CompTIA

Exam Questions 220-1002

CompTIA A+ Certification Exam: Core 2

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
A customer purchased a 3TB HDD to use with a Windows 7 PC and wants to have letter “J” assigned only to the drive. Which of the following types of partitioning should be performed to give the customer full use of the 3 TB drive?

A. GPT
B. Dynamic
C. Basic
D. Extended

Answer: A

NEW QUESTION 2
A company has hired a new IT firm to manage its network switches and routers.
The firm is geographically separated from the company and will need to able to securely access the devices. Which of the following will provide the ability to access these devices?

A. Telnet
B. SSH
C. RDP
D. VNC

Answer: B

NEW QUESTION 3
A manager with a restricted user account receives the following error message: Windows Update cannot currently check for updates because the service is not running.
The manager contacts the help desk to report the error. A technician remotely connects to the user’s computer and identifies the problem. Which of the following should the technician do NEXT?

A. Reboot the computer
B. Restart the network services
C. Roll back the device drivers
D. Rebuild the Windows profiles

Answer: B

NEW QUESTION 4
A network administrator recently learned users have been accessing websites that are restricted based on content by the firewall. To prevent users from circumventing the firewall rules, which of the following Windows settings should the administrator locks to prevent them from being changed?

A. Default gateway
B. Proxy server
C. WINS server
D. DHCP settings

Answer: B

NEW QUESTION 5
Which of the following installation methods will allow a technician to resolve issues that may arise while the installation is being performed?

A. Unattended installation
B. Remote installation
C. Repair installation
D. Image deployment installation

Answer: D

NEW QUESTION 6
During the firmware upgrade of a web server, a power outage occurred. The outage caused a failure within the upgrade. Which of the following plans must be implemented to revert back to the most recent version of the firmware?

A. Backout plan
B. Contingency plan
C. Alternative plan
D. Backup plan

Answer: D

NEW QUESTION 7
An employee is unable to view in-office network folders while working at home. Which of the following is the MOST likely cause of the problem?

A. Untrusted software
B. Outdated antivirus
C. MDM policies
D. Inactive VPNs

Answer: D

NEW QUESTION 8
An office manager emails a technical support contractor about a new desktop for one of the workers. The office manager provides a specific configuration for the desktop. The technician notes the request will require the purchase of a new system. New system purchases are not in the scope of the support agreement. Which of the following should the technician do NEXT?

A. Create a risk analysis report for review
B. Submit a change order for approval
C. Insist the worker accepts the standard desktop
D. Document the request and place the order

Answer: B

NEW QUESTION 9
Ann, an end user, is working with highly regulated data and often notices the high volume of traffic in her work area. Ann requests help with limiting the exposure of data as people walk by.
Which of the following security measures should be used?

A. Biometric device
B. Common access card
C. Cable lock
D. Privacy screen
E. Mantrap

Answer: D

NEW QUESTION 10
Joe. a technician, receives notification that a share for production data files on the network Is encrypted. Joe suspects a crypto virus Is active. He checks the rights of the network share to see which departments have access. He then searches the user directories of those departmental users who are looking for encrypted files. He narrows his search to a single user's computer. Once the suspected source of the virus is discovered and removed from the network, which of the following should Joe do NEXT?

A. Educate the end user on safe browsing and email habits.
B. Scan and remove the malware from the infected system.
C. Create a system restore point and reboot the system.
D. Schedule antivirus scans and perform Windows updates.

Answer: D

NEW QUESTION 10
Which of the following user types should be used in a Windows environment to grant Internet access without allowing the permanent storage of files on the system?

A. Local Administrator
B. Standard User
C. Power User
D. Guest User

Answer: D

NEW QUESTION 15
A user is working on a shared computer and attempts to open the email application, which freezes when opened. A technician logs into the computer, and the email application works without issue. The technician has the user log back in, but the application still freezes when opened. Which of the following is the NEXT step the technician should take to resolve the issue?

A. Check for and apply software updates
B. Perform repair installation on the application
C. Add the user to the local administrators group
D. Rebuild the user’s mail profile

Answer: D

NEW QUESTION 18
A technician is installing Windows 7 64-bit OS on a VM but keeps getting errors. The specifications for the malware are:
Two 1GHz CPUs 2GB of memory 15GB hard drive
800x600 screen resolution
Which of the following should the technician do to resolve the problem?

A. Increase the number of CPUs
B. Increase the amount of memory
C. Increase the amount of hard drive space
D. Increase the screen resolution

Answer: C

NEW QUESTION 21
Which of the following BEST describes the Guest account on a Windows system?

