PREPKLOUD FIELD GUIDE SERIES

CompTIA A+ Core 2 (220-1202) Field Guide

A help-desk-first guide to operating systems, security, software troubleshooting, and operational procedures.

First edition · 2026 · prepkloud.com

About this guide

CompTIA A+ is the most widely recognized entry-level certification for IT support roles. To earn it you must pass two exams: Core 1 (220-1201), which focuses on hardware, networking, mobile devices, and virtualization, and Core 2 (220-1202), which this guide covers. Core 2 tests whether you can support users on modern operating systems, secure their devices, fix software problems, and follow professional procedures.

Exam facts, as published by CompTIA when this guide was written: part of the A+ V15 series launched in 2025; up to 90 questions, including multiple-choice and performance-based questions; 90 minutes; passing score 700 on a 100–900 scale; about 12 months of hands-on experience in a help desk or desktop support role recommended. Always confirm current details on the official CompTIA A+ page and the official 220-1202 exam objectives before you schedule.

220-1202 domain	Weight	Chapters
1. Operating Systems	28%	2–6
2. Security	28%	7–9
3. Software Troubleshooting	23%	10–11
4. Operational Procedures	21%	12–13

CompTIA. All questions are original. They are not recalled, leaked, or copied exam items. Practise commands and settings only on devices you own or are authorized to manage.

Contents

CHAPTER 1 · EXAM METHOD

How 220-1202 works and how to prepare

Core 2 is a practical support exam. Many questions describe a user's problem and ask what you should do *first*, *next*, or *best*. Performance-based questions may ask you to run through a troubleshooting sequence, choose the right command, configure a setting, or order the malware removal steps.

What the questions reward

- **The least disruptive fix first.** Restart the service before reinstalling the OS.
- **The right tool for the job.** Know which Windows utility or command shows what.
- **Security by default.** Least privilege, strong authentication, and encryption.
- **Process.** Documented change, tested backups, and professional communication.

> **Exam mindset**
>
> Think like a careful help desk technician. Gather information, back up data before risky changes, make one change at a time, verify the fix with the user, and document what you did. Answers that skip backups, bypass change control, or grant excessive rights are usually wrong.

Question strategy

- Read the last sentence first. "First" questions often want information gathering or a backup.
- Look for the operating system in the question: Windows, macOS, Linux, iOS, or Android change the answer.
- Skip long performance-based questions and return to them, so they do not consume your time.
- With up to 90 questions in 90 minutes, aim for about a minute each.

Recall

- Can I name the four domains and their weights?
- Which two exams make up A+?

Operating systems, file systems, and installation

Common operating systems

OS	Typical use
Windows	Most business desktops and laptops.
macOS	Apple desktops and laptops.
Linux	Servers, developer workstations, embedded devices.
ChromeOS	Browser-centric laptops, common in education.
iOS / iPadOS	Apple phones and tablets.
Android	Phones and tablets from many manufacturers.

Watch for **end-of-life** status. An OS that no longer receives security updates is a risk and should be upgraded or isolated.

File systems

File system	Key facts
NTFS	Default for Windows system drives; permissions, encryption (EFS), compression, journaling.

ReFS	Windows Resilient File System designed for data integrity on large volumes.
FAT32	Widely compatible; maximum file size 4 GB.
exFAT	For flash drives; large files and wide cross-platform support.
ext4 / XFS	Common Linux file systems.
APFS	Default Apple file system for macOS and iOS.

Installation and upgrade

- **Boot methods:** USB, network boot (PXE), internal partition, external drive, or image deployment.
- **Install types:** clean install, in-place upgrade, image deployment, repair installation, remote network installation, zero-touch deployment, and recovery partition.
- **Partitioning: GPT** (modern, used with UEFI, many partitions, large disks) versus **MBR** (legacy, up to four primary partitions, 2 TB disk limit).
- **Formatting:** quick format (removes the file table) versus full format (also checks for bad sectors).
- **Upgrade considerations:** back up user data, check hardware and application compatibility, confirm licensing, and know whether an upgrade path is supported.

Scenario

A user needs to copy a 6 GB video to a USB stick that must work on both Windows and macOS. Format it as **exFAT**. FAT32 cannot store a file larger than 4 GB, and NTFS has limited macOS write support.

Recall

- GPT versus MBR: which supports disks above 2 TB?
- Which file system is the Windows system default?

Windows editions, settings, and tools

Windows 11 editions

Feature	Home	Pro	Enterprise
Join a corporate domain	No	Yes	Yes
Group Policy Editor	No	Yes	Yes
BitLocker	No (device encryption only on some hardware)	Yes	Yes
Remote Desktop host	No	Yes	Yes
Advanced management and security features	No	Some	Most

Windows 11 requires TPM 2.0, UEFI with Secure Boot capability, and a supported processor. These are common reasons an upgrade fails.

Windows tools and management console snap-ins

Tool	Use it to
Task Manager	End unresponsive apps, view performance, manage startup apps.
Event Viewer (eventvwr.msc)	Read system, application, and security logs.

Disk Management (diskmgmt.msc)	Create, extend, shrink, and format partitions.
Device Manager (devmgmt.msc)	Update, roll back, or disable drivers.
Services (services.msc)	Start, stop, and set startup type for services.
Task Scheduler (taskschd.msc)	Run tasks on a schedule or event.
Performance Monitor (perfmon.msc)	Track counters over time.
Local Users and Groups (lusrmgr.msc)	Manage local accounts (not on Home).
Group Policy Editor (gpedit.msc)	Configure local policy (not on Home).
Certificate Manager (certmgr.msc)	View and manage user certificates.
System Configuration (msconfig)	Boot options such as Safe Mode, and service selection.
System Information (msinfo32)	Hardware and software inventory.
Resource Monitor (resmon)	Detailed CPU, memory, disk, and network use per process.
Registry Editor (regedit)	Edit the registry. Back up first.
Disk Cleanup (cleanmgr)	Remove temporary and unneeded files.

Settings and Control Panel

Know where to find Windows Update, privacy, display, power options (sleep, hibernate, fast startup), accounts, apps, File Explorer options (show hidden files and extensions), and Device Manager. Many tasks can be done in either Settings or Control Panel.

Recall

- Which tool rolls back a driver?
- Which editions can join a domain?

The Windows command line

Command	Purpose
ipconfig /all, /release, /renew, /flushdns	Show or refresh IP configuration; clear DNS cache.
ping	Test reachability of a host.
tracert / pathping	Show the route to a host / route plus loss statistics.
netstat	Show active connections and listening ports.
nslookup	Query DNS records.
net use	Map or disconnect a network drive.
net user	Manage user accounts.
hostname / whoami / winver	Show computer name / current user / Windows version.
gpupdate /force	Reapply Group Policy now.
gpresult /r	Show which policies applied.
sfc /scannow	Scan and repair protected system files.
chkdsk /f /r	Fix file system errors / locate bad sectors.
diskpart	Manage disks and partitions from the command line.

format	Format a volume.
robocopy / xcopy / copy	Copy files; robocopy is robust and can mirror directories.
cd, dir, md, rmdir	Navigate and manage folders.
shutdown /r /t 0	Restart immediately.
[command] /?	Show help for a command.

Elevation

Many commands, such as sfc, chkdsk, and diskpart, need an administrator prompt. If a command reports access denied, run the terminal as administrator rather than weakening permissions.

Scenario

A user reaches websites by IP address but not by name after a DNS change. Run **ipconfig /flushdns**, then test with **nslookup**.

Recall

- Which command shows which Group Policies applied?
- Which command repairs protected system files?

Windows networking, macOS, and Linux

Windows networking

- **Workgroup versus domain:** a workgroup is peer-to-peer with local accounts; a domain uses central accounts and policy in Active Directory.
- **Shared resources:** printers, file shares, and mapped drives. Administrative shares end with $ (for example C$).
- **Network profile:** public (restrictive) versus private (allows discovery).
- **Windows Defender Firewall:** allow apps or ports only as needed.
- **Configuration:** static versus DHCP addressing, DNS servers, gateway, proxy settings, metered connections, and VPN.

macOS essentials

Feature	Purpose
Finder	File manager.
Spotlight	System-wide search.
Keychain	Stores passwords and certificates.

Time Machine	Built-in backup.
FileVault	Full-disk encryption.
Mission Control	View open windows and desktops.
Terminal	Command line.
System Settings	Configuration, including Privacy & Security.
.dmg, .pkg, .app	Disk image, installer package, application bundle.

