

220-1102 Dumps

CompTIA A+ Certification Exam: Core 2

<https://www.certleader.com/220-1102-dumps.html>



NEW QUESTION 1

An employee has repeatedly contacted a technician about malware infecting a work computer. The technician has removed the malware several times, but the user's PC keeps getting infected. Which of the following should the technician do to reduce the risk of future infections?

- A. Configure the firewall.
- B. Restore the system from backups.
- C. Educate the end user
- D. Update the antivirus program.

Answer: C

Explanation:

Malware is software that infects computer systems to damage, disable or exploit the computer or network for various malicious purposes⁵. Malware is typically distributed via email attachments, fake internet ads, infected applications or websites, and often relies on user interaction to execute⁶. Therefore, one of the most effective ways to prevent malware infections is to educate the end user about the common signs and sources of malware, and how to avoid them⁷. Configuring the firewall, restoring the system from backups, and updating the antivirus program are also important security measures, but they do not address the root cause of the user's repeated infections, which is likely due to a lack of awareness or caution.

References⁵: Malware: what it is, how it works, and how to stop it - Norton⁶: How to Prevent Malware: 15 Best Practices for Malware Prevention⁷: 10 Security Tips for How to Prevent Malware Infections - Netwrix

NEW QUESTION 2

A user is no longer able to start the OS on a computer and receives an error message indicating there is no OS found. A technician reviews the audit logs and notes that the user's system posted a S.M.A.R.T. error just days before this issue. Which of the following is the MOST likely cause of this issue?

- A. Boot order
- B. Malware
- C. Drive failure
- D. Windows updates

Answer: C

Explanation:

A S.M.A.R.T. error is a warning that a hard drive is about to fail or has failed. This means that the OS cannot be loaded from the drive and the user will see an error message indicating there is no OS found. The most likely cause of this issue is drive failure.

NEW QUESTION 3

Which of the following data is MOST likely to be regulated?

- A. Name in a Phone book
- B. Name on a medical diagnosis
- C. Name on a job application
- D. Name on a employer's website

Answer: B

Explanation:

A name on a medical diagnosis (B) is most likely to be regulated. This is because it falls under the category of protected health information (PHI), which is subject to regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States. These regulations aim to protect the privacy and security of individuals' health information.

NEW QUESTION 4

A user turns on a new laptop and attempts to log in to specialized software, but receives a message stating that the address is already in use. The user logs on to the old desktop and receives the same message. A technician checks the account and sees a comment that the user requires a specifically allocated address before connecting to the software. Which of the following should the technician do to MOST likely resolve the issue?

- A. Bridge the LAN connection between the laptop and the desktop.
- B. Set the laptop configuration to DHCP to prevent conflicts.
- C. Remove the static IP configuration from the desktop.
- D. Replace the network card in the laptop, as it may be defective.

Answer: C

Explanation:

The new laptop was set up with the static IP it needs to connect to the software. The old desktop is still configured with that IP, hence the conflict.

NEW QUESTION 5

A technician is securing a new Windows 10 workstation and wants to enable a Screensaver lock. Which of the following options in the Windows settings should the technician use?

- A. Ease of Access
- B. Privacy
- C. Personalization
- D. Update and Security

Answer: C

Explanation:

The technician should use the Personalization option in the Windows settings to enable a Screensaver lock. The Personalization option allows users to customize the appearance and behavior of their desktop, such as themes, colors, backgrounds, lock screen and screensaver. The technician can enable a Screensaver lock by choosing a screensaver from the drop-down menu, setting a wait time in minutes and checking the box that says "On resume, display logon screen". This will lock the computer and require a password or PIN to log back in after the screensaver is activated. Ease of Access is an option in the Windows settings that allows users to adjust accessibility features and settings, such as narrator, magnifier, high contrast and keyboard shortcuts. Ease of Access is not related to enabling a

Screensaver lock. Privacy is an option in the Windows settings that allows users to manage privacy and security settings, such as location, camera, microphone and app permissions. Privacy is not related to enabling a Screensaver lock. Update and Security is an option in the Windows settings that allows users to check and install updates, troubleshoot problems, backup files and restore system. Update and Security is not related to enabling a Screensaver lock. References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 1.7

NEW QUESTION 6

A customer called the help desk to report that a machine that was recently updated is no longer working. The support technician checks the latest logs to see what updates were deployed, but nothing was deployed in more than three weeks. Which of the following should the support technician do to BEST resolve the situation?

- A. Offer to wipe and reset the device for the customer.
- B. Advise that the help desk will investigate and follow up at a later date.
- C. Put the customer on hold and escalate the call to a manager.
- D. Use open-ended questions to further diagnose the issue.

Answer: D

Explanation:

Open-ended questions are questions that require more than a yes or no answer and encourage the customer to provide more details and information. Using open-ended questions can help the support technician to understand the problem better, identify the root cause, and find a suitable solution.

Some examples of open-ended questions are:

- ? What exactly is not working on your machine?
- ? When did you notice the problem?
- ? How often does the problem occur?
- ? What were you doing when the problem happened?
- ? What have you tried to fix the problem?

Offering to wipe and reset the device for the customer is not a good option, as it may result in data loss and inconvenience for the customer. It should be used as a last resort only if other troubleshooting steps fail. Advising that the help desk will investigate and follow up at a later date is not a good option, as it may leave the customer unsatisfied and frustrated. It should be used only if the problem requires further research or escalation and cannot be resolved on the first call. Putting the customer on hold and escalating the call to a manager is not a good option, as it may waste time and resources. It should be used only if the problem is beyond the support technician's scope or authority and requires managerial intervention.

NEW QUESTION 7

A system drive is nearly full, and a technician needs to free up some space. Which of the following tools should the technician use?

- A. Disk Cleanup
- B. Resource Monitor
- C. Disk Defragment
- D. Disk Management

Answer: A

Explanation:

Disk Cleanup is a tool that can free up some space on a system drive that is nearly full. It can delete temporary files, cached files, recycle bin files, old system files and other unnecessary data. Resource Monitor is a tool that shows the network activity of each process on a Windows machine. Disk Defragment is a tool that optimizes the performance of a hard drive by rearranging the data into contiguous blocks. Disk Management is a tool that allows creating, formatting, resizing and deleting partitions on a hard drive. Verified References: <https://www.comptia.org/blog/how-to-use-disk-cleanup> <https://www.comptia.org/certifications/a>

NEW QUESTION 8

Antivirus software indicates that a workstation is infected with ransomware that cannot be quarantined. Which of the following should be performed first to prevent further damage to the host and other systems?

- A. Turn off the machine.
- B. Run a full antivirus scan.
- C. Remove the LAN card.
- D. Install a different endpoint solution.

Answer: A

Explanation:

Turning off the machine is the first and most urgent step to prevent further damage to the host and other systems. Ransomware can encrypt files, steal data, and spread to other devices on the network if the infected machine remains online. Turning off the machine will stop the ransomware process and isolate the machine from the network. The other options are either ineffective or risky. Running a full antivirus scan may not detect or remove the ransomware, especially if it is a new or unknown variant. Removing the LAN card may disconnect the machine from the network, but it will not stop the ransomware from encrypting or deleting files on the local drive. Installing a different endpoint solution may not be possible or helpful if the ransomware has already compromised the system or blocked the installation.

References: 1 3 steps to prevent and recover from ransomware(<https://www.microsoft.com/en-us/security/blog/2021/09/07/3-steps-to-prevent-and-recover-from-ransomware/>)2 #StopRansomware Guide | CISA(<https://www.cisa.gov/stopransomware/ransomware-guide>).

NEW QUESTION 9

The courts determined that a cybercrimes case could no longer be prosecuted due to the agency's handling of evidence. Which of the following was MOST likely violated during the investigation?

- A. Open-source software
- B. EULA
- C. Chain of custody
- D. AUP

Answer: C

Explanation:

Chain of custody is a process that documents how evidence is collected, handled, stored and transferred during a cybercrime investigation. It ensures that the evidence is authentic, reliable and admissible in court. If the chain of custody is violated during an investigation, it can compromise the integrity of the evidence and lead to the case being dismissed. Open-source software, EULA (end-user license agreement) and AUP (acceptable use policy) are not related to cybercrime investigations or evidence handling. Verified References: <https://www.comptia.org/blog/what-is-chain-of-custody> <https://www.comptia.org/certifications/a>

NEW QUESTION 10

A technician is creating a tunnel that hides IP addresses and secures all network traffic. Which of the following protocols is capable of enduring enhanced security?

- A. DNS
- B. IPS
- C. VPN
- D. SSH

Answer: C

Explanation:

A VPN (virtual private network) is a protocol that creates a secure tunnel between two devices over the internet, hiding their IP addresses and encrypting their traffic. DNS (domain name system) is a protocol that translates domain names to IP addresses. IPS (intrusion prevention system) is a device that monitors and blocks malicious network traffic. SSH (secure shell) is a protocol that allows remote access and command execution on another device. Verified References: <https://www.comptia.org/blog/what-is-a-vpn> <https://www.comptia.org/certifications/a>

NEW QUESTION 10

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?

- A. Run sfc / scannow on the drive as the administrator.
- B. Run cleanmgr on the drive as the administrator
- C. Run chkdsk on the drive as the administrator.
- D. Run dfrgui on the drive as the administrator.

Answer: C

Explanation:

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

NEW QUESTION 11

A user reports a virus is on a PC. The user installs additional real-time protection antivirus software, and the PC begins performing extremely slow. Which of the following steps should the technician take to resolve the issue?

- A. Uninstall one antivirus software program and install a different one.
- B. Launch Windows Update, and then download and install OS updates
- C. Activate real-time protection on both antivirus software programs
- D. Enable the quarantine feature on both antivirus software programs.
- E. Remove the user-installed antivirus software program.

Answer: E

Explanation:

Removing the user-installed antivirus software program is the best way to resolve the issue of extremely slow performance caused by installing additional real-time protection antivirus software on a PC. Having more than one antivirus software program running at the same time can cause conflicts, resource consumption and performance degradation. Uninstalling one antivirus software program and installing a different one, activating real-time protection on both antivirus software programs, enabling the quarantine feature on both antivirus software programs and launching Windows Update are not effective ways to resolve the issue. Verified References: <https://www.comptia.org/blog/why-you-shouldnt-run-multiple-antivirus-programs-at-the-same-time> <https://www.comptia.org/certifications/a>

NEW QUESTION 13

Which of the following is also known as something you know, something you have, and something you are?

- A. ACL
- B. MFA
- C. SMS
- D. NFC

Answer: B

Explanation:

MFA stands for Multi-Factor Authentication, which is a method of verifying a user's identity using two or more different factors of authentication. The three factors

of authentication are something you know, something you have, and something you are. These factors correspond to different types of information or evidence that only the legitimate user should possess or provide. For example:

? Something you know: a password, a PIN, a security question, etc.

? Something you have: a smart card, a token, a mobile device, etc.

? Something you are: a fingerprint, a face, an iris, etc.

