CompTIA

Exam Questions 220-1102

CompTIA A+ Certification Exam: Core 2

About Exambible

Your Partner of IT Exam

Found in 1998

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

Our Advances

* 99.9% Uptime

  All examinations will be up to date.

* 24/7 Quality Support

  We will provide service round the clock.

* 100% Pass Rate

  Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1
A 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 2
A technician is troubleshooting a customer's PC and receives a phone call. The technician does not take the call and sets the phone to silent. Which of the following BEST describes the technician's actions?

A. Avoid distractions
B. Deal appropriately with customer's confidential material
C. Adhere to user privacy policy
D. Set and meet timelines

Answer: A

Explanation:
The technician has taken the appropriate action by not taking the call and setting the phone to silent in order to avoid any distractions and remain focused on the task at hand. This is a good example of how to maintain focus and productivity when working on a customer's PC, and will help to ensure that the job is completed in a timely and efficient manner.

NEW QUESTION 3
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 4
As part of a CYOD policy a systems administrator needs to configure each user's Windows device to require a password when resuming from a period of sleep or inactivity. Which of the following paths will lead the administrator to the correct settings?

A. Use Settings to access Screensaver settings
B. Use Settings to access Screen Timeout settings
C. Use Settings to access General
D. Use Settings to access Display.

Answer: A

Explanation:
The systems administrator should use Settings to access Screensaver settings to configure each user’s Windows device to require a password when resuming from a period of sleep or inactivity1

NEW QUESTION 5
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.skillsoft.com/course/comptia-a-core-2-safety-procedures-environmental-impacts-cbdf0f2c-61c0-4f

NEW QUESTION 6
A Chief Executive Officer has learned that an exploit has been identified on the web server software, and a patch is not available yet. Which of the following attacks MOST likely occurred?

A. Brute force
B. Zero day
C. Denial of service
D. On-path

Answer: B

Explanation:
A zero-day attack is an attack that exploits a previously unknown vulnerability in a computer application, meaning that the attack occurs on “day zero” of awareness of the vulnerability

- Configuring AAA Services. Retrieved from https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-0/security/configuration/guide/sc40crsb

NEW QUESTION 7
A help desk team lead contacts a systems administrator because the technicians are unable to log in to a Linux server that is used to access tools. When the administrator tries to use remote desktop to log in to the server, the administrator sees the GUI is crashing. Which of the following methods can the administrator use to troubleshoot the server effectively?

A. SFTP
B. SSH
C. VNC
D. MSRA

Answer: C

Explanation:
The administrator can use Virtual Network Computing (VNC) to troubleshoot the server effectively. VNC is a graphical desktop sharing system that allows the administrator to remotely control the desktop of a Linux
server.

NEW QUESTION 8
A technician installed a known-good, compatible motherboard on a new laptop. However, the motherboard is not working on the laptop. Which of the following should the technician MOST likely have done to prevent damage?

A. Removed all jewelry
B. Completed an inventory of tools before use
C. Practiced electrical fire safety
D. Connected a proper ESD strap

Answer: D

Explanation:
The technician should have connected a proper ESD strap to prevent damage to the motherboard. ESD (electrostatic discharge) can cause damage to electronic components, and an ESD strap helps to prevent this by grounding the technician and preventing the buildup of static electricity. Removing all jewelry is also a good practice, but it is not the most likely solution to this problem.

NEW QUESTION 9
A user has requested help setting up the fingerprint reader on a Windows 10 laptop. The laptop is equipped with a fingerprint reader and is joined to a domain Group Policy enables Windows Hello on all computers in the environment. Which of the following options describes how to set up Windows Hello Fingerprint for the user?

A. Navigate to the Control Panel utility, select the Security and Maintenance submenu, select Change Security and Maintenance settings, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete
B. Navigate to the Windows 10 Settings menu, select the Accounts submenu, select Sign in options, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete.
C. Navigate to the Windows 10 Settings menu, select the Update & Security submenu select Windows Security, select Windows Hello Fingerprint and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete
D. Navigate to the Control Panel utility, select the Administrative Tools submenu, select the user account in the list, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete.