Linux essentials

Command	Purpose
ls, pwd, cd	List files, show current directory, change directory.
cp, mv, rm, mkdir	Copy, move or rename, remove, create directory.
chmod / chown	Change permissions / change owner.
sudo / su	Run one command as root / switch user.
apt / dnf	Package managers (Debian-based / Red Hat-based).
ip, ping, dig, curl	Network configuration and testing.
df, du	Disk free space / directory usage.
ps, top	Show processes / live resource usage.
grep, find, cat	Search text, find files, display file contents.
nano, man	Text editor, manual pages.

Linux file permissions use read (4), write (2), and execute (1) for owner, group, and others. **chmod 755** means owner rwx, group and others r-x.

Recall

- Which macOS feature encrypts the disk?
- What does chmod 644 grant?

Applications and cloud productivity tools

Installing applications

- **Check requirements:** OS version, 32-bit versus 64-bit, CPU, RAM, storage, graphics, and dependencies.
- **Distribution:** app store, downloaded installer, network share, or managed deployment.
- **Impact:** consider the device, the network, the business, licensing, and user permissions.
- **Trust:** install only from reputable, verified sources; check digital signatures and hashes where available.

A 64-bit OS can run most 32-bit apps, but a 32-bit OS cannot run 64-bit apps.

Cloud-based productivity tools

Modern support work includes cloud services such as hosted email, cloud storage and synchronization, collaboration and conferencing tools, and identity services.

- **Email:** configure accounts and troubleshoot sign-in, sync, and mailbox limits.
- **Storage and sync:** understand sync conflicts, sharing permissions, and version history.

- **Collaboration:** chat, meetings, shared documents.
- **Identity synchronization:** on-premises accounts linked to cloud identities, often with single sign-on.
- **Licensing:** subscription licences assigned per user or device; missing licences are a common cause of "feature unavailable" errors.

> **Scenario**
>
> A new employee can sign in but cannot open the desktop office apps. Check whether a product **licence** is assigned to the account.

Recall

- Can a 32-bit OS run a 64-bit app?
- Name two cloud productivity support issues.

Security controls and Windows security

Physical security

Access control vestibules (mantraps), badge readers, video surveillance, alarm systems, motion sensors, door and equipment locks, guards, fences, and biometric locks. Physical access often defeats logical controls, so it matters.

Logical security

- **Principle of least privilege:** users get only the access they need.
- **Access control lists (ACLs)** define which users or systems may access a resource.
- **Multifactor authentication (MFA):** something you know, have, or are. Examples: authenticator app, hardware token, SMS (weaker), biometrics.
- **Mobile device management (MDM)** enforces policies on phones and tablets.
- **Email security:** SPF, DKIM, and DMARC help detect spoofed senders.
- **Identity and access management** and **single sign-on (SSO).**

Windows security features

Feature	Purpose
Microsoft Defender Antivirus	Built-in anti-malware; keep definitions updated.
Windows Defender Firewall	Host firewall with per-profile rules.
User Account Control (UAC)	Prompts before changes that need administrator rights.
BitLocker / BitLocker To Go	Full-volume encryption / removable drive encryption. Store the recovery key safely.
EFS	File and folder encryption on NTFS.
Windows Hello	PIN, face, or fingerprint sign-in.

Users, groups, and permissions

- Use standard user accounts for daily work; administrators only for admin tasks. Disable the guest account.
- **NTFS versus share permissions:** when accessing over the network, the *most restrictive* combination applies.
- Permissions are inherited by default. Copying a file to a new location usually takes the destination's permissions; moving within the same volume keeps them.
- **Active Directory** basics: domains, organizational units, group policy, login scripts, home folders, and folder redirection.

Scenario

A share grants Everyone Full Control, but NTFS grants the Sales group Read. A salesperson over the network gets **Read**, the most restrictive combination.

Recall

- How do NTFS and share permissions combine?
- What does UAC protect against?

Wireless, authentication, and malware

Wireless security

- **WPA3** is the strongest current standard; **WPA2** with AES is acceptable where WPA3 is unsupported. Avoid WEP, WPA, and TKIP.
- **Personal** mode uses a pre-shared key; **Enterprise** mode authenticates each user through RADIUS.
- **Authentication protocols:** RADIUS, TACACS+ (separates authentication, authorization, and accounting, common for network devices), and Kerberos (ticket-based, used by Active Directory).

Malware types

Type	Behaviour
Virus	Attaches to files and spreads when they run.
Trojan	Disguised as legitimate software.
Ransomware	Encrypts data and demands payment.
Rootkit	Hides deep in the system, often with elevated privileges.
Keylogger	Records keystrokes.

