Get 220-1102 Actual Free Exam Q&As to Prepare for Your CompTIA Certification [Q111-Q131
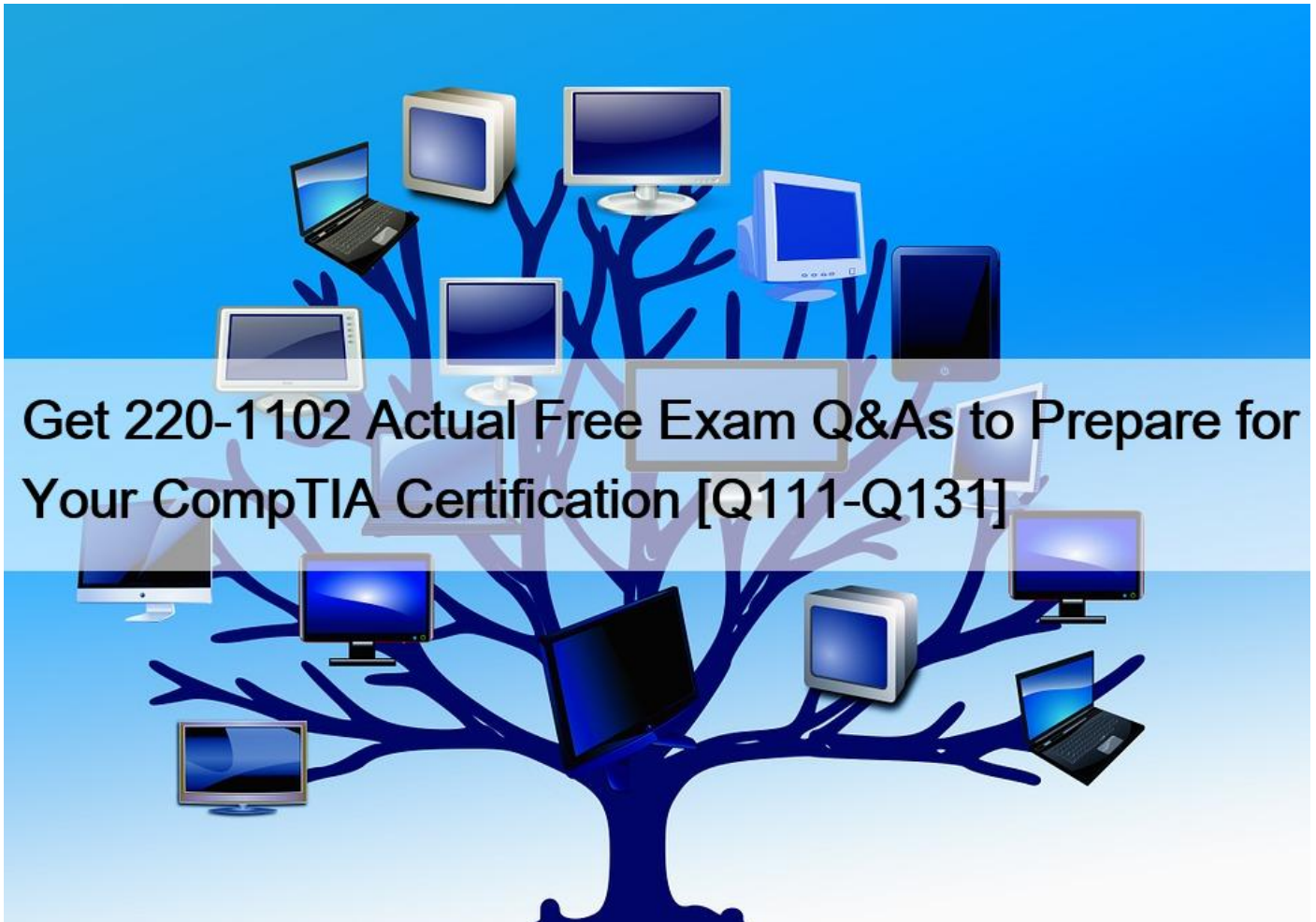

Get 220-1102 Actual Free Exam Q&As to Prepare for Your CompTIA Certification

CompTIA Actual Free Exam Questions And Answers

CompTIA 220-1102 Exam Syllabus Topics:

