Exam Report: C.7 CompTIA 220-902 Certification Practice Exam

Candidate: Stangl, Thomas (Email: tstangl@ciat.edu)

View results by: ◯ Objective Analysis   ⦿ Individual Responses

Individual Responses

▼ **Question 1:**   Incorrect

You have a laptop running Windows 10. User Account Control (UAC) has been disabled.

How would you re-enable UAC on the laptop? (Select two. Each choice is a possible answer.)

☐ In the Control Panel, select System and Security, then System. Click System protection.

☐ In the Control Panel, select User Accounts, then Credential Manager.

☐ In the Control Panel, select System and Security, then System. Click Advanced system settings.

➡ ☐ In the Control Panel, select System and Security, then Security and Maintenance.

➡ ☐ In the Control Panel, select User Accounts, then User Accounts.

Explanation

To configure UAC in Windows 10:

- In Control Panel, go to User Accounts.
- Select User Accounts, then Change User Account Control settings.
- In the Control Panel, go to System and Security.
- Select Security and Maintenance > Security, then select Change settings under User Account Control.

You can also use the Change User Account Control settings link in System and Security. Edit the local security policy to configure UAC and control settings not available through the Control Panel.

References

LabSim for PC Pro, Section 9.4.
[pcpro2016_all_questions_en.exm WINDOWS_APP_01]

▼ **Question 2:**   Incorrect

The sales engineers in your organization use virtual machines to model deployments in the lab prior to actually implementing them in your customers' physical environments. You are concerned that a malicious insider could gain access to the sensitive data on these virtual machines. What should you do? (Select two.)

☐ Configure the hypervisor to use full virtualization.

➡ ☐ Disable the USB ports on the hypervisor hardware.

☐ Configure the hypervisor to use paravirtualization.

➡ ☐ Use file and folder permissions to restrict access to the virtual hard disk files.

☐ Create snapshots of each virtual machine on a regular schedule.

Explanation

Virtual machine portability represents a security issue. Because virtual machines are easy to copy, an attacker, such as a malicious insider with a USB drive, can very easily make a copy of a virtual machine that contains proprietary or sensitive information. To prevent this, you should implement file system and share permissions that restrict access to the virtual machine disk files. You should lock the hypervisor host when not in use. You should also consider disabling the USB ports on the hypervisor host.

Full and paravirtualization are mechanisms that define how physical hardware is accessed by virtual machines running on a hypervisor host. Creating snapshots of the virtual machines

protects them from disasters and malware infections, but it doesn't secure the data within the virtual machines.

References

LabSim for PC Pro, Section 10.5.
[pcpro2016_all_questions_en.exm VIRTUAL_MACHINE_03]

▼ **Question 3:**   Incorrect

You have a Windows 7 computer that was recently upgraded from Windows XP. An installed application worked fine in Windows XP, but now does not run in Windows 7. You have checked the application vendor's website, but there is no update available.

Which options should you try to run the application? (Select two.)

➡ ☐ Run the application in compatibility mode.

☐ Run the application in its own memory space.

☐ Make all users who need to run the application members of the local Administrators group.

➡ ☐ Run the application in XP Mode.

Explanation

You can try two options:

• Use the compatibility mode in Windows to run older applications as if they were running under a different operating system version. Older applications are often written to require full system access, which is not allowed on Windows Vista because of UAC. Compatibility mode creates a shim or a layer that makes the application think it has access to the system that is typically denied in Windows 7.
• Run the application in XP Mode. Windows XP Mode (XPM) is a virtual machine package for Windows Virtual PC that provides a pre-installed, licensed copy of Windows XP Professional that you can use to run XP applications.

Granting users administrative privileges gives them rights to the entire system, not just to the single application. On Windows 7, most applications already run in a separate memory space.

References

LabSim for PC Pro, Section 9.14.
[pcpro2016_all_questions_en.exm SYS_ERROR_07]

▼ **Question 4:**   Incorrect

Which of the following forms of networking is highly susceptible to eavesdropping (data interception) and must be secured accordingly?

○ ISDN

○ Dial-up

○ DSL

○ Satellite

➡ ○ Wireless

Explanation

All forms of networking are potentially vulnerable to eavesdropping. Wireless networks by definition broadcast network transmissions openly and therefore can be detected by outsiders. Subsequently wireless networks should maintain data encryption to minimize the risk of transmitting information to unintended recipients.

References

LabSim for PC Pro, Section 12.8.
[pcpro2016_all_questions_en.exm ENCRYPT_05]

▼ **Question 5:**   Incorrect

You're using a Linux distribution that uses RPM for package management. Which command would you use to install **httpd**, the Apache HTTP Server package, and all its dependencies?

○ apt-get update httpd

○ apt-get install httpd -dep

○ apt-get install httpd

○

⭕ yum update httpd

⭕ ps -e

⭕ ps -ef

⭕ yum install httpd -dep

➡ ⭕ yum install httpd

Explanation

On a Linux distribution that uses RPM for package management, entering yum install httpd at the command line will install the Apache HTTP Server package and all its dependencies. YUM automatically locates and downloads RPM packages for you by searching one or more repositories on the Internet. It can install a software package and all of its dependencies at the same time.

References

LabSim for PC Pro, Section 9.7.
[pcpro2016_all_questions_en.exm LINAPP_01]

▼ **Question 6:**   Incorrect

You manage over 100 desktop computers, all currently running Windows Vista. You recently purchased replacement computers that have Windows 10 pre-installed. You want to move user data and settings from the old computers to the new computers.

Which tool should you use?

⭕ File Settings and Transfer Wizard

➡ ⭕ User State Migration Tool

⭕ Windows 10 Upgrade Assistant

⭕ Windows Easy Transfer

Explanation

You should choose the User State Migration Tool (USMT) when you need to perform large-scale migrations or need greater control over the migration process.

The Windows Easy Transfer wizard is best suited for small scale migrations. (It is not the appropriate choice for large-scale deployments). Legacy Windows XP systems used the File and Settings Transfer Wizard to transfer user profiles and data. You use the Upgrade Assistant tool to determine your computer's hardware readiness for Windows 10.

References

LabSim for PC Pro, Section 10.4.
[pcpro2016_all_questions_en.exm WINDOWS_POSTINSTALL_06]

▼ **Question 7:**   Incorrect

Which Windows tool lets you perform automatic backups at regular times (such as on specific days at specific times)?

⭕ Task Manager

➡ ⭕ Task Scheduler

⭕ Event Manager

⭕ Disk Management

Explanation

Use the Task Scheduler to schedule actions (such as a backup) to occur on a regular basis. You can use the Schedule option in Backup and Restore in Control Panel to schedule when backups occur. (This approach actually creates a scheduled task.) You use Task Manager to view current operating statistics such as the running processes and CPU and memory usage. You use Disk Management to manage hard disks, partitions, and volumes on your storage devices.

References

LabSim for PC Pro, Section 9.10.
[pcpro2016_all_questions_en.exm REGULAR BACKUPS_02]

▼ **Question 8:**   Incorrect

Mary reports that an application's shortcut icon no longer launches the application. You check your documentation and find that you have installed a new disk drive in her computer. What should you do first so Mary can run the application?

○ Download and install any necessary application updates.

➡ ○ Check the shortcut properties to make sure it is pointing to the correct file location.

○ Remove the disk drive you installed earlier.

○ Give Mary additional permissions to the application's files and directories.

Explanation

The first thing to try would be to verify that the shortcut is pointing to the correct location. Installing a new disk drive might have modified the drive letters, thereby making the shortcut path invalid.

References

LabSim for PC Pro, Section 9.14.
[pcpro2016_all_questions_en.exm TRB_OS_10]

▼ **Question 9:**   Incorrect

What is the surest way to prevent the loss of important information on your mobile device if it is lost, stolen, destroyed, or there is a natural disaster?

○ Don't put important information on your mobile device.

➡ ○ Configure your device to remotely backup important data to the Cloud.

○ Configure your device to backup important data to your personal computer.

○ Only use apps, such as email apps, that store data on the app provider's servers.

Explanation

The surest way to prevent the loss of important information on your mobile device is to configure your device to remotely backup important data to the Cloud.

Backing up data to your personal computer is not a bad idea, but if there's a natural disaster your data is safer in the Cloud than it is on a single machine that could be damaged in the same disaster that affects your mobile device. Not putting important information on your mobile device is a practical impossibility, as is only using apps that store data (like messages in gmail) on the app provider's servers.

References

LabSim for PC Pro, Section 8.8.
[pcpro2016_all_questions_en.exm MOBTRB_03]

▼ **Question 10:**   Incorrect

Which of the following will improve the security of sensitive information on your device if it is lost or stolen? (Select all that apply.)

➡ ☐ Locator applications

☐ Keeping up to date with OS updates and patches

➡ ☐ A screen lock

☐ Anti-malware software

☐ Remote backup

➡ ☐ Remote wipe

Explanation

Being able to do a remote wipe of your device will keep sensitive information from falling into the wrong hands if your mobile device is lost or stolen. Having a screen lock will help keep casual users from getting access to your device, but determined hackers can find ways around a screen lock. Locator applications might help you find your device, before a determined hacker does, if you misplace it.

Keeping the operating systems up to date with the latest updates and patches will not protect your device if it falls into a determined hacker's possession. A remote backup is an essential disaster recovery solution but will not prevent hacker exploitation or virus infection. Being up to date and having anti-malware apps, for Android devices, will note protect your device in a determined hacker's possession.

References

[pcpro2016_all_questions_en.exm MOBILE_SEC_02]

▼ **Question 11:**   Incorrect

When you load a partition management utility on a workstation running an OEM version of Windows 8.1, you notice that there is a hidden partition located at the beginning of the workstation's hard drive. You decide to delete it to free up space on the drive.

Should you do this?

    ◯ No, this is your system's swap partition.

➡ ◯ No, this is the system's recovery partition.

    ◯ Yes, you can safely delete this partition.

    ◯ No, this is your system's parallel installation partition.

Explanation

You shouldn't delete this partition because it is the workstation's recovery partition. Many computer manufacturers create a hidden partition on the hard disk drive that contains a base image of the Windows system. You can use a utility provided by the manufacturer to restore your system to its original state when it was shipped from the factory using the image in the recovery partition.

References

LabSim for PC Pro, Section 9.12.
[pcpro2016_all_questions_en.exm WINDOWS_RESTORE_03]

▼ **Question 12:**   Incorrect

What is the purpose of an MSDS?

    ◯ It prevents dust from accumulating on electrical equipment.

    ◯ It protects the service technician from large voltages.

➡ ◯ It documents how to safely handle and dispose of hazardous materials.

    ◯ It monitors the potential for electrostatic discharge.

Explanation

A Material Safety Data Sheet (MSDS) documents how to safely handle and dispose of hazardous materials.

References

LabSim for PC Pro, Section 2.1.
[pcpro2016_all_questions_en.exm PC 2016 MSDS]

▼ **Question 13:**   Incorrect

To protect your Windows 7 system, you've used System Restore to automatically protect your system using restore points. You've also used Backup and Restore in Control Panel to configure a nightly backup of your user's data files. Will this adequately protect your system in the event of a hard disk failure?

    ◯ No, you need enable previous file versions in System Restore.

    ◯ No, you need to implement a RAID 0 array to protect your data.

➡ ◯ No, you need to create an image of your Windows system as well.

    ◯ Yes, your workstation system is protected.

