CompTIA A+ Core 2 (220-1202)

100 Questions & Answers

*Welcome to your complete **A+ Core 2 (220-1202)** practice question set.*
*This collection is designed not just to quiz you — but to reinforce your understanding and prepare you for **real-world performance** in IT support and systems administration.*

Learning Objectives and Expectations

You'll get:

- **Realistic questions** reflecting the latest CompTIA exam format and phrasing
- **Structured delivery**: 10 questions followed by 10 answers with concise explanations
- **Exam-relevant breakdowns** to help you understand why each correct answer matters — and what to remember on test day

A+ Core 2 Domains at a Glance

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

- 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)

Questions by Domain

Domain	Title	Questions Assigned	Question Numbers
Domain 1	Operating Systems (31%)	31 Questions	Q1, Q2, Q3, Q4, Q7, Q12, Q16, Q21, Q24, Q27, Q31, Q32, Q33, Q35, Q39, Q40, Q44, Q45, Q52, Q54, Q55, Q60, Q63, Q64, Q66, Q71, Q72, Q74, Q78, Q79, Q81
Domain 2	Security (25%)	25 Questions	Q5, Q6, Q8, Q10, Q13, Q15, Q20, Q22, Q26, Q28, Q34, Q38, Q41, Q47, Q50, Q57, Q58, Q62, Q65, Q69, Q76, Q83, Q86, Q91, Q99
Domain 3	Software Troubleshooting (22%)	22 Questions	Q9, Q11, Q14, Q17, Q18, Q23, Q25, Q30, Q36, Q42, Q43, Q48, Q53, Q59, Q61, Q67, Q68, Q70, Q75, Q77, Q80, Q93
Domain 4	Operational Procedures (22%)	22 Questions	Q19, Q29, Q37, Q46, Q49, Q51, Q56, Q73, Q82, Q84, Q85, Q87, Q88, Q89, Q90, Q92, Q94, Q95, Q96, Q97, Q98, Q100

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.

Missing a few tricky or unfamiliar questions won't hurt you.
Stay calm, trust your preparation, and keep working forward. You've got this.

Questions 1–10

Q1.
Which of the following features is only available in Windows Pro and Enterprise editions?
A) Local user accounts
B) BitLocker
C) Windows Defender
D) File Explorer

Q2.
What is the purpose of the `sfc /scannow` command in Windows?
A) Check the hard drive for bad sectors
B) Scan and restore corrupt system files
C) Display IP configuration details
D) Format the system drive

Q3.
Which file system supports file-level encryption using EFS and allows setting granular permissions?
A) FAT32
B) exFAT
C) NTFS
D) HFS+

Q4.
A technician needs to remotely manage a user's Windows PC using a secure CLI tool. Which option is BEST?
A) Telnet
B) SSH
C) RDP
D) Netstat

Q5.
Which of the following is considered a "fileless" malware threat?
A) Trojan executable
B) Rogue antivirus software
C) PowerShell-based attack running in memory
D) Logic bomb stored in the registry

Q6.
Which type of social engineering attack targets high-level executives with customized messages?
A) Phishing
B) Whaling

C) Spear phishing
D) Vishing

Q7.
Which tool allows a technician to configure which applications start when Windows boots?
A) Disk Management
B) Task Manager
C) System Restore
D) Event Viewer

Q8.
A technician is setting up a mobile device for a company employee. Which of the following ensures company policies are enforced on the device?
A) Remote Desktop Protocol
B) FileVault
C) MDM
D) VPN

Q9.
Which type of backup only captures the data that has changed since the last full backup?
A) Full
B) Incremental
C) Differential
D) Snapshot

Q10.
Which of the following protocols is used for secure file transfer over an encrypted connection?
A) FTP
B) Telnet
C) SFTP
D) TFTP

Answers 1–10

A1.
Answer: B) BitLocker
Explanation: BitLocker is a full-disk encryption feature available only in Windows Pro, Enterprise, and Education editions. It's not available in Home.

A2.
Answer: B) Scan and restore corrupt system files
Explanation: The sfc /scannow command checks for and repairs corrupted Windows system files using known good versions.

A3.
Answer: C) NTFS
Explanation: NTFS supports file-level security permissions and encryption via the Encrypting File System (EFS). FAT32 and exFAT do not.

A4.
Answer: B) SSH
Explanation: SSH (Secure Shell) is a secure remote CLI access protocol. RDP is graphical. Telnet is insecure. Netstat is not a remote tool.

A5.
Answer: C) PowerShell-based attack running in memory
Explanation: Fileless malware operates entirely in memory, often leveraging tools like PowerShell, and doesn't write files to disk.

A6.
Answer: B) Whaling
Explanation: Whaling is a type of phishing that specifically targets high-ranking executives or VIPs in an organization.

A7.
Answer: B) Task Manager
Explanation: Task Manager (Startup tab) in Windows 10/11 shows which apps start at boot and allows you to disable or enable them.

A8.
Answer: C) MDM
Explanation: Mobile Device Management (MDM) enforces organizational security and policy settings on smartphones and tablets.

A9.
Answer: B) Incremental
Explanation: An incremental backup captures only the data that changed since the last full or incremental backup. Fast to run, slower to restore.

A10.
Answer: C) SFTP
Explanation: SFTP (SSH File Transfer Protocol) uses encryption to securely transfer files. FTP and TFTP are unencrypted.

Questions 11–20

Q11.
A technician receives a call from a user reporting pop-ups and strange browser behavior. Which of the following is the MOST likely cause?
A) Driver conflict
B) DNS misconfiguration
C) Malware infection
D) Disk fragmentation

Q12.
Which Control Panel utility is used to uninstall a desktop application in Windows?
A) Devices and Printers
B) Programs and Features
C) System
D) Internet Options

Q13.
Which of the following threats is characterized by code that triggers when specific conditions are met, such as a certain date?
A) Worm
B) Logic bomb
C) Rootkit
D) Trojan

Q14.
What is the purpose of Windows BitLocker?
A) Hide files from users
B) Prevent accidental deletion
C) Secure a drive with full-disk encryption
D) Speed up SSD performance

Q15.
Which of the following is the BEST method to ensure an unauthorized user cannot access confidential data on a lost company phone?
A) Screen timeout
B) Remote wipe
C) Strong password
D) Encryption

Q16.
Which of the following tools would be used to manage Windows services (start, stop, disable)?
A) Event Viewer
B) Task Manager

C) services.msc
D) Device Manager

Q17.
Which of the following is considered biometric authentication?
A) Smart card
B) PIN
C) Facial recognition
D) Password

Q18.
Which setting should a technician verify FIRST if a user reports they cannot access the internet but can access internal network resources?
A) DNS server
B) IP address
C) Subnet mask
D) Default gateway

Q19.
Which backup type includes all changes since the last **full backup**, regardless of other backups?
A) Incremental
B) Snapshot
C) Differential
D) File-level

Q20.
Which of the following best describes the "principle of least privilege"?
A) Always give administrator rights
B) Users should have only the permissions they need
C) Disable all user accounts
D) Allow full control to power users

Answers 11–20

A11.
Answer: C) Malware infection
Explanation: Browser pop-ups and erratic behavior often indicate adware, spyware, or a browser hijacker — all forms of malware.

A12.
Answer: B) Programs and Features
Explanation: This utility allows you to uninstall or modify existing desktop applications on a Windows system.

A13.
Answer: B) Logic bomb
Explanation: Logic bombs are malicious code designed to trigger under specific conditions, such as a date or action.

A14.
Answer: C) Secure a drive with full-disk encryption
Explanation: BitLocker encrypts entire drives to protect data in case of loss or theft.

A15.
Answer: B) Remote wipe
Explanation: A remote wipe erases all data from a lost/stolen phone, protecting confidential information immediately.

A16.
Answer: C) services.msc
Explanation: This tool provides a GUI to start, stop, and manage service behavior on Windows systems.

A17.
Answer: C) Facial recognition
Explanation: Biometric authentication uses unique physical characteristics like fingerprints or facial features.

A18.
Answer: D) Default gateway
Explanation: The default gateway allows access outside the local network (e.g., to the internet). If it's missing or incorrect, external access fails.

A19.
Answer: C) Differential
Explanation: A differential backup copies all data changed since the last full backup, even if multiple backups have occurred.

A20.
Answer: B) Users should have only the permissions they need
Explanation: This principle minimizes security risks by restricting user access to only what's necessary for their role.