MFA provides a higher level of security than single-factor authentication, which only uses one factor, such as a password. MFA reduces the risk of unauthorized access, identity theft, and data breaches, as an attacker would need to compromise more than one factor to impersonate a user. MFA is commonly used for online banking, email accounts, cloud services, and other sensitive applications

NEW QUESTION 15

A technician is working with a company to determine the best way to transfer sensitive personal information between offices when conducting business. The company currently uses USB drives and is resistant to change. The company's compliance officer states that all media at rest must be encrypted. Which of the following would be the BEST way to secure the current workflow?

- A. Deploy a secondary hard drive with encryption on the appropriate workstation
- B. Configure a hardened SFTP portal for file transfers between file servers
- C. Require files to be individually password protected with unique passwords
- D. Enable BitLocker To Go with a password that meets corporate requirements

Answer: D

Explanation:

The BEST way to secure the current workflow of transferring sensitive personal information between offices when conducting business is to enable BitLocker To Go with a password that meets corporate requirements. This is because BitLocker To Go is a full-disk encryption feature that encrypts all data on a USB drive, which is what the company currently uses, and requires a password to access the data.

NEW QUESTION 20

A company is deploying mobile phones on a one-to-one basis, but the IT manager is concerned that users will root/jailbreak their phones. Which of the following technologies can be implemented to prevent this issue?

- A. Signed system images
- B. Antivirus
- C. SSO
- D. MDM

Answer: D

Explanation:

MDM stands for Mobile Device Management, and it is a way of remotely managing and securing mobile devices that are used for work purposes¹. MDM can enforce policies and restrictions on the devices, such as preventing users from installing unauthorized apps, modifying system settings, or accessing root privileges². MDM can also monitor device status, wipe data, lock devices, or locate lost or stolen devices¹.

NEW QUESTION 23

Which of the following is MOST likely used to run .vbs files on Windows devices?

- A. winmgmt.exe
- B. powershell.exe
- C. cscript.exe
- D. explorer.exe

Answer: C

Explanation:

A .vbs file is a Virtual Basic script written in the VBScript scripting language. It contains code that can be executed within Windows via the Windows-based script host (Wscript.exe), to perform certain admin and processing functions¹. Cscript.exe is a command-line version of the Windows Script Host that provides command-line options for setting script properties. Therefore, cscript.exe is most likely used to run .vbs files on Windows devices. References: ¹:

<https://fileinfo.com/extension/vbs> : [https://docs.microsoft.com/en-us/windows-server/administration/windows- commands/cscript](https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/cscript)

NEW QUESTION 26

A technician has verified that a user's computer has a virus, and the antivirus software is out Of date. Which of the following steps should the technician take NEXT?

- A. Quarantine the computer.
- B. use a previous restore point,
- C. Educate the end user about viruses
- D. Download the latest virus definitions

Answer: D

Explanation:

This will ensure that the antivirus software is up-to-date, and can detect any new viruses that may have been released since the last virus definition update.

The CompTIA A+ Core 2 220-1102 exam covers this topic in the following domains: 1.3 Explain the importance of security awareness and 2.2 Given a scenario, use secure data management and disaster recovery principles.

NEW QUESTION 28

A technician suspects a rootkit has been installed and needs to be removed. Which of the following would BEST resolve the issue?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

If a rootkit has caused a deep infection, then the only way to remove the rootkit is to reinstall the operating system. This is because rootkits are designed to be difficult to detect and remove, and they can hide in the operating system's kernel, making it difficult to remove them without reinstalling the operating system
<https://www.minitool.com/backup-tips/how-to-get-rid-of-rootkit-windows-10.html>

NEW QUESTION 32

The web browsing speed on a customer's mobile phone slows down every few weeks and then returns to normal after three or four days. Restarting the device does not usually restore performance. Which of the following should a technician check FIRST to troubleshoot this issue?

- A. Data usage limits
- B. Wi-Fi connection speed
- C. Status of airplane mode
- D. System uptime

Answer: B

Explanation:

The technician should check the Wi-Fi connection speed first to troubleshoot this issue. Slow web browsing speed on a mobile phone can be caused by a slow Wi-Fi connection. The technician should check the Wi-Fi connection speed to ensure that it is fast enough to support web browsing. If the Wi-Fi connection speed is slow, the technician should troubleshoot the Wi-Fi network to identify and resolve the issue.

NEW QUESTION 35

A hard drive that previously contained PII needs to be repurposed for a public access workstation. Which of the following data destruction methods should a technician use to ensure data is completely removed from the hard drive?

- A. Shredding
- B. Degaussing
- C. Low-level formatting
- D. Recycling

Answer: A

Explanation:

Shredding is a data destruction method that physically destroys the hard drive by cutting it into small pieces using a machine. Shredding ensures that data is completely removed from the hard drive and cannot be recovered by any means. Shredding is suitable for hard drives that contain PII (personally identifiable information) which is any information that can be used to identify, contact, or locate an individual. Degaussing, low-level formatting, and recycling are not data destruction methods that can guarantee complete data removal from a hard drive.

NEW QUESTION 36

HOTSPOT

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.

TEST QUESTION

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

INSTRUCTIONS
Click on individual tickets 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.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Show Question



Reset All Answers

Details

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

No Ticket Selected

Please select a ticket from the list

	Date	Priority	
ing to boot. Screen I...	7/13/2022	High	
to access Z: on my co...	7/13/2022	Low	

Details

#8675309

Priority

Category

Assigned To

Assigned Date

Open

High

Technical / Bug Reports

helpdesk@fictional.com

7/13/2022

Subject

PC is failing to boot. Screen is displaying error message, see attachment.

Attachments

[bootmgr not found.png](#)

Issue

Resolution

Verify/Resolve

ing to boot. Screen i...

7/13/2022

High

access Z: on my co...

7/13/2022

Low

#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

[bootimage_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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

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 ▼

Resolution

Reinstall Operating System ▼

Verify/Resolve

chkdsk ▼

Close Ticket

NEW QUESTION 39

A user reports a workstation has been performing strangely after a suspicious email was opened on it earlier in the week. Which of the following should the technician perform FIRST?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

[https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-\(3-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0))

When a user reports that their workstation is behaving strangely after opening a suspicious email, the first step a technician should take is to run a virus scan on the computer. This is because opening a suspicious email is a common way for viruses and malware to infect a computer. Running a virus scan can help identify and remove any infections that may be causing the computer to behave strangely.

NEW QUESTION 43

A technician is unable to completely start up a system. The OS freezes when the desktop background appears, and the issue persists when the system is restarted. Which of the following should the technician do next to troubleshoot the issue?

- A. Disable applicable BIOS options.
- B. Load the system in safe mode.
- C. Start up using a flash drive OS and run System Repair.
- D. Enable Secure Boot and reinstall the system.

Answer: B

Explanation:

Loading the system in safe mode is a common troubleshooting step that allows the technician to isolate the problem by disabling unnecessary drivers and services. This can help determine if the issue is caused by a faulty device, a corrupted system file, or a malware infection.

NEW QUESTION 45

A technician is creating a location on a Windows workstation for a customer to store meeting minutes. Which of the following commands should the technician use?

- A. c: \minutes
- B. dir
- C. md
- D. rmdir

Answer: D

Explanation:

The command md stands for make directory and is used to create a new directory or folder in the current location. In this case, the technician can use md minutes to create a folder named minutes in the C: drive. The other commands are not relevant for this task. c: \minutes is not a command but a path to a folder. dir is used to display a list of files and folders in the current directory. rmdir is used to remove or delete an existing directory or folder.

NEW QUESTION 47

Which of the following operating systems is most commonly used in embedded systems?

- A. Chrome OS
- B. macOS
- C. Windows
- D. Linux

Answer: D

Explanation:

Linux is the most commonly used operating system in embedded systems because it is open source, free, customizable, and supports a wide range of architectures and devices. Linux also offers many advantages for embedded development, such as real-time capabilities, modularity, security, scalability, and reliability. Linux can run on embedded systems with limited resources, such as memory, storage, or power, and can be tailored to the specific needs of the application. Linux also has a large and active community of developers and users who contribute to its improvement and innovation. Some examples of embedded systems that use Linux are smart TVs, routers, drones, robots, smart watches, and IoT devices

NEW QUESTION 50

An organization is updating the monitors on kiosk machines. While performing the upgrade, the organization would like to remove physical input devices. Which of the following utilities in the Control Panel can be used to turn on the on-screen keyboard to replace the physical input devices?

- A. Devices and Printers
- B. Ease of Access
- C. Programs and Features
- D. Device Manager

Answer: B

Explanation:

Ease of Access is a utility in the Control Panel that allows users to adjust various accessibility settings on Windows, such as the on-screen keyboard, magnifier, narrator, high contrast, etc. The on-screen keyboard can be turned on by going to Ease of Access > Keyboard and toggling the switch to On. Alternatively, the on-screen keyboard can be opened by pressing Windows + Ctrl + O keys or by typing osk.exe in the Run dialog box.

References: 1 Use the On-Screen Keyboard (OSK) to type(<https://support.microsoft.com/en-us/windows/use-the-on-screen-keyboard-osk-to-type-ecbb5e08-5b4e-d8c8-f794-81dbf896267a>)2 How to Enable or Disable the On-Screen Keyboard in Windows 10 - Lifewire(<https://www.lifewire.com/enable-or-disable-on-screen-keyboard-in-windows-10-5180667>)3 On-Screen Keyboard Settings, Tips and Tricks in Windows 11/10(<https://www.thewindowsclub.com/windows-onscreen-keyboard>).

NEW QUESTION 52

Which of the following defines the extent of a change?

- A. Scope
- B. Purpose
- C. Analysis
- D. Impact

Answer: A

Explanation:

The term that defines the extent of a change is scope. Scope is a measure of the size, scale and boundaries of a project or an activity. Scope defines what is included and excluded in the project or activity, such as goals, requirements, deliverables, tasks and resources. Scope helps determine the feasibility, duration and cost of the project or activity. Scope also helps manage the expectations and needs of the stakeholders involved in the project or activity. Purpose is the reason or objective for doing a project or an activity. Purpose defines why the project or activity is important or necessary, such as solving a problem, meeting a need or achieving a goal. Purpose helps provide direction, motivation and justification for the project or activity. Analysis is the process of examining, evaluating and interpreting data or information related to a project or an activity. Analysis helps identify, understand and prioritize issues, risks, opportunities and solutions for the project or activity. Impact is the effect or outcome of a project or an activity on something or someone else. Impact defines how the project or activity affects or influences other factors, such as performance, quality, satisfaction or value. Impact helps measure the success and effectiveness of the project or activity.

References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 5.2

NEW QUESTION 54

A company is recycling old hard drives and wants to quickly reprovision the drives for reuse. Which of the following data destruction methods should the company

use?