Explanation

You also need to create a system image in addition to a backup of your user data. This will allow you to restore your windows system and your user data in the event of a disk failure. Using a RAID 0 array or implementing previous file versions will not protect your user data or the Windows system in the event of a disk failure.

References

LabSim for PC Pro, Section 9.10.
[pcpro2016_all_questions_en.exm SYSTEM RESTORE_02]

▼ **Question 14:**   Incorrect

You have a computer that runs Windows 10. Where would you go to verify the system has recognized the anti-malware software installed on the system?

○ Windows Firewall

○ System

○ Network and Sharing Center

➡ ○ Security and Maintenance

Explanation

Use Security and Maintenance in Control Panel to check the current security status of your computer. Security and Maintenance displays whether you have anti-malware, firewall, and automatic updates configured.

Use the firewall to open and close firewall ports. Use System to perform tasks such as viewing system information and enabling Remote Desktop. Use the Network and Sharing Center to view the status of your network connections.

References

LabSim for PC Pro, Section 12.6.
[pcpro2016_all_questions_en.exm MALWARE_08]

▼ **Question 15:**   Incorrect

What is required to control access to the file system using file and folder permissions on a Windows-based computer?

➡ ○ NTFS-formatted partition

○ EFS

○ FAT32-formatted partition

○ Ext4-formatted partition

Explanation

File permissions are only available under Windows for files on a partition formatted with NTFS, not FAT32. The Encrypting File Service (EFS) with Windows encrypts individual files. The Ext4 file system is used on Linux systems.

References

LabSim for PC Pro, Section 5.5.
[pcpro2016_all_questions_en.exm NTFS FEATURES]

▼ **Question 16:**   Incorrect

To increase security on your company's internal network, the administrator has disabled as many ports as possible. Now, however, you can browse the Internet, but you are unable to perform secure credit card transactions when making purchases from ecommerce websites.

Which port needs to be enabled to allow secure transactions?

○ 80

○ 21

➡ ○ 443

○ 23

○ 69

Explanation

To perform secure transactions, SSL on port 443 needs to be enabled. HTTPS uses port 443 by default.

References

LabSim for PC Pro, Section 12.10.
[pcpro2016_all_questions_en.exm FIREWALL_03]

▼ **Question 17:**   Incorrect

Which of the following networking devices or services prevents the establishment of VPN connections in most situations?

○ Switch

○ Firewall

○ Router

➡ ○ NAT

Explanation

NAT performs network address translation on all communications going in our out of a network. For this reason, the external IP address seen for a system inside of the NAT network is not the real IP address assigned to that system. This prevents the use of VPN protocols.

References

LabSim for PC Pro, Section 12.12.
[pcpro2016_all_questions_en.exm VPN_02]

▼ **Question 18:**   Incorrect

While using a Windows 8.1 system, you accidentally downloaded and installed a malware package from a phishing email exploit. You were able to reboot the system into Safe Mode and use System Restore to revert the system to point in time before the malware infection occurred.

Given this information, which of the following are true? (Select two.)

☐ You must restore your user data from backup.

➡ ☐ You must reinstall any applications that were installed after the restore point was taken.

☐ The applications installed on the system were not affected when it was reverted to the restore point.

☐ All files created or modified since the restore point was created must be restored from backup.

➡ ☐ Your user files were not affected when the system was reverted to the restore point.

Explanation

After reverting the system to a prior restore point in this scenario, the following facts are true:

• Your user files were not affected when the system was reverted to the restore point.
• You must reinstall any applications that were installed after the restore point was taken.

On Windows 8.1 and later, restore points contain snapshots of system files, registry settings, program files, and any other batch, script, or executable files. When you restore a system to a restore point, previous settings are restored, while subsequent changes are removed. For example, any applications installed after the restore point was created are no longer installed. However, user data is not affected when reverting to a restore point. Any changes made to user data after a restore point is created is retained if the restore point is restored.

References

LabSim for PC Pro, Section 9.11.
[pcpro2016_all_questions_en.exm RT SYSTEM RESTORE 02]

▼ **Question 19:**   Incorrect

You work at the IT Help Desk in your company. An employee calls to report a problem with her workstation and a service ticket is assigned to you. You respond to the service ticket immediately and arrive at the employee's workstation within minutes; however, when you begin speaking to her, you can't understand what she is saying because she is speaking Spanish, and you do not understand Spanish.

What should you do?

○ Use hand gestures to communicate

➡ ○ Find an interpreter

○ Ignore the user and start working on the computer

○ Walk away and assign the problem to someone else

Explanation

If you do not understand the language of a customer, then find an interpreter before solving the problem. Refusing to help will most-likely confuse, irritate, or offend the customer. You may be able to solve the problem without talking to the customer, but this action might take longer to discover the problem, and does not reflect professionalism in the workplace. Using hand gestures will most likely not work at all for technical communications.

LabSim for PC Pro, Section 2.2.
[pcpro2016_all_questions_en.exm PROFESSIONALISM 12]

▼ **Question 20:**   Incorrect

🖥 To answer this question, complete the lab using information below.   [**Launch Lab**]

You did not complete the lab correctly.

You work as the IT Administrator for a small corporate network. The
receptionist, Maggie Brown, uses an iPad to manage employee schedules and
messages. Her email settings on the device are configured to communicate with
an IMAP mail server over insecure port 143.

Also, you have just deployed a new wireless access point called CorpNet and
Maggie needs to connect using the new password.

1. Your first task is to use the **Mail, Contacts, Calendars** configuration
   option to go to Maggie Brown's email account settings and change the
   advanced configuration to **Use SSL** to securely communicate with the
   IMAP server over server port **993**.
2. Your second task is to connect Maggie to the new CorpNet wireless
   access point through the Wi-Fi configuration. Type in the password,
   @CorpNetWeRSecure!& for the new WI-FI connection.