A. This account is designed to have the ability to set permissions for other users on the syste
B. Users of this account have the capability to perform any operation or task on the system.
C. This account is designed to provide basic permission for completing common daily task
D. Users of this account are restricted from performing things like installing new software.
E. This account is designed for users who require specific administrator rights or permission
F. Users of this account are restricted from installing software but can change time zones.
G. This account is designed for users who require temporary access to a computer and do not need to store user-specific setting
H. Users of this account have very limited permissions.

Answer: D

NEW QUESTION 25
A desktop technician is attempting to upgrade several machines to Windows 10. After releasing there is only one disc for the installation, the technician decides to upgrade over the network. Which of the following boot methods initiates such an upgrade?

A. SSD
B. Optical drive
C. Flash drive
D. PXE

Answer: D

NEW QUESTION 29
Corporate management is concerned about the security of the company's mobile phones, in the event they are lost or stolen. Management instructs the IT staff to ensure the data on the devices is not accessible by unauthorized users. Which of the following would provide the BEST level of protection in this scenario? (Choose two.)

A. Use full device encryption
B. Enable a pattern lock
C. Implement remote wipe features
D. Use device lockout policies
E. Require complex administrator passwords
F. Disable unknown application installations

Answer: AC

NEW QUESTION 33
A wireless access point is going to be configured in a small office located in a crowded building. Which of the following should the installation technician perform to increase the security of the wireless network? (Select two.)

A. Reduce the transmit power
B. Reduce the channel availably
C. Disable the DHCP server
D. Enable QoS management
E. Disable the SSID broadcast
F. Implement WPA encryption

Answer: AE

NEW QUESTION 36
A user reports malware activity on an isolated workstation used for testing It is running an end-of-life OS. and a USB drive is the only method used to transfer files After removing the malware and replacing the USB drive with a brand new one. the technician gives the approval to use the equipment. The next day the user reports the same malware activity is present after powering on the system Which of the following did the technician forget to do to prevent reinfection?

A. Connect to the network and update the OS with the latest security patches
B. Scan and dean the USB device used to transfer data from the equipment
C. Disable System Restore and remove all restore points from the system
D. Update the local antivirus and set it to scan automatically every evening

Answer: D

NEW QUESTION 40
A technician is troubleshooting a printer issue on a Windows computer and wants to disable the printer to test a theory. Which of the following should the technician use to accomplish this?

A. Devices and Printers
B. Sync Center
C. Device Manger
D. Power Options

Answer: C

NEW QUESTION 45
Which of the following threats uses personalized information in an attempt at obtaining information?

A. Whaling
B. Impersonation
C. Spoofing
D. Spear phishing

Answer: D

NEW QUESTION 49
A technician needs to deploy a remote access technology to be able to access desktop computers. When a technician logs in to a user's computer, the user and the technician must be able to see the desktop simultaneously and use the mouse and keyboard. Which of the following would be BEST suited for this task?

A. VNC
B. Telnet
C. SSH
D. RDP

Answer: C

NEW QUESTION 52
A security administrator does some network testing and identifies significant issues with security on desktop computers. As part of remediation, the network administrator is developing documentation based on best practices for applying updates to end users' computers. The network administrator must create the process documentation needed to submit back to the security administrator for approval. Which of the following process documents would the network administrator MOST likely create? (Choose two.)

A. Risk analysis
B. End-user acceptance
C. Backout plan
D. Plan for change
E. Business processes
F. Request for proposal

Answer: CD

NEW QUESTION 53
A SOHO user reports desktop applications are performing slowly, and no emails have been received all morning. A technician remotes in and determines Internet pages' load slowly or not at all, CPU performance is normal, and the local router can successfully ping.
The remote connection drops periodically. Which of the following steps should the technician take NEXT to resolve the problem?

A. Reboot into safe mode, uninstall the latest OS update, and run a repair on the OS
B. Update the antivirus software, run an antivirus scan, verify the browser settings, and check all email settings
C. Reboot to BIOS setup, verify the TPM is enabled, and start a System Restore from safe mode
D. Send a test email, open a command prompt to check the file system, and empty the browser cache

Answer: B

NEW QUESTION 58
A computer becomes infected with malware, which manages to steal all credentials stored on the PC. The malware then uses elevated credentials to infect all other PCs at the site. Management asks the IT staff to take action to prevent this from reoccurring. Which of the following would BEST accomplish this goal?

A. Use an antivirus product capable of performing heuristic analysis
B. Use a host-based intrusion detection system on each computer
C. Disallow the password caching of accounts in the administrators group
D. Install a UTM in between PC endpoints to monitor for suspicious traffic
E. Log all failed login attempts to the PCs and report them to a central server

Answer: D

NEW QUESTION 62
A user's smartphone is experiencing limited bandwidth when at home. The user reports to a technician that the device functions properly when at work or in the car. Which of the following troubleshooting steps should the technician take NEXT?

