CompTIA A+ Core 2 (220-1202)

Full Learning Guide

*Welcome to your complete Core 2 learning guide. This manual is designed to **teach you every domain deeply** — not just summarize, but help you understand, apply, and pass with confidence.*

Learning Objectives and Expectations

You'll master:

- Every CompTIA A+ Core 2 (220-1202) exam objective
- Every critical operating system, security and troubleshooting concept
- How OS tools, malware, authentication, and support practices work
- How to think like an IT technician — not just pass a multiple-choice test

A+ Core 2 Domains

Each domain is weighted differently, with **Operating Systems** and **Security** being the most tested.

Domain 1: Operating Systems (31%)
Domain 2: Security (25%)
Domain 3: Software Troubleshooting (22%)
Domain 4: Operational Procedures (22%)

Quick Reminder: How the Exam Works

- **Number of Questions**: Up to 90
- **Format**: Multiple Choice + Performance-Based Questions (PBQs)
- **Time Limit**: 90 minutes
- **Passing Score**: 700/900
- **Test Provider**: Pearson VUE (in-person or online)
- **Companion Exam**: Must also pass Core 1 (220-1201) to be certified

Top 10 A+ Core 2 Exam Tips

1. **Review Key Tools and Terms Before Test Day**: Focus on command-line tools (sfc, chkdsk, ipconfig), malware types, user account controls, file systems, and system recovery options.
2. **Don't Panic at PBQs**: Simulations can take time. If it's too long or unclear, flag it and come back after multiple choice.
3. **Use Process of Elimination**: Narrow down options based on what you know to make educated guesses when needed.
4. **Read Carefully — Especially for "NOT," "BEST," or "FIRST"**: These words change the expected answer.
5. **Skip and Flag if Stuck**: Don't waste 4 minutes on one question. Come back if needed.
6. **Get Familiar with Windows Tools**: Know where to go for settings, user accounts, services, and disk issues.
7. **Memorize the Malware Removal Steps and Troubleshooting Process**: They're classic questions — and often show up in performance-based tasks.
8. **Keep Your Calm**: Stay composed, especially if you hit unfamiliar material. Breathe, refocus, and move on.
9. **Never Leave a Question Blank**: There's no penalty for guessing — make sure every item is answered.
10. **Use the Final Minutes to Revisit Flags**: But only change answers if you're sure. First instincts are often correct.

Remember — You Don't Need 100% to Pass!

The A+ Core 2 passing score is **700 out of 900**, or about **78%**. That means you can miss **up to 20 questions** and still pass.

Stay focused, manage your time, and trust your preparation. Even if you blank on a few questions, you're still in the passing zone. The key is to be steady, strategic, and confident.

Domain 1: Operating Systems (31%)

The purpose of this domain is to test your knowledge and skills in managing various desktop operating systems, including Windows, macOS, Linux, and virtualization environments. Expect questions on installation, configuration, navigation, troubleshooting, command-line tools, and deployment scenarios.

1.1 Compare and contrast common operating system types and their purposes

Windows

- **Primary OS used in business and personal desktops**
- Known for:
  - GUI interface (Start Menu, Taskbar)
  - High compatibility with software/hardware
- Multiple editions:
  - **Home:** For consumers. Limited admin features.
  - **Pro:** Domain join, BitLocker, Remote Desktop, Group Policy.
  - **Enterprise:** Advanced features (AppLocker, DirectAccess), used in large companies.

macOS

- Unix-based operating system for Apple computers
- Seamless integration with Apple ecosystem (iCloud, AirDrop, Continuity)
- Uses **Finder** instead of Windows Explorer
- Uses **System Preferences** for settings
- Important system folders:
  - /Applications: Installed apps
  - /Users: User data
  - /System: System files
  - /Library: OS and app resources

Linux

- Open-source Unix-like OS with multiple distributions (Ubuntu, Fedora, Debian)
- Free and customizable
- Common in servers and embedded systems
- Uses command line heavily (Bash shell)

- Common file systems: **ext4**, **XFS**
- Important folders:
  - /etc: Configuration files
  - /home: User files
  - /var: Variable data like logs
  - /bin, /usr/bin: Binaries (executable files)

Mobile Operating Systems

- **Android**: Open-source (based on Linux), used by many phone manufacturers
- **iOS**: Proprietary Apple OS, closed system, secure app environment
- Purpose-built for touch interface and mobile hardware

1.2 Compare and contrast features of Microsoft Windows editions

Windows Editions:

Edition	Key Features
Home	Basic version, no domain join, no BitLocker
Pro	Domain join, BitLocker, Remote Desktop, Group Policy
Enterprise	Enterprise features like AppLocker, DirectAccess
Education	Similar to Enterprise, used in schools
Pro for Workstations	ReFS file system, high RAM/CPU support

Key Feature Differences:

- **Domain Join** – Only Pro and higher can join Active Directory
- **BitLocker** – Disk encryption, available on Pro and higher
- **Group Policy Editor (gpedit.msc)** – Manage system policies
- **Remote Desktop Host** – Pro and up support being remoted into
- **Hyper-V** – Built-in virtualization, Pro and up

1.3 Install and configure operating systems using appropriate methods

Installation Types:

- **Clean install**: Wipes system and installs OS from scratch
- **Upgrade**: Moves from older version while keeping data/settings
- **In-place upgrade**: Maintains files and programs