- A. Degaussing
- B. Standard formatting
- C. Low-level wiping
- D. Deleting

Answer: C

Explanation:

Low-level wiping is the best data destruction method for recycling old hard drives for reuse. Low-level wiping is a process that overwrites every bit of data on a hard drive with zeros or random patterns, making it impossible to recover any data from the drive. Low-level wiping also restores the drive to its factory state, removing any bad sectors or errors that may have accumulated over time. Low-level wiping can be done using specialized software tools or hardware devices that connect to the drive. Degaussing, standard formatting, and deleting are not suitable data destruction methods for recycling old hard drives for reuse. Degaussing is a process that exposes a hard drive to a strong magnetic field, destroying both the data and the drive itself. Degaussing renders the drive unusable for reuse. Standard formatting is a process that erases the data on a hard drive by removing the file system structure, but it does not overwrite the data itself. Standard formatting leaves some data recoverable using forensic tools or software utilities. Deleting is a process that removes the data from a hard drive by marking it as free space, but it does not erase or overwrite the data itself. Deleting leaves most data recoverable using undelete tools or software utilities.

References:

? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 15

? CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 105

NEW QUESTION 59

The network was breached over the weekend System logs indicate that a single user's account was successfully breached after 500 attempts with a dictionary attack. Which of the following would BEST mitigate this threat?

- A. Encryption at rest
- B. Account lockout
- C. Automatic screen lock
- D. Antivirus

Answer: B

Explanation:

Account lockout would best mitigate the threat of a dictionary attack1

NEW QUESTION 60

A manager called the help desk to ask for assistance with creating a more secure environment for the finance department- which resides in a non-domain environment. Which of the following would be the BEST method to protect against unauthorized use?

- A. Implementing password expiration
- B. Restricting user permissions
- C. Using screen locks
- D. Disabling unnecessary services

Answer: B

Explanation:

Restricting user permissions is a method of creating a more secure environment for the finance department in a non-domain environment. This means that users will only have access to the files and resources that they need to perform their tasks and will not be able to modify or delete other files or settings that could compromise security or functionality.

NEW QUESTION 63

Which of the following Linux commands would be used to install an application?

- A. yum
- B. grep
- C. ls
- D. sudo

Answer: D

Explanation:

The Linux command used to install an application is sudo. The sudo command allows users to run programs with the security privileges of another user, such as the root user. This is necessary to install applications because it requires administrative privileges1

NEW QUESTION 65

A user contacted the help desk to report pop-ups on a company workstation indicating the computer has been infected with 137 viruses and payment is needed to remove them. The user thought the company-provided antivirus software would prevent this issue. The help desk ticket states that the user only receives these messages when first opening the web browser. Which of the following steps would MOST likely resolve the issue? (Select TWO)

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

"The user thought the company-provided antivirus software would prevent this issue." The most likely steps to resolve the issue are to deploy an ad-blocking

extension to the browser and perform a reset on the user's web browser. Ad-blocking extensions can help to prevent pop-ups and other unwanted content from appearing in the browser, and resetting the browser can help to remove any malicious extensions or settings that may be causing the issue.

NEW QUESTION 68

A technician needs to perform after-hours service starting at 10:00 p.m. The technician is currently 20 minutes late. The customer will also be late. Which of the following should the technician do considering proper communication techniques and professionalism?

- A. Do not notify the customer if arriving before the customer.
- B. Dismiss the customer and proceed with the after-hours work.
- C. Contact the customer if the technician is arriving late.
- D. Disclose the experience via social media.

Answer: C

Explanation:

The best option for the technician to demonstrate proper communication techniques and professionalism is to contact the customer if the technician is arriving late. This shows respect for the customer's time and expectations, and allows the customer to adjust their schedule accordingly. It also helps to maintain a positive relationship and trust between the technician and the customer. The technician should apologize for the delay and provide a realistic estimate of their arrival time. The technician should also thank the customer for their patience and understanding.

The other options are not appropriate or professional. Do not notify the customer if arriving before the customer is not a good practice, as it may cause confusion or frustration for the customer. The customer may have made other plans or arrangements based on the technician's original schedule, and may not be available or prepared for the service. Dismiss the customer and proceed with the after-hours work is rude and disrespectful, as it ignores the customer's needs and preferences. The customer may have questions or concerns about the service, or may want to supervise or verify the work. The technician should always communicate with the customer before, during, and after the service.

Disclose the experience via social media is unethical and unprofessional, as it may violate the customer's privacy and the company's policies. The technician should not share any confidential or sensitive information about the customer or the service on social media, or make any negative or inappropriate comments about the customer or the situation. References:

- ? CompTIA A+ Certification Exam Core 2 Objectives1
- ? CompTIA A+ Core 2 (220-1102) Certification Study Guide2
- ? 8 Ways You Can Improve Your Communication Skills3
- ? Professionalism in Communication | How To Do It And How It Pays4

NEW QUESTION 73

Which of the following would MOST likely be used to change the security settings on a user's device in a domain environment?

- A. Security groups
- B. Access control list
- C. Group Policy
- D. Login script

Answer: C

Explanation:

Group Policy is the most likely tool to be used to change the security settings on a user's device in a domain environment. Group Policy is a feature of Windows that allows administrators to manage and configure settings for multiple devices and users in a centralized way. Group Policy can be used to enforce security policies such as password

complexity, account lockout, firewall rules, encryption settings, etc.

NEW QUESTION 78

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?

- A. Internet-based upgrade
- B. Repair installation
- C. Clean install
- D. USB repair
- E.

In place upgrade

Answer: C

Explanation:

The desktop specialist should use a clean install to refresh the laptop. A clean install will remove all data and applications from the laptop and install a fresh copy of Windows 10, ensuring that the laptop is ready for the newly hired employee.

NEW QUESTION 82

A technician is replacing the processor in a desktop computer prior to opening the computer, the technician wants to ensure the internal components are protected. Which of the following safety procedures would BEST protect the components in the PC? (Select TWO).

- A. Utilizing an ESD strap
- B. Disconnecting the computer from the power source
- C. Placing the PSU in an antistatic bag
- D. Ensuring proper ventilation
- E. Removing dust from the ventilation fans
- F. Ensuring equipment is grounded

Answer: AC

Explanation:

The two safety procedures that would best protect the components in the PC are:

- ? Utilizing an ESD strap
- ? Placing the PSU in an antistatic bag

<https://www.professormesser.com/free-a-plus-training/220-902/computer-safety-procedures-2/>

<https://www.skillssoft.com/course/comptia-a-core-2-safety-procedures-environmental-impacts-cbdf0f2c-61c0-4f4a-a659-dc98f1f00158>

NEW QUESTION 84

Which of the following operating systems is considered closed source?

- A. Ubuntu
- B. Android

C. CentOS
D. OSX

Answer: D

Explanation:

OSX (now macOS) is an operating system that is considered closed source, meaning that its source code is not publicly available or modifiable by anyone except its

developers. It is owned and maintained by Apple Inc. Ubuntu, Android and CentOS are operating systems that are considered open source, meaning that their source code is publicly available and modifiable by anyone who wants to contribute or customize them. Verified References:
<https://www.comptia.org/blog/open-source-vs-closed-source-software> <https://www.comptia.org/certifications/a>

NEW QUESTION 89

Which of the following should be used to control security settings on an Android phone in a domain environment?

- A. MDM
- B. MFA
- C. ACL
- D. SMS

Answer: A

Explanation:

The best answer to control security settings on an Android phone in a domain environment is to use “Mobile Device Management (MDM)”. MDM is a type of software that is used to manage and secure mobile devices such as smartphones and tablets. MDM can be used to enforce security policies, configure settings, and remotely wipe data from devices. In a domain environment, MDM can be used to manage Android phones and enforce security policies such as password requirements, encryption, and remote wipe capabilities12

NEW QUESTION 93

All the desktop icons on a user's newly issued PC are very large. The user reports that the PC was working fine until a recent software patch was deployed. Which of the following would BEST resolve the issue?

- A. Rolling back video card drivers

- B. Restoring the PC to factory settings
- C. Repairing the Windows profile
- D. Reinstalling the Windows OS

Answer: A

Explanation:

Rolling back video card drivers is the best way to resolve the issue of large desktop icons on a user's newly issued PC. This means restoring the previous version of the drivers that were working fine before the software patch was deployed. The software patch may have caused compatibility issues or corrupted the drivers, resulting in display problems

NEW QUESTION 97

Which of the following is the best reason for sandbox testing in change management?

- A. To evaluate the change before deployment
- B. To obtain end-user acceptance
- C. To determine the affected systems
- D. To select a change owner

Answer: A

Explanation:

Sandbox testing is a method of testing changes in a simulated environment that mimics the real one, without affecting the actual production system. Sandbox testing is useful for change management because it allows the testers to evaluate the change before deployment, and ensure that it works as intended, does not cause any errors or conflicts, and meets the requirements and expectations of the stakeholders. Sandbox testing also helps to protect the investment in the existing system, as it reduces the risk of introducing bugs or breaking functionality that could harm the customer experience or the business operations. Sandbox testing also gives the testers more control over the customer experience, as they can experiment with different scenarios and configurations, and optimize the change for the best possible outcome.

References:

1: Change Management and Sandbox - Quickbase1 2: Embracing change: Build, test, and adapt in a sandbox environment - Zendesk3

NEW QUESTION 99

Which of the following file extensions should a technician use for a PowerShell script?

- A.

.ps1

- B. .py
- C. .sh
- D. .bat
- E. .cmd

Answer: A

Explanation:

A PowerShell script is a plain text file that contains one or more PowerShell commands. Scripts have a .ps1 file extension and can be run on your computer or in a remote session. PowerShell scripts can be used to automate tasks and change settings on Windows devices. To create and run a PowerShell script, you need a text editor (such as Visual Studio Code or Notepad) and the PowerShell Integrated Scripting Environment (ISE) console. You also need to enable the correct execution policy to allow scripts to run on your system

NEW QUESTION 103

A user has been unable to receive emails or browse the internet from a smartphone while traveling. However, text messages and phone calls are working without issue. Which of the following should a support technician check FIRST?

User account status

- ~~A~~: Mobile OS version
- C. Data plan coverage
- D. Network traffic outages

Answer: C

Explanation:

The first thing that a support technician should check to resolve the issue of not being able to receive emails or browse the internet from a smartphone while traveling is the data plan coverage. The data plan coverage determines how much data and where the user can use on the smartphone's cellular network. The data plan coverage may vary depending on the user's location, carrier and subscription. The data plan coverage may not include or support certain areas or countries that the user is traveling to, or may charge extra fees or limit the speed or amount of data that the user can use. The data plan coverage does not affect text messages and phone calls, which use different network services and protocols. User account status is not likely to cause the issue of not being able to receive emails or browse the internet from a smartphone while traveling, unless the user account has been suspended or terminated by the carrier or the email provider. Mobile OS version is not likely to cause the issue of not being able to receive emails or browse the internet from a smartphone while traveling, unless the mobile OS has a major bug or compatibility problem with the network or the email app. Network traffic outages may cause the issue of not being able to receive emails or browse the internet from a smartphone while traveling, but they are less likely and less common than data plan coverage issues, and they should also affect text messages and phone calls. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.5

NEW QUESTION 106

Which of the following is an advantage of using WPA2 instead of WPA3?