Answer: B

Explanation:
Navigate to the Windows 10 Settings menu, select the Accounts submenu, select Sign in options, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete. Windows Hello Fingerprint can be set up by navigating to the Windows 10 Settings menu, selecting the Accounts submenu, selecting Sign in options, and then selecting Windows Hello Fingerprint. The user will then be asked to place a fingerprint on the fingerprint reader repeatedly until Windows indicates that setup is complete. Windows Hello Fingerprint allows the user to log into the laptop using just their fingerprint, providing an additional layer of security.

NEW QUESTION 10
During a recent flight an executive unexpectedly received several dog and cat pictures while trying to watch a movie via in-flight Wi-Fi on an iPhone. The executive has no records of any contacts sending pictures like these and has not seen these pictures before. To BEST resolve this issue, the executive should:

A. set AirDrop so that transfers are only accepted from known contacts
B. completely disable all wireless systems during the flight
C. discontinue using iMessage and only use secure communication applications
D. only allow messages and calls from saved contacts

Answer: A

Explanation:
To best resolve this issue, the executive should set AirDrop so that transfers are only accepted from known contacts (option A). AirDrop is a feature on iOS devices that allows users to share files, photos, and other data between Apple devices. By setting AirDrop so that it only accepts transfers from known contacts, the executive can ensure that unwanted files and photos are not sent to their device. Additionally, the executive should ensure that the AirDrop setting is only enabled when it is necessary, as this will protect their device from any unwanted files and photos.

NEW QUESTION 10
A systems administrator is tasked with configuring desktop systems to use a new proxy server that the organization has added to provide content filtering. Which of the following Windows utilities IS the BEST choice for accessing the necessary configuration to complete this goal?

A. Security and Maintenance
B. Network and Sharing Center
C. Windows Defender Firewall
D. Internet Options

Answer: D

Explanation:
The best choice for accessing the necessary configuration to configure the desktop systems to use a new proxy server is the Internet Options utility. This utility can be found in the Control Panel and allows you to configure the proxy settings for your network connection. As stated in the CompTIA A+ Core 2 exam objectives, technicians should be familiar with the Internet Options utility and how to configure proxy settings.

NEW QUESTION 14
A user is being directed by the help desk to look up a Windows PC's network name so the help desk can use a remote administration tool to assist the user. Which of the following commands would allow the user to give the technician the correct information? (Select TWO).

A. ipconfig /all
B. hostname
C. netstat /?
D. nslookup localhost
E. arp —a
F. ping :: 1

Answer: AB

Explanation:
The user can use the following commands to give the technician the correct information: ipconfig
/all and hostna1m.e
The ipconfig /all command displays the IP address, subnet mask, and default gateway
all adapters on the computer 1. The hostname command displays the name of the comp1u. ter

NEW QUESTION 16
Sensitive data was leaked from a user's smartphone. A technician discovered an unapproved application was installed, and the user has full access to the device's command shell. Which of the following is the NEXT step the technician should take to find the cause of the leaked data?

A. Restore the device to factory settings.
B. Uninstall the unapproved application.
C. Disable the ability to install applications from unknown sources.
D. Ensure the device is connected to the corporate WiFi network.

Answer: B

Explanation:
The technician should disable the user’s access to the device’s command shell. This will prevent the user from accessing sensitive data and will help to prevent further data leaks. The technician should then investigate the unapproved application to determine if it is the cause of the data leak. If the application is found to be the cause of the leak, the technician should uninstall the application and restore the device to factory settings. If the application is not the cause of the leak, the technician should investigate further to determine the cause of the leak. Disabling the ability to install applications from unknown sources can help to prevent future data leaks, but it is not the next step the technician should take in this scenario. Ensuring the device is connected to the corporate WiFi network is not relevant to this scenario1

NEW QUESTION 21
Which of the following is the MOST cost-effective version of Windows 10 that allows remote access through Remote Desktop?

A. Home
B. Pro for Workstations
C. Enterprise
D. Pro

Answer: D

Explanation:
The most cost-effective version of Windows 10 that allows remote access through Remote Desktop is Windows 10 Pro. Windows 10 Pro includes Remote Desktop, which allows users to connect to a remote
computer and access its desktop, files, and applications. Windows 10 Home does not include Remote Desktop, while Windows 10 Pro for Workstations and Windows 10 Enterprise are more expensive versions of Windows 10 that include additional features for businesses

NEW QUESTION 23
A user's system is infected with malware. A technician updates the anti-malware software and runs a scan that removes the malware. After the user reboots the system, it once again becomes infected with malware. Which of the following will MOST likely help to permanently remove the malware?