Spyware / stalkerware	Monitors activity without consent.
Cryptominer	Uses resources to mine cryptocurrency.
Boot sector virus	Infects the boot process.
Fileless malware	Runs in memory using legitimate tools, leaving few files.

Tools

Anti-malware and antivirus, Windows Recovery Environment, Safe Mode, software firewalls, anti-phishing training, and user education. Re-imaging is often the most reliable fix for a deeply infected system such as a rootkit.

Best-practice malware removal

1. Investigate and verify malware symptoms.
2. Quarantine the infected system (disconnect from the network).
3. Disable System Restore in Windows Home.
4. Remediate: update anti-malware software, then scan and remove using Safe Mode or a pre-installation environment.
5. Schedule scans and run updates.
6. Enable System Restore and create a restore point in Windows Home.
7. Educate the end user.

Why disable System Restore?

Restore points can contain infected files. Disabling it before cleaning prevents reinfection from an old restore point; re-enable it once the system is clean.

Recall

- Can I list the seven malware removal steps in order?
- Which protocol separates authentication, authorization, and accounting?

Social engineering, threats, and device hardening

Social engineering

Attack	Description
Phishing / spear phishing / whaling	Fraudulent email; targeted at a person; targeted at executives.
Vishing / smishing	Voice call / SMS phishing.
QR code phishing	Malicious QR codes leading to fake sites.
Shoulder surfing	Watching someone enter information.
Tailgating / piggybacking	Following someone through a secure door, without or with their consent.
Impersonation	Pretending to be IT, a manager, or a vendor.
Dumpster diving	Searching discarded material for information.
Evil twin	Rogue Wi-Fi access point imitating a legitimate one.

Other threats

DoS and DDoS, zero-day attacks, spoofing, on-path (man-in-the-middle) attacks, brute-force and dictionary attacks, insider threats,

SQL injection, cross-site scripting (XSS), business email compromise, and supply chain attacks.

Hardening

- **Workstations:** strong passwords or passphrases, screen lock timeouts, disable AutoRun, patching, least privilege, disable unused accounts, and encryption.
- **SOHO routers:** change default credentials, update firmware, use WPA3 or WPA2-AES, disable WPS and unused services, change default SSID, disable remote admin, and use guest networks.
- **Browsers:** trusted sources, extensions from official stores only, pop-up blockers, clearing cache and data, private browsing, secure connections, and password managers.
- **Mobile devices:** screen locks, remote wipe, locator apps, OS updates, device encryption, and MDM policies.

Data destruction and disposal

Method	Notes
Physical destruction	Drilling, shredding, degaussing (magnetic media only), incineration.
Erasing / wiping	Overwrite so data cannot be recovered; allows reuse.
Standard format	Does not reliably remove data.

Certificate of destruction	Proof from a third-party disposal vendor.

Degaussing does not work on SSDs. For SSDs, use manufacturer secure erase or physical destruction.

Recall

- Tailgating versus piggybacking?
- Which disposal method fails on SSDs?

Troubleshooting Windows

Work from least to most disruptive: gather information, check recent changes, try a quick fix, then escalate to deeper repairs. Always back up user data before destructive actions.

Symptom	Likely causes and fixes
Blue screen (BSOD)	Recent driver or update, failing hardware. Check Event Viewer and the stop code, roll back the driver or update, test memory and disk.
Sluggish performance	Too many startup apps, low disk space, malware, pending updates. Use Task Manager, Disk Cleanup, and a malware scan.
Boot problems	Corrupt boot files or failed update. Use Startup Repair in Windows RE, System Restore, or uninstall the latest update.
Frequent shutdowns	Overheating or power issues. Check cooling, power settings, and logs.
Service fails to start	Dependency or account issue. Check Services and Event Viewer; restart dependencies.
Application crashes	Corrupt install, missing updates, incompatibility. Repair or reinstall; check compatibility settings.
Low memory warnings	Memory leak or too many apps. Identify the process in Task Manager.
USB controller resource warnings	Too many devices on one controller. Move devices to another port or controller.

Time drift	Time sync disabled or CMOS battery failing. Resync time, replace battery.
Profile fails to load	Corrupt user profile. Rebuild the profile and migrate the user's data.