- A. Connection security
- B. Encryption key length
- C. Device compatibility
- D. Offline decryption resistance

Answer: C

Explanation:

Device compatibility is an advantage of using WPA2 instead of WPA3. WPA2 is the previous version of the Wi-Fi Protected Access protocol, which provides security and encryption for wireless networks. WPA3 is the latest version, which offers improved security features, such as stronger encryption, enhanced protection against brute-force attacks, and easier configuration. However, WPA3 is not backward compatible with older devices that only support WPA2 or earlier protocols. Therefore, using WPA3 may limit the range of devices that can connect to the wireless network. Connection security, encryption key length, and offline decryption resistance are advantages of using WPA3 instead of WPA2. References:

- ? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 24
- ? CompTIA A+ Certification All-in-One Exam Guide (Exams 220-1101 & ..., page 1000

NEW QUESTION 110

A user updates a mobile device's OS. A frequently used application becomes consistently unresponsive immediately after the device is launched. Which of the following troubleshooting steps should the user perform FIRST?

- A. Delete the application's cache.
- B. Check for application updates.
- C. Roll back the OS update.
- D. Uninstall and reinstall the application.

Answer: B

Explanation:

Checking for application updates is the first troubleshooting step that the user should perform, because the application may not be compatible with the new OS version and may need an update to fix the issue. Deleting the application's cache, rolling back the OS update, or uninstalling and reinstalling the application are possible solutions, but they are more time-consuming and disruptive than checking for updates. References: : <https://www.comptia.org/training/resources/exam-objectives/comptia-a-core-2-exam-objectives>
: <https://www.lifewire.com/how-to-update-apps-on-android-4173855>

NEW QUESTION 111

A department manager submits a help desk ticket to request the migration of a printer's port utilization from USB to Ethernet so multiple users can access the printer. This will be a new network printer, thus a new IP address allocation is required. Which of the following should happen immediately before network use is authorized?

- A. Document the date and time of the change.
- B. Submit a change request form.
- C. Determine the risk level of this change.
- D. Request an unused IP address.

Answer: B

Explanation:

A change request form is a document that describes the proposed change, the reason for the change, the impact of the change, and the approval process for the change. A change request form is required for any planned changes to the network, such as adding a new network printer, to ensure that the change is authorized, documented, and communicated to all stakeholders. Submitting a change request form should happen immediately before network use is authorized, as stated in the Official CompTIA A+ Core 2 Study Guide. The other options are either too late (documenting the date and time of the change) or too early (determining the risk level of the change and requesting an unused IP address) in the change management process.

NEW QUESTION 113

A user attempts to install additional software and receives a UAC prompt. Which of the following is the BEST way to resolve this issue?

- A. Add a user account to the local administrator's group.
- B. Configure Windows Defender Firewall to allow access to all networks.
- C. Create a Microsoft account.
- D. Disable the guest account.

Answer: A

Explanation:

A user account that belongs to the local administrator's group has the permission to install software on a Windows machine. If a user receives a UAC (user account control) prompt when trying to install software, it means the user does not have enough privileges and needs to enter an administrator's password or switch to an administrator's account. Adding the user account to the local administrator's group can resolve this issue. Configuring Windows Defender Firewall, creating a Microsoft account and disabling the guest account are not related to this issue. Verified References: <https://www.comptia.org/blog/user-account-control>
<https://www.comptia.org/certifications/a>

NEW QUESTION 114

A change advisory board just approved a change request. Which of the following is the MOST likely next step in the change process?

- A. End user acceptance
- B. Perform risk analysis
- C. Communicate to stakeholders
- D. Sandbox testing

Answer: D

Explanation:

The risk analysis should be performed before it's taken to the board. The step after the board approves the change is End User Agreement Reference: https://www.youtube.com/watch?v=Ru77iZxuEIA&list=PLG49S3nxzAnna96gzhJrzkii4hH_mgW4b&index=59

NEW QUESTION 119

A remote user is having issues accessing an online share. Which of the following tools would MOST likely be used to troubleshoot the Issue?

- A. Screen-sharing software
- B. Secure shell
- C. Virtual private network
- D. File transfer software

Answer: A

Explanation:

Screen-sharing software is a tool that allows a technician to remotely view and control a user's screen over the internet. It can be used to troubleshoot issues with accessing an online share, as well as other problems that require visual inspection or guidance. Secure shell (SSH) is a protocol that allows remote access and command execution on another device, but it does not allow screen-sharing. Virtual private network (VPN) is a protocol that creates a secure tunnel between two devices over the internet, but it does not allow remote troubleshooting. File transfer software is a tool that allows transferring files between two devices over the internet, but it does not allow screen-sharing. Verified References: <https://www.comptia.org/blog/what-is-screen-sharing-software>
<https://www.comptia.org/certifications/a>

NEW QUESTION 120

An employee calls the help desk regarding an issue with a laptop PC. After a Windows update, the user can no longer use certain locally attached devices, and a reboot has not fixed the issue. Which of the following should the technician perform to fix the issue?

- A. Disable the Windows Update service.
- B. Check for updates.
- C. Restore hidden updates.
- D. Rollback updates.

Answer: D

Explanation:

The technician should perform a rollback of the Windows update that caused the issue with the locally attached devices. A rollback is a process of uninstalling an update and restoring the previous version of the system. This can help to fix any compatibility or performance issues caused by the update¹. To rollback an update, the technician can use the Settings app, the Control Panel, or the System Restore feature. The technician should also check for any device driver updates that might be needed after rolling back the update. Disabling the Windows Update service is not a good practice, as it can prevent the system from receiving important security and feature updates. Checking for updates might not fix the issue, as the update that caused the issue might still be installed. Restoring hidden updates is not relevant, as it only applies to updates that have been hidden by the user to prevent them from being installed².

References: 1: <https://www.windowscentral.com/how-uninstall-and-reinstall-updates-windows-10> 2: <https://support.microsoft.com/en-us/windows/show-or-hide-updates-in-windows-10-9c9f0a4f-9a6e-4c8e-8b44-afbc6b33f3cf>

NEW QUESTION 122

A macOS user is installing a new application. Which of the following system directories is the software MOST likely to install by default?

- A. /etc/services
- B. /Applications
- C. /usr/bin
- D. C:\Program Files

Answer: B

Explanation:

The software is most likely to install by default in the /Applications directory, which is the standard location for macOS applications. This directory can be accessed from the Finder sidebar or by choosing Go > Applications from the menu bar. The /Applications directory contains all the applications that are available to all users on the system¹. Some applications might also offer the option to install in the ~/Applications directory, which is a personal applications folder for a single user². The /etc/services directory is a system configuration file that maps service names to port numbers and protocols³. The /usr/bin directory is a system directory that contains executable binaries for various commands and utilities⁴. The C:\Program Files directory is a Windows directory that does not exist on macOS.

NEW QUESTION 123

Which of the following is used to ensure users have the appropriate level of access to perform their job functions?

- ☐ A. Access control list
- ☒ B. Multifactor authentication
- ☐ C. Least privilege
- ☐ D. Mobile device management

Answer: C

Explanation:

Least privilege is the principle that is used to ensure users have the appropriate level of access to perform their job functions. Least privilege means granting users only the minimum amount of access rights and permissions they need to perform their tasks, and nothing more. Least privilege reduces the risk of unauthorized access, data leakage, malware infection, or accidental damage by limiting what users can do on the system or network. Access control list, multifactor authentication, and mobile device management are not principles, but rather mechanisms or methods that can implement least privilege. Access control list is a list that specifies the users or groups that are allowed or denied access to a resource, such as a file, folder, or printer. Multifactor authentication is a method that requires users to provide two or more pieces of evidence to prove their identity, such as a password, a token, or a biometric factor. Mobile device management is a tool that allows managing and securing mobile devices, such as smartphones or tablets, that are used by employees to access corporate data or applications. References:

? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 25

? [CompTIA Security+ SY0-601 Certification Study Guide], page 1003

NEW QUESTION 127

A company implemented a BYOD policy and would like to reduce data disclosure caused by malware that may infect these devices. Which of the following should the company deploy to address these concerns?

- A. UAC
- B. MDM

- C. LDAP
- D. SSO

Answer: B

Explanation:

MDM stands for mobile device management, which is a type of software solution that allows remote management and security of mobile devices. MDM can help a company reduce data disclosure caused by malware that may infect these devices by enforcing security policies, such as encryption, password protection, antivirus software, and remote wipe. MDM can also monitor and control the access of personal devices to corporate data and networks. UAC stands for user account control, which is a feature of Windows that prompts users for permission or an administrator password before making changes that affect the system. UAC may not be effective in preventing malware infection or data disclosure on personal devices. LDAP stands for lightweight directory access protocol, which is a protocol for accessing and managing information stored in a directory service, such as user names and passwords. LDAP does not directly address the issue of malware infection or data disclosure on personal devices. SSO stands for single sign-on, which is a feature that allows users to access multiple applications or services with one set of credentials. SSO may not prevent malware infection or data disclosure on personal devices, and may even increase the risk if the credentials are compromised.

<https://www.nist.gov/news-events/news/2021/03/mobile-device-security-bring-your-own-device-byod-draft-sp-1800-22>

NEW QUESTION 128

A bank would like to enhance building security in order to prevent vehicles from driving into the building while also maintaining easy access for customers. Which of the following BEST addresses this need?

- A. Guards
- B. Bollards
- C. Motion sensors
- D. Access control vestibule

Answer: B

Explanation:

Bollards are the best solution to enhance building security in order to prevent vehicles from driving into the building while also maintaining easy access for customers. References: 2. Bollards. Retrieved from <https://en.wikipedia.org/wiki/Bollard>

NEW QUESTION 129

A user tries to access commonly used web pages but is redirected to unexpected websites. Clearing the web browser cache does not resolve the issue. Which of the following should a technician investigate NEXT to resolve the issue?

- A. Enable firewall ACLs.
- B. Examine the localhost file entries.
- C. Verify the routing tables.
- D. Update the antivirus definitions.

Answer: B

Explanation:

A possible cause of the user being redirected to unexpected websites is that the localhost file entries have been modified by malware or hackers to point to malicious or unwanted websites. The localhost file is a text file that maps hostnames to IP addresses and can override DNS settings. By examining the localhost file entries, a technician can identify and remove any suspicious or unauthorized entries that may cause the redirection issue. Enabling firewall ACLs may not resolve the issue if the firewall rules do not block the malicious or unwanted websites. Verifying the routing tables may not resolve the issue if the routing configuration is correct and does not affect the web traffic. Updating the antivirus definitions may help prevent future infections but may not remove the existing malware or changes to the localhost file. References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 1.3

NEW QUESTION 131

A user requires local administrative access to a workstation. Which of the following Control Panel utilities allows the technician to grant access to the user?

- A. System
- B. Network and Sharing Center
- C. User Accounts
- D. Security and Maintenance

Answer: C

Explanation:

User Accounts is a Control Panel utility that allows the technician to manage user accounts and groups on a workstation. The technician can use User Accounts to grant local administrative access to a user by adding the user to the Administrators group. The Administrators group has full control over the workstation and can perform tasks such as installing software, changing system settings, and accessing all files.