References

LabSim for PC Pro, Section 8.5.
[pcpro2016_all_questions_en.exm IPADEMAIL]

▼ **Question 21:**   Incorrect

You have a computer where a removable disk drive has been formatted with NTFS. You want the
drive to use FAT32 to be compatible with more operating systems. The drive is currently
configured using drive letter D:. What should you do?

○ Back up the data on the D: drive. Run convert.exe.

○ Upgrade the disk to a dynamic disk.

➡ ○ Back up the data on the D: drive. Reformat the D: drive using FAT32. Restore the data.

○ Back up the data on the D: drive. Run format /fs:NTFS.

Explanation

The only way to go from NTFS to FAT32 is to reformat the drive. Because reformatting destroys
all data, you should back up the drive before formatting, then restore the data after formatting
the drive.

References

LabSim for PC Pro, Section 10.3.
[pcpro2016_all_questions_en.exm CONVERT TO FAT32]

▼ **Question 22:**   Incorrect

A small business named BigBikes, Inc. has hired you to evaluate their wireless network security
practices. As you analyze their facility, you note the following:

• They use an 802.11a wireless network.
• The wireless network SSID is set to BWLAN.
• The wireless network is not broadcasting the network SSID.
• The wireless network uses WPA2 with AES security.
• Omni-directional access points are positioned around the periphery of the building.

Based on this information, what should you recommend your client do to increase their wireless
network security?

○ Configure the wireless network to use WEP security.

○ Upgrade to an 802.11g wireless network.

➡ ○ Implement directional access points.

○ Change the SSID to something similar to BigBikeInc.

○ Enable SSID broadcast.

Explanation

You should recommend that they implement directional access points along the periphery of the building. Using omni-directional APs in these locations can cause the wireless network radio signal to emanate outside the building, making it readily available to malicious individuals.

Enabling SSID broadcasts and using an SSID that is easily identifiable reduces the security of the wireless network; as would switching to WEP security. Switching to an 802.11g network offers no speed or security benefits and would require retrofitting all wireless equipment in the organization.

References

LabSim for PC Pro, Section 12.9.
[pcpro2016_all_questions_en.exm SECURITY_BEST_07]

▼ **Question 23:**   Incorrect

You are working at the command line and want to add the Read-only attribute to a file and remove the Hidden attribute. Which command would you use?

○ attrib add r remove h

○ attrib +ro -h

➡ ○ attrib +r -h

○ attrib /add r /remove /h

Explanation

Use attrib +r -h to add the Read-only attribute and remove the Hidden attribute.

References

LabSim for PC Pro, Section 11.2.
[pcpro2016_all_questions_en.exm FILEMAN_11]

▼ **Question 24:**   Incorrect

You're working on a Mac computer that has an issue with a non-responsive application. You need to stop the application using the Force Quit feature.

Which of the following keyboard shortcuts can be used to access the Force Quit feature?

○ **Command+Esc**

○ **Command+Q**

○ **Command+Spacebar**

➡ ○ **Command+Option+Esc**

Explanation

Force Quit can be accessed from the Apple menu or the keyboard shortcut
Command+Option+Esc. Force Quit is used to stop non-responsive processes and applications. It can also be used to restart the Finder service.

References

LabSim for PC Pro, Section 1.6.
[pcpro2016_all_questions_en.exm FORCE QUIT]

▼ **Question 25:**   Incorrect

Match the Mac key labels on the left with the corresponding Mac key descriptions on the right.

The primary modifier key on Apple systems, used like the Ctrl key on a Windows system

C

Primarily used for text document navigation

D

Used for application and navigation shortcuts

A

Typically only found on Apple notebooks and is used to access the F1–F12 keys on the keyboard

B

Explanation

The *Command* key is the primary modifier key on Apple systems. For users familiar with Windows systems, the Command key can be thought of as the Ctrl key.

The *Option* key is used for application shortcuts and navigation shortcuts. For example, Option+Right/Left Arrow navigates between words in a text document.

The *Control* key is primarily used for text document navigation. For example, Control+H deletes the character to the left of the cursor.

The *Fn* key is typically only found on Apple notebooks and is used to access the F1–F12 keys on the keyboard.

References

LabSim for PC Pro, Section 1.6.
[pcpro2016_all_questions_en.exm MAC_KEYS]

▼ **Question 26:**   Incorrect

On Windows 10, using Storage Spaces eliminates the need for which of the following tasks? (Select two.)

- ☐ Creating RAID arrays
- ☐ Formatting hard drives
- ➡ ☐ Repartitioning drives
- ☐ Running defragmentation
- ➡ ☐ Resizing volumes
- ☐ Using Disk Cleanup

Explanation

Storage spaces eliminates the need for such tasks as:

- Repartitioning drives
- Resizing volumes
- Backing up data in order to repartition

References

LabSim for PC Pro, Section 5.8.
[pcpro2016_all_questions_en.exm STORSPACE_02]

▼ **Question 27:**   Incorrect

On a Windows system, which Task Manager tab would you use to adjust the priority given to a specific program?

- ➡ ○ Details
- ○ Performance
- ○ Processes
- ○ App History
- ○ Services

Explanation

Use the Details tab to adjust the priority of a specific process (either application or service). The App History tab lets you monitor apps from the Microsoft Store that are running on the system. The Performance tab shows you overall system utilization and statistics. The Services tab lets you view all running services; you can use this tab to start and stop services. The Processes tab displays a list of running applications; you can use this tab to stop an application that is not responding.

References

LabSim for PC Pro, Section 9.1.
[pcpro2016_all_questions_en.exm WINDOWS_SYSTOOLS_06]

▼ **Question 28:**   Incorrect

Which of the following network services or protocols uses TCP/IP port 22?

- ○ IMAP4

- ○ NNTP

- ○ TFTP

➡ ○ SSH

Explanation

The Secure Shell (SSH) service uses TCP/IP port 22. SSH is a terminal emulation program which provides a secure authenticated connection to a remote system over the network. It is most commonly used with UNIX and Linux systems, but can be used on Windows as well.