A. Reset the device's network settings
B. Check the data usage statistics on the device
C. Verify the SSID with which the device is associated
D. Run any pending application or OS updates

Answer: C

NEW QUESTION 64
A network administrator needs to be able to securely connect to a local router from within the office. Which of the following protocols should the administrator ensure is enabled on the router?

A. RDP
B. SSH
C. TFTP
D. HTTP

Answer: B

NEW QUESTION 68
A user's phone contains customer's PII. The user cannot have the phone automatically wiped because the data is very valuable. Which of the following is the BEST method of securing the phone?

A. Fingerprint lock
B. Passcode lock
C. Swipe lock
D. PIN lock

Answer: A

NEW QUESTION 73
Every time a user manually runs an antivirus scan, the workstation becomes unresponsive, and the user has to reboot A technician is dispatched and sees an antivirus pop-up in the system tray, indicating the computer is severely damaged, and a "click here" button to resolve it. There is a timer in the pop-up. counting down the time until the computer is no longer usable. Which of the following should the technician do NEXT?

A. Research the pop-up to see if it is a legitimate malware solution.
B. Click on the pop-up window to resolve the issue before the time runs out.
C. Send an email to all staff members warning them of malware on their system.
D. Disconnect the Ethernet cable from the workstation and disable WiFi.

Answer: D

NEW QUESTION 75
A technician is installing the latest OS on a user's system. The user wants all of the settings and file to remain intact during the installation.
Which of the following upgrade methods should the technician use?

A. network installation
B. clean install
C. in-place upgrade
D. image deployment

Answer: C

NEW QUESTION 79
Which of the following devices provides protection against brownouts?

A. battery backup
B. surge suppressor
C. rack grounding
D. line conditioner

Answer: A

NEW QUESTION 83
A user calls a technician to report issues when logging in to a vendor's website. The technician is able to log in successfully before going to the office. However, the technician is unable to log in when in the user's office. The user also informs the technician of strange pop-up notifications. Which of the following are the MOST likely causes of these issues? (Select TWO).

A. System files have been deleted
B. Proxy settings are configured improperly
C. The OS has been updated recently.
D. There are disabled services on the vendor website.
E. Program file permissions have changed recently.
F. There is a rogue anti-malware program.

Answer: DF

NEW QUESTION 84
Which of the following Windows Enterprise OS version Offers BitLocker as a feature that can be enabled?

A. Windows 7
B. Windows 8
C. Windows 8.1
D. Windows 10

Answer: A

NEW QUESTION 87
A user reports slow performance on a computer. A technician checks the computer and finds the RAM utilization Is very high. The technician restarts the computer, and the RAM use is still high. The technician discovers a program running in the background Is using most of the RAM. The user only uses this program once at the end of the year to produce a report. Which of the following steps should the technician take to improve the computer's performance?

A. Uninstall and reinstall the program.
B. Perform a repair installation of the program
C. Install the latest updates for the program.
D. Disable the program on startup.

Answer: A

NEW QUESTION 90
Joe, a user, calls the help desk from a coffee shop while on a business trip to report the WiFi hotspot on his phone is extremely slow. The technician runs a speed test from a laptop connected to the hotspot and gets 200Kbps. Ann, Joe's coworker with whom he is travelling, also has a hotspot on her phone, and the speed test result on that hotspot is 15Mbps. The technician checks the hotspot settings on Joe's phone and sees the following:

Network name:	**Joe's Hotspot**
Security:	WPA2/PSK
Password:	hotspot
Band:	2.4GHz
Client DHCP start address:	192.168.23.1

Which of the following is the MOST likely cause of the problem?

A. Joe should be using WEP security on his hotspot for faster throughput
B. Someone else is using Joe's hotspot due to weak password
C. Joe's hotspot gave him an invalid IP address
D. Joe is likely in a poor signal area and should try another area

Answer: B

NEW QUESTION 93
Which of the following should be enacted to reduce a company's liability and exposure to a potential lawsuit?

A. Acceptable use policy
B. Incident documentation policy
C. Password compliance policy
D. Change control policy

Answer: C

NEW QUESTION 94
A user calls a technician regarding an iOS mobile device that is having problems with standby time after a new update was applied. The technician verifies no new applications were installed since the update, but the device still has poor standby time even after the update is removed. Which of the following is the MOST likely cause of the issue?

A. Zero-day malware
B. Safari code injection
C. OS corruption
D. Overheating
E. Time sync failure

Answer: D

NEW QUESTION 97
A network administrator has noticed unusual activity with a user's login credentials on the network. The user is attempting multiple simultaneous login across the network, some of which are attempting to access workstations and servers to which the user does not have access.
Which of the following should the network administrator do NEXT?

A. Delete the user's AD account.
B. Decrease the user's AD privileges.
C. Disable the user's AD account.
D. Reset the password on the user's AD account.