References: 1: User Accounts (Control Panel) (<https://docs.microsoft.com/en-us/windows/win32/shell/user-accounts>) : Local Users and Groups practices/local-users-and-groups) (<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/local-users-and-groups>)

NEW QUESTION 133

A technician is attempting to mitigate micro power outages, which occur frequently within the area of operation. The outages are usually short, with the longest occurrence lasting five minutes. Which of the following should the technician use to mitigate this issue?

- A. Surge suppressor
- B. Battery backup
- C. CMOS battery
- D. Generator backup

Answer: B

Explanation:

A battery backup, also known as an uninterruptible power supply (UPS), is a device that provides backup power during a power outage. When the power goes out, the battery backup provides a short amount of time (usually a few minutes up to an hour, depending on the capacity of the device) to save any work and safely shut down the equipment.

NEW QUESTION 137

Which of the following command-line tools will delete a directory?

- A. md
- B. del
- C. dir
- D. rd
- E. cd

Answer: D

Explanation:

To delete an empty directory, enter `rd Directory` or `rmdir Directory`. If the directory is not empty, you can remove files and subdirectories from it using the `/s` switch. You can also use the `/q` switch to suppress confirmation messages (quiet mode).

NEW QUESTION 142

A systems administrator installed the latest Windows security patch and received numerous tickets reporting slow performance the next day. Which of the following should the administrator do to resolve this issue?

- A. Rebuild user profiles.
- B. Roll back the updates.
- C. Restart the services.
- D. Perform a system file check.

Answer: B

Explanation:

Rolling back the updates is the best way to resolve the issue of slow performance caused by installing the latest Windows security patch. This can be done by using the System Restore feature or by uninstalling the specific update from the Control Panel. Rebuilding user profiles, restarting the services and performing a system file check are not likely to fix the issue, since they do not undo the changes made by the update. Verified References: <https://www.comptia.org/blog/how-to-roll-back-windows-updates> <https://www.comptia.org/certifications/a>

NEW QUESTION 145

After a company installed a new SOHO router customers were unable to access the company-hosted public website. Which of the following will MOST likely allow customers to access the website?

- A. Port forwarding
- B. Firmware updates
- C. IP filtering
- D. Content filtering

Answer: B

Explanation:

If customers are unable to access the company-hosted public website after installing a new SOHO router, the company should check for firmware updates¹. Firmware updates can fix bugs and compatibility issues that may be preventing customers from accessing the website¹. The company should also ensure that the router is properly configured to allow traffic to the website¹. If the router is blocking traffic to the website, the company should configure the router to allow traffic to the website¹.

NEW QUESTION 149

A technician is selling up a newly built computer. Which of the following is the FASTEST way for the technician to install Windows 10?

- A. Factory reset
- ☒ B. In-place upgrade
- C. System Restore
- D. Unattended installation

Answer: D

Explanation:

An unattended installation is the fastest way to install Windows 10 on a newly built computer. It uses an answer file that contains all the configuration settings and preferences for the installation, such as language, product key, partition size, etc. It does not require any user interaction or input during the installation process. Factory reset, System Restore and in-place upgrade are not methods of installing Windows 10 on a new computer, but ways of restoring or updating an existing Windows installation. Verified References: <https://www.comptia.org/blog/what-is-an-unattended-installation> <https://www.comptia.org/certifications/a>

NEW QUESTION 154

Before leaving work, a user wants to see the traffic conditions for the commute home. Which of the following tools can the user employ to schedule the browser to automatically launch a traffic website at 4:45 p.m.?

- ☒ A. perfmon.msc
- B. taskschd.msc

- C. lusrmgr.msc
- D. Eventvwr.msc

Answer: A

Explanation:

The user can use the Task Scheduler (taskschd.msc) to schedule the browser to automatically launch a traffic website at 4:45 p.m. The Task Scheduler is a tool in Windows that allows users to schedule tasks to run automatically at specified times or in response to certain events.

NEW QUESTION 158

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

- A. Biometric lock
- B. Badge reader
- C. USB token
- D. Video surveillance
- E. Locking rack
- F. Access control vestibule

Answer: AB

Explanation:

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.

NEW QUESTION 159

A call center handles inquiries into billing issues for multiple medical facilities. A security analyst notices that call center agents often walk away from their workstations, leaving patient data visible for anyone to see. Which of the following should a network administrator do to BEST prevent data theft within the call center?

- A. Encrypt the workstation hard drives.
- B. Lock the workstations after five minutes of inactivity.
- C. Install privacy screens.
- D. Log off the users when their workstations are not in use.

Answer: B

Explanation:

The BEST solution for preventing data theft within the call center in this scenario would be to lock the workstations after a period of inactivity. This would prevent unauthorized individuals from accessing patient data if call center agents were to step away from their workstations without logging out.

NEW QUESTION 160

A user needs assistance changing the desktop wallpaper on a Windows 10 computer. Which of the following methods will enable the user to change the wallpaper using a Windows 10 Settings tool?

- A. Open Settings, select Accounts, select Your info, click Browse, and then locate and open the image the user wants to use as the wallpaper.
- B. Open Settings, select Personalization, click Browse, and then locate and open the image the user wants to use as the wallpaper.
- C. Open Settings, select System, select Display, click Browse, and then locate and open the image the user wants to use as the wallpaper.
- D. Open Settings, select Apps, select Apps & features, click Browse, and then locate and open the image the user wants to use as the wallpaper.

Answer: B

Explanation:

The user can change the wallpaper using a Windows 10 Settings tool by following these steps:

- 1. Open Settings by pressing the Windows key and typing Settings, or by clicking the gear icon in the Start menu.
- 2. Select Personalization from the left navigation menu.
- 3. On the right side of the window, click Background.
- 4. In the Background settings, click the drop-down menu and select Picture as the background type.
- 5. Click Browse and then locate and open the image the user wants to use as the wallpaper.

The other options are incorrect because they do not lead to the Background settings or they do not allow the user to browse for an image. Accounts, System, and Apps are not related to personalization settings. Your info, Display, and Apps & features are not related to wallpaper settings.

References: 1: <https://support.microsoft.com/en-us/windows/change-your-desktop-background-image-175618be-4cf1-c159-2785-ec2238b433a8> 2: <https://www.computerhope.com/issues/ch000592.htm>

NEW QUESTION 164

An organization is creating guidelines for the incorporation of generative AI solutions. In which of the following would these guidelines be published?

- A. Standard operating procedure
- B. Acceptable use policy
- C. Security protocols
- D. Data flow diagram

Answer: B

Explanation:

An acceptable use policy (AUP) is a document that defines the rules and expectations for the users of a system, network, or service. It typically covers topics such

as the purpose, scope, responsibilities, and restrictions of using the system, network, or service¹. An AUP is a suitable place to publish the guidelines for the incorporation of generative AI solutions, as it can inform the users of the benefits, risks, and ethical implications of using such tools. It can also specify the conditions and limitations for using generative AI solutions, such as the types of data, content, and applications that are allowed or prohibited, the security and privacy requirements, the legal and regulatory compliance, and the accountability and reporting mechanisms²³.

References: 1 What is an Acceptable Use Policy (AUP)? - Definition from Techopedia([https://security.stackexchange.com/questions/84168/the-difference-of-security-](https://security.stackexchange.com/questions/84168/the-difference-of-security-policy-and-acceptable-use-policy)

[policy-and-acceptable-use-policy](https://security.stackexchange.com/questions/84168/the-difference-of-security-policy-and-acceptable-use-policy)). 2 Guide on the use of Generative AI -

[Canada.ca\(https://www.canada.ca/en/government/system/digital-government/digital-](https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/guide-use-generative-ai.html) government-innovations/responsible-use-ai/guide-use-generative-ai.html)³

Key Considerations for Developing Organizational Generative AI Policies - ISACA(<https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-44/key-considerations-for-developing-organizational-generative-ai-policies>).

NEW QUESTION 165

A call center technician receives a call from a user asking how to update Windows. Which of the following describes what the technician should do?

- A. Have the user consider using an iPad if the user is unable to complete updates.
- B. Have the user text the user's password to the technician.
- C. Ask the user to click in the Search field, type Check for Updates, and then press the Enter key.
- D. Advise the user to wait for an upcoming, automatic patch.

Enter key

Answer: C

Explanation:

The technician should guide the user to update Windows through the built-in "Check for Updates" feature. This can be done by having the user click in the Search field, type "Check for Updates", and then press the Enter key. This will bring up the Windows Update function, which will search for any available updates and give the user the option to install them.

NEW QUESTION 169

A suite of security applications was installed a few days ago on a user's home computer.

The user reports that the computer has been running slowly since the installation. The user notices the hard drive activity light is constantly solid. Which of the following should be checked FIRST?

- A. Services in Control Panel to check for overutilization
- B. Performance Monitor to check for resource utilization
- C. System File Checker to check for modified Windows files
- D. Event Viewer to identify errors

Answer: C

Explanation:

System File Checker to check for modified Windows files. System File Checker (SFC) is a Windows utility that can be used to scan for and restore corrupt Windows system files. SFC can be used to detect and fix any modified or corrupted system files on a computer, and thus should be checked first when a user reports that their computer has been running slowly since the installation of security applications [1][2]. By checking SFC, any modified or corrupted system files can be identified and fixed, potentially improving the overall performance of the computer.

NEW QUESTION 171

A user is unable to access several documents saved on a work PC. A technician discovers the files were corrupted and must change several system settings within Registry Editor to correct the issue. Which of the following should the technician do before modifying the registry keys?

- A. Update the anti-malware software.
- B. Create a restore point.
- C. Run the PC in safe mode.
- D. Roll back the system updates.

Answer: B

Explanation:

A restore point is a snapshot of the system settings and configuration at a specific point in time². Creating a restore point before modifying the registry keys allows the technician to revert the system back to a previous state if something goes wrong or causes instability². Updating the anti-malware software, running the PC in safe mode, and rolling back the system updates are not necessary steps before modifying the registry keys.

NEW QUESTION 176

An administrator responded to an incident where an employee copied financial data to a portable hard drive and then left the company with the data. The administrator documented the movement of the evidence. Which of the following concepts did the administrator demonstrate?

- A. Preserving chain of custody
- B. Implementing data protection policies
- C. Informing law enforcement
- D. Creating a summary of the incident

Answer: A

Explanation:

Preserving chain of custody is a concept that refers to the documentation and tracking of who handled, accessed, modified, or transferred a piece of evidence, when, where, why, and how. Preserving chain of custody can help establish the authenticity, integrity, and reliability of the evidence, as well as prevent tampering, alteration, or loss of the evidence. An administrator who documented the movement of the evidence demonstrated the concept of preserving chain of custody. Implementing data protection policies, informing law enforcement, and creating a summary of the incident are not concepts that describe the action of documenting the movement of the evidence.

NEW QUESTION 179

A small business owner wants to install newly purchased software on all networked PCs. The network is not configured as a domain, and the owner wants to use the easiest method possible. Which of the following is the MOST deficient way for the owner to install the application?