TopicDetailsTopic 1- Given a scenario, use best practice procedures for malware removal- Given a scenario, apply application installation and configuration conceptsTopic 2- Summarize various security measures and their purposes- Explain common methods for securing mobile and embedded devicesTopic 3- Given a scenario, install and configure browsers and relevant security settings- Identify common features and tools of the Linux client- desktop OSTopic 4- Given a scenario, configure Microsoft Windows networking features on a client- desktop- Explain common social-engineering attacks, threats, and vulnerabilitiesTopic 5- Summarize environmental impacts and local environmental controls- Identify basic features of Microsoft Windows editionsTopic 6- Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods- Given a scenario, use the appropriate Microsoft Windows 10Topic 7- Given a scenario, troubleshoot common personal computer (PC) security issues- Given a scenario, troubleshoot common mobile OS and application issues

QUESTION 111

A technician suspects the boot disk of a user’s computer contains bad sectors. Which of the following should the technician verify in the command prompt to address the issue without making any changes?
* Run sfc / scannow on the drive as the administrator.
* Run clearnmgr on the drive as the administrator
* Run chkdsk on the drive as the administrator.
* Run dfrgui on the drive as the administrator.
The technician should verify bad sectors on the user’s computer by running chkdsk on the drive as the administrator. Chkdsk (check disk) is a command-line utility that detects and repairs disk errors, including bad sectors. It runs a scan of the disk and displays any errors that are found

QUESTION 112

A Windows user reported that a pop-up indicated a security issue. During inspection, an antivirus system identified malware from a recent download, but it was unable to remove the malware. Which of the following actions would be BEST to remove the malware while also preserving the user’s files?
* Run the virus scanner in an administrative mode.
* Reinstall the operating system.
* Reboot the system in safe mode and rescan.
* Manually delete the infected files.
Explanation

Rebooting the system in safe mode will limit the number of programs and processes running, allowing the antivirus system to more effectively identify and remove the malware. Rescanning the system will allow the antivirus system to identify and remove the malware while preserving the user’s files.

QUESTION 113

A technician is reimaging a desktop PC. The technician connects the PC to the network and powers it on. The technician attempts to boot the computer via the NIC to image the computer, but this method does not work. Which of the following is the MOST likely reason the computer is unable to boot into the imaging system via the network?
* The computer’s CMOS battery failed.
* The computer’s NIC is faulty.
* The PXE boot option has not been enabled
* The Ethernet cable the technician is using to connect the desktop to the network is faulty.
The most likely reason the computer is unable to boot into the imaging system via the network is that the PXE boot option has not been enabled. PXE (Preboot Execution Environment) is an environment that allows computers to boot up over the network, instead of from a local disk. In order for this to work, the PXE boot option must be enabled in the computer’s BIOS settings. As stated in the CompTIA A+ Core 2 exam objectives, technicians should know how to enable PXE in BIOS to enable network booting on a computer.

QUESTION 114

A wireless network is set up, but it is experiencing some interference from other nearby SSIDs. Which of the following can BEST resolve the interference?
* Changing channels
* Modifying the wireless security
* Disabling the SSIO broadcast

* Changing the access point name

QUESTION 115

A user is unable to access a website, which is widely used across the organization, and receives the following error message:

The security certificate presented by this website has expired or is not yet valid.

The technician confirms the website works when accessing it from another computer but not from the user’s computer. Which of the following should the technician perform NEXT to troubleshoot the issue?
* Reboot the computer.
* Reinstall the OS.
* Configure a static 12
* Check the computer’s date and time.
The error message indicates that the security certificate presented by the website has either expired or is not yet valid. This can happen if the computer’s clock has the wrong date or time, as SSL/TLS certificates have a specific validity period. If the clock is off by too much, it may cause the certificate to fail to validate. Therefore, the technician should check the computer’s date and time and ensure that they are correct.

QUESTION 116

Following the latest Windows update PDF files are opening in Microsoft Edge instead of Adobe Reader. Which of the following utilities should be used to ensure all PDF files open in Adobe Reader?
* Network and Sharing Center
* Programs and Features
* Default Apps
* Add or Remove Programs

QUESTION 117

Which of the following must be maintained throughout the forensic evidence life cycle when dealing with a piece of evidence?
* Acceptable use
* Chain of custody
* Security policy
* Information management

QUESTION 118

A user has requested help setting up the fingerprint reader on a Windows 10 laptop. The laptop is equipped with a fingerprint reader and is joined to a domain Group Policy enables Windows Hello on all computers in the environment. Which of the following options describes how to set up Windows Hello Fingerprint foe the user?
* Navigate to the Control Panel utility, select the Security and Maintenance submenu, select Change Security and Maintenance settings, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete
* Navigate to the Windows 10 Settings menu, select the Accounts submenu, select Sign in options, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete.
* Navigate to the Windows 10 Settings menu, select the Update & Security submenu select Windows Security, select Windows Hello Fingerprint and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete
* Navigate to the Control Panel utility, select the Administrative Tools submenu, select the user account in the list, select Windows

Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete.