A. Enabling System Restore
B. Educating the user
C. Booting into safe mode
D. Scheduling a scan

Answer: B

Explanation:
Although updating the anti-malware software and running scans are important steps in removing malware, they may not be sufficient to permanently remove the malware if the user keeps engaging in behaviors that leave the system vulnerable, such as downloading unknown files or visiting malicious websites. Therefore, educating the user on safe computing practices is the best way to prevent future infections and permanently remove the malware.
Enabling System Restore, Booting into safe mode, and scheduling a scan are not the most efficient ways to permanently remove the malware. Enabling System Restore and Booting into safe mode may help in some cases, but they may not be sufficient to permanently remove the malware. Scheduling a scan is also important for detecting and removing malware, but it may not be sufficient to prevent future infections.
https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0)

NEW QUESTION 26
A technician is configuring a SOHO device Company policy dictates that static IP addresses cannot be used. The company wants the server to maintain the same IP address at all times. Which of the following should the technician use?

A. DHCP reservation
B. Port forwarding
C. DNS A record
D. NAT

Answer: A

Explanation:
The technician should use DHCP reservation to maintain the same IP address for the server at all times. DHCP reservation allows the server to obtain an IP address dynamically from the DHCP server, while ensuring that the same IP address is assigned to the server each time it requests an IP address.

NEW QUESTION 30
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 35
A technician is unable to join a Windows 10 laptop to a domain Which of the following is the MOST likely reason?

A. The domain's processor compatibility is not met
B. The laptop has Windows 10 Home installed
C. The laptop does not have an onboard Ethernet adapter
D. The Laptop does not have all current Windows updates installed

Answer: B

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

NEW QUESTION 36
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 patche is important for maintaining the security of the network equipment, but it is not the first action the technician should take1

NEW QUESTION 37
A user is attempting to browse the internet using Internet Explorer. When trying to load a familiar web page, the user is unexpectedly redirected to an unfamiliar website. Which of the following would MOST likely solve the issue?

A. Updating the operating system
B. Changing proxy settings
C. Reinstalling the browser
D. Enabling port forwarding

Answer: C

Explanation:
Reinstalling the browser would most likely solve the issue. This would remove any malicious software or add-ons that may be causing the issue and restore the browser to its default settings.

NEW QUESTION 40
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. taskschd.msc
B. perfmon.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 45
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 46
A technician at a customer site is troubleshooting a laptop A software update needs to be downloaded but the company's proxy is blocking traffic to the update site. Which of the following should the technician perform?

A. Change the DNS address to 1.1.1.1
B. Update Group Policy
C. Add the site to the client's exceptions list
D. Verity the software license is current.

Answer: C

Explanation:
The technician should add the update site to the client’s exceptions list to bypass the proxy. This can be done through the client’s web browser settings, where the proxy settings can be configured. By adding the update site to the exceptions list, the client will be able to access the site and download the software update.

NEW QUESTION 49
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. Escalate the ticket to Tier 2.

B. Run a virus scan.
C. Utilize a Windows restore point.
D. Reimage the computer.

Answer: B

Explanation:
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 50
A user is configuring a new SOHO Wi-Fi router for the first time. Which of the following settings should the user change FIRST?

A. Encryption
B. Wi-Fi channel
C. Default passwords
D. Service set identifier

Answer: C

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

NEW QUESTION 55
A user is setting up a computer for the first time and would like to create a secondary login with permissions that are different than the primary login. The secondary login will need to be protected from certain content such as games and websites. Which of the following Windows settings should the user utilize to create the secondary login?

A. Privacy
B. Accounts
C. Personalization
D. Shared resources

Answer: B

Explanation:
To create a secondary login with different permissions in Windows 10, the user should utilize the Accounts setting. Here are the steps to create a new user account with different permissions:

- Right-click the Windows Start menu button.
- Select Control Panel.
- Select User Accounts.
- Select Manage another account.
- Select Add a new user in PC settings.
- Use the Accounts dialog box to configure a new account.1

NEW QUESTION 59
An incident handler needs to preserve evidence for possible litigation. Which of the following will the incident handler MOST likely do to preserve the evidence?