The Trivial File Transfer Protocol (TFTP) is a connectionless service for downloading files from a remote system. TFTP uses TCP/IP port 69. The Network News Transfer Protocol (NNTP) is used to access and download messages from newsgroup servers. NNTP uses TCP/IP port 119. The Internet Message Access Protocol version 4 (IMAP4) is used to download email from remote servers. IMAP 4 uses TCP/IP port 143.

References

LabSim for PC Pro, Section 9.5.
[pcpro2016_all_questions_en.exm REMOTE_02]

▼ **Question 29:**   Incorrect

You have a workstation running a 64-bit version of Windows 8.1 Professional that you would like to upgrade to Windows 10 Professional. You want to perform the upgrade with the least amount of effort and cost.

What should you do?

- ○ Purchase a 32-bit full version of Windows 10; perform an in-place upgrade.

- ○ Purchase a 64-bit upgrade version of Windows 10; perform a custom installation.

➡ ○ Purchase a 64-bit upgrade version of Windows 10; perform an in-place upgrade.

- ○ Purchase a 64-bit full version of Windows 10; perform a custom installation.

Explanation

You can purchase a 64-bit upgrade version of Windows 10 when moving from Windows 7. In this scenario, you can perform an in-place upgrade because you are moving to the same or higher edition.

If you were moving to a lower edition (such as a Home edition), you would need to perform a new installation. You can't upgrade from a 64-bit version of Windows to a 32-bit version of Windows.

References

LabSim for PC Pro, Section 10.2.
[pcpro2016_all_questions_en.exm WINDOWS_PREINSTALL_10]

▼ **Question 30:**   Incorrect

You are the administrator of a Linux server. Following best practices for system security and effective administration, you always login to the system with a standard non-root user account. You only elevate your privileges to root user level when you need to do an administrative task.

What do you enter at the command prompt that will, by default, switch you to the root user and require you to enter the root password?

| | su - |

Explanation

At the command prompt, enter **su −** (su followed by a space and a dash) and the system will

switch you to the root user and require you to enter the root password. You will then be able to perform tasks that require root user administrative privileges. After completing these tasks, you should log out as root and return to the standard user account by entering **exit**.

References

LabSim for PC Pro, Section 11.5.
[pcpro2016_all_questions_en.exm LINUX_FILES_06]

▼ **Question 31:**   Incorrect

You need to configure a Windows workstation with the IP address of the proxy server for your network. Click the tab in the Internet Properties window that you would use to do this.
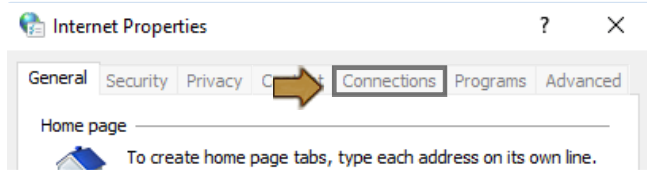
Explanation

To configure the IP address of the proxy server, go to Control Panel and select Internet Options. Click the Connections tab and then select LAN settings. In the dialog displayed you can enable a proxy server for the LAN and then enter the proxy server's IP address and port number.

References

LabSim for PC Pro, Section 12.11.
[pcpro2016_all_questions_en.exm PROXY_05-PB]

▼ **Question 32:**   Incorrect

Which of the following protocols provides authentication and encryption services for VPN traffic?

    ◯ SSL

    ◯ TCP

    ◯ L2TP

➡ ◯ IPsec

Explanation

IPsec is a security implementation that provides security for all other TCP/IP based protocols. IPsec provides authentication through a protocol called IPsec Authentication Header (AH) and encryption services through a protocol called IPsec Encapsulating Security Payloads (ESP).

The Transmission Control Protocol (TCP) is a transport layer connection-oriented protocol that provides data transmission services. It is not a secure protocol, and relies on other measures, such as IPsec, to provide security. The Secure Sockets Layer (SSL) is an application layer protocol that is designed to secure network traffic from certain other protocols, such as Hypertext Transfer Protocol (HTTP) and Post Office Protocol version 3 (POP3). It does not provide security for protocols lower in the TCP/IP protocol stack, such as TCP and UDP. The Layer 2 Tunneling Protocol (L2TP) is a protocol used to encapsulate Point-to-Point protocol (PPP) traffic.

References

LabSim for PC Pro, Section 12.12.
[pcpro2016_all_questions_en.exm VPN_07]

▼ **Question 33:**   Incorrect

You're using the vi editor to manage a text file on a Linux system. You want to type new text into the file; when you type you want the existing text that comes after the cursor to be pushed down.

What mode do you need to be in to do this?

➡ ◯ Insert Mode

    ◯ Replace Mode

    ◯ Command Mode

    ◯ Text Mode

    ◯ Command Line Mode

Explanation

In the vi editor you need to switch to Insert Mode to be able to type new text in the file and have

existing text that comes after the cursor pushed down.

In Replace Mode, the existing text that comes after the cursor would be replaced when you typed new text. In Command Line Mode, you can enter commands to save the file and exit, exit the file without saving, save the file with a new name, etc. In Command Mode you can perform many useful editing tasks in this mode, such as cut and paste, copy and paste, deleting text, etc. There is no "Text Mode" in vi.

References

LabSim for PC Pro, Section 11.5.
[pcpro2016_all_questions_en.exm LINUX_FILES_01]

▼ **Question 34:**   Incorrect

In which of the following situations would restoring from a system image be the best option?

➡ ◯ You need to restore a Windows system after a catastrophic hard drive failure.

◯ You accidentally deleted several important e-mails and need to restore them.

◯ You need to restore several word processing files that were accidentally deleted from your Documents folder.