Answer: C

NEW QUESTION 100
An end user's PC is taking a long time to boot. Which of the following operations would be the BEST to resolve this issue with minimal expense? (Select two.)

A. Remove applications from startup
B. Defragment the hard drive
C. Install additional RAM
D. Install a faster hard drive
E. End the processes in Task Manager
F. Run the Disk Cleanup utility

Answer: AB

NEW QUESTION 101
A new company policy states that all end-user access to network resources will be controlled based on the users' roles and responsibilities within the organization. Which of the following security concepts has the company just enabled?

A. Certificates
B. Least privilege
C. Directory permissions
D. Blacklists

Answer: B

NEW QUESTION 106
A technician recently installed a new secondary hard drive in a Windows 10 desktop. After the installation, the computer displayed the following error message: No Operating System Found. However, after unplugging the new hard drive, the error message no longer appeared. The technician then reconnected the new drive to continue troubleshooting. Which of the following steps should the technician take NEXT?

A. Reboot into safe mode
B. Check the boot order
C. Format the drive
D. Perform Windows Recovery
E. Run the chkdsk command

Answer: B

NEW QUESTION 108
A technician is investigating the cause of a Windows 7 PC running very slow. While reviewing Task Manager, the technician finds one process is using more than 90% of the CPU. Outbound network traffic on port 25 Is very high, while Inbound network traffic Is low. Which of the following tasks should be done FIRST?

A. Disconnect the network cable.
B. Update the antivirus software.
C. Run an antivirus scan.
D. Shut down the PC

Answer: A

NEW QUESTION 111
Which of the following is the MOST secure wireless security protocol?

A. AES
B. WPA
C. WPA2
D. WEP

Answer: A

NEW QUESTION 115
Following an incident, an administrator is gathering forensic evidence from a server for a human resources investigation. Which of the following best practices is MOST important to document throughout the process to maintain integrity of the findings?

A. Acceptable use policy violations
B. Server configuration
C. Chain of custody
D. Data loss incidents

Answer: C

NEW QUESTION 120
A user's mobile device is losing its battery change very quickly. The user report charge at 9:00 a.m. but has 22% battery by 1:00 p.m. The user has installed several applications, and the phone is relatively new, high-end phon. The user claims most of the usage involves checking emails for a few minutes three or four times per hours. Windows of the following should a technician perform FIRST to diagnose the issue properly?

A. Check the application and their resources usage.
B. Order a replacement battery and see if the phone maintain its charge.
C. Configure the email software to work on a fetch schedule instead of the push setting
D. Wipe the phone screen brightness to 30%.
E. Uninstall all the applications on the phone and see if the battery issues remain.

Answer: A

NEW QUESTION 123
The IT department has installed new software in the folder C:\Program Files\Business Application\. Ann, a user, runs the business application and tries to save her work. When doing so, Ann receives the following error:
Cannot save file C: \Program Files\Business Application\file1.wrk – Access is denied.
Which of the following would be the MOST secure solution to this error?

A. Add Ann to the local Power Users group
B. Set the software to save to the %APPDATA% folder

C. Add Ann to the local administrator group
D. Give Ann write access to C:\Program Files\
E. Give Ann permission to elevate her permissions through a UAC prompt

Answer: E

NEW QUESTION 126
A user's computer reports it has many virus infections and directs the user to call a phone number for assistance. A technician removes the hard drive and virus scans the drive with another computer. The scan does not identify any viruses Which of the following is MOST likely the problem?

A. Rootkit
B. Zero-day malware
C. Rogue antivirus
D. Old virus definitions

Answer: D

NEW QUESTION 130
A network administrator has noticed unusual activity with a user's login credentials on the network. The user is attempting multiple simultaneous logins across the network, some of which are attempting to access workstations and servers to which the user does not have access Which of the following should the network administrator do NEXT?

A. Delete the user's AD account
B. Decrease the user's AD privileges
C. Disable the user's AD account
D. Reset the password on the user's AD account

Answer: A

NEW QUESTION 132
A MAC user’s operating system became corrupted, and files were deleted after malware was downloaded. The user needs to access the data that was previously stored on the MAC. Which of the following built-in utilities should be used?

A. Time Machine
B. Snapshot
C. System Restore
D. Boot Camp

Answer: A

NEW QUESTION 137
A user reports that a cell phone application is loading slowly and not functioning properly Which of the following should a technician do FIRST to remedy this issue?

A. Remove and reinstall the application.
B. Hard reset the cell phone.
C. Reconnect the wireless network connection
D. Close all running applications

Answer: D

NEW QUESTION 142
.....

Relate Links

100% Pass Your 220-1002 Exam with Exambible Prep Materials

https://www.exambible.com/220-1002-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/