Questions 11–20

Q21.
Which of the following tools can be used to encrypt specific files or folders on an NTFS-formatted volume?
A) BitLocker
B) Disk Cleanup
C) EFS
D) Group Policy

Q22.
A technician wants to restrict an application from running on all domain computers. Which feature should they use?
A) Windows Firewall
B) AppLocker
C) Event Viewer
D) Task Scheduler

Q23.
Which of the following is MOST important to verify before deploying a Windows feature update to production systems?
A) Drive fragmentation
B) User permissions
C) Application compatibility
D) BitLocker recovery key

Q24.
Which Windows command would show the status of all current network connections and listening ports?
A) netstat
B) ipconfig
C) tracert
D) ping

Q25.
Which of the following is a data loss prevention technique?
A) Auto-mounting USB drives
B) Allowing unrestricted cloud uploads
C) Blocking transfer of confidential files via email
D) Accepting unsigned device drivers

Q26.
A user cannot access their encrypted files after transferring them to a new computer. Which is the MOST likely reason?
A) BitLocker was not enabled

B) File system was FAT32
C) EFS certificate was not transferred
D) The user lacked administrator privileges

Q27.
Which feature in Windows allows restoring the system to a previous working state without affecting user files?
A) System Restore
B) Backup and Restore
C) Recovery Drive
D) Reset This PC

Q28.
Which of the following would BEST help prevent unauthorized devices from connecting to a secure company Wi-Fi network?
A) Disable SSID broadcast
B) Use WEP encryption
C) Implement MAC filtering and WPA3
D) Enable guest access

Q29.
Which backup method takes the longest to perform but offers the fastest recovery time?
A) Incremental
B) Full
C) Snapshot
D) Differential

Q30.
Which of the following actions is MOST appropriate after removing malware from a corporate system?
A) Disable the antivirus
B) Reinstall Windows
C) Educate the user on security best practices
D) Delete user files for safety

Answers 21–30

A21.
Answer: C) EFS
Explanation: Encrypting File System (EFS) is a feature of NTFS that allows file/folder-level encryption based on user accounts.

A22.
Answer: B) AppLocker
Explanation: AppLocker allows administrators to define rules about which applications can or cannot run on Windows systems.

A23.
Answer: C) Application compatibility
Explanation: Verifying that applications work with the new OS version is essential to avoid business disruptions post-update.

A24.
Answer: A) netstat
Explanation: netstat shows active TCP connections, listening ports, and other network statistics.

A25.
Answer: C) Blocking transfer of confidential files via email
Explanation: This is a classic DLP (Data Loss Prevention) policy — protecting sensitive data from leaving the network.

A26.
Answer: C) EFS certificate was not transferred
Explanation: EFS relies on a user's encryption certificate. If not backed up and imported, encrypted files cannot be read.

A27.
Answer: A) System Restore
Explanation: System Restore rolls back system files and settings to a previous restore point but preserves user files.

A28.
Answer: C) Implement MAC filtering and WPA3

Explanation: MAC filtering blocks unrecognized devices. WPA3 provides the strongest Wi-Fi encryption.

A29.
Answer: B) Full
Explanation: A full backup includes everything and restores quickly since it's self-contained — but takes longer to create.

A30.
Answer: C) Educate the user on security best practices
Explanation: User education helps prevent reinfection and is the final step in the malware removal process.

Questions 31–40

Q31.
Which of the following allows users to access Windows resources using a central authentication system?
A) Local account
B) NTFS permissions
C) Active Directory
D) Device Manager

Q32.
Which Windows utility allows you to manage startup behavior, services, and boot options?
A) msconfig
B) diskmgmt.msc
C) gpedit.msc
D) regedit

Q33.
A technician wants to confirm the effective permissions a user has on a folder. Where should they check?
A) Task Manager
B) Local Security Policy
C) Folder Properties > Security tab
D) Group Policy Editor

Q34.
Which of the following protocols provides secure communication between an email client and server?
A) IMAP
B) POP3
C) SMTP
D) SSL/TLS

Q35.
Which of the following commands is used to modify disk partitions in Windows?
A) chkdsk
B) diskpart
C) format
D) sfc

Q36.
What is the purpose of a standard user account in Windows?
A) Provide full system access
B) Restrict the user from all changes

C) Allow day-to-day tasks without admin rights
D) Grant domain-level privileges

Q37.
A technician is deploying systems using a standard image. What should they ensure is configured to avoid SID duplication?
A) Windows Product Key
B) Licensing server
C) Sysprep
D) BitLocker

Q38.
Which of the following is a sign of a phishing attack?
A) DNS server failure
B) Fake login page link in an email
C) Random MAC address on device
D) Pop-up ads in a browser

Q39.
Which of the following file types is commonly used for Windows installation automation?
A) .dll
B) .ini
C) .bat
D) .xml

Q40.
Which of the following tools is used to create a complete image backup of a Windows system?
A) System Restore
B) Disk Cleanup
C) Backup and Restore (Windows 7)
D) Task Scheduler

Answers 31–40

A31.
Answer: C) Active Directory
Explanation: AD is used in domain environments to manage users, permissions, and devices centrally.