◯ You recently installed a new application and now the system behaves erratically.

Explanation

Restoring the system using a system image would be the appropriate way to restore a system after a catastrophic hard disk failure.

Using a restore point would be best suited to a situation where you've installed a misbehaving application or driver and need to revert the system to a prior state. You could use a system image to restore lost files, restore lost emails, or remove a misbehaving application, but it isn't the best option because you must restore the entire system. You can't choose individual items to restore. In addition, any changes to the system that were made since the image was created will be lost.

References

LabSim for PC Pro, Section 9.12.
[pcpro2016_all_questions_en.exm WINDOWS_RESTORE_06]

▼ **Question 35:**   Incorrect

Match the disk types on the left with the corresponding descriptions and features on the right. Each disk type may be used once, more than once, or not at all.

Support up to 128 volumes

Dynamic Disks

Use primary and extended partitions

Basic Disks

Supported by all operating systems

Basic Disks

Support volumes that use discontiguous disk space

Dynamic Disks

Store partitioning information in a hidden database on all such disks in the system

Dynamic Disks

Only support volumes made up of contiguous disk space

Basic Disks

Explanation

Basic disks include the following characteristics:

- Use primary and extended partitions
- Supported by all operating systems
- Only support volumes made up of contiguous disk space

Dynamic disks include the following characteristics:

- Support up to 128 volumes
- Support volumes that use discontiguous disk space
- Store partitioning information in a hidden database on all such disks in the system

References

LabSim for PC Pro, Section 5.5.
[pcpro2016_all_questions_en.exm DISK TYPES]

▼ **Question 36:**   Incorrect

You provide desktop support at the branch office of a bank. One of the Windows workstations you manage is used by a bank employee to set up new customer accounts and fill out customer loan applications. Each user account on the system has been assigned a strong password. A cable lock has been installed to prevent it from being stolen.

What else could you do to increase the security of this system? (Select two.)

☐ Move the system to a locked room

☐ Disable the network jack to which the system is connected

➡ ☐ Remove the optical drive

➡ ☐ Disable all USB ports in the BIOS/UEFI firmware configuration

☐ Disconnect the system from the network

Explanation

Because this system is used in a public are in close proximity to customers, you should disable all USB ports in the BIOS/UEFI firmware configuration and also remove the optical drive if it is capable of burning optical discs. This will help prevent data from being stolen from the system if it is left unattended.

Because this system is used by bank personnel to service customers, it really can't be locked in a separate room. Likewise, disconnecting from the network or disabling its network jack would also make it unable to perform its required function.

References

LabSim for PC Pro, Section 12.3.
[pcpro2016_all_questions_en.exm PHYSICAL_SECURITY_09]

▼ **Question 37:**   Incorrect

You are configuring the local security policy of a Windows system. You want to require users to create passwords that are at least 10 characters long. You also want to prevent logon after three unsuccessful logon attempts. Which policies should you configure? (Select two.)

➡ ☐ Account lockout threshold

☐ Account lockout duration

☐ Enforce password history

➡ ☐ Minimum password length

☐ Password complexity

☐ Maximum password age

Explanation

Set the Minimum password length policy to require a password equal to or longer than the specified length. Set the Account lockout threshold policy to lock an account after the specified number of incorrect logon attempts. Incorrect policy choices for this scenario are: Enforce password history requires users to input a unique (previously unused) password when changing the password. This prevents users from reusing previous passwords. Maximum password age forces users to change the password after the specified time interval. Password complexity prevents using passwords that are easy to guess or easy to crack. It forces passwords to include letters, symbols, and numbers, and also requires passwords of at least 7 characters. However, you cannot configure a longer password length requirement with this policy. Account lockout duration determines the length of time the account will be disabled (in minutes). When the time period expires, the account will be unlocked automatically.

References

LabSim for PC Pro, Section 12.7.
[pcpro2016_all_questions_en.exm AUTHORIZATION_09]

▼ **Question 38:**   Incorrect

When conducting a forensic investigation, and assuming that the attack has been stopped, which of the following actions should you perform first?

➡ ○

      Document what's on the screen
- ⚪ Stop all running processes
- ⚪ Remove the hard drive
- ⚪ Turn off the system

Explanation

Preserving evidence while conducting a forensic investigation is a trade-off. Any attempt to collect evidence may actually destroy the very data needed to identify an attack or attacker. Of the choices given, documenting what's on the screen is the least intrusive and the least likely to destroy critical evidence. Halting, disassembling, or stopping running processes may erase evidence.

References

LabSim for PC Pro, Section 12.2.
[pcpro2016_all_questions_en.exm PC16 DOCUMENT THE SCREEN]

▼ **Question 39:**   Incorrect

Which of the following will help reduce the threat of static discharge when working on computer hardware? (Select two.)

➡ ☐ Store unused components in static shielding bags.

➡ ☐ Remain in physical contact with the server chassis at all times.

☐ Touch the leads on the PC components with your finger to dissipate any static charge.

☐ Reduce the humidity in the room to around 30%.

☐ Place your hardware on an insulating layer of 1/4 inch Styrofoam.

☐ Leave the system plugged into a grounded wall outlet.

Explanation

To reduce the threat of static discharge when working on PC hardware, you should:

- Store unused components in static shielding bags.
- Remain in physical contact with the server chassis at all times.

Reducing the humidity will actually increase the likelihood of a static discharge. Leaving the system plugged into a grounded wall outlet may theoretically reduce the likelihood of a static discharge, but it's also extremely dangerous and should never be done. Always unplug your systems before working on them. Using Styrofoam near computer components will increase the build up of static electricity and should be avoided. You should never touch the leads of a component. If a static discharge occurs, the current will be carried directly to the most sensitive parts of the component.