A. Encrypt the files
B. Clone any impacted hard drives
C. Contact the cyber insurance company
D. Inform law enforcement

Answer: B

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

NEW QUESTION 64
A user calls the help desk and reports a workstation is infected with malicious software. Which of the following tools should the help desk technician use to remove the malicious software? (Select TWO).

A. File Explorer
B. User Account Control
C. Windows Backup and Restore
D. Windows Firewall
E. Windows Defender
F. Network Packet Analyzer

Answer: AE

Explanation:
The correct answers are E. Windows Defender and A. File Explorer. Windows Defender is a built-in antivirus program that can detect and remove malicious software from a workstation. File Explorer can be used to locate and delete files associated with the malicious software1

NEW QUESTION 66
A technician is working to resolve a Wi-Fi network issue at a doctor's office that is located next to an apartment complex. The technician discovers that employees and patients are not the only people on the network. Which of the following should the technician do to BEST minimize this issue?

A. Disable unused ports.
B. Remove the guest network
C. Add a password to the guest network
D. Change the network channel.

Answer: D

Explanation:
Changing the network channel is the best solution to minimize the issue of employees and patients not being the only people on the Wi-Fi network5
References: 3. Sample CompTIA Security+ exam questions and answers. Retrieved from https://www.techtarget.com/searchsecurity/quiz/Sample-CompTIA-Security-exam-questions-and-answers

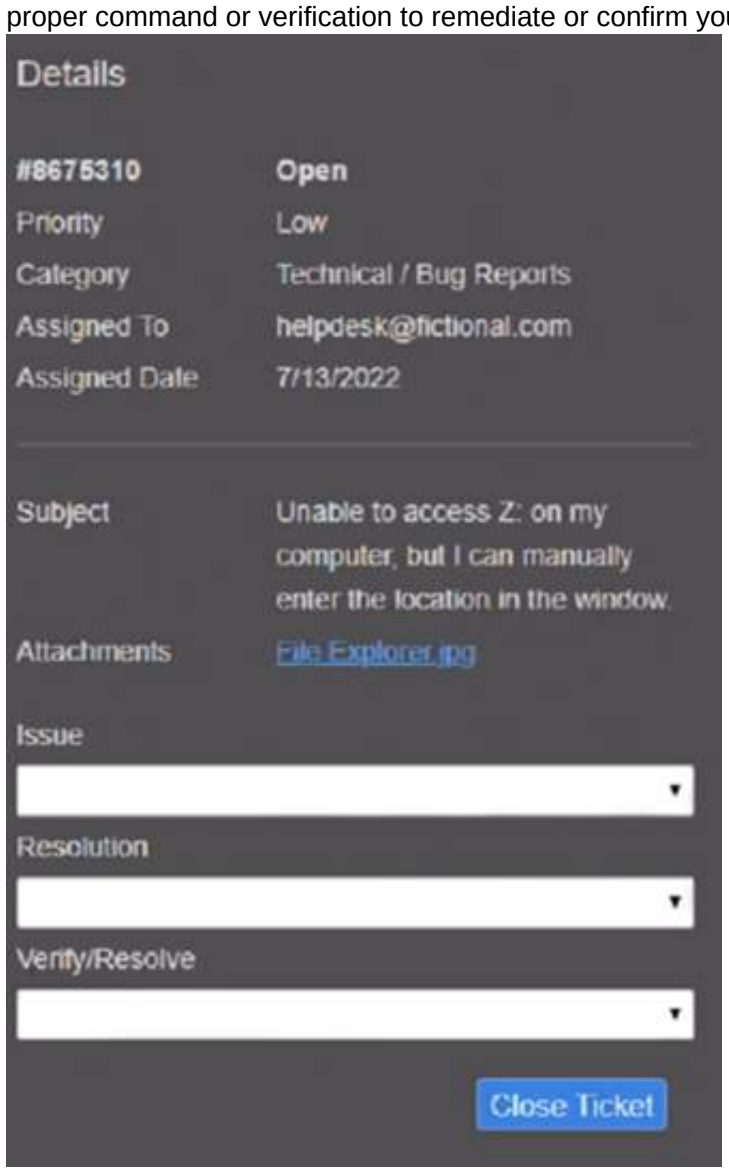
NEW QUESTION 71
A Microsoft Windows PC needs to be set up for a user at a targe corporation. The user will need access to the corporate domain to access email and shared drives. Which of the following versions of Windows would a technician MOST likely deploy for the user?

