CompTIA A+

220-1202 Core 2 — Cheat Sheet Study Guide

Operating Systems · Security · Software Troubleshooting · Operational Procedures

Domain 1: Operating Systems — 31% of exam

Windows Editions	
Windows 10/11 Home	Consumer; no domain join; no Group Policy; BitLocker drive enc only
Windows 10/11 Pro	Domain join; Group Policy; BitLocker; Hyper-V; RDP host
Windows 10/11 Pro for WS	Workstation; ReFS; more RAM/CPUs than Pro
Windows 10/11 Enterprise	Full feature set; AppLocker; DirectAccess; VDA
Windows Server	Separate product; AD DS, DNS, DHCP, IIS, file server roles

Windows File Systems	
NTFS	Default for Windows; permissions, encryption (EFS), journaling, large files
FAT32	Cross-platform; max 4 GB file size; no permissions; USB drives
exFAT	Extended FAT; large files (>4 GB); USB/SD; no journaling
CDFS/UDF	Optical disc file system

Windows Control Panel / Settings	
Device Manager	Hardware, drivers, conflicts (yellow !)
Disk Management	Partitions, volumes, format, drive letters
Task Manager	Processes, Performance, Startup, Services tabs
Event Viewer	System, Application, Security logs
Local Users & Groups	User accounts, groups, passwords (Pro+)
Services.msc	Start/stop/configure Windows services

Essential CMD / PowerShell Commands	
dir / ls	List directory contents
cd / chdir	Change directory; cd .. = up one level
md / mkdir	Make new directory
del / rm	Delete file(s)
copy / cp	Copy file to destination
xcopy / robocopy	Advanced copy; xcopy /s = subdirs; robocopy preferred
sfc /scannow	System File Checker — repairs corrupt OS files
DISM /Online /Cleanup-Image /RestoreHealth	Repair Windows image from WU
chkdsk C: /f /r	/f fixes errors; /r locates bad sectors; requires restart

ipconfig /all	Full IP config; /release, /renew, /flushdns
gpupdate /force	Force Group Policy refresh immediately
shutdown /r /t 0	Restart immediately; /s = shutdown; /l = logoff
net user	Manage local user accounts from CMD
tasklist / taskkill	List processes / kill process by PID or name
regedit	Registry editor — HKLM, HKCU, HKCR, HKU, HKCC

Windows Registry Hives	
HKEY_LOCAL_MACHINE (HKLM)	System-wide settings; hardware, OS, services
HKEY_CURRENT_USER (HKCU)	Settings for logged-in user
HKEY_CLASSES_ROOT (HKCR)	File associations, COM objects
HKEY_USERS (HKU)	All user profiles on the system
HKEY_CURRENT_CONFIG (HKCC)	Current hardware profile

Windows Boot Process	
UEFI/BIOS POST	Power-on self-test; hardware init
Boot Manager	winload.efi selects OS
Windows Loader	Loads kernel (ntoskrnl.exe)
Kernel Init	HAL, drivers loaded; smss.exe starts
Session Manager	winlogon.exe — login screen
Safe Mode (F8)	Minimal drivers; for troubleshooting

macOS Essentials	
Finder	File manager equivalent to Windows Explorer
System Preferences/Settings	Control Panel equivalent
Spotlight (Cmd+Space)	System-wide search
Terminal	Bash/Zsh shell; Unix commands
Time Machine	Built-in backup; hourly/daily/weekly snapshots
FileVault	Full-disk encryption; AES-256
Gatekeeper	Blocks unnotarized apps; replaces old antivirus role
Keychain	Password/certificate manager; built into macOS

Linux Essentials	
ls -la	List all files with permissions
chmod	Change file permissions (e.g., chmod 755)
chown	Change file ownership
sudo	Run as superuser/root
apt / yum / dnf	Package managers (Debian / RHEL)
ps aux	List all running processes
grep	Search text in files or output
df -h	Disk free space; du = disk usage
/etc	Config files; /home = user dirs; /var = logs

Domain 2: Security — 25% of exam

Malware Types	
Virus	Attaches to files; requires user action to spread
Worm	Self-replicates across network; no host file needed
Trojan	Disguised as legit software; opens backdoor
Ransomware	Encrypts files; demands payment for key
Spyware	Secretly monitors activity; keyloggers common type
Adware	Injects/displays unwanted ads
Rootkit	Hides itself in OS; hardest to remove
Botnet/Bot	Infected machine controlled remotely (C2 server)
Cryptominer	Uses CPU/GPU to mine cryptocurrency covertly

Social Engineering Attacks	
Phishing	Fake email to steal creds; most common attack vector
Spear phishing	Targeted phishing; personalized to specific person/org
Vishing	Voice/phone phishing
Smishing	SMS/text phishing
Whaling	Phishing targeting executives (CEO, CFO)
Tailgating	Following authorized person through secure door
Piggybacking	Tailgating with victim's consent
Shoulder surfing	Watching screen/keyboard input
Dumpster diving	Recovering sensitive info from trash
Impersonation	Posing as trusted person (IT support, vendor)

Authentication & Access Control	
MFA	Multi-factor: something you know/have/are
Single Sign-On (SSO)	One login for multiple apps; Kerberos, SAML
AAA	Authentication, Authorization, Accounting
Least Privilege	Users get only permissions they need
ACL	Access Control List — rules for resource access
RBAC	Role-Based Access Control — by job function
LDAP	Lightweight Directory Access Protocol; port 389/636
Active Directory	Windows domain auth; domain controller
Password policy	Length, complexity, expiration, history

Encryption & PKI	
Symmetric	Same key encrypt/decrypt (AES, 3DES) — fast
Asymmetric	Public/private key pair (RSA, ECC) — slower
AES	Advanced Encryption Standard; 128/192/256-bit; current gold standard
TLS/SSL	Encrypts data in transit; HTTPS uses TLS 1.2/1.3
Certificate	Digital document proving identity; issued by CA
CA	Certificate Authority; issues and signs certs
Self-signed cert	Not trusted by browsers; internal use only
BitLocker	Windows FDE; requires TPM 2.0 (or USB key)
TPM	Trusted Platform Module; stores encryption keys

Windows Security Tools	
Windows Defender	Built-in AV/AM; real-time protection
Windows Firewall	Host-based; inbound/outbound rules
Windows Security Center	Dashboard for all security components
UAC	User Account Control; prompts for elevation
Local Security Policy	secpol.msc; password/audit/rights policies
Group Policy (GPO)	gpedit.msc; domain or local policy enforcement
MBSA / Baseline	Microsoft Baseline Security Analyzer (legacy)

Physical Security	
Door locks	Keypad, badge reader, biometric
Mantrap / Airlock	Two-door entry; prevent tailgating
Cable locks	Kensington lock; laptop/device physical lock
Safe / locking cabinet	Secure hardware, media, backups
Privacy screen	Prevent shoulder surfing
Equipment labels	Asset tags with serial numbers
CCTV / Cameras	Deter and record physical intrusions

Domain 3: Software Troubleshooting — 22% of exam

Windows OS Troubleshooting	
Slow performance	Check Task Manager; startup items; disk health; RAM
BSOD	Stop code + minidump; analyze with WinDbg; check drivers, RAM
Boot failure	Startup Repair; bootrec /fixmbr /fixboot /rebuildbcd
No logon	Safe Mode; reset password; account lockout policy
Missing DLL	Reinstall app; sfc /scannow; restore from backup
App won't install	Check compatibility, .NET version, admin rights, disk space
High CPU/RAM	Identify in Task Manager; malware scan; driver update
File won't delete	Check permissions; unlock with Process Explorer / Unlocker
Windows Update stuck	Stop wuauserv; clear SoftwareDistribution folder; restart
Profile corruption	Create new profile; copy AppData; rejoin domain if needed

Malware Removal (CompTIA Steps)	
1. Identify & investigate	Unusual behavior; high CPU; unknown processes
2. Quarantine	Disconnect from network immediately
3. Disable System Restore	Prevent malware hiding in restore points
4. Scan & remove	Boot to safe mode; use updated AV/AM tools
5. Schedule scans	Set regular automated scans
6. Enable System Restore	Re-enable; create new clean restore point
7. Educate end user	Phishing, safe browsing, software sources

Mobile & Browser Issues	
App not loading	Force stop, clear cache/data, reinstall
Device too slow	Close background apps; clear storage; factory reset
Wi-Fi won't connect	Forget network, re-enter; toggle airplane mode
Battery draining fast	Screen brightness, background apps, battery saver mode
Browser redirects	Malware/adware; reset browser; remove extensions
Pop-ups in browser	Enable pop-up blocker; check for adware
Slow browser	Clear cache/history; disable extensions; reinstall
Autofill not working	Check browser settings; clear form data; re-enable

Domain 4: Operational Procedures — 22% of exam

Documentation & Ticketing	
Change management	Request → Approval → Implement → Review; avoid unplanned changes
Incident report	Document what happened, impact, resolution, date/time
Knowledge base	Searchable repo of solutions and procedures
Network diagram	Physical + logical topologies; keep updated
SOP	Standard Operating Procedure — step-by-step instructions
AUP	Acceptable Use Policy — defines allowed usage
SLA	Service Level Agreement — uptime/response time guarantees
MOU	Memorandum of Understanding — informal agreement
NDA	Non-Disclosure Agreement — confidentiality

Backup Types	
Full backup	All data every time; slowest to back up, fastest to restore
Incremental	Only changes since LAST backup; fast backup, slow restore
Differential	Changes since LAST FULL; medium backup, medium restore
Synthetic full	Merges full + incrementals into new full without re-reading source
3-2-1 Rule	3 copies, 2 media types, 1 offsite location
RTO	Recovery Time Objective — max acceptable downtime
RPO	Recovery Point Objective — max acceptable data loss window

Safety & Environmental	
ESD precautions	Wrist strap, anti-static mat, bags for components
Battery disposal	Li-Ion: hazardous; use certified recycler (R2/e-Stewards)
Toner disposal	Do not vacuum; use dry method or OEM kit; SDS sheet
Ventilation	Proper airflow; server rooms: hot/cold aisles
Fire suppression	Server rooms: clean agent (FM-200, Halon alt); not water
Lifting technique	Lift with legs, not back; team lift for heavy equip
Electrical safety	No food/drink near equipment; proper grounding

Remote Access & Support Tools	
RDP	Remote Desktop Protocol; port 3389; Windows built-in
VPN	Virtual Private Network; encrypts tunnel to corp network
SSH	Secure Shell; port 22; encrypted CLI remote access
VNC	Virtual Network Computing; cross-platform screen share
TeamViewer / AnyDesk	Commercial remote support; NAT traversal
Screen sharing (macOS)	Built-in via System Preferences; VNC compatible
MSRA	Windows Remote Assistance; invitation-based

Professionalism & Communication	
Set expectations	Inform user of timeline; provide updates
Active listening	Don't interrupt; repeat back to confirm understanding
Avoid jargon	Speak in plain language with non-tech users
Confidentiality	Don't discuss user data or tickets with unauthorized parties
Escalation	Know when to escalate; document before handing off
Cultural sensitivity	Respectful, neutral communication with all users
Follow up	Verify fix works after resolution; close ticket properly

Basic Scripting & Automation	
PowerShell (.ps1)	Windows automation; Get-Process, Set-ExecutionPolicy, Invoke-Command
Batch / CMD (.bat/.cmd)	Legacy Windows scripting; @echo off; %variable%
Bash (.sh)	Linux/macOS shell scripting; chmod +x to execute
Python (.py)	Cross-platform; common for automation; pip for packages
VBScript (.vbs)	Legacy Windows; still used in some corporate environments
JavaScript (.js)	Web automation; Node.js for server-side scripting
Execution policy	PowerShell: Restricted (default) → RemoteSigned/Unrestricted for scripts