A32.
Answer: A) msconfig
Explanation: msconfig (System Configuration) allows you to configure startup behavior, boot settings, and services.

A33.
Answer: C) Folder Properties > Security tab
Explanation: The Security tab shows NTFS permissions and the Effective Access of specific users or groups.

A34.
Answer: D) SSL/TLS
Explanation: SSL/TLS provides secure encryption for protocols like IMAP, SMTP, and POP3.

A35.
Answer: B) diskpart
Explanation: diskpart is a CLI tool used for advanced partition management.

A36.
Answer: C) Allow day-to-day tasks without admin rights
Explanation: Standard accounts are limited to basic usage, reducing risk from accidental or malicious changes.

A37.
Answer: C) Sysprep
Explanation: Sysprep prepares a Windows image for duplication by removing the SID and customizing the setup experience.

A38.
Answer: B) Fake login page link in an email
Explanation: A phishing attack often uses fake websites to capture login credentials.

A39.
Answer: D) .xml
Explanation: XML files (like unattend.xml) are used in unattended Windows installations for automation.

A40.
Answer: C) Backup and Restore (Windows 7)
Explanation: Despite its name, this tool in Windows 10/11 allows full image-based system backups.

Questions 41–50

Q41.
A user reports that their files were suddenly renamed and the extensions were changed to .locked. What is the MOST likely cause?
A) System restore was run
B) A disk formatting operation
C) Ransomware infection
D) Corrupt user profile

Q42.
Which of the following technologies allows devices to be managed securely over the internet without a VPN?
A) Remote Desktop
B) File History
C) Cloud MDM
D) Group Policy

Q43.
Which option would BEST help prevent phishing emails from reaching users' inboxes?
A) Local antivirus
B) Browser pop-up blocker
C) Email security gateway
D) VPN

Q44.
A technician needs to schedule a script to run every Sunday at 2:00 AM. Which tool should they use?
A) Task Scheduler
B) Event Viewer
C) Services.msc
D) System Configuration

Q45.
Which Windows feature allows you to automatically restore previous versions of a file?
A) BitLocker
B) Disk Cleanup
C) Volume Shadow Copy
D) Credential Manager

Q46.
What is the main difference between a full backup and a differential backup?
A) A full backup requires a full restore point
B) A differential backup resets the archive bit

C) A full backup backs up only system files
D) A differential backup stores changes since the last full backup

Q47.
What should a technician do FIRST when responding to a suspected malware infection on a domain-connected workstation?
A) Run System Restore
B) Disconnect from the network
C) Delete the user's profile
D) Reinstall Windows

Q48.
Which of the following best describes the purpose of Group Policy in a Windows domain environment?
A) Manages disk partitions and storage
B) Controls software updates
C) Enforces centralized configuration and security settings
D) Provides access to shared printers and folders

Q49.
A technician uses robocopy instead of xcopy to move a large amount of data. What is one major benefit?
A) Robocopy compresses files during transfer
B) Robocopy copies hidden partitions
C) Robocopy can resume failed file transfers
D) Robocopy uses less memory

Q50.
Which of the following protocols is MOST often used to encrypt web browser traffic?
A) FTP
B) SSH
C) HTTPS
D) Telnet

Answers 41–50

A41.
Answer: C) Ransomware infection
Explanation: .locked file extensions are commonly used by ransomware, which encrypts files and demands payment.

A42.
Answer: C) Cloud MDM
Explanation: Cloud-based Mobile Device Management solutions allow remote policy enforcement without requiring a VPN.

A43.
Answer: C) Email security gateway
Explanation: An email gateway can detect and block phishing emails before they reach users' inboxes.

A44.
Answer: A) Task Scheduler
Explanation: Task Scheduler automates the execution of scripts and programs at specified times.

A45.
Answer: C) Volume Shadow Copy
Explanation: Volume Shadow Copy creates backup snapshots, allowing users to restore previous file versions.

A46.
Answer: D) A differential backup stores changes since the last full backup
Explanation: Differential backups grow over time and allow faster restoration than incrementals but require the last full backup.

A47.
Answer: B) Disconnect from the network
Explanation: Isolating the infected device prevents the malware from spreading to other systems.

A48.
Answer: C) Enforces centralized configuration and security settings
Explanation: Group Policy allows IT to push policies like password complexity, software restrictions, and drive mappings.

A49.
Answer: C) Robocopy can resume failed file transfers
Explanation: Robocopy is robust, supports resume, and is more suitable for large-scale or unreliable transfers.

A50.
Answer: C) HTTPS
Explanation: HTTPS encrypts HTTP traffic using TLS/SSL to secure communication between a browser and server.

Questions 51–60

Q51.
A technician discovers that a user's system has been compromised and is part of a botnet. What type of malware is MOST likely responsible?
A) Rootkit
B) Ransomware
C) Worm
D) Trojan

Q52.
Which command would you use to release and renew an IP address from a DHCP server in Windows?
A) netstat
B) nslookup
C) ipconfig
D) tracert

Q53.
A user complains their laptop is very slow and the hard drive light is constantly active. What should the technician check FIRST?
A) Disk fragmentation
B) Running background tasks
C) Monitor refresh rate
D) Device Manager

Q54.
Which Windows utility is used to view detailed system logs, application crashes, and startup errors?
A) Task Manager
B) Event Viewer
C) Performance Monitor
D) Resource Monitor

Q55.
What does the principle of “least privilege” help reduce?
A) File system fragmentation
B) Device driver corruption
C) Insider threat and accidental misuse
D) Wireless interference

Q56.
Which of the following is the BEST method to recover a Windows system that won’t boot and shows “BOOTMGR is missing”?
A) Perform a full format

B) Use sfc /scannow
C) Use the Recovery Environment and run bootrec
D) Reset the BIOS

Q57.
A technician wants to ensure that a sensitive file cannot be recovered after deletion. Which method should be used?
A) Move file to Recycle Bin
B) Format the drive
C) Shred the file with a wipe utility
D) Rename and delete the file

Q58.
Which of the following security features helps prevent someone from accessing your computer while you're away?
A) BIOS password
B) Lock screen timeout
C) BitLocker
D) MAC filtering

Q59.
A user can connect to internal shared folders and printers but cannot access the internet. What is the MOST likely cause?
A) Incorrect DNS server
B) Invalid subnet mask
C) No default gateway
D) Firewall misconfiguration

Q60.
Which of the following is an example of multi-factor authentication (MFA)?
A) Username and password
B) Fingerprint and retina scan
C) Smart card and PIN
D) Password and security question

Answers 51–60

A51.
Answer: D) Trojan
Explanation: Trojans often open backdoors, allowing attackers to remotely control systems and add them to botnets.

A52.
Answer: C) ipconfig
Explanation: Use ipconfig /release followed by ipconfig /renew to refresh the DHCP-assigned IP address.

A53.
Answer: B) Running background tasks
Explanation: Excessive background processes (like malware or updates) can slow performance and heavily use the hard drive.

A54.
Answer: B) Event Viewer
Explanation: Event Viewer provides detailed logs for system, security, and application events — essential for troubleshooting.

A55.
Answer: C) Insider threat and accidental misuse
Explanation: Least privilege minimizes risk by limiting user access to only what they need.

A56.
Answer: C) Use the Recovery Environment and run bootrec
Explanation: The bootrec tool can rebuild the boot configuration to fix "BOOTMGR is missing" errors.

A57.
Answer: C) Shred the file with a wipe utility
Explanation: Shredding overwrites the file location, making recovery with forensic tools nearly impossible.

A58.
Answer: B) Lock screen timeout
Explanation: Auto-locking the screen after inactivity prevents unauthorized physical access.

A59.
Answer: C) No default gateway
Explanation: The default gateway is required for accessing networks outside the local subnet (i.e., the internet).

A60.
Answer: C) Smart card and PIN
Explanation: MFA requires two different factor types. Smart card = something you have, PIN = something you know.

Questions 61–70

Q61.
Which of the following backup types resets the archive bit and includes only files that have changed since the last backup of any type?
A) Full
B) Differential
C) Incremental
D) Snapshot

Q62.
What does the command sfc /scannow specifically check and repair?
A) Boot sector
B) Partition table
C) Core Windows system files
D) Registry keys

Q63.
Which of the following best describes phishing?
A) Redirecting a user's browser to a fake website
B) Intercepting wireless traffic
C) Physically stealing passwords
D) Exploiting a buffer overflow

Q64.
Which of the following is the MOST secure method for wiping a magnetic hard drive before disposal?
A) Quick format
B) Delete partition
C) Low-level format or overwrite
D) Rename and delete files

Q65.
Which of the following can BEST prevent shoulder surfing in public areas?
A) Enable screen lock timeout
B) Use a privacy screen filter
C) Install anti-malware
D) Encrypt the hard drive

Q66.
A technician finds a user's PC infected with malware that installed a rootkit. What is the MOST reliable way to remove the threat?
A) Run antivirus in Safe Mode
B) Use msconfig to disable startup items

C) Format and reinstall the OS
D) Boot to Safe Mode and uninstall applications

Q67.
Which account type in Windows is best for performing administrative tasks securely?
A) Local Standard User
B) Guest
C) Domain Admin
D) Local Administrator (used only when needed)

Q68.
What tool would be used to manage and review login attempts and security-related audit logs?
A) Task Manager
B) Event Viewer
C) System Restore
D) Performance Monitor

Q69.
Which of the following policies helps prevent users from leaving sensitive data unattended on their desks?
A) Clean desk policy
B) Acceptable use policy
C) Password policy
D) Data retention policy

Q70.
A technician wants to reduce the risk of social engineering in the organization. What is the BEST solution?
A) Implement biometric locks
B) Conduct regular employee training
C) Configure antivirus scanning
D) Set complex password requirements

Answers 61–70

A61.
Answer: C) Incremental
Explanation: Incremental backups copy only data that has changed since the last full or incremental backup and reset the archive bit.

A62.
Answer: C) Core Windows system files
Explanation: sfc /scannow scans and replaces corrupted or missing Windows system files with cached clean copies.

A63.
Answer: A) Redirecting a user's browser to a fake website
Explanation: Phishing tricks users into revealing sensitive data via deceptive emails or fake websites.

A64.
Answer: C) Low-level format or overwrite
Explanation: Overwriting the disk multiple times ensures that data cannot be recovered using forensic tools.

A65.
Answer: B) Use a privacy screen filter
Explanation: Privacy filters make it difficult for others to view your screen from side angles, protecting sensitive info.

A66.
Answer: C) Format and reinstall the OS
Explanation: Rootkits deeply embed themselves into the system. The only sure removal method is a clean OS installation.

A67.
Answer: D) Local Administrator (used only when needed)
Explanation: It's best to use a standard account daily and elevate privileges only when administrative tasks are required.

A68.
Answer: B) Event Viewer
Explanation: Event Viewer logs system, security, and application events — including login attempts and audit policies.

A69.
Answer: A) Clean desk policy
Explanation: This policy ensures sensitive data (like printed documents or flash drives) is not left unattended.

A70.
Answer: B) Conduct regular employee training
Explanation: Human behavior is a primary attack vector. Educating staff on social engineering risks is the most effective defense.

Questions 71–80

Q71.
Which Windows utility would you use to configure policies that apply only to the local computer, not the domain?
A) Group Policy Management Console
B) Local Security Policy
C) Active Directory Users and Computers
D) Remote Server Administration Tools

Q72.
Which tool is BEST for safely removing temporary files and freeing up disk space?
A) Disk Management
B) System Restore
C) Disk Cleanup
D) msconfig

Q73.
Which of the following is a symptom of spyware on a user's computer?
A) Blue screen during startup
B) Pop-ups and browser redirection
C) Slow startup with no internet access
D) Fan running constantly at full speed

Q74.
Which of the following best explains why a technician would use DISM /RestoreHealth?
A) Reset default permissions
B) Rebuild the boot sector
C) Repair Windows image components
D) Clear DNS cache

Q75.
A technician receives a ticket about a user being unable to install software due to a restriction. What tool is likely enforcing this rule?
A) Task Scheduler
B) Windows Defender
C) AppLocker
D) Event Viewer

Q76.
Which security concept describes separating guest devices from corporate devices on a Wi-Fi network?
A) VLAN segmentation
B) MAC filtering