Repair tools, least to most disruptive

1. Restart the application or service.
2. Update or roll back drivers and updates.
3. Run sfc /scannow and check the disk.
4. Boot into Safe Mode to isolate drivers and startup items.
5. Use System Restore.
6. Use Reset this PC (keep files or remove everything).
7. Re-image or reinstall the OS.

> **Scenario**
>
> After a graphics driver update, a PC shows a blue screen on every boot. Boot into **Safe Mode** and **roll back the driver** in Device Manager before considering a reset.

Recall

- What is the least disruptive repair for a crashing app?
- What causes clock drift that returns after every restart?

Troubleshooting mobile and security issues

Mobile OS and app issues

Symptom	First steps
App fails to launch or closes	Force stop, clear cache, update, reinstall.
Device slow or battery drains fast	Check battery usage by app, close background apps, update the OS.
Screen does not auto-rotate	Check rotation lock and the app's support.
OS fails to update	Check storage space, battery charge, network, and device support.
Random reboots	Update OS and apps; check for faulty apps in safe mode.
Connectivity issues	Toggle Wi-Fi, Bluetooth, or airplane mode; forget and rejoin networks; reset network settings.

Mobile security issues

- **Signs:** high data use, unexpected apps, unusual permission requests, fake security warnings, pop-ups, and leaked personal files.

- **Causes:** apps from untrusted sources (sideloading, APK files), **rooted** (Android) or **jailbroken** (iOS) devices that bypass security controls, and developer mode left enabled.
- **Response:** remove suspicious apps, update the OS, run a security scan, and factory reset if compromise is confirmed, after backing up approved data.

PC security issues

Symptom	Common cause
Browser redirects and pop-ups	Adware, malicious extension, or changed DNS or proxy settings.
Certificate warnings	Wrong system time, on-path attack, or a genuinely invalid certificate.
Missing or renamed files	Ransomware or other malware.
Unwanted notifications	Browser notification permission granted to a malicious site.
Security software disabled	Malware trying to protect itself.
Degraded performance, high CPU	Cryptominer or other malware.

> **Scenario**
>
> Every HTTPS site shows a certificate warning on one laptop only. Check the **system date and time** first. A wrong clock makes valid certificates look expired.

Recall

- What makes a rooted or jailbroken device risky?
- Name two causes of browser redirection.

Documentation, change management, and backups

Documentation and support systems

- **Ticketing systems:** record user information, device, description, category, severity, escalation level, and clear progress notes and resolution.
- **Asset management:** inventory lists, asset tags, procurement life cycle, warranty and licensing, and assigned users.
- **Documentation types:** standard operating procedures (SOPs), knowledge base articles, incident reports, acceptable use policy (AUP), network diagrams, and new-user and end-user termination checklists.

Change management

A documented business process for changes includes: a request form, purpose of the change, scope, date and time, affected systems, risk analysis and level, a change board approval, a test in a sandbox, a rollback (backout) plan, responsible staff, and end-user acceptance.

> **Remember**
>
> If a change fails, follow the documented rollback plan. Do not improvise fixes on production outside the approved change window.

Backups and recovery

Type	Backs up	Restore needs
Full	Everything.	The last full backup.
Incremental	Changes since the last backup of any type.	Last full plus every incremental since.
Differential	Changes since the last full backup.	Last full plus the latest differential.
Synthetic full	A full backup assembled from a previous full plus incrementals.	The synthetic full.

- **3-2-1 rule:** three copies of data, on two different media, with one copy offsite.
- **Rotation schemes:** grandfather-father-son (GFS) keeps daily, weekly, and monthly backups.
- **Testing:** a backup is only proven by a successful test restore.
- **On-site versus off-site** (including cloud) storage trade speed of restore for protection from site-wide disasters.

Recall

- Incremental versus differential: which is faster to restore?
- What does 3-2-1 mean?

Safety, privacy, professionalism, scripting, remote access, and AI

Safety

- **ESD:** use an antistatic wrist strap and mat; handle components by the edges.
- **Electrical safety:** disconnect power before working; never open power supplies or CRTs.
- **Lifting:** lift with your legs, keep your back straight, and get help with heavy loads.
- **Fire:** use the correct extinguisher: Class C for electrical fires in the US classification used by the exam (other countries use different letters, so follow local signage), typically CO2 or dry chemical.
- **Compliance:** follow local government regulations and safety data sheets (SDS) for handling and disposing of batteries, toner, and chemicals.

Environment and power

Control temperature, humidity, and ventilation. Use surge suppressors against spikes, and an uninterruptible power supply (UPS) to ride through outages and shut down safely.

Privacy, licensing, and prohibited content

- **Incident response:** report through proper channels, preserve evidence, document, and maintain **chain of custody**.
- **Regulated data:** personally identifiable information (PII), payment card data (PCI DSS), protected health information (PHI), and privacy laws such as GDPR.
- **Licensing:** EULAs, personal versus corporate licences, subscriptions, open-source licences, and digital rights management (DRM). Unlicensed software is a compliance risk.
- **Data retention** requirements define how long records must be kept.

Communication and professionalism

Be on time, dress appropriately, use clear language without jargon, listen actively without interrupting, set and meet expectations, avoid distractions such as personal calls, respect confidential information, and follow up after resolution.

Scripting basics

Extension	Script type
.bat	Windows batch file
.ps1	PowerShell
.vbs	VBScript
.sh	Shell script (Linux and macOS)
.js	JavaScript

.py	Python

Use cases: basic automation, restarting machines, remapping drives, installing apps, automated backups, gathering information, and initiating updates. Risks: introducing malware, changing system settings unintentionally, and crashing browsers or systems through resource mishandling. Test scripts before wide use.

Remote access

Remote Desktop Protocol (RDP), VPN, virtual network computing (VNC), secure shell (SSH), remote monitoring and management (RMM) tools, screen-sharing software, and file transfer tools. Secure them with MFA, least privilege, patched software, and by not exposing RDP directly to the internet.

Artificial intelligence basics

Support staff increasingly use AI assistants. Understand appropriate use under company policy, the risk of **hallucinations** (confident but wrong output), **bias**, and **data privacy**: never paste confidential customer data into a tool that is not approved for it. Verify AI-generated commands before running them.

Recall

- Which extension indicates a PowerShell script?
- What is an AI hallucination?

Practice questions and explanations

Answer each question before reading the explanation. These are original scenarios, not recalled CompTIA questions.

Operating systems (1–9)

1. A user must copy a 5 GB file to a USB drive used on both Windows and macOS. Which file system?

exFAT.
FAT32 is limited to 4 GB per file; exFAT is widely supported on both systems.

2. A technician wants to join a new laptop to the company domain but the option is missing. What is the likely reason?

The laptop runs Windows Home.
Pro, Enterprise, and Education editions can join a domain.

3. Which tool rolls back a recently updated driver?

Device Manager.
Open the device's properties and choose Roll Back Driver.

4. Which command shows which Group Policy settings were applied to a user?

gpresult /r.

gpupdate /force reapplies policy but does not report it.

5. Websites work by IP address but not by name after a DNS server change. What should you run first?

ipconfig /flushdns.

Stale cached DNS entries may point to old addresses.

6. On Linux, which command gives the owner read, write, and execute, and everyone else read and execute?

chmod 755.

7 = 4+2+1 (rwx), 5 = 4+1 (r-x).

7. A macOS user wants automatic hourly backups to an external drive. Which built-in feature?

Time Machine.

FileVault encrypts; it does not back up.

8. A new disk is 4 TB and the system uses UEFI. Which partition style?

GPT.

MBR is limited to 2 TB disks and four primary partitions.

9. A new employee can sign in to the cloud portal but cannot use the office desktop apps. What should you check?

Whether a licence is assigned to the account.
Identity and licensing are separate.

Security (10–18)

10. A share grants Everyone Full Control; NTFS grants Sales Read. What does a salesperson get over the network?

Read.
The most restrictive combination of share and NTFS permissions applies.

11. What is the first step of the best-practice malware removal process?

Investigate and verify malware symptoms.
Quarantine follows once infection is confirmed.

12. Why disable System Restore on Windows Home before removing malware?

Restore points may contain the malware and cause reinfection.
Re-enable it and create a new restore point after cleaning.

13. Which wireless configuration is most secure for a small office that supports it?

WPA3.

Use WPA2 with AES only if WPA3 is unavailable; avoid TKIP and WEP.

14. An attacker follows an employee through a badge door without the employee noticing. What is this?

Tailgating.

Piggybacking involves the employee knowingly allowing entry.

15. Which disposal method is ineffective on SSDs?

Degaussing.

SSDs store data electronically, not magnetically.

16. A user receives a text claiming to be the bank and asking them to verify details via a link. What attack?

Smishing.