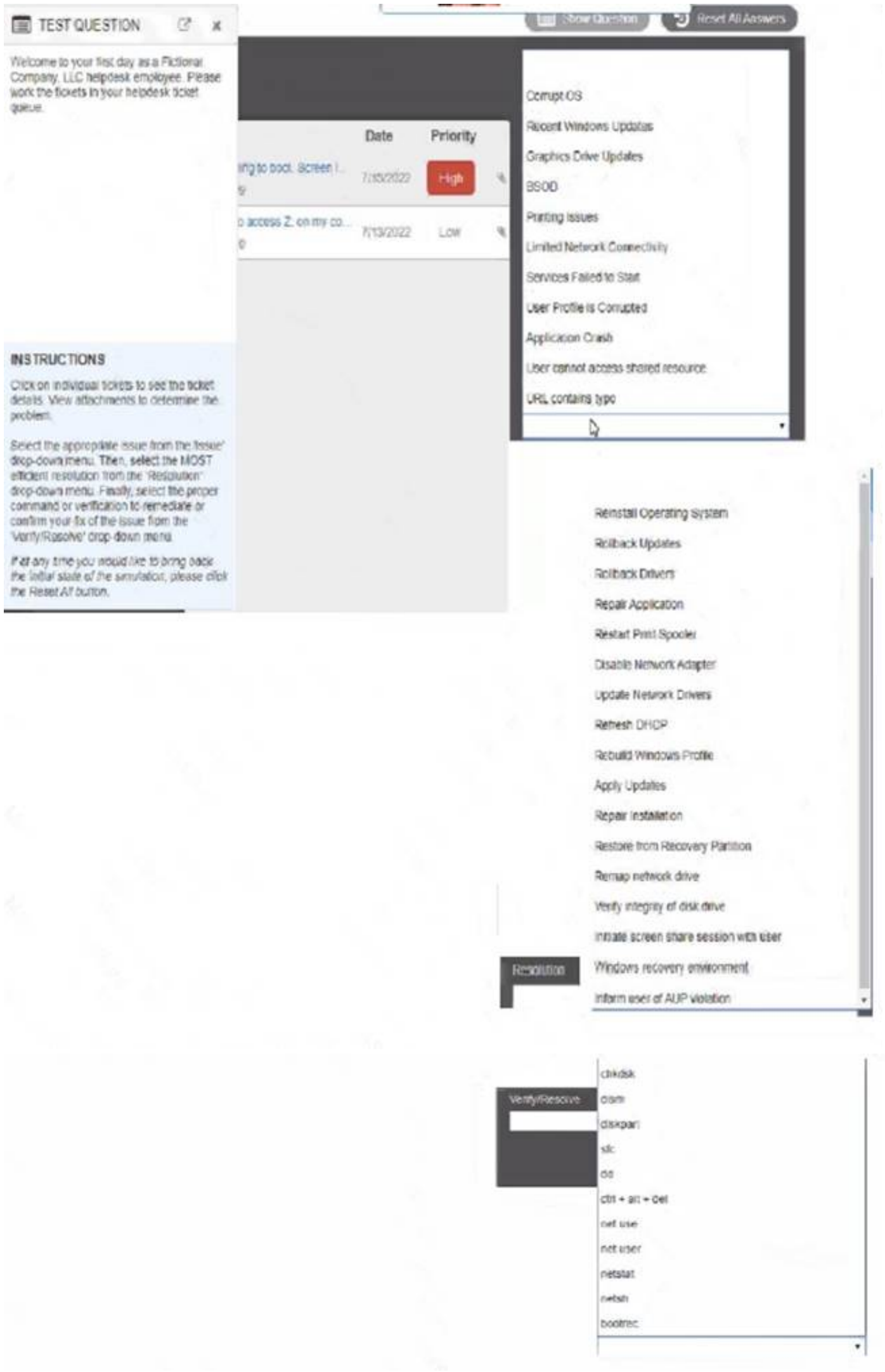
A. Windows Enterprise Edition
B. Windows Professional Edition
C. Windows Server Standard Edition
D. Windows Home Edition

Answer: B

Explanation:
The Windows Professional Edition is the most likely version that a technician would deploy for a user at a target corporation. This version of Windows is designed for business use and provides the necessary features and capabilities that a user would need to access the corporate domain, such as email and shared drives.