- A. Use a network share to share the installation files.
- B. Save software to an external hard drive to install.
- C. Create an imaging USB for each PC.
- D. Install the software from the vendor's website

Answer: B

Explanation:

Saving software to an external hard drive and installing it on each individual PC is the most inefficient method for the small business owner. This method requires manual intervention on each PC, and there is a higher risk of error or inconsistencies between PCs. Additionally, if the software needs to be updated or reinstalled in the future, this process would need to be repeated on each PC.

NEW QUESTION 180

A user reports that antivirus software indicates a computer is infected with viruses. The user thinks this happened while browsing the internet. The technician does not recognize the interface with which the antivirus message is presented. Which of the following is the NEXT step the technician should take?

- A. Shut down the infected computer and swap it with another computer
- B. Investigate what the interface is and what triggered it to pop up
- C. Proceed with initiating a full scan and removal of the viruses using the presented interface
- D. Call the phone number displayed in the interface of the antivirus removal tool

Answer: B

Explanation:

The technician should not proceed with initiating a full scan and removal of the viruses using the presented interface or call the phone number displayed in the interface of the antivirus removal tool.

Shutting down the infected computer and swapping it with another computer is not necessary at this point.

The technician should not immediately assume that the message is legitimate or perform any actions without knowing what the interface is and what triggered it to pop up. It is important to investigate the issue further, including checking the legitimacy of the antivirus program and the message it is displaying.

NEW QUESTION 185

Malware is installed on a device after a user clicks on a link in a suspicious email. Which of the following is the best way to remove the malware?

- A. Run System Restore.
- B. Place in recovery mode.
- C. Schedule a scan.
- D. Restart the PC.

Answer: B

Explanation:

Recovery mode is a special boot option that allows the user to access advanced tools and features to troubleshoot and remove malware from the device.

Recovery mode can also restore the system to a previous state or reset the device to factory settings. Running System Restore, scheduling a scan, or restarting the PC may not be effective in removing the malware, as it may still be active or hidden in the system files.

NEW QUESTION 187

In an organization with a standardized set of installed software, a developer submits a request to have new software installed. The company does not currently have a license for this software, but the developer already downloaded the installation file and is requesting that the technician install it. The developer states that the management team approved the business use of this software. Which of the following is the best action for the technician to take?

- A. Contact the software vendor to obtain the license for the user, and assist the user with installation once the license is purchased.
- B. Run a scan on the downloaded installation file to confirm that it is free of malicious software, install the software, and document the software installation process.
- C. Indicate to the developer that formal approval is needed; then, the IT team should investigate the software and the impact it will have on the organization before installing the software.
- D. Install the software and run a full system scan with antivirus software to confirm that the operating system is free of malicious software.

Answer: C

Explanation:

Installing new software on an organization's system or device can have various implications, such as compatibility, security, performance, licensing, and compliance issues. Therefore, it is important to follow the best practices for software installation, such as doing research on the software, checking the system requirements, scanning the installation file for malware, and obtaining the proper license. The technician should not install the software without formal approval from the management team, as this could violate the organization's policies or regulations. The technician should also not install the software without investigating the software and its impact on the organization, as this could introduce potential risks or problems to the system or device. The technician should indicate to the developer that formal approval is needed, and then work with the IT team to evaluate the software and its suitability for the organization before installing it.

NEW QUESTION 191

A computer technician is investigating a computer that is not booting. The user reports that the computer was working prior to shutting it down last night. The technician notices a removable USB device is inserted, and the user explains the device is a prize the user received in the mail yesterday. Which of the following types of attacks does this describe?

- A. Phishing
- B. Dumpster diving
- C. Tailgating

D. Evil twin

Answer: A

Explanation:

Phishing is the correct answer for this question. Phishing is a type of attack that uses fraudulent emails or other messages to trick users into revealing sensitive information or installing malicious software. Phishing emails often impersonate legitimate entities or individuals and offer incentives or threats to lure users into clicking on malicious links or attachments. In this scenario, the user received a removable USB device in the mail as a prize, which could be a phishing attempt to infect the user's computer with malware or gain access to the user's data. Dumpster diving, tailgating, and evil twin are not correct answers for this question.

Dumpster diving is a type of attack that involves searching through trash bins or recycling containers to find discarded documents or devices that contain valuable information. Tailgating is a type of attack that involves following an authorized person into a restricted area without proper identification or authorization. Evil twin is a type of attack that involves setting up a rogue wireless access point that mimics a legitimate one to intercept or manipulate network traffic. References:

? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 25

? [CompTIA Security+ SY0-601 Certification Study Guide], page 1004

NEW QUESTION 195

A technician is working on a way to register all employee badges and associated computer IDs. Which of the following options should the technician use in order to achieve this objective?

- A. Database system
- B. Software management
- C. Active Directory description
- D. Infrastructure as a Service

Answer: A

Explanation:

A database system is a software application that allows storing, organizing, and managing data in a structured way. A database system can be used to register all employee badges and associated computer IDs by creating a table or a record for each employee that contains their badge number, computer ID, name, and other relevant information. A database system can also facilitate searching, updating, and deleting data as needed. Software management is a general term that refers to the process of planning, developing, testing, deploying, and maintaining software applications. It does not directly address the issue of registering employee badges and computer IDs. Active Directory description is a field in Active Directory that can be used to store additional information about an object, such as a user or a computer. It is not a software application that can be used to register employee badges and computer IDs by itself. Infrastructure as a Service (IaaS) is a cloud computing model that provides servers, storage, networking, and software over the internet. It does not directly address the issue of registering employee badges and computer IDs either.

<https://www.idcreator.com/>

<https://www.alphacard.com/photo-id-systems/card-type/employee-badges>

NEW QUESTION 198

Which of the following allows access to the command line in macOS?

- A. PsExec
- B. command.com
- C. Terminal
- D. CMD

Answer: C

Explanation:

Terminal is an application that allows access to the command line in macOS. The command line is an interface that allows users to interact with the operating system and perform various tasks by typing commands and arguments. Terminal can be used to launch programs, manage files and folders, configure settings, troubleshoot issues, and run scripts in macOS. PsExec, command.com, and CMD are not applications that allow access to the command line in macOS.

NEW QUESTION 199

A technician has been tasked with using the fastest and most secure method of logging in to laptops. Which of the following log-in options meets these requirements?

- A. PIN
- B. Username and password
- C. SSO
- D. Fingerprint

Answer: A

Explanation:

This is because a PIN is a fast and secure method of logging in to laptops, and it is more secure than a password because it is not susceptible to keyloggers.

NEW QUESTION 202

A user receives a call from someone claiming to be a technical support agent. The caller asks the user to log in to the computer. Which of the following security measures should the user take to ensure security and privacy?

- A. Only accept calls from known people.
- B. Disregard any suspicious emails.
- C. Update the antivirus software.
- D. Enable two-factor authentication.
- E. Install a malware scanner.

Answer: A

Explanation:

This is a scenario of a potential tech support scam, where a fraudster pretends to be a technical support agent and tries to trick the user into giving them access to the computer, personal information, or money. The user should not trust any unsolicited calls from unknown people claiming to be from tech support, as they might be trying to install malware, steal data, or charge for fake services. The user should only accept calls from known people, such as their IT department, their service provider, or their software vendor, and verify their identity before logging in to the computer. The user should also report any suspicious calls to the appropriate authorities or organizations.

References:

- ? How to protect against tech support scams1
- ? Avoid and report Microsoft technical support scams2
- ? How to Protect Against Technical Support Scams3
- ? How To Recognize and Avoid Tech Support Scams4

NEW QUESTION 205

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?

- A. Changing channels
- B. Modifying the wireless security
- C. Disabling the SSID broadcast
- D. Changing the access point name

Answer: A

Explanation:

Changing channels can best resolve interference from other nearby SSIDs. Wireless networks operate on different channels, and changing the channel can help to avoid interference from other nearby networks.

NEW QUESTION 210

A data center is required to destroy SSDs that contain sensitive information. Which of the following is the BEST method to use for the physical destruction of SSDs?

- A. Wiping
- B. Low-level formatting
- C. Shredding
- D. Erasing

Answer: C

Explanation:

Shredding is the best method to use for the physical destruction of SSDs because it reduces them to small pieces that cannot be recovered or accessed. Wiping, low-level formatting, and erasing are not effective methods for destroying SSDs because they do not physically damage the flash memory chips that store data1.

NEW QUESTION 212

Security software was accidentally uninstalled from all servers in the environment. After requesting the same version of the software be reinstalled, the security analyst learns that a change request will need to be filled out. Which of the following is the BEST reason to follow the change management process in this scenario?

- A. Owners can be notified a change is being made and can monitor it for performance impact
- B. Most Voted
- C. A risk assessment can be performed to determine if the software is needed.
- D. End users can be aware of the scope of the change.
- E. A rollback plan can be implemented in case the software breaks an application.

Answer: A

Explanation:

change management process can help ensure that owners are notified of changes being made and can monitor them for performance impact (A). This can help prevent unexpected issues from arising.

NEW QUESTION 213

A company wants to remove information from past users' hard drives in order to reuse the hard drives. Which of the following is the MOST secure method?

- A. Reinstalling Windows
- B. Performing a quick format
- C. Using disk-wiping software
- D. Deleting all files from command-line interface

Answer: C

Explanation:

Using disk-wiping software is the most secure method for removing information from past users' hard drives in order to reuse the hard drives. Disk-wiping software can help to ensure that all data on the hard drive is completely erased and cannot be recovered.

NEW QUESTION 214

Which of the following commands can a technician use to get the MAC address of a Linux distribution?

- A. net use
- B. ifconfig
- C. netstat
- D. ping

Answer: B

Explanation:

The ifconfig command is a tool for configuring network interfaces that any Linux system administrator should know. It is used to bring interfaces up or down, assign and remove addresses and routes, manage ARP cache, and much more¹. One of the information that ifconfig can display is the MAC address of each network interface, which is a unique identifier of the physical layer of the network device. The MAC address is usually shown as a hexadecimal string separated by colons, such as 00:0c:29:3f:5c:1f. To get the MAC address of a Linux distribution, a technician can use the ifconfig command without any arguments, which will show the details of all the active network interfaces, or specify the name of a particular interface, such as eth0 or wlan0, to show only the details of that interface.

References¹: Linux Commands - CompTIA A+ 220-1102 - 1.11 - Professor Messer IT Certification Training Courses¹

NEW QUESTION 216

A technician needs to reimage a desktop in an area without network access. Which of the following should the technician use? (Select two).

- ☒ A. PXE
- ☐ B. Optical media
- ☐ C. Partition
- ☐ D. Boot record
- ☐ E. SMB
- ☐ F. USB

Answer: AC

Explanation:

A technician needs to reimage a desktop in an area without network access, which means that the technician cannot use network-based methods such as PXE or SMB to deploy the image. Therefore, the technician should use offline methods that involve removable media such as USB or optical media. USB and optical media are common ways to store and transfer system images, and they can be used to boot the desktop and initiate the reimaging process. The technician will need to create a bootable USB or optical media that contains the system image and the imaging software, and then insert it into the desktop and change the boot order in the BIOS or UEFI settings. The technician can then follow the instructions on the screen to reimage the desktop

NEW QUESTION 220

A developer is creating a shell script to automate basic tasks in Linux. Which of the following file types are supported by default?