- **Image deployment**: Using a captured image to clone OS

Installation Methods:

- **Bootable USB/DVD**
- **Network (PXE boot)**
- **Recovery Partition**
- **Virtual Machine installation**

Partitioning Concepts:

- **MBR (Master Boot Record)**:
  - Max 4 primary partitions
  - Max disk size: 2TB
- **GPT (GUID Partition Table)**:
  - Supports more partitions
  - Required for UEFI
  - Supports large drives (>2TB)

File Systems:

- **NTFS** – Windows default, supports permissions, encryption
- **FAT32** – Legacy, max 4GB files
- **exFAT** – For flash drives, supports large files
- **ReFS** – Resilient File System, used in Windows Server and Workstation

Boot Methods:

- **BIOS** (legacy)
- **UEFI** (modern):
  - Secure Boot
  - Requires GPT disks

Real-World Scenarios:

- Installing Windows 11 may fail without Secure Boot and TPM 2.0
- Dual-boot systems use a bootloader (GRUB, Windows Boot Manager)

1.4 Apply application installation and configuration concepts

- Use **Programs and Features** in Control Panel to install/uninstall apps
- Use **Windows Installer (.msi)** or executable (.exe)
- Software restrictions may block installations via Group Policy

- **Installers may require admin privileges**
- Check compatibility: 32-bit vs 64-bit

1.5 Configure and use virtual machines

- **Hypervisor Type 1** – Bare metal (e.g., VMware ESXi)
- **Hypervisor Type 2** – Hosted (e.g., VirtualBox, Hyper-V on Windows)
- Key settings:
  - RAM, CPU cores
  - Disk space
  - Network bridging or NAT
- Snapshots allow rollback to a saved state
- Used for testing, labs, and OS isolation

1.6 Identify common Microsoft Windows features and tools

Graphical Utilities:

Utility	Purpose
Control Panel	Legacy settings interface
Settings	New Windows 10/11 interface
Device Manager	View/update drivers
Disk Management	Partition disks
Task Manager	Monitor apps and resources
System Configuration (msconfig)	Boot options, disable startup items
Event Viewer	View system logs
Services.msc	Start/stop system services
Performance Monitor	Advanced performance metrics
Registry Editor	Advanced tweaks (use caution)
Command Prompt / PowerShell	CLI tools for administration

1.7 Use Microsoft Windows Control Panel utilities

Key Applets to Know:

- **System** – OS version, performance, domain join
- **Devices and Printers** – Manage hardware
- **Internet Options** – Proxy, certificate, security settings

- **Programs and Features** – Manage apps
- **User Accounts** – Create/manage local users
- **File Explorer Options** – Show hidden files, extensions
- **Credential Manager** – Store saved passwords
- **BitLocker** – Full-disk encryption
- **Power Options** – Sleep, hibernate, power plans

1.8 Use Windows command line tools

File and Directory Management:

- dir – List files
- cd – Change directory
- copy, xcopy, robocopy – Copy files
- del, rmdir – Delete files/directories

System Utilities:

- sfc /scannow – Scan and fix system files
- chkdsk /f /r – Check disk for errors
- diskpart – Manage partitions
- format – Format drives
- tasklist, taskkill – View/kill processes

Network Tools:

- ipconfig – Show IP settings
- ping, tracert, pathping – Network diagnostics
- netstat – View active connections
- nslookup – Query DNS
- net use, net user – Manage shares and users

Misc:

- shutdown – Reboot or shut down
- gpupdate, gpresult – Refresh or view policies
- regedit – Open registry editor
- whoami – Show current user

1.9 Use features and tools of the macOS and Linux client/desktop OS

macOS:

- **Finder** – File browser
- **System Preferences** – Settings manager
- **Keychain** – Password management
- **Terminal** – Command line access
- **Time Machine** – Backup solution
- **Disk Utility** – Manage partitions and disks
- **Force Quit** – Terminate apps (Option + Command + Esc)

Linux:

- **File structure**:
  - /home, /etc, /bin, /usr, /var
- **Common commands**:
  - ls, cd, cp, mv, rm
  - chmod, chown, df, du
  - ps, top, kill
  - apt, yum, dnf – Package managers
  - systemctl – Manage services
- **Desktop environments**: GNOME, KDE

1.10 Summarize the importance of operating system security and updates

- **Windows Update**: Automatically patches vulnerabilities
- **Patch management**:
  - Test updates before wide rollout in enterprise
  - Schedule during maintenance windows
- **Feature updates**: New functionality (e.g., Windows 11 upgrade)
- **Quality updates**: Bug and security fixes

Domain 1 Summary – Operating Systems (31%)

Things You Must Memorize:

• Windows editions: Home, Pro, Enterprise, Education – key features like BitLocker, domain join
• Installation types: clean install, in-place upgrade, image deployment
• File systems: NTFS, FAT32, exFAT, ReFS – know usage and limits
• MBR vs GPT, BIOS vs UEFI – partition types and boot firmware differences
• Windows tools: Control Panel, Settings, Device Manager, Task Manager, Disk Management
• Command-line tools: ipconfig, chkdsk, sfc, netstat, taskkill, robocopy, shutdown, whoami
• macOS tools: Finder, Time Machine, Keychain, Disk Utility, Terminal
• Linux basics: ls, cd, chmod, sudo, apt, /etc, /home, df, ps, kill
• Virtualization: VM concepts, snapshots, Hyper-V, Type 1 vs Type 2 hypervisors
• Cloud basics: OneDrive, Google Drive, SaaS tools like Office 365
• Zero-touch deployment, PXE, boot methods (USB, DVD, network)

Domain 2: Security (25%)

This domain tests your knowledge of security fundamentals across devices, operating systems, users, data, and networks. You'll need to understand types of threats, best practices, authentication methods, device hardening, and basic secure configuration.

2.1 Identify and protect against various types of malware

Common Malware Types:

Malware Type	Description	Key Behavior
Virus	Attaches to files/programs; spreads when host is executed	Requires user action to spread
Worm	Self-replicating; spreads via network	No user interaction needed
Trojan Horse	Disguised as legitimate software	Opens backdoors, often disables security
Spyware	Collects info like keystrokes, browsing	Often installs silently
Adware	Displays ads, pop-ups, or hijacks browser	Can track user behavior
Ransomware	Encrypts files, demands payment	Usually via phishing or exploit
Rootkit	Hides itself by modifying system files	Grants privileged access
Keylogger	Records user keystrokes	Often embedded in spyware
Botnet/Zombie	System added to attacker-controlled network	Used in DDoS, spam
Logic Bomb	Executes after trigger (e.g. date, event)	Can delete or damage files
Fileless Malware	Operates in memory only	Evades antivirus by avoiding disk
PUP (Potentially Unwanted Program)	Unwanted apps bundled with legitimate software	Slows down system, shows ads
Stalkerware	Tracks user activity covertly	Usually used by abusers/spouses

Signs of Infection:

- System slowdowns

- Unwanted pop-ups or toolbars
- Redirected web traffic
- Apps crashing or freezing
- Files encrypted or missing
- Antivirus disabled
- Suspicious processes (check in Task Manager)

2.2 Compare and contrast types of social engineering

Social Engineering Methods:

Type	Description	Example
Phishing	Deceptive email or message asking for login info	"Your bank account is locked, click here to unlock"
Spear Phishing	Targeted phishing using personal details	"Hi John, here's your HR form"
Whaling	Targets executives or high-level personnel	CEO receives fake invoice email
Vishing	Phishing via phone call	Fake IRS call demanding payment
Smishing	Phishing via SMS	"Your Amazon package is delayed, click this link"
Pretexting	Impersonating someone to gain info	Pretending to be IT to ask for passwords
Tailgating	Following someone into a restricted area	Walking through secure door with someone else
Shoulder Surfing	Observing login info or PIN	Looking over someone's shoulder at ATM
Dumpster Diving	Retrieving sensitive info from trash	Finding sticky notes with passwords
QR Code Scams	Malicious QR code redirects to phishing page	QR code in fake parking notice
Business Email Compromise (BEC)	Impersonating executives to initiate money transfers	"Send $10,000 to vendor urgently"

2.3 Compare and contrast security best practices

Password Practices:

- Use complex passwords (uppercase, lowercase, numbers, special characters)

- Minimum 8–12 characters
- Use **passphrases**: “RedCar$Climbs!Mountain”
- Change passwords periodically (but not excessively unless needed)
- Avoid reuse and dictionary words
- Use **password managers** to store securely

Account Security:

- **Account lockout** after failed attempts
- **Account expiration** for temp accounts
- Disable unused accounts
- Limit **admin privileges**

Authentication Methods:

Factor Type	Examples
Something you know	Password, PIN
Something you have	Smart card, token, phone
Something you are	Fingerprint, face scan
Somewhere you are	GPS/location
Something you do	Typing rhythm, signature

- **Multifactor Authentication (MFA)** = Two or more of these
- **Passwordless Authentication** = Face/biometric + device possession (like Windows Hello)

Biometrics:

- Fingerprint readers
- Facial recognition (Windows Hello)
- Voice recognition
- Iris/retina scans

Smart Cards & Tokens:

- Physical smart card + PIN
- Hardware token generating codes (RSA key fob)
- **Authenticator apps** (Google Authenticator, Microsoft Authenticator)

2.4 Given a scenario, detect, remove, and prevent malware using appropriate tools and methods

Malware Removal Process:

1. **Identify and research symptoms**
2. **Quarantine** the infected system
3. **Disable System Restore** (if on Windows)
4. **Remediate** the system:
    - Update anti-malware definitions
    - Run full scan in Safe Mode
5. **Schedule future scans and updates**
6. **Re-enable System Restore**
7. **Educate user to prevent recurrence**

Tools for Removal:

- Windows Defender
- Malwarebytes
- Microsoft Safety Scanner
- Bootable antivirus rescue disks (Kaspersky, ESET)

Command-line tools:

- sfc /scannow – System File Checker
- chkdsk /f – Fix file system issues
- msconfig – Disable startup items
- taskmgr – Kill malicious processes

2.5 Compare and contrast wireless security protocols and authentication methods

Wireless Security Standards:

Standard	Encryption	Notes
WEP	RC4	Obsolete, crackable in minutes
WPA	TKIP	Better than WEP, still weak
WPA2	AES	Industry standard (use this)
WPA3	AES + improved handshake	Latest standard, stronger security

- **WPA2-PSK**: Home use, shared password
- **WPA2-Enterprise**: Corporate, uses **RADIUS** server for authentication
- Avoid WEP and WPA unless no other choice

Other Wireless Concepts:

- **Disabling SSID broadcast**: Hides network name (does not provide security)
- **MAC filtering**: Whitelist specific devices (easy to spoof)
- **Guest networks**: Isolate traffic from primary network

- **Captive portals**: Webpage prompts before connecting (e.g., hotel Wi-Fi)

2.6 Implement device hardening techniques

Hardening Methods:

Technique	Purpose
Disable unused services	Reduces attack surface
Disable Bluetooth/NFC	Prevents local wireless attacks
Turn off auto-run/auto-play	Blocks USB malware spread
Use strong admin passwords	Prevents privilege abuse
Firmware updates	Fixes vulnerabilities in BIOS/UEFI
Antivirus/anti-malware	Protects against malicious software
Application whitelisting	Only approved apps run
Account permissions	Least privilege model
Encrypt storage	Prevents access if device lost/stolen

Mobile Device Hardening:

- Enable screen lock (PIN, biometric)
- Enable encryption
- Use **remote wipe**
- Use **MDM** (Mobile Device Management) to enforce policies
- Disable app sideloading

2.7 Summarize best practices associated with securing workstations

Security Techniques:

- **Screen Lock**: Password-protected auto-lock after inactivity
- **Login Time Restrictions**: Limit hours of access
- **User Education**: Avoid phishing, safe browsing habits
- **Patch Management**: OS and app updates
- **Antivirus**: Always up-to-date and enabled
- **Disable unused ports**: Block USB, serial, etc.
- **Host-based firewall**: Control traffic to/from system
- **File and folder permissions**: Apply NTFS ACLs
- **BitLocker/EFS**: Encrypt drive or file
- **Group Policy (Windows)**: Enforce security settings across domain

2.8 Compare and contrast methods for securing mobile and embedded devices

Mobile Devices:

- **Screen locks**: PIN, biometric
- **Remote wipe**: Erase data if lost/stolen
- **Locator tools**: Find lost device
- **OS/app updates**: Fix vulnerabilities
- **Avoid untrusted apps**: Use official app stores
- **Mobile antivirus**: For malware defense
- **Encryption**: Built-in on most modern phones
- **MDM**: Corporate control over devices

Embedded Systems:

- Devices like routers, smart TVs, HVAC controllers
- Often run minimal Linux-based OS
- **Change default credentials**
- **Disable remote admin if not needed**
- **Update firmware** when available
- **Network segmentation** to isolate devices

2.9 Use appropriate data destruction methods

Method	Description	Use Case
Shredding	Physically destroying paper or drives	Most secure
Degaussing	Uses strong magnets to wipe hard drives	Obsolete for SSDs
Drill/Hammer	Physically destroy platters or chips	For unusable drives
Wipe Utilities	Software overwrites all data	DBAN, KillDisk
Secure Erase (ATA)	Command built into drive	Faster, secure for SSDs

- **Standard Format**: Removes file system, but data recoverable
- **Low-Level Format**: Writes over data; not usually needed unless reselling
- Always **verify** data destruction (e.g., certificate of destruction)

2.10 Implement basic forensic procedures

- **Chain of Custody**:
  - Document every person who handles evidence
  - Required in legal investigations
- **Preserve Evidence**:
  - Power off system? No—unless risk of destruction. Snapshot memory if needed.
  - Clone drive before analysis
- **Isolate System**:
  - Remove from network to prevent data tampering
- **Document Everything**:
  - Who, what, when, where
- **Avoid Contamination**:
  - Don’t run tools unless authorized (could alter evidence)

Domain 2 Summary – Security (25%)

Things You Must Memorize:

• Malware types: virus, worm, Trojan, rootkit, ransomware, keylogger, spyware, PUP, fileless
• Social engineering: phishing, spear phishing, whaling, vishing, smishing, tailgating, dumpster diving
• Authentication methods: password, PIN, smart card, token, biometric, MFA
• Account security: lockout policies, expiration, disable unused accounts, password complexity
• Wireless security: WEP (bad), WPA, WPA2 (use), WPA3 – pre-shared vs enterprise
• Device hardening: disable ports/services, firmware updates, screen locks, encryption
• Malware removal steps: Identify, Quarantine, Disable Restore, Remediate, Scan, Enable Restore, Educate
• Mobile security: MDM, remote wipe, screen lock, app control
• File destruction: shredding, degauss, wipe utilities, drill/hammer
• Security tools: antivirus, firewall, Windows Defender, update policies
• Security policies: AUP, DLP, password policy, clean desk, incident response
• Zero Trust security model: never trust, always verify
• Secure DNS, email security gateway, proxy settings, browser best practices

Domain 3: Software Troubleshooting (22%)

This domain covers identifying, troubleshooting, and resolving software-related issues on operating systems, applications, and mobile platforms. You'll also apply structured troubleshooting steps and understand error behaviors and recovery methods.

3.1 Troubleshoot common Windows OS problems

This section focuses on fixing errors, performance issues, crashes, and update failures in Windows.

Startup Issues:

Symptom	Cause	Resolution
Failure to boot	Corrupted boot files, incorrect boot order	Boot into recovery; use bootrec /fixmbr and /fixboot
Missing OS	No OS or bootloader found	Check BIOS boot order or reinstall OS
Bootmgr is missing	Boot files corrupt	Use installation media > Repair > Command Prompt
Blue Screen of Death (BSOD)	Critical system or driver failure	Record STOP code, reboot into Safe Mode, update or roll back drivers
Black screen on boot	GPU driver failure, explorer.exe not starting	Use Ctrl+Shift+Esc to run explorer.exe manually

Shutdown & Restart Problems:

- Unresponsive shutdown → check running processes in Task Manager
- Unexpected restarts → overheating, bad PSU, or faulty RAM

App Crashes:

- Reinstall application
- Use Event Viewer > Application Log for crash details
- Run sfc /scannow to check system file integrity
- Disable add-ins (for MS Office crashes)
- Check for permissions or compatibility settings

Slow Performance:

Cause	Fix
Too many startup apps	Use Task Manager > Startup tab
Malware infection	Run AV scan
Insufficient RAM	Upgrade RAM or reduce running programs
HDD fragmentation	Run Optimize Drives (only on HDDs)
Failing drive	Use chkdsk and SMART monitoring

Updates Fail to Install:

- Clear C:\Windows\SoftwareDistribution
- Run Windows Update Troubleshooter
- Use DISM /RestoreHealth + sfc /scannow
- Check disk space and disable AV temporarily
- Install update manually via Microsoft Update Catalog

Error Messages:

Message	Meaning
"DLL not found"	Missing shared library
"Application not responding"	Frozen app
"Out of memory"	App demanding more RAM than system provides

3.2 Troubleshoot common personal computer security issues

These relate to infection, unauthorized access, or improper settings.

Common Symptoms of Infections:

- Frequent crashes
- Browser hijacking (default page/search engine changes)
- Pop-ups or fake antivirus warnings
- High CPU usage from unknown processes
- Security tools disabled
- Network activity with no apps running

Tools for Diagnosis:

- Antivirus/antimalware software
- Task Manager (unusual processes)
- msconfig / services.msc (rogue startup entries)
- Safe Mode + Offline Scanner (Malwarebytes, Microsoft Safety Scanner)

Remediation Steps (7-Step Process):

1. Identify malware symptoms
2. Quarantine system
3. Disable System Restore
4. Remediate (update AV, run scans)
5. Schedule regular scans
6. Re-enable System Restore
7. Educate user (safe browsing, email caution)

Browser Hijack/Pop-ups:

- Remove unknown extensions
- Reset browser to defaults
- Check proxy settings and hosts file
- Use AdwCleaner or similar tool

Unwanted Programs (PUPs):

- Remove from Programs and Features
- Reset browser settings
- Use Revo Uninstaller or similar deep-cleaning tools

3.3 Troubleshoot common mobile OS and application issues

Includes iOS, Android, and sometimes ChromeOS.

Common Mobile Problems:

Problem	Solution
App not loading/crashing	Force close, clear cache, update/reinstall
Touchscreen unresponsive	Reboot, remove case/screen protector
Poor battery life	Check battery usage, update apps, disable background refresh
No internet	Reset network settings, toggle airplane mode
Cannot install app	Check storage space, OS version compatibility
App permissions	Go to Settings > Apps > Permissions and toggle as needed
Overheating	Close background apps, remove case, avoid direct sun
Camera not working	Force restart, check if app has camera permission

Mobile Security Symptoms:

- Unusual data usage

- Unauthorized SMS or calls
- Slow performance
- Battery drain
- Suspicious apps

Fix: Factory reset device, reconfigure manually, update OS

3.4 Troubleshoot common application issues

Installation Failures:

Cause	Resolution
Corrupted installer	Redownload
Wrong OS version	Use compatible installer
Permissions issue	Run installer as Administrator
Antivirus block	Disable temporarily, then install
Missing prerequisites	Install .NET Framework, C++ Redistributable, etc.

Compatibility Problems:

- Use **Compatibility Mode** (right-click > Properties)
- Use 32-bit version on 32-bit OS
- Update app or OS to compatible version

Service Failures:

Service	Symptoms	Fix
Print Spooler	Print jobs stuck	Restart spooler service
Windows Update	Error codes	Use Troubleshooter or reset service
DHCP Client	No IP address	Use static IP or restart service

Permissions Issues:

- Check NTFS permissions
- Take ownership of files
- Confirm UAC prompts are approved

Data Loss Prevention (DLP):

- Corporate policies may block copying files to USB or cloud
- If user can't save or send files, check if DLP policies are active

---

3.5 Explain common OS security alert and notification behaviors

Behavior	Cause	Action
UAC prompt	App requires elevated privileges	Click Yes if expected
Antivirus warning	Detected threat	Quarantine or remove
Windows Defender alert	Suspicious app behavior	Investigate app source
Firewall prompt	App trying to access network	Allow only if trusted

---

3.6 Use appropriate Microsoft Windows 10/11 troubleshooting tools

System Tools:

- **Event Viewer** – View system, application, and security logs
- **System Configuration (msconfig)** – Boot, services, startup control
- **Task Manager** – View running apps/processes and resource use
- **Reliability Monitor** – Timeline of app crashes and errors
- **Performance Monitor** – Detailed performance stats (RAM, CPU, Disk IO)

Command-Line Tools:

Command	Purpose
sfc /scannow	Scan and fix system files
DISM /Online /Cleanup-Image /RestoreHealth	Fix corrupt component store
chkdsk	Fix disk errors
ipconfig /flushdns	Clear DNS cache
netstat	View network connections
tasklist, taskkill	View/kill processes

Safe Mode:

- Loads basic drivers/services
- Use for removing malware or problematic drivers
- Access via:
  - msconfig
  - Shift+Restart > Troubleshoot > Startup Settings

System Restore:

- Rollback to restore point (does not affect files)
- Use if a new driver or update caused a problem

Reset This PC:

- Settings > Recovery > Reset
  - Keep my files (reinstalls OS but saves files)
  - Remove everything (full clean install)

3.7 Summarize the process of troubleshooting and documentation

CompTIA 6-Step Troubleshooting Model:

1. **Identify the problem**
   - Gather user input
   - Observe system behavior
   - Review logs (Event Viewer)
2. **Establish a theory of probable cause**
   - Use experience, knowledge, and documentation
3. **Test the theory**
   - Validate it or develop new ones
4. **Establish a plan of action and implement the solution**
   - Consider user impact, backup before major changes
5. **Verify full system functionality**
   - Reboot, test full workflows
6. **Document findings, actions, and outcomes**
   - Use ticketing system or KB articles
   - Helps future troubleshooting and compliance

Documentation Includes:

- Problem description
- Steps taken
- Final resolution
- Any changes to system or config

Domain 3 Summary – Software Troubleshooting (22%)

Things You Must Memorize:

• Windows startup issues: boot failure, BSOD, missing OS, Bootmgr error, black screen
• Recovery tools: Safe Mode, System Restore, Startup Repair, Reset this PC
• Commands: sfc /scannow, DISM, bootrec, chkdsk, msconfig, taskmgr, services.msc
• Common symptoms: crashing apps, slow performance, pop-ups, login errors, missing DLLs
• App install errors: wrong architecture, missing prereqs, permissions, compatibility mode
• Mobile issues: app crashes, overheating, connectivity loss, permission issues, OS updates
• Malware signs: browser hijack, rogue processes, CPU spikes, AV disabled
• Troubleshooting methodology: Identify, Theory, Test, Plan, Verify, Document
• Documentation: ticketing, KB articles, resolution notes
• Browser fix steps: remove extensions, reset settings, clear cache, proxy reset
• Data loss protection (DLP): restrict USB/cloud, block unapproved data transfers
• Security tools: offline scanner, safe boot AV, Task Manager analysis

Domain 4: Operational Procedures (22%)

This domain tests your understanding of how to work professionally in IT environments. It includes safety procedures, change management, documentation, communication, scripting basics, and environmental concerns.

4.1 Identify basic safety procedures and potential hazards

ESD (Electrostatic Discharge):

- Static electricity can damage sensitive components.
- Use:
  - **ESD wrist straps** grounded to chassis.
  - **Antistatic mats** on work surfaces.
  - **Antistatic bags** to store parts.
- Touch the metal case to ground yourself before touching internal components.

Electrical Safety:

- Always unplug equipment before servicing.
- Avoid touching capacitors inside power supplies or CRT monitors.
- Never bypass the ground pin on a power plug.

Proper Lifting Techniques:

- Bend at the knees, not your waist.
- Lift with your legs.
- Get help or use carts for heavy items (servers, UPS units, printers).

Tool Safety:

- Use proper tools for the job.
- Store tools securely when not in use.
- Ensure tools are insulated for electrical tasks.

Environmental Controls:

- Maintain correct server room temperature (approx. 18–27°C or 64–80°F).
- Humidity should be controlled to avoid static buildup or condensation.

- Use HVAC, sensors, and filtration systems.

4.2 Explain environmental impacts and appropriate controls

Material Disposal:

Material	Disposal Method
Batteries	Recycle via approved centers
Toner/Ink cartridges	Return to manufacturer or recycle
Electronics	Use e-waste recycling vendors
CRT monitors	Hazardous waste; handle with care
Hard drives	Degauss, wipe, shred, or physically destroy
Paper with PII	Shred or incinerate

Environmental Compliance:

- Follow **local and national regulations** for disposal.
- Maintain **MSDS/SDS** (Safety Data Sheets) for chemicals.
- Know how to respond to spills or leaks (especially from UPS batteries).

4.3 Explain the importance of documentation and corporate policies

Documentation Types:

Type	Purpose
Network topology diagram	Shows physical/logical network layout
Knowledge base/articles	Document fixes, procedures
Change documentation	Track changes, approvals, and rollback plans
Inventory/Asset management	Tracks devices, software, licenses
Incident reports	Record outages, security events, and resolutions
Standard Operating Procedures (SOPs)	Define repeatable tasks

Corporate Policies:

- **Acceptable Use Policy (AUP)**: What users can/cannot do with company resources.

- **Password policy**: Defines password complexity, expiration, reuse rules.
- **Data classification policy**: Labels data as public, internal, confidential, secret.
- **Privacy policy**: Explains how user/customer data is handled.

4.4 Demonstrate proper communication techniques and professionalism

Best Practices:

Practice	Description
Active listening	Listen fully before responding
Clarifying questions	Ensure understanding (e.g., “Can you walk me through what happened?”)
Avoid jargon	Use plain language
Positive attitude	Show patience and willingness to help
Cultural sensitivity	Be respectful of all backgrounds and beliefs
Avoid distractions	Focus entirely on the customer
Respect confidentiality	Do not disclose sensitive data seen during support

Phone Etiquette:

- Greet professionally.
- Speak clearly and at a moderate pace.
- Don’t interrupt.
- Recap solution at end of call.
- Thank the customer.

Email Etiquette:

- Use formal language.
- Be concise and structured.
- Avoid slang or abbreviations.
- Sign with your name and contact info.

4.5 Explain the basics of change management

Why Change Management?

- Reduces risk
- Ensures accountability

- Maintains service availability

Change Types:

Type	Description
Standard	Pre-approved, low-risk (e.g., patch updates)
Normal	Requires approval and planning
Emergency	Implemented quickly due to critical issues (e.g., patch for zero-day exploit)

Change Process Steps:

1. Document the change
2. Get approval
3. Communicate to users
4. Schedule during a maintenance window
5. Implement the change
6. Verify success
7. Document the outcome

4.6 Identify basics of disaster prevention and recovery

Backup Types:

Type	Description
Full	Copies all selected data
Incremental	Copies changes since last backup (fast, small)
Differential	Copies changes since last full (larger, simple restore)
Snapshot	Instant image of system (used in virtualization)

Backup Considerations:

- Test backups regularly
- Keep **offsite** or **cloud** backups
- Encrypt sensitive backup data
- Store multiple versions

Recovery Terms:

Term	Definition
MTTR (Mean Time to Repair)	Avg. time to fix and restore
MTBF (Mean Time Between Failures)	Avg. time between failures
RTO (Recovery Time Objective)	Max acceptable downtime

Term	Definition
RPO (Recovery Point Objective)	Max acceptable data loss (time-wise)

4.7 Explain common safety procedures and policies

Fire Safety:

- **Class C fire extinguishers** for electrical fires
- Know location of extinguishers and exits
- Don’t use water on electrical equipment

Safety Compliance:

- Follow **OSHA** standards (U.S.)
- Wear **PPE** when required
- Follow **Clean Desk Policy**: no unsecured sensitive info

4.8 Explain the importance of physical security controls

Control	Purpose
Badge access	Restrict entry to authorized users
Mantraps	Prevent tailgating
Security guards	Deter and respond to intrusions
Video surveillance	Record activity, deter intruders
Cable locks	Secure laptops and devices
Locked server rooms	Prevent unauthorized access
Privacy filters	Prevent shoulder surfing
Motion sensors	Detect unauthorized movement
Key management	Secure and control access to physical keys

4.9 Summarize the basics of scripting and automation

Why Scripting Matters:

- Automates repetitive tasks
- Saves time and reduces error

File Types and Uses:

File	Purpose
.bat	Windows batch file
.ps1	Windows PowerShell script
.sh	Bash shell script for Linux/macOS
.py	Python script
.vbs	Visual Basic script (Windows)
.js	JavaScript file (mostly browser or Node.js)

Use Cases:

- Automate backups
- Map drives on login
- Clean temp files
- Install software silently

Best Practices:

- Use comments in scripts for clarity
- Test in staging before production
- Use version control (e.g., Git)

4.10 Explain remote access technologies

Tech	Use
RDP (Remote Desktop Protocol)	Access Windows desktops remotely
VPN (Virtual Private Network)	Secure remote access to networks
VNC (Virtual Network Computing)	Cross-platform remote control
TeamViewer/AnyDesk	Third-party tools for remote support
SSH (Secure Shell)	Secure remote command-line on Linux
Telnet	Legacy insecure protocol (don't use in production)

Security Best Practices:

- Use strong passwords and MFA
- Limit remote access to need-to-know
- Use encrypted protocols (RDP with NLA, SSH)
- Close ports when not needed

4.11 Identify proper use of organizational policies, best practices, and procedures

Data Handling:

- Handle PII and PHI with care
- Follow **GDPR**, **HIPAA**, **PCI-DSS** if applicable
- Encrypt sensitive data in transit and at rest

Incident Response:

- **Identify** the issue
- **Report** to appropriate personnel
- **Preserve** evidence (screenshots, logs)
- **Contain** the issue (e.g., isolate infected system)
- **Recover** and document

Chain of Custody:

- Record every handler of evidence
- Ensure integrity in case of legal proceedings

4.12 Explain the importance of learning emerging technologies

Artificial Intelligence:

- Used in security tools, support chatbots
- Be cautious of **bias** and **hallucinations**
- Verify AI-generated data

SaaS & Cloud Services:

- Microsoft 365, Google Workspace
- Remote productivity tools
- Require reliable internet and backup plans

IoT Devices:

- Smart thermostats, locks, cameras
- Update firmware
- Segment networks for IoT securit

Domain 4 Summary – Operational Procedures (22%)

Things You Must Memorize:

- Safety: ESD protection, fire classes (C = electrical), PPE, lifting technique
- Disposal: e-waste, shredding HDDs, recycle batteries, toner returns
- Environmental: MSDS/SDS, HVAC needs, temperature & humidity ranges
- Documentation types: network diagrams, SOPs, asset list, change log, KBs
- Policies: AUP, password, data classification, privacy, incident response
- Communication: active listening, clear language, documentation, escalation
- Change management: standard vs normal vs emergency changes
- Backups: full, incremental, differential, snapshot – test regularly
- Recovery terms: RTO, RPO, MTTR, MTBF – define downtime expectations
- Scripting: .bat, .ps1, .sh, .py, .vbs – automate IT tasks
- Remote tools: RDP, SSH, VPN, TeamViewer, VNC – secure access methods
- Chain of custody: preserve evidence, log handlers
- AI awareness: bias, hallucinations, responsible use in helpdesk/chatbots

Terms and Definitions

Operating Systems

Term	Definition
NTFS	Windows file system with support for permissions, encryption, large files
exFAT	File system for flash drives; supports large files, no journaling
MBR	Legacy partition table, supports 2TB disks and 4 primary partitions
GPT	Modern partitioning with support for large drives and UEFI
UEFI	Firmware replacing BIOS; supports Secure Boot and GPT
BitLocker	Full-disk encryption available in Windows Pro and Enterprise
EFS	Encrypting File System; file/folder-level NTFS encryption
PXE Boot	Preboot Execution Environment; boots from network for OS deployment
Hyper-V	Microsoft virtualization platform (Type 1 hypervisor)
Snapshot	A saved VM state for quick rollback
PowerShell	Command-line and scripting shell for system automation
Command Prompt	Windows command-line tool for executing CLI commands

Security – Threats & Engineering

Term	Definition
Virus	Infects and spreads via files; requires execution
Worm	Self-replicates over network without user action
Trojan	Disguised malware posing as legitimate software
Spyware	Secretly gathers user data (e.g., keystrokes, sites)
Adware	Displays unwanted advertisements
Ransomware	Encrypts files and demands ransom payment
Rootkit	Hides malware and enables privileged access
PUP	Potentially Unwanted Program; installed with other software
Fileless Malware	Operates in RAM only; avoids antivirus detection
Phishing	Fraudulent emails tricking users into revealing data
Spear Phishing	Targeted phishing using personal information
Whaling	Phishing directed at executives
Vishing	Voice call phishing
Smishing	SMS-based phishing
Pretexting	Attacker uses fake identity or scenario to gain trust
Tailgating	Following someone into a secure area without credentials
Zero Trust	"Never trust, always verify" security model

Authentication & Access Control

Term	Definition
MFA	Multi-Factor Authentication (e.g., password + fingerprint)
Smart Card	Physical card with embedded chip for authentication
Token	Device generating one-time authentication codes
Biometric Authentication	Uses physical traits: fingerprint, face, iris, etc.
Passwordless Authentication	Login method using trusted devices and biometrics (e.g., Windows Hello)
Principle of Least Privilege	Users get only necessary access
Group Policy	Centralized configuration and security settings in Windows

Networking & Wireless Security

Term	Definition
WEP	Obsolete wireless security; easily cracked
WPA/WPA2	Wi-Fi Protected Access; WPA2 uses AES encryption
WPA3	Latest Wi-Fi standard with stronger encryption and key exchange
SSID	Wireless network name
MAC Filtering	Controls access based on device MAC addresses
RADIUS	Remote Authentication Dial-In User Service; used in WPA2-Enterprise
VPN	Encrypts traffic over the internet to connect remotely to private networks
Firewall	Software or hardware that filters network traffic

Software Troubleshooting & Tools

Term	Definition
BSOD	Blue Screen of Death; critical Windows system crash
Safe Mode	Loads Windows with minimal drivers for troubleshooting
System Restore	Reverts system state to earlier point without affecting files
Startup Repair	Repairs common boot issues
Event Viewer	Logs system, security, and application events
DISM	Repairs Windows component store and system image
Task Manager	Shows running processes and system performance

Policies & Procedures

Term	Definition
AUP	Acceptable Use Policy; defines allowed use of company systems
SOP	Standard Operating Procedure; step-by-step for regular tasks
Change Management	Structured process for implementing system changes
Chain of Custody	Tracks evidence handling to maintain integrity
Clean Desk Policy	No sensitive documents left out; protects confidentiality
Incident Response	Process for identifying and resolving security events
MTTR	Mean Time to Repair; avg time to resolve an issue
RTO	Recovery Time Objective; max allowed downtime
RPO	Recovery Point Objective; max allowed data loss (in time)

Backup & Recovery

Term	Definition
Full Backup	Backs up all selected data
Incremental Backup	Backs up only data changed since last backup
Differential Backup	Backs up changes since last **full** backup
Snapshot	Point-in-time image of system or VM
Offsite Backup	Stored in a remote location for disaster recovery

Remote Access & Physical Security

Term	Definition
RDP	Remote Desktop Protocol; remote GUI access to Windows
SSH	Secure Shell; remote CLI access for Linux/Unix systems
VNC	Cross-platform remote desktop sharing
TeamViewer	Third-party tool for remote support and file sharing
VPN	Securely tunnels network traffic over the internet
Mantrap	Dual-door physical access control
Cable Lock	Physically secures laptops to desks or furniture
Privacy Filter	Screen filter that limits visibility from side angles
MDM	Mobile Device Management; controls corporate mobile policies