NEW QUESTION 74
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.

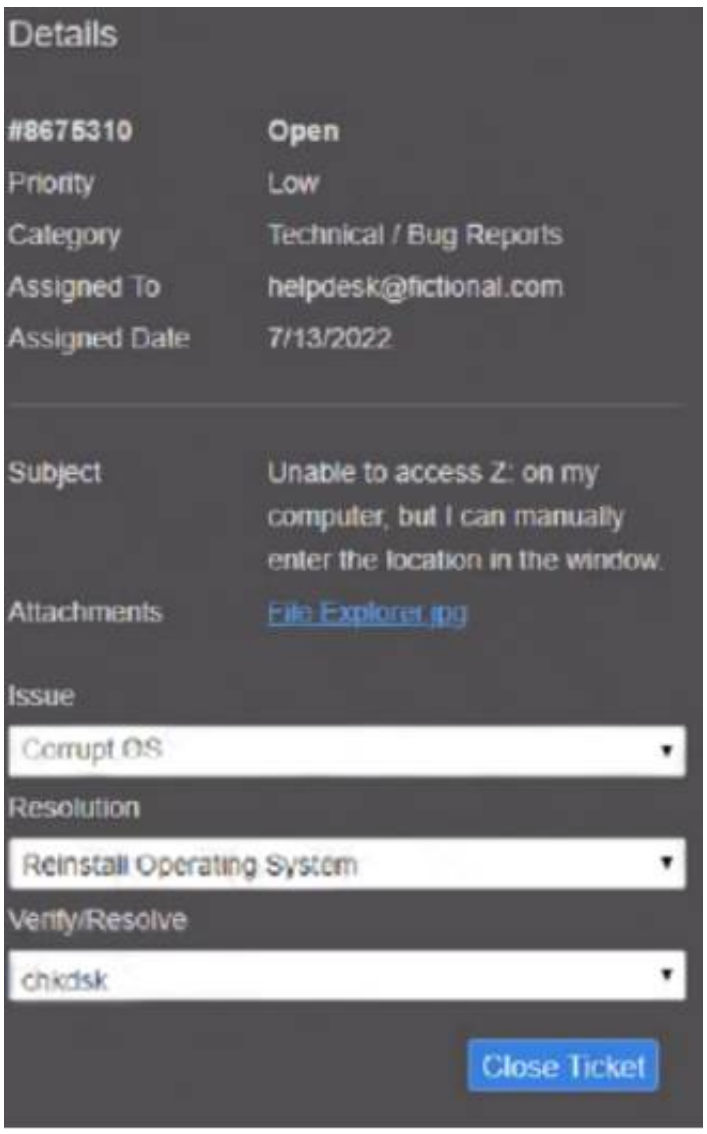




A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated



NEW QUESTION 75
A technician is setting up a backup method on a workstation that only requires two sets of tapes to restore. Which of the following would BEST accomplish this task?

A. Differential backup
B. Off-site backup
C. Incremental backup
D. Full backup

Answer: D

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

NEW QUESTION 76
A company wants to remove information from past users' hard drives in order to reuse the hard drives Witch 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 80
A technician suspects a rootkit has been installed and needs to be removed. Which of the following would BEST resolve the issue?

A. Application updates
B. Anti-malware software
C. OS reinstallation
D. File restore

Answer: C

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 83
A technician is setting up a desktop computer in a small office. The user will need to access files on a drive shared from another desktop on the network. Which of the following configurations should the technician employ to achieve this goal?