- A. .py
- B. .js
- C. .vbs
- D. .sh

Answer: D

Explanation:

<https://www.educba.com/shell-scripting-in-linux/>

NEW QUESTION 225

A technician needs to document who had possession of evidence at every step of the process. Which of the following does this process describe?

- A. Rights management
- B. Audit trail
- C. Chain of custody
- D. Data integrity

Answer: C

Explanation:

The process of documenting who had possession of evidence at every step of the process is called chain of custody

NEW QUESTION 227

A technician just completed a Windows 10 installation on a PC that has a total of 16GB of RAM. The technician notices the Windows OS has only 4GB of RAM available for use. Which of the following explains why the OS can only access 4GB of RAM?

- A. The UEFI settings need to be changed.
- B. The RAM has compatibility issues with Windows 10.
- C. Some of the RAM is defective.
- D. The newly installed OS is x86.

Answer: D

Explanation:

The newly installed OS is x86. The x86 version of Windows 10 can only use up to 4GB of RAM. The x64 version of Windows 10 can use up to 2TB of RAM¹.

NEW QUESTION 229

A systems administrator received a request to limit the amount of cellular data a user's Windows 10 tablet can utilize when traveling. Which of the following can the administrator do to best solve the user's issue?

- A. Turn on airplane mode.
- B. Set the connection to be metered.
- C. Configure the device to use a static IP address.
- D. Enable the Windows Defender Firewall.

Answer: B

Explanation:

Setting the connection to be metered is the best solution for limiting the amount of cellular data a user's Windows 10 tablet can utilize when traveling. A metered connection is a network connection that has a data limit or charges fees based on the amount of data used. Windows 10 allows users to set any network connection as metered, which reduces the amount of data that Windows and some apps use in the background. For example, setting a connection as metered will prevent Windows from downloading updates automatically, stop some apps from syncing data online, and disable some live tiles on the Start menu. Setting a connection as metered can help users save cellular data and avoid extra charges when traveling. Turning on airplane mode, configuring the device to use a static IP address, and enabling the Windows Defender Firewall are not effective solutions for limiting the amount of cellular data a user's Windows 10 tablet can utilize when traveling. Turning on airplane mode will disable all wireless connections on the device, including Wi-Fi, Bluetooth, and cellular data. This will prevent the user from accessing any online services or applications on the tablet. Configuring the device to use a static IP address will assign a fixed IP address to the device instead of obtaining one dynamically from a DHCP server. This will not affect the amount of cellular data the device uses, and it may cause IP conflicts or connectivity issues on some networks. Enabling the Windows Defender Firewall will block or allow incoming and outgoing network traffic based on predefined or custom rules. This will not reduce the amount of cellular data the device

uses, and it may interfere with some apps or services that require network access. References:

? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 19

? CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 108

NEW QUESTION 231

A user is trying to use a third-party USB adapter but is experiencing connection issues. Which of the following tools should the technician use to resolve this issue?

- A. taskschd.msc
- B. eventvwr.msc
- C. de vmgm
- D. msc
- E. diskmgmt.msc

Answer: C

Explanation:

The tool that the technician should use to resolve the connection issues with the third-party USB adapter is devmgmt.msc. Devmgmt.msc is a command that opens the Device

Manager, which is a utility that allows users to view and manage the hardware devices and drivers installed on a computer. The technician can use the Device Manager to check the status, properties and compatibility of the USB adapter and its driver, and perform actions such as updating, uninstalling or reinstalling the driver, enabling or disabling the device, or scanning for hardware changes. Taskschd.msc is a command that opens the Task Scheduler, which is a utility that allows users to create and manage tasks that run automatically at specified times or events. The Task Scheduler is not relevant or useful for resolving connection issues with the USB adapter. Eventvwr.msc is a command that opens the Event Viewer, which is a utility that allows users to view and monitor the system logs and events. The Event Viewer may provide some information or clues about the connection issues with the USB adapter, but it does not allow users to manage or troubleshoot the device or its driver directly. Diskmgmt.msc is a command that opens the Disk Management, which is a utility that allows users to view and manage the disk drives and partitions on a computer. The Disk Management is not relevant or useful for resolving connection issues with the USB adapter. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.6

NEW QUESTION 233

A Windows computer is experiencing slow performance when the user tries to open

programs and files. The user recently installed a new software program from an external website.

Various websites are being redirected to an unauthorized site, and Task Manager shows the CPU usage is consistently at 100%. Which of the following should the technician do first?

- A. Uninstall the new program.
- B. Check the HOSTS file.
- C. Restore from a previous backup.
- D. Clear the web browser cache.

Answer: A

Explanation:

The symptoms that the user's Windows computer is experiencing suggest that the new software program that the user installed from an external website may be malicious or incompatible with the system. The program may be consuming a lot of CPU resources, slowing down the performance of other programs and files. The program may also be altering the browser settings or the HOSTS file, causing the web redirection to an unauthorized site. The first step that the technician should do is to uninstall the new program from the Control Panel or the Settings app, and then restart the computer. This may resolve the issue and restore the normal functionality of the computer. If the problem persists, the technician may need to perform additional steps, such as scanning for malware, checking the HOSTS file, clearing the web browser cache, or restoring from a previous backup

NEW QUESTION 238

A company has just refreshed several desktop PCs. The hard drives contain PII. Which of the following is the BEST method to dispose of the drives?

- A. Drilling
- B. Degaussing
- C. Low-level formatting
- D. Erasing/wiping

Answer: D

Explanation:

Erasing/wiping the hard drives is the best method to dispose of the drives containing PII

NEW QUESTION 239

A user is setting up backups on a workstation. The user wants to ensure that the restore process is as simple as possible. Which of the following backup types should the user select?

- A. Full
- B. Incremental
- C. Differential
- D. Synthetic

Answer: A

Explanation:

Full backup is the best option to ensure that the restore process is as simple as possible. A full backup is a backup type that copies all the data from the source to the destination, regardless of whether the data has changed or not. A full backup provides the most complete and consistent backup of the data, and it allows the user to restore the data from a single backup set without relying on any previous or subsequent backups. Incremental, differential, and synthetic backups are not as simple as full backups for restoring data. An incremental backup is a backup type that copies only the data that has changed since the last backup, whether it was full or incremental. An incremental backup requires less time and space than a full backup, but it also requires multiple backup sets to restore the data completely. A differential backup is a backup type that copies only the data that has changed since the last full backup. A differential backup requires more time and space than an incremental backup, but it also requires fewer backup sets to restore the data than an incremental backup. A synthetic backup is a backup type that combines a full backup with one or more incremental or differential backups to create a consolidated backup set. A synthetic backup requires less time and bandwidth than a full backup, but it also requires more processing power and storage space than an incremental or differential backup.

References:

? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 15

? CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 458

NEW QUESTION 241

A technician receives a call from a user who is on vacation. The user provides the necessary credentials and asks the technician to log in to the user's account and read a critical email that the user has been expecting. The technician refuses because this is a violation of the:

- A. acceptable use policy.
- B. regulatory compliance requirements.
- C. non-disclosure agreement
- D. incident response procedures

Answer: A

Explanation:

Logging into a user's account without their explicit permission is a violation of the acceptable use policy, which outlines the rules and regulations by which a user must abide while using a computer system. By logging into the user's account without their permission, the technician would be violating this policy. Additionally, this action could be seen as a breach of confidentiality, as the technician would have access to information that should remain confidential.

NEW QUESTION 246

A laptop that was in the evidence room of a police station is missing. Which of the following is the best reason to refer to chain of custody documentation?

- A. To determine which party had the machine and when.
- B. To remotely wipe sensitive data from the machine.
- C. To gather the information needed to replace the machine.
- D. To alert the owner that the password needs to be changed.

Answer: A

Explanation:

Chain of custody documentation is a record of the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence. It is important to maintain a chain of custody to ensure the integrity and authenticity of the evidence, and to prevent tampering or contamination. If a laptop that was in the evidence room of a police station is missing, the best reason to refer to chain of custody documentation is to determine which party had the machine and when. This can help to identify the possible suspects, locate the missing laptop, and verify if the evidence on the laptop was compromised or not

NEW QUESTION 247

Which of the following is the proper way for a technician to dispose of used printer consumables?

- A. Proceed with the custom manufacturer's procedure.
- B. Proceed with the disposal of consumables in standard trash receptacles.
- C. Empty any residual ink or toner from consumables before disposing of them in a standard recycling bin.
- D. Proceed with the disposal of consumables in standard recycling bins.

Answer: A

Explanation:

When it comes to disposing of used printer consumables, it is important to follow the manufacturer's instructions or guidelines for proper disposal, as different types of consumables may require different disposal procedures. Some manufacturers provide specific instructions for proper disposal, such as sending the used consumables back to the manufacturer or using special recycling programs.

Therefore, the proper way for a technician to dispose of used printer consumables is to proceed with the custom manufacturer's procedure, if provided. This option

ensures that the disposal is handled in an environmentally friendly and safe manner.

NEW QUESTION 250

A technician connects an additional monitor to a PC using a USB port. The original HDMI monitor is mounted to the left of the new monitor. When moving the mouse to the right from the original monitor to the new monitor, the mouse stops at the end of the screen on the original monitor. Which of the following will allow the mouse to correctly move to the new monitor?

- A. Rearranging the monitor's position in display settings
- B. Swapping the cables for the monitors
- C. Using the Ctrl+Alt+> to correct the display orientation
- D. Updating the display drivers for the video card

Answer: B

Explanation:

The correct answer is B. Swapping the cables for the monitors. When the second monitor is connected with the HDMI port, it is necessary to swap the cables for the monitors so that the mouse can move from the original monitor to the new monitor. This is because the HDMI port is designed to only support one monitor, and the mouse will not be able to move from one to the other without the cables being swapped.

According to CompTIA A+ Core 2 documents, "When connecting multiple displays to a system, the cables used to connect the displays must be swapped between the displays. For example, if a monitor is connected to a system using a VGA cable, the VGA cable must be moved to the next display to allow the mouse to move between the two displays."

NEW QUESTION 251

A user is receiving repeated pop-up advertising messages while browsing the internet. A malware scan is unable to locate the source of an infection. Which of the following should the technician check NEXT?

- A. Windows updates
- B. DNS settings
- C. Certificate store
- D. Browser plug-ins

Answer: D

Explanation:

Browser plug-ins are software components that add functionality to a web browser, such as playing videos, displaying animations, etc. However, some browser plug-ins can also be malicious or compromised and cause unwanted pop-up advertising messages while browsing the internet. A malware scan may not be able to locate the source of the infection if it is hidden in a browser plug-in. Windows updates, DNS settings and certificate store are not likely sources of pop-up advertising messages. Verified References: <https://www.comptia.org/blog/browser-security> <https://www.comptia.org/certifications/a>

NEW QUESTION 253

A user requested that the file permissions on a Linux device be changed to only allow access to a certain group of users. Which of the following commands should be used to complete the user's request?