QUESTION 119

A technician needs to transfer a large number of files over an unreliable connection. The technician should be able to resume the process if the connection is interrupted. Which of the following tools can be used?

* afc
* ehkdsk
* git clone
* zobocopy

QUESTION 120

A user receives a notification indicating the data plan on the user’s corporate phone has reached its limit. The user has also noted the performance of the phone is abnormally slow. A technician discovers a third-party GPS application was installed on the phone. Which of the following is the MOST likely cause?

* The GPS application is installing software updates.
* The GPS application contains malware.
* The GPS application is updating its geospatial map data.
* The GPS application is conflicting with the built-in GPS.

The GPS application contains malware. The third-party GPS application is likely the cause of the slow performance of the phone. The application may contain malware that is using up system resources and slowing down the phone. The user should uninstall the application and run a malware scan on the phone1

QUESTION 121

Which of the following provide the BEST way to secure physical access to a data cento server room? (Select TWO).

* Biometric lock
* Badge reader
* USB token
* Video surveillance
* Locking rack
* Access control vestibule

A biometric lock requires an authorized user to provide a unique biometric identifier, such as a fingerprint, in order to gain access to the server room. A badge reader requires an authorized user to swipe an access card in order to gain access. Both of these methods ensure that only authorized personnel are able to access the server room. Additionally, video surveillance and access control vestibules can be used to further secure the server room. Finally, a locking rack can be used to physically secure the servers, so that they cannot be accessed without the appropriate key.

QUESTION 122

A user is configuring a new SOHO Wi-Fi router for the first time. Which of the following settings should the user change FIRST?

* Encryption
* Wi-Fi channel
* Default passwords
* Service set identifier

QUESTION 123

A technician is setting up a new laptop for an employee who travels, Which of the following is the BEST security practice for this scenario?

* PIN-based login
* Quarterly password changes
* Hard drive encryption
* A physical laptop lock

Explanation

Encrypting the laptop’s hard drive will ensure that any sensitive data stored on the laptop is secure, even if the laptop is lost or stolen. Encryption ensures that the data cannot be accessed by anyone without the correct encryption key. This is an important security measure for any laptop used by an employee who travels, as it helps to protect the data stored on the laptop from unauthorized access.

QUESTION 124

Welcome to your first day as a Fictional Company. LLC helpdesk employee. Please work the tickets in your helpdesk ticket queue.

Click on individual tickers to see the ticket details. View attachments to determine the problem.

Select the appropriate issue from the ‘issue’ drop-down menu. Then, select the MOST efficient resolution from the ‘Resolution’ drop-down menu. Finally, select the proper command or verification to remediate or confirm your fix of the issue from the Verify Resolve drop-down menu.

	Date	Priority
ing to boot. Screen i... g	7/13/2022	High
o access Z: on my co... 0	7/13/2022	Low

Details

#8675309	Open
Priority	High
Category	Technical / Bug Reports
Assigned To	helpdesk@fictional.com
Assigned Date	7/13/2022

Subject	PC is failing to boot. Screen is displaying error message, see attachment.
Attachments	bootmgr not found png

Issue

Corrupt OS
Recent Windows Updates
Graphics Drive Updates
BSOD
Printing Issues
Limited Network Connectivity
Services Failed to Start
User Profile is Corrupted
Application Crash
User cannot access shared resource
URL contains typo

Resolution

Reinstall Operating System
Rollback Updates
Rollback Drivers
Repair Application
Restart Print Spooler
Disable Network Adapter
Update Network Drivers
Refresh DHCP
Rebuild Windows Profile
Apply Updates
Repair Installation
Restore from Recovery Partition
Remap network drive
Verify integrity of disk drive
Initiate screen share session with user
Windows recovery environment
Inform user of AUP violation

Verify/Resolve

chkdsk
dism
diskpart
sfc
dd
ctrl + alt + del
net use
net user
netstat
netsh
bootrec

	Date	Priority
...ing to boot. Screen i... g	7/13/2022	High
...o access Z: on my co... 0	7/13/2022	Low

Details

#8675309	Open
Priority	High
Category	Technical / Bug Reports
Assigned To	helpdesk@fictional.com
Assigned Date	7/13/2022

Subject	PC is failing to boot. Screen is displaying error message, see attachment.
Attachments	bootmgr not found png

Issue

- Corrupt OS
- Recent Windows Updates
- Graphics Drive Updates
- BSOD
- Printing Issues
- Limited Network Connectivity
- Services Failed to Start
- User Profile is Corrupted
- Application Crash
- User cannot access shared resource
- URL contains typo

Resolution

- Reinstall Operating System
- Rollback Updates
- Rollback Drivers
- Repair Application
- Restart Print Spooler
- Disable Network Adapter
- Update Network Drivers
- Refresh DHCP
- Rebuild Windows Profile
- Apply Updates
- Repair Installation
- Restore from Recovery Partition
- Remap network drive
- Verify integrity of disk drive
- Initiate screen share session with user
- Windows recovery environment
- Inform user of AUP violation

Verify/Resolve

- chkdsk
- dism
- diskpart
- sfc
- dd
- ctrl + alt + del
- net use
- net user
- netstat
- netsh
- bootrec

QUESTION 125

A customer reported that a home PC with Windows 10 installed in the default configuration is having issues loading applications after a reboot occurred in the middle of the night. Which of the following is the FIRST step in troubleshooting?

* Install alternate open-source software in place of the applications with issues
* Run both CPU and memory tests to ensure that all hardware functionality is normal
* Check for any installed patches and roll them back one at a time until the issue is resolved
* Reformat the hard drive, and then reinstall the newest Windows 10 release and all applications.

QUESTION 126

A user is configuring a new SOHO Wi-Fi router for the first time. Which of the following settings should the user change FIRST?

* Encryption
* Wi-Fi channel
* Default passwords
* Service set identifier

the user should change the default passwords first when configuring a new SOHO Wi-Fi router1

QUESTION 127

An incident handler needs to preserve evidence for possible litigation. Which of the following will the incident handler MOST likely do to preserve the evidence?

* Encrypt the files
* Clone any impacted hard drives
* Contact the cyber insurance company
* Inform law enforcement

The incident handler should clone any impacted hard drives to preserve evidence for possible litigation1

QUESTION 128

A technician is setting up a backup method on a workstation that only requires two sets of tapes to restore.

Which of the following would BEST accomplish this task?

* Differential backup
* Off-site backup
* Incremental backup
* Full backup

Explanation

A full backup involves creating a copy of all data on the workstation, including system files and user-created data, and storing it on a set of tapes. This ensures that all data is backed up, and ensures that the data can be restored in the event of a system failure or data loss.

QUESTION 129

A desktop specialist needs to prepare a laptop running Windows 10 for a newly hired employee. Which of the following methods should the technician use to refresh the laptop?

* Internet-based upgrade

* Repair installation
* Clean install
* USB repair
* In place upgrade

QUESTION 130

A user’s mobile phone has become sluggish A systems administrator discovered several malicious applications on the device and reset the phone. The administrator installed MDM software. Which of the following should the administrator do to help secure the device against this threat in the future? (Select TWO).
* Prevent a device root
* Disable biometric authentication
* Require a PIN on the unlock screen
* Enable developer mode
* Block a third-party application installation
* Prevent GPS spoofing

QUESTION 131

A technician is installing new network equipment in a SOHO and wants to ensure the equipment is secured against external threats on the Internet. Which of the following actions should the technician do FIRST?
* Lock all devices in a closet.
* Ensure all devices are from the same manufacturer.
* Change the default administrative password.
* Install the latest operating system and patches
The technician should change the default administrative password FIRST to ensure the network equipment is secured against external threats on the Internet. Changing the default administrative password is a basic security measure that can help prevent unauthorized access to the network equipment. Locking all devices in a closet is a physical security measure that can help prevent theft or damage to the devices, but it does not address external threats on the Internet. Ensuring all devices are from the same manufacturer is not a security measure and does not address external threats on the Internet. Installing the latest operating system and patches is important for maintaining the security of the network equipment, but it is not the first action the technician should take1

220-1102 Questions Truly Valid For Your CompTIA Exam: https://www.vceprep.com/220-1102-latest-vce-prep.html]