C) IP whitelisting
D) NAT

Q77.
Which of the following would BEST prevent unauthorized flash drives from being used on company systems?
A) Format all USB drives
B) Disable USB ports via BIOS or Group Policy
C) Encrypt all USB storage
D) Enable auto-run

Q78.
What is the main purpose of using a restore point in Windows?
A) Undo OS-level changes while preserving personal files
B) Remove malware from a system
C) Restore deleted user files
D) Perform a full system image recovery

Q79.
Which Windows feature allows a user to encrypt the entire system drive?
A) EFS
B) Windows Defender
C) BitLocker
D) Windows Hello

Q80.
A technician needs to confirm whether a failed login attempt occurred. Where should they check?
A) Device Manager
B) Task Manager
C) Event Viewer > Security logs
D) Disk Management

Answers 71–80

A71.
Answer: B) Local Security Policy
Explanation: Local Security Policy manages security settings on standalone systems or workgroup PCs not joined to a domain.

A72.
Answer: C) Disk Cleanup
Explanation: Disk Cleanup removes temp files, cached data, and other non-critical files to free space.

A73.
Answer: B) Pop-ups and browser redirection
Explanation: Spyware often causes unwanted pop-ups, browser hijacking, or unauthorized data collection.

A74.
Answer: C) Repair Windows image components
Explanation: DISM repairs corrupted Windows component store files and is often used after `sfc /scannow` fails.

A75.
Answer: C) AppLocker
Explanation: AppLocker prevents unauthorized applications from executing on a Windows system.

A76.
Answer: A) VLAN segmentation
Explanation: VLANs isolate network traffic logically, keeping guests and corporate devices separate for security.

A77.
Answer: B) Disable USB ports via BIOS or Group Policy
Explanation: This prevents use of USB drives entirely — a strong method to stop data theft or malware spread.

A78.
Answer: A) Undo OS-level changes while preserving personal files
Explanation: Restore points roll back system settings, drivers, and registry without touching personal data.

A79.
Answer: C) BitLocker
Explanation: BitLocker provides full-disk encryption for system volumes and requires TPM or a password.

A80.
Answer: C) Event Viewer > Security logs
Explanation: Failed and successful logins are logged in Event Viewer under the Security log category.

Questions 81–90

Q81.
A technician is setting up automatic software updates and scheduled scans. Which of the following would be the BEST tool to manage this?
A) Windows Defender Offline
B) Task Scheduler
C) Event Viewer
D) Resource Monitor

Q82.
A user's computer is infected with malware that disables antivirus programs and makes changes to system settings. What type of malware is this MOST likely?
A) Adware
B) Keylogger
C) Trojan
D) Ransomware

Q83.
Which of the following should a technician use to prevent data loss during an unexpected power outage?
A) Surge protector
B) UPS
C) Power strip
D) Voltage converter

Q84.
Which Windows command can be used to test DNS name resolution issues?
A) netstat
B) ping
C) nslookup
D) chkdsk

Q85.
Which of the following can be used to limit a standard user's access to specific system configuration settings and features in Windows?
A) Windows Firewall
B) Disk Management
C) Local Group Policy Editor
D) Device Manager

Q86.
A technician needs to protect all laptops in an organization from data theft if they are lost or stolen. What solution is BEST?
A) Set BIOS password

B) Enable screen lock
C) Apply full-disk encryption
D) Configure RAID 1

Q87.
What is the MOST appropriate step to take before performing a risky change to a user's system?
A) Schedule a scan
B) Create a restore point
C) Run Disk Cleanup
D) Check for driver updates

Q88.
Which type of Windows account has the most limited access and is often disabled by default?
A) Administrator
B) Local account
C) Guest
D) Standard user

Q89.
A technician is trying to stop a process that is using high CPU resources. Which tool should they use?
A) Event Viewer
B) Task Manager
C) System Information
D) Resource Monitor

Q90.
Which of the following is the BEST way to dispose of an old company hard drive that stored confidential data?
A) Quick format
B) Move to recycle bin
C) Secure erase or physical destruction
D) Partition the drive

Answers 81–90

A81.
Answer: B) Task Scheduler
Explanation: Task Scheduler allows for automation of scans, backups, updates, and script execution at specific times.

A82.
Answer: C) Trojan
Explanation: Trojans disguise themselves as safe programs but can disable AV, open backdoors, or modify system settings.