- ☒ A. cat
- ☐ B: chmod
- ☐ C. pwd
- ☐ D. cacls

Answer: B

Explanation:

The chmod command is used to change the permissions of files and directories in Linux. It can grant or revoke read, write, and execute permissions for the owner, the group, and others. To change the file permissions to only allow access to a certain group of users, the chmod command can use either the symbolic or the numeric mode. For example, to give read and write permissions to the group and no permissions to others, the command can be:

chmod g+rw,o-rwx filename or

chmod 660 filename

References: 1 Chmod Command in Linux (File Permissions) | Linuxize(<https://linuxize.com/post/chmod-command-in-linux/>) 2 How To Change File or Directory Permissions in Linux | Tom's Hardware(<https://www.tomshardware.com/how-to/change-file-directory-permissions-linux>).

NEW QUESTION 254

A technician is setting up a conference room computer with a script that boots the application on login. Which of the following would the technician use to accomplish this task? (Select TWO).

- A. File Explorer
- B. Startup Folder
- C. System Information
- D. Programs and Features
- E. Task Scheduler
- F. Device Manager

Answer: BE

Explanation:

? B. Startup Folder1: The Startup folder is a special folder that contains shortcuts to programs or scripts that will run automatically when a user logs on. The technician can create a shortcut to the script and place it in the Startup folder for the conference room computer or for all users.

? E. Task Scheduler23: The Task Scheduler is a tool that allows you to create tasks that run at specified times or events. The technician can create a task that runs the script at logon for the conference room computer or for all users.

NEW QUESTION 256

A technician is troubleshooting an issue involving programs on a Windows 10 machine that are loading on startup but causing excessive boot times. Which of the following should the technician do to selectively prevent programs from loading?

- A. Right-click the Windows button, then select Run entering shell startup and clicking OK, and then move items one by one to the Recycle Bin
- B. Remark out entries listed HKEY_LOCAL_MACHINE>SOFTWARE>Microsoft>Windows>CurrentVersion>Run
- C. Manually disable all startup tasks currently listed as enabled and reboot checking for issue resolution at startup
- D. Open the Startup tab and methodically disable items currently listed as enabled and reboot, checking for issue resolution at each startup.

Answer: D

Explanation:

This is the most effective way to selectively prevent programs from loading on a Windows 10 machine. The Startup tab can be accessed by opening Task Manager and then selecting the Startup tab. From there, the technician can methodically disable items that are currently listed as enabled, reboot the machine, and check for issue resolution at each startup. If the issue persists, the technician can then move on to disabling the next item on the list.

NEW QUESTION 260

A company needs to securely dispose of data stored on optical discs. Which of the following is the MOST effective method to accomplish this task?

- A. Degaussing
- B. Low-level formatting
- C. Recycling
- D. Shredding

Answer: D

Explanation:

Shredding is the most effective method to securely dispose of data stored on optical discs¹²

References: 4. How Can I Safely Destroy Sensitive Data CDs/DVDs? - How-To Geek. Retrieved from <https://www.howtogeek.com/174307/how-can-i-safely-destroy-sensitive-data-cdsdvds/> 5. Disposal — UK Data Service. Retrieved from <https://ukdataservice.ac.uk/learning-hub/research-data-management/store-your-data/disposal/>

NEW QUESTION 261

A technician needs to format a USB drive to transfer 20GB of data from a Linux computer to a Windows computer. Which of the following filesystems will the technician MOST likely use?

- A. FAT32
- B. ext4
- C. NTFS
- D. exFAT

Answer: C

Explanation:

Since Windows systems support FAT32 and NTFS "out of the box" and Linux supports a whole range of them including FAT32 and NTFS, it is highly recommended to format the partition or disk you want to share in either FAT32 or NTFS, but since FAT32 has a file size limit of 4.2 GB, if you happen to work with huge files, then it is better you use NTFS

NEW QUESTION 263

A large organization is researching proprietary software with vendor support for a multiuser environment. Which of the following EULA types should be selected?

- A. Corporate
- B. Perpetual
- C. Open-source
- D. Personal

Answer: A

Explanation:

A corporate EULA is a type of end-user license agreement that is designed for a large organization that needs to use proprietary software with vendor support for a multiuser environment. A corporate EULA typically grants the organization a volume license that allows it to install and use the software on multiple devices or servers, and to distribute the software to its employees or affiliates. A corporate EULA also usually provides the organization with technical support, maintenance, updates, and warranty from the software vendor, as well as some customization options and discounts. A corporate EULA may also include terms and conditions that specify the rights and obligations of both parties, such as confidentiality, liability, indemnification, termination, and dispute resolution¹².

A corporate EULA is a better option than the other choices because:

? A perpetual EULA (B) is a type of end-user license agreement that grants the user a permanent and irrevocable license to use the software, without any time limit or expiration date. However, a perpetual EULA does not necessarily include vendor support, updates, or warranty, and it may not allow the user to install the software on multiple devices or servers, or to distribute the software to other users. A perpetual EULA may also be more expensive than a corporate EULA, as it requires a one-time payment upfront, rather than a recurring subscription fee³⁴.

? An open-source EULA © is a type of end-user license agreement that grants the user a license to use, modify, and redistribute the software, which is publicly available and free of charge. However, an open-source EULA does not provide any vendor support, maintenance, updates, or warranty, and it may impose some restrictions or obligations on the user, such as disclosing the source code, attributing the original author, or using a compatible license for derivative works. An open-source EULA may not be suitable for a large organization that needs proprietary software with vendor support for a multiuser environment⁵⁶.

? A personal EULA (D) is a type of end-user license agreement that grants the user a license to use the software for personal, non-commercial purposes only. A personal EULA may limit the number of devices or servers that the user can install the software on, and prohibit the user from distributing, copying, or reselling the software to other users. A personal EULA may also provide limited or no vendor support, maintenance, updates, or warranty, and it may have a fixed or renewable term. A personal EULA may not meet the needs of a large organization that needs proprietary software with vendor support for a multiuser environment⁷.

References:

1: What is a Corporate License Agreement? - Definition from Techopedia1 2: Corporate License Agreement - Template - Word & PDF2 3: What is a Perpetual License? - Definition from Techopedia3 4: Perpetual vs. Subscription Software Licensing: Which Is Best for You?4 5: What is an Open Source License? - Definition from Techopedia5 6: Open Source Licenses: Which One Should You Use?6 7: What is a Personal License Agreement? - Definition from Techopedia7 : Personal License Agreement - Template - Word & PDF

NEW QUESTION 264

A remote user's smartphone is performing very slowly. The user notices that the performance improves slightly after rebooting but then reverts back to performing slowly. The user also notices that the phone does not get any faster after connecting to the company's corporate guest network. A technician sees that the phone has a large number of applications installed on it. Which of the following is the most likely cause of the issue?

- A. The user is in a poor signal area.
- B. The user has too many processes running.
- C. The smartphone has malware on it.
- D. The smartphone has been jailbroken.

Answer: B

Explanation:

One of the common reasons for a slow smartphone performance is having too many apps installed and running in the background. These apps consume the device's memory (RAM) and CPU resources, which can affect the speed and responsiveness of the phone. Rebooting the phone can temporarily clear the RAM and stop some background processes, but they may resume after a while. Connecting to a different network does not affect the performance of the phone, unless the network is congested or has a poor signal. The user can improve the phone's performance by uninstalling unused apps, clearing app caches, and restricting background activities12. Malware can also slow down a phone, but it is not the most likely cause in this scenario, as the user does not report any other symptoms of infection, such as pop-ups, battery drain, or data usage spikes3. Jailbreaking a phone can also affect its performance, but it is not a cause, rather a consequence, of the user's actions. Jailbreaking is the process of removing the manufacturer's restrictions on a phone, which allows the user to install unauthorized apps, customize the system, and access root privileges4. However, jailbreaking also exposes the phone to security risks, voids the warranty, and may cause instability or compatibility issues5.

References1: Speed up a slow Android device - Android Help - Google Help2: Why your phone slows down over time and what you can do to stop it | TechRadar3: How to tell if your phone has a virus | Norton4: What is Jailbreaking? - Definition from Techopedia5: What is Jailbreaking an iPhone? - Lifewire

NEW QUESTION 268

Which of the following security methods supports the majority of current Wi-Fi-capable devices without sacrificing security?

- A. WPA3
- B. MAC filleting
- C. RADIUS
- D. TACACS+

Answer: A

Explanation:

WPA3 (Wi-Fi Protected Access 3) is a wireless security method that supports the majority of current Wi-Fi-capable devices without sacrificing security. It is backward compatible with WPA2 devices and offers enhanced encryption and authentication features. MAC filtering is another wireless security method, but it can be easily bypassed by spoofing MAC addresses. RADIUS (Remote Authentication Dial-In User Service) and TACACS+ (Terminal Access Controller Access-Control System Plus) are network authentication protocols, but they are not wireless security methods by themselves. Verified References: <https://www.comptia.org/blog/wireless-security-standards> <https://www.comptia.org/certifications/a>

NEW QUESTION 273

A technician is installing a new business application on a user's desktop computer. The machine is running Windows 10 Enterprise 32-bit operating system. Which of the following files should the technician execute in order to complete the installation?

- A. Installer_x64.exe
- B. Installer_Files.zip
- C. Installer_32.msi
- D. Installer_x86.exe
- E. Installer_Win10Enterprise.dmg

Answer: D

Explanation:

The 32-bit operating system can only run 32-bit applications, so the technician should execute the 32-bit installer. The "x86" in the file name refers to the 32-bit architecture.

<https://www.digitaltrends.com/computing/32-bit-vs-64-bit-operating-systems/>

NEW QUESTION 276

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?

- A. Lock all devices in a closet.
- B. Ensure all devices are from the same manufacturer.
- C. Change the default administrative password.
- D. Install the latest operating system and patches

Answer: C

Explanation:

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

NEW QUESTION 277

A technician is troubleshooting a computer with a suspected short in the power supply. Which of the following is the FIRST step the technician should take?

- A. Put on an ESD strap
- B. Disconnect the power before servicing the PC.
- C. Place the PC on a grounded workbench.
- D. Place components on an ESD mat.

Answer: B

Explanation:

The first step a technician should take when troubleshooting a computer with a suspected short in the power supply is B. Disconnect the power before servicing the PC. This is to prevent any electrical shock or damage to the components. A power supply can be dangerous even when unplugged, as capacitors can maintain a line voltage charge for a long time¹. Therefore, it is important to disconnect the power cord and press the power button to discharge any residual power before opening the case². The other steps are also important for safety and proper diagnosis, but they should be done after disconnecting the power.

NEW QUESTION 278

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 220-1102 Exam with Our Prep Materials Via below:

<https://www.certleader.com/220-1102-dumps.html>