server

Correct answer: C

Explanation: Incident management restores service; problem management investigates the underlying root cause of recurring incidents. Another incident ticket just repeats the cycle, training does not fix a server fault, and buying hardware is premature without diagnosis.

S24. A user accidentally overwrites an important spreadsheet and needs yesterday's version. No backup software is installed, but the PC runs Windows with default settings. Which feature may provide an earlier copy?

A) Previous Versions via the file's Properties dialog
B) System Restore to roll back the operating system
C) Disk Defragmenter to reorganize the drive
D) BitLocker drive encryption settings

Correct answer: A

Explanation: Previous Versions, powered by restore points and shadow copies, can recover earlier versions of individual files. System Restore reverts system files and settings but not user documents, while defragmentation and BitLocker are unrelated to file recovery.

S25. A technician wants a permanent "Safe Mode" entry in the Windows boot menu so it can be selected at startup without pressing keys. Which tool creates this additional boot entry?

A) Diskpart
B) System Information (msinfo32)
C) The bcdedit command
D) The DirectX Diagnostic Tool

Correct answer: C

Explanation: bcdedit manages the boot configuration data store, including copying the current entry and flagging it for Safe Mode. Diskpart manages disks and partitions, System Information only displays data, and the DirectX Diagnostic Tool tests multimedia components.

S26. After configuring a new service, a technician wants to confirm right now whether it is actually running. Which command shows the service's current state?

A) systemctl mask backup.service
B) apt list backup.service

C) systemctl is-enabled backup.service
D) systemctl status backup.service
Correct answer: D
Explanation: systemctl status displays whether a service is active (running), along with recent log lines. mask disables a service entirely, apt list queries packages rather than service state, and is-enabled reports whether the service starts at boot rather than whether it is running now.
S27. A Python script holds a list of server names and must run the same status check once for each server. Which construct repeats the check for every item in the list?
A) A for loop: for server in servers:
B) A single print statement
C) An import statement alone
D) A function definition that is never called
Correct answer: A
Explanation: A for loop iterates over each element of a list, executing its body once per server. A lone print runs once, import only loads modules, and a function definition that is never called never executes.
S28. A company's attorney instructs IT to preserve all emails of an employee involved in a lawsuit and to suspend automatic mailbox deletion for those accounts. What is this directive called?
A) A backup rotation
B) A legal hold
C) A retention policy update
D) An acceptable use policy
Correct answer: B
Explanation: A legal (litigation) hold requires preserving potentially relevant data and suspending normal deletion routines. Backup rotations keep cycling media on schedule, a retention policy sets routine deletion timeframes rather than suspending them, and an acceptable use policy governs user behavior rather than evidence preservation.
S29. A user opens an Excel file received by email, but the ribbon shows "Protected View" and macros will not run. The file is from a trusted sender. What is the safest way to proceed?
A) Enable macros in the Normal template so they always run
B) Lower the macro security setting to the minimum for all documents
C) Close the file, unblock it in Properties, then reopen it
D) Enable all macros in the Trust Center settings
Correct answer: C
Explanation: Files from the internet open in Protected View; unblocking that specific file in its Properties dialog marks it trusted while keeping global protections intact. Lowering macro security globally, editing the Normal template, or enabling all macros in the Trust Center exposes the whole system.
S30. Reviewing help desk data, a technician notices VPN connection tickets spike every Monday morning. What is this analytical practice called, and what does it enable?
A) Trend analysis - it reveals patterns for proactive fixes
B) A backup rotation - it schedules tape changes
C) Root cause analysis - it finds why one ticket happened
D) Capacity planning - it buys more VPN licenses immediately
Correct answer: A
Explanation: Trend analysis examines historical ticket data for recurring patterns, allowing IT to address root causes proactively (such as a Monday VPN capacity issue) instead of reacting each time. Root cause analysis targets single incidents, capacity planning sizes resources, and backup rotations manage media.