A83.
Answer: B) UPS
Explanation: An Uninterruptible Power Supply provides backup power during outages, preventing sudden shutdowns and data loss.

A84.
Answer: C) nslookup
Explanation: nslookup is a diagnostic tool for querying DNS to test domain name resolution.

A85.
Answer: C) Local Group Policy Editor
Explanation: The Group Policy Editor (gpedit.msc) allows administrators to define access controls and system restrictions for users.

A86.
Answer: C) Apply full-disk encryption
Explanation: Encrypting the disk (BitLocker, FileVault) ensures data is inaccessible without proper credentials, even if the device is stolen.

A87.
Answer: B) Create a restore point
Explanation: A restore point captures the system state and allows rollback in case the change causes issues.

A88.
Answer: C) Guest

Explanation: The Guest account is highly restricted, cannot make changes, and is usually disabled to prevent misuse.

A89.
Answer: B) Task Manager
Explanation: Task Manager lets users end unresponsive or resource-heavy processes quickly and safely.

A90.
Answer: C) Secure erase or physical destruction
Explanation: Physically destroying or securely erasing a drive ensures confidential data is unrecoverable.

Questions 91–100

Q91.
A technician needs to view the system uptime and CPU usage over time. Which utility should they use?
A) Event Viewer
B) Resource Monitor
C) Task Scheduler
D) Windows Defender

Q92.
Which of the following is a strong example of multi-factor authentication?
A) Username and password
B) Password and PIN
C) Password and fingerprint
D) Security question and password

Q93.
Which of the following actions should a technician take FIRST after confirming a PC is infected with malware?
A) Reboot the system
B) Delete all infected files
C) Isolate the system from the network
D) Reinstall the OS

Q94.
A user reports that their web browser homepage keeps changing and new toolbars appear daily. What is the MOST likely cause?
A) DNS spoofing
B) Rogue antivirus
C) PUP/adware infection
D) User profile corruption

Q95.
Which built-in Windows feature can help recover the operating system without losing user files?
A) Clean install
B) Disk Management
C) Reset this PC – Keep my files
D) Task Manager

Q96.
Which of the following utilities is BEST for managing and monitoring Windows performance in real time?
A) Disk Management

B) Performance Monitor
C) Windows Update
D) Services.msc

Q97.
A technician receives reports that several users are getting pop-ups and redirected searches. What tool is BEST to scan and remove this threat?
A) chkdsk
B) msconfig
C) Anti-malware scanner
D) Disk Cleanup

Q98.
Which of the following commands clears the DNS cache on a Windows system?
A) ipconfig /flushdns
B) nslookup
C) netstat -n
D) ping localhost

Q99.
A technician is implementing DLP on all company laptops. What is the PRIMARY goal of this action?
A) Improve performance
B) Encrypt local file storage
C) Prevent data from leaving the organization
D) Block malware downloads

Q100.
Which type of threat disguises itself as a legitimate file or software to trick users into installing it?
A) Worm
B) Ransomware
C) Rootkit
D) Trojan

Answers 91–100

A91.
Answer: B) Resource Monitor
Explanation: Resource Monitor gives detailed real-time stats on CPU, memory, disk, and network usage, including uptime.

A92.
Answer: C) Password and fingerprint
Explanation: MFA requires two different types of factors (e.g., something you know and something you are).

A93.
Answer: C) Isolate the system from the network
Explanation: Disconnecting the infected device prevents the spread of malware across the network.

A94.
Answer: C) PUP/adware infection
Explanation: Potentially Unwanted Programs (PUPs) often modify browser settings, add toolbars, and cause pop-ups.

A95.
Answer: C) Reset this PC – Keep my files
Explanation: This feature reinstalls Windows while preserving user documents and files.

A96.
Answer: B) Performance Monitor
Explanation: Performance Monitor offers detailed real-time and logged metrics on system performance.

A97.
Answer: C) Anti-malware scanner
Explanation: Anti-malware tools can detect and remove adware, spyware, and browser hijackers effectively.

A98.
Answer: A) ipconfig /flushdns
Explanation: This command clears cached DNS entries from the local resolver cache.

A99.
Answer: C) Prevent data from leaving the organization
Explanation: DLP tools monitor and control data transfers, preventing leaks via email, cloud, or removable devices.

A100.
Answer: D) Trojan
Explanation: A Trojan pretends to be legitimate software but performs malicious activities once executed.