References

LabSim for PC Pro, Section 2.1.
[pcpro2016_all_questions_en.exm PC 2016 ESD1]

▼ **Question 40:**   Incorrect

Don is an accountant in the Finance department, and for the last several months has been testing an online accounting program. After speaking with his manager, Don receives permission to download a streamlined version of the software, which requires a local installation. After downloading, Don tries to install the application on his Windows 10 workstation, but the operating system does not allow it. Out of frustration, he calls the Help Desk. The Help Desk personnel comes to Don's machine and installs the application without issue.

Which of the following is the most likely reason Don could not install the application?

- ⚪ Insufficient disk space
- ⚪ Failed device driver
- ⚪ Incorrect service pack level
- ➡ ⚪ Insufficient permissions

Explanation

Most likely, Don cannot install the application because he has insufficient permissions. The Help Desk personnel has permissions to install applications, but Don does not. Insufficient space would keep an application from installing if it required more space than what is available, but in this case the Help Desk personnel was able to install it without issue. Device drivers are only needed

for devices connecting to the computer, such as a keyboard or mouse. Service packs generally contain security-related hotfixes and do not affect the ability to install legitimate applications.

References

LabSim for PC Pro, Section 9.14.
[pcpro2016_all_questions_en.exm TRB_OS_03]

▼ **Question 41:**   Incorrect

You have a computer that currently has Windows Vista installed. You want to upgrade the system to Windows 10. You want to retain as much of the application, user profile, and user data as possible. You want to perform the upgrade with the least amount of effort possible.

What should you do?

○ Perform an in-place upgrade of Windows Vista to Windows 10 using the existing hard drive. Boot into Windows 10 and run Scanstate, then run Loadstate.

➡ ○ Run Scanstate in Windows Vista. Perform a clean (custom) installation of Windows 10 on the existing hard drive. Boot into Windows 10 and re-install all applications. Run Loadstate.

○ Perform an in-place upgrade of Windows Vista to Windows 10 using the existing hard drive.

○ Run Scanstate in Windows Vista. Perform a clean (custom) installation of Windows 10 on the existing hard drive. Boot into Windows 10 and run Loadstate.

Explanation

Before performing the installation, run Scanstate to save settings from your existing Windows installation. When moving from Windows Vista to Windows 10, you must perform a clean (custom) installation; you cannot perform an in-place upgrade. Following the installation, you will need to re-install all applications. After you have re-installed all applications, run Loadstate to restore your previous settings and data to the new installation.

References

LabSim for PC Pro, Section 10.4.
[pcpro2016_all_questions_en.exm WINDOWS_POSTINSTALL_05]

▼ **Question 42:**   Incorrect

Following Windows installation, you enabled the built-in Administrator account. You remove the password for this account. You enable Remote Desktop on your computer using the default settings. From home, you try to access your computer using Remote Desktop using the Administrator account, but you are unable to log on. What should you do?

○ Unlock the Administrator account

○ Disable fast user switching on the computer

➡ ○ Configure a password for the Administrator account

○ Make the Administrator account a member of the Remote Desktop Users group

Explanation

When accessing shared folders or Remote Desktop on a network computer, the user account must have been configured with a password. User accounts with blank passwords cannot be used to gain network access to a computer. By default, members of the Administrators group are allowed Remote Desktop access. To allow non-administrators access, add them to the list of authorized users for Remote Desktop. The user accounts you specify are made members of the Remote Desktop Users group. Accounts are locked automatically through the account lockout settings when too many incorrect passwords have been entered. Fast user switching is only configurable on Windows XP and does not affect the ability to log on with Remote Desktop.

References

LabSim for PC Pro, Section 12.7.
[pcpro2016_all_questions_en.exm AUTHORIZATION_13]

▼ **Question 43:**   Incorrect

You want to use Hibernation on your Windows notebook. What does it need to have?

➡ ○ Enough free hard drive space

○ A minimum of 1 GB of RAM

○ A Pentium IV or better processor

○ UPS

Explanation

Hibernation saves everything that is in RAM to the hard drive. Therefore, you need at least as much free disk space as you have RAM. Hibernation does not depend on the processor capabilities or the amount of RAM. A UPS is used to supply power to a device if the regular AC power is interrupted.

References

LabSim for PC Pro, Section 8.3.
[pcpro2016_all_questions_en.exm NOTEBOOK_POWER_03]

▼ **Question 44:**   Incorrect

Which of the following devices can store large amounts of electricity even when unplugged?

➡ ○ CRT monitor

○ LCD monitor

○ DVD optical drive

○ Hard disk drive

Explanation

A cathode ray tube (CRT) can store large amounts of electricity even when unplugged. You should never open a CRT monitor, as the capacitors within the CRT can store enough electricity to be lethal. LCD monitors do not use large capacitors and are much safer to work on than CRT monitors (although the CCFL backlight has mercury vapor in it, which could be harmful if the tube is broken). Optical drives and hard disk drives do not store electricity in sufficient quantity to be harmful.

References

LabSim for PC Pro, Section 2.1.
[pcpro2016_all_questions_en.exm PC 2016 MONITOR SAFETY]

▼ **Question 45:**   Incorrect

You have an application that you would like to run every Monday at 3 p.m. on your Windows workstation. Which tool would you use to configure the application to run automatically?

➡ ○ Task Scheduler

○ Msconfig

○ Msinfo32

○ Services

○ Task Manager

Explanation

The Task Scheduler is a tool that you can use to automatically start an application or run a script based on events. Triggers identify conditions that start the task. Triggers include day and time, logon, and in response to other system events.

You use the Services MMC to view and manage services on your computer. You use the Msconfig utility to configure how the Windows operating system will boot. You use Msinfo32 to view system information. You can use Task Manager to configure startup applications, but you can't use it to automatically run an application at a specific time.

References

LabSim for PC Pro, Section 9.6.
[pcpro2016_all_questions_en.exm WINDOWS_APP_10]

▼ **Question 46:**   Incorrect

You need to configure settings for a USB printer that you have just connected to your Windows 7 system. Which option in Control Panel should you use to do this?