Vishing uses voice calls.

17. Which protocol is ticket-based and used by Active Directory for authentication?

Kerberos.

RADIUS and TACACS+ are commonly used for network access and device administration.

18. What should you change first on a new SOHO router?

The default administrator credentials.

Default passwords are publicly known.

Software troubleshooting (19–24)

19. After a graphics driver update, a PC shows a BSOD at boot. What is the best next step?

Boot into Safe Mode and roll back the driver.

Reinstalling Windows is far more disruptive.

20. A PC's clock is wrong after every power-off. What is the likely cause?

A failing CMOS battery.

Time sync can fix the clock temporarily, but the battery needs replacing.

21. Every HTTPS site shows a certificate error on one laptop. What should you check first?

The system date and time.

An incorrect clock makes valid certificates appear invalid.

22. A browser keeps redirecting searches to an unfamiliar site. What are the likely causes?

A malicious extension, adware, or changed DNS or proxy settings.

Remove the extension, scan for malware, and check network settings.

23. A phone has high data use, unfamiliar apps, and fake security pop-ups. What is the likely cause?

Malware, often from an app installed from an untrusted source.

Remove the apps, update, scan, and factory reset if needed.

24. A user's profile will not load and they get a temporary profile. What is the fix?

Rebuild the user profile and migrate the user's data.

A corrupt profile is a common cause of temporary profiles.

Operational procedures (25–30)

25. Backups run full on Sunday and incremental Monday to Friday. The server fails Thursday evening. What is needed to restore?

Sunday's full plus the Monday, Tuesday, Wednesday, and Thursday incrementals.
With differentials you would need only the full and the latest differential.

26. A change fails during the maintenance window. What should the technician do?

Follow the documented rollback plan.
Improvised fixes outside the approved change add risk.

27. Which fire extinguisher class is used for electrical fires?

Class C (US classification), such as CO2.
Other countries use different letters. Water-based extinguishers must not be used on electrical equipment.

28. A technician finds illegal content on a device during repair. What should they do?

Stop, report it through the proper channels, and preserve the evidence with chain of custody.
Do not delete, copy, or share the material.

29. Which file extension indicates a PowerShell script?

.ps1.

.bat is a batch file; .sh is a shell script.

30. An AI assistant suggests a command to fix a user's problem. What should you do before running it?

Verify what the command does and check that it follows policy.

AI output can be wrong, and running unverified commands can cause damage.

Six-week plan, cheat sheet, and glossary

Week	Focus	Output
1	OS types, file systems, installation, Windows editions	An edition comparison table from memory.
2	Windows tools and the command line	Run each listed command in a lab VM and note the output.
3	Windows networking, macOS, Linux, apps, cloud tools	A Linux command sheet and a macOS feature list.
4	Security controls, Windows security, wireless, malware	The seven malware removal steps written from memory.
5	Social engineering, hardening, software troubleshooting	A symptom-to-fix table for ten common problems.
6	Operational procedures and timed practice	Two timed practice sets; book the exam when results are consistently strong.

Cheat sheet

- **File size over 4 GB, cross-platform:** exFAT.
- **Over 2 TB or UEFI:** GPT.

- **Domain join, BitLocker, gpedit, RDP host:** Pro or Enterprise, not Home.
- **Share + NTFS permissions:** most restrictive wins.
- **Malware removal:** investigate, quarantine, disable restore, remediate, schedule and update, enable restore, educate.
- **Wireless:** WPA3 > WPA2-AES; avoid TKIP and WEP.
- **Repairs:** least disruptive first; back up before destructive steps.
- **Certificate errors everywhere:** check the clock.
- **Restore needs:** incremental = full + all incrementals; differential = full + latest.
- **Failed change:** rollback plan.

Glossary

AUP

Acceptable use policy defining permitted use of company systems.

BitLocker

Windows full-volume encryption.

Chain of custody

Documented record of who handled evidence and when.

ESD

Electrostatic discharge, which can damage components.

MDM

Mobile device management for enforcing device policy.

PII
Personally identifiable information.

RMM
Remote monitoring and management tools.

SOP
Standard operating procedure.

UAC
User Account Control prompts for elevation.

UPS
Uninterruptible power supply.

Before test day, compare this guide with CompTIA's official 220-1202 objectives, practise the commands and tools in a virtual machine you control, and rework every question you missed. The best answer is usually the safest, least disruptive step that follows policy.