A. Configure the network as private
B. Enable a proxy server
C. Grant the network administrator role to the user
D. Create a shortcut to public documents

Answer: A

Explanation:
The technician should configure the network as private to allow the user to access files on a drive shared from another desktop on the network1

NEW QUESTION 86
A user created a file on a shared drive and wants to prevent its data from being accidentally deleted by others. Which of the following applications should the technician use to assist the user with hiding the file?

A. Device Manager
B. Indexing Options
C. File Explorer
D. Administrative Tools

Answer: C

Explanation:
The technician should use the File Explorer application to assist the user with hiding the file 1. The user can right-click the file and select Properties. In the Properties dialog box, select the Hidden check box, and then click OK 1.

NEW QUESTION 91
A technician is setting up a SOHO wireless router. The router is about ten years old. The customer would like the most secure wireless network possible. Which of the following should the technician configure?

A. WPA2 with TKIP
B. WPA2 with AES
C. WPA3withAES-256
D. WPA3 with AES-128

Answer: B

Explanation:
This is because WPA2 with AES is the most secure wireless network configuration that is available on a ten-year-old SOHO wireless router.

NEW QUESTION 93
An IT services company that supports a large government contract replaced the Ethernet cards on several hundred desktop machines to comply With regulatory requirements. Which of the following disposal methods for the non-compliant cards is the MOST environmentally friendly?

A. incineration
B. Resale
C. Physical destruction
D. Dumpster for recycling plastics

Answer: D

Explanation:
When disposing of non-compliant Ethernet cards, the most environmentally friendly option is to use a dumpster for recycling plastics. This method is the most effective way to reduce the amount of waste that is sent to landfills, and it also helps to reduce the amount of energy used in the production of new materials. Additionally, recycling plastics helps to reduce the amount of toxic chemicals that can be released into the environment.
According to CompTIA A+ Core 2 documents, "The most environmentally friendly disposal method for
non-compliant Ethernet cards is to use a dumpster for recycling plastics. This method is the most effective way to reduce the amount of waste that is sent to landfills, and it also helps to reduce the amount of energy used in the production of new materials."
https://sustainability.yale.edu/blog/how-sustainably-dispose-your-technological-waste

NEW QUESTION 96
A technician is setting up a new laptop. The company's security policy states that users cannot install virtual machines. Which of the following should the technician implement to prevent users from enabling virtual technology on their laptops?

A. UEFI password
B. Secure boot
C. Account lockout
D. Restricted user permissions

Answer: B

Explanation:
A technician setting up a new laptop must ensure that users cannot install virtual machines as the company's security policy states One way to prevent users from enabling virtual technology is by implementing Secure Boot. Secure Boot is a feature of UEFI firmware that ensures the system only boots using firmware that is trusted by the manufacturer. It verifies the signature of all bootloaders, operating systems, and drivers before running them, preventing any unauthorized

modifications to the boot process. This will help prevent users from installing virtual machines on the laptop without authorization.

NEW QUESTION 99
Which of the following is MOST likely contained in an EULA?

A. Chain of custody
B. Backup of software code
C. Personally identifiable information
D. Restrictions of use

Answer: D

Explanation:
An EULA (End-User License Agreement) is a legally binding contract between a software supplier and a customer or end-user, generally made available to the customer via a retailer acting as an intermediary. A EULA specifies in detail the rights and restrictions which apply to the use of the software. Some of the main terms included in an EULA are the terms and scope of the license, any licensing fees, warranties and disclaimers, limitation of liability, revocation or termination of the license, and intellectual property information and restrictions on using the license (e.g. modification and copying1)
https://www.termsfeed.com/blog/eula-vs-terms-conditions/

NEW QUESTION 103
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 108
A technician found that an employee is mining cryptocurrency on a work desktop. The company has decided that this action violates its guidelines. Which of the following should be updated to reflect this new requirement?

A. MDM
B. EULA
C. IRP
D. AUP

Answer: D

Explanation:
AUP (Acceptable Use Policy) should be updated to reflect this new requirement. The AUP is a document that outlines the acceptable use of technology within an organization. It is a set of rules that employees must follow when using company resources. The AUP should be updated to include a policy on cryptocurrency mining on work desktops

NEW QUESTION 111
.....

Relate Links

100% Pass Your 220-1102 Exam with Exambible Prep Materials

https://www.exambible.com/220-1102-exam/

Contact us

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

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