➡ ○ Hardware and Sound

○ System and Security

○ Appearance and Personalization

○ Network and Internet

Explanation

You can view (and configure) printers on Windows 7 by clicking on Hardware and Sound in Control Panel. The System and Security area in Control Panel is used to access the Action Center, configure the Windows Firewall, and configure automatic backups. Network and Internet is used to manage network connections. Appearance and Personalization is used to configure desktop themes and screen resolution.

References

LabSim for PC Pro, Section 9.1.
[pcpro2016_all_questions_en.exm WINDOWS_PREFS_08]

▼ **Question 47:**   Incorrect

To protect user data on a Windows 7 system, you've configured System Restore to automatically create restore points for the C:\ volume.

Given that your user profile data is stored in the default directory (C:\Users), will this strategy adequately protect your users' data?

➡️ ◯ No, you need to create a backup of your user data as well.

◯ No, you need to implement a RAID 0 array to protect your data.

◯ No, you need to enable File History.

◯ Yes, your workstation data is protected.

Explanation

Using restore points alone is an incomplete strategy for protecting user data. You should also use Backup and Restore in Control Panel to backup user data. This is because System Restore on Windows 7 maintains restore points (and prior file versions) on the same hard disk as the data being protected. In the event of a disk failure, all data will be lost, including restore points.

A RAID 0 array does not provide data redundancy. File History is not available on Windows 7 systems.

References

LabSim for PC Pro, Section 9.11.
[pcpro2016_all_questions_en.exm RT WINDOWS_RESTORE_01]

▼ **Question 48:**   Incorrect

Which of the following is most helpful in keeping a computer cool? (Select two.)

☐ Install a thermostat in the fan circuit.

➡️ ☐ Verify that cooling fans are not circulating air in the wrong directions.

➡️ ☐ Vacuum dust from the system regularly.

☐ Remove a slot cover from the back of the computer.

☐ Use a high-wattage power supply.

Explanation

Vacuuming dust from the system is critical for keeping the computer cool. In addition, verify that your cooling fans are blowing air in the right direction and are not working against each other. Do not remove any slot covers in an attempt to cool the computer. A lack of slot covers decreases the fan's ability to remove hot air from inside the computer.

References

LabSim for PC Pro, Section 2.4.
[pcpro2016_all_questions_en.exm PC 2016 KEEP COOL]

▼ **Question 49:**   Incorrect

Which of the following disk maintenance utilities optimizes the performance of your hard drive by verifying the file system integrity of a hard disk and fixing the errors it detects?

◯ Disk Defragmenter

➡️ ◯ Check Disk

◯ Disk Management

◯ Disk Cleanup

Explanation

Check Disk is a utility that verifies the file system integrity of a hard disk. Check Disk detects disk integrity errors and fixes them.

Disk Defragmenter optimizes the performance of your hard drive by joining fragments of files that are in different locations on your hard drive into a single location. The more information that is on the drive, the more time it will take to defragment the drive. Disk Cleanup helps manage disks by locating and disposing of files that can be safely removed from the disk. Disk Management is a tool for viewing, modifying, and creating partitions.
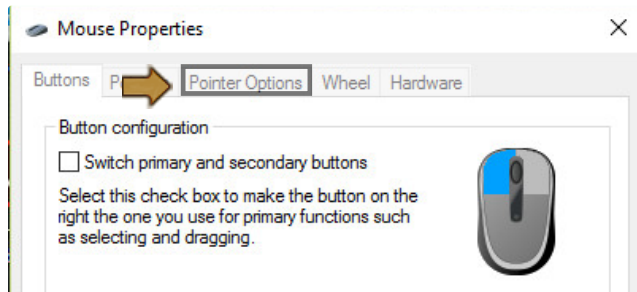
References

LabSim for PC Pro, Section 5.9.
[pcpro2016_all_questions_en.exm DISK MAINT UTILITIES_03]

▼ **Question 50:**   Incorrect

While using a new Windows system, you find that the mouse pointer tracks much more slowly on the screen than you would prefer. You want to increase the mouse pointer speed.

Click the tab you would use in the Mouse Properties window to do this.

Explanation

Mouse properties can be set in Control Panel by going to Hardware and Sound > Mouse. You use the Pointer Options tab to configure the pointer speed, snap-to, and visibility settings.

The Buttons tab configures the button configuration, double-click speed, and ClickLock settings. The Pointers tab configures the pointer scheme. The Wheel tab configures vertical and horizontal scrolling settings. The Hardware tab is used to configure driver settings.

References

LabSim for PC Pro, Section 9.2.
[pcpro2016_all_questions_en.exm RT MOUSE PREFS 01-PB]

▼ **Question 51:**   Incorrect

Which of the following describes a Man-in-the-Middle attack?

➡ ○ An attacker intercepts communications between two network hosts by impersonating each host.

○ A person over the phone convinces an employee to reveal their logon credentials.

○ An IP packet is constructed which is larger than the valid size.

○ Malicious code is planted on a system where it waits for a triggering event before activating.

Explanation

A Man-in-the-Middle attack is a technological attack where a malicious person intercepts network communications between two hosts, posing as the sender to the receiver and as the receiver to the sender.

Convincing an employee over the phone to reveal his logon credentials is an example of a social engineering attack. Constructing an IP packet which is larger than the valid size is a form of Denial of Service attack. Planting malicious code on a system where it waits for a triggering event before activating is a logic bomb.

References

LabSim for PC Pro, Section 12.13.
[pcpro2016_all_questions_en.exm TRB_SECURITY_09]

▼ **Question 52:**   Incorrect

Don is an accountant in the Finance department. For the last several months he has been testing an online accounting program. After speaking with his manager, Don received permission to download a streamