CompTIA A+ Core 2 (220-1202)

Quick Exam Refresher

*This is your **condensed, high-impact review guide** for the CompTIA A+ Core 2 exam. It's built for quick recall and confidence-building right before test day — not deep instruction.*

A+ Core 2 Domains at a Glance

Each domain is weighted differently, with Operating Systems and Security making up the majority of the exam:

- 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 (~78%)
- **Test Provider:** Pearson VUE (onsite or online)

Remember — you don't need to be perfect 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.

Focus on strong recall, eliminate wrong answers confidently, and manage your time wisely.

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

Domain 1: Operating Systems (31%)

Key Focus: Windows features, installs, command-line tools, virtualization

• Windows Editions:

- *Home*: No BitLocker or domain join
- *Pro*: BitLocker, RDP host, Group Policy
- *Enterprise*: Volume licensing, AppLocker, DirectAccess

• Install & Boot:

- *Clean install vs in-place upgrade*
- *Image deployment, PXE boot, zero-touch provisioning*
- *MBR (legacy, ≤2TB, 4 partitions) vs GPT (UEFI, modern)*

• File Systems:

- *NTFS* (permissions, encryption), *FAT32* (legacy), *exFAT* (USB), *ReFS* (Workstation)

• Essential Tools – GUI & CLI:

- *GUI*: Device Manager, Disk Management, Event Viewer, Task Manager
- *CLI*: ipconfig, chkdsk, sfc, DISM, robocopy, netstat, shutdown

• macOS/Linux Concepts:

- *macOS*: Time Machine, Disk Utility, Keychain, Terminal
- *Linux*: ls, chmod, apt, df, kill, sudo, directory layout

• Virtualization:

- *Type 1 vs Type 2*, Hyper-V, snapshots, VM resources

• Cloud Integration:

- OneDrive, Office 365, Dropbox, SaaS apps, sync features

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

Domain 2: Security (25%)

Key Focus: Threat types, secure access, device hardening, wireless protection

Malware Types:

- **Virus, Worm, Trojan** – Spread by files/network
- **Ransomware** – Encrypts files for payment
- **Spyware, Keylogger** – Steals data quietly
- **Rootkit** – Hides deep in system
- **Fileless Malware** – Lives in RAM
- **PUPs** – Unwanted programs bundled with legit software

Social Engineering:

Phishing, spear phishing, whaling, vishing, smishing, tailgating, dumpster diving.

Authentication & Permissions:

- MFA, biometrics, smart cards, tokens, Windows Hello
- Group Policy, least privilege model

Account Policies:

- Lockouts, expiration dates, disabled unused accounts, strong password rules

Wi-Fi Security:

- **WEP** = avoid
- **WPA2** = standard (AES)
- **WPA3** = best
- **WPA2-Enterprise** = RADIUS auth

Device Hardening:

Disable unused ports/services, apply updates, enforce encryption, AV/firewall.

Mobile Security:

MDM, screen lock, encryption, app control, remote wipe

Zero Trust & DLP:

No default trust; verify all access. DLP blocks unapproved data transfers (USB, cloud, email)

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

Domain 3: Software Troubleshooting (22%)

Key Focus: Diagnosing OS issues, malware behavior, recovery tools

Common Issues:

Boot failures, BSODs, login errors, slow system, update errors

Recovery Tools:

Safe Mode, System Restore, Reset This PC, Startup Repair, WinRE

Windows Tools:

Task Manager, msconfig, Event Viewer, services.msc, sfc, DISM

Malware Symptoms:

Pop-ups, browser redirects, AV disabled, CPU/network spikes

Data Destruction:

Use wipe tools, degaussers, shredders; confirm secure erase on SSDs

7-Step Malware Removal:

Identify → Quarantine → Disable Restore → Scan/Remove → Schedule scans → Enable Restore → Educate user

6-Step Troubleshooting Model:

Identify → Theory → Test → Fix → Verify → Document

App/Mobile Issues:

Crashes, failed installs, permissions, overheating, unresponsive screen

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

Domain 4: Operational Procedures (22%)

Key Focus: Safety, documentation, change control, professionalism

Safety & Disposal:

Use wrist straps, PPE; recycle e-waste; shred drives; Class C fire extinguishers for electronics

Documentation:

SOPs, asset lists, change logs, network diagrams, KB articles

Policies:

AUP, password policy, incident response, clean desk, chain of custody

Backups:

Full = all
Incremental = since any
Differential = since full
Know: RTO (restore time), RPO (data loss window)

Change Management:

Standard = routine
Normal = requires review
Emergency = urgent fix
Always document and test changes

Remote Access & Security:

RDP, VPN, SSH, VNC; always use encryption and MFA

Scripting Basics:

.bat, .ps1, .sh, .py — automate backups, cleanup, tasks

Professionalism:

Listen actively, avoid jargon, be respectful, escalate when needed, always document

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

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

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

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

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

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

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

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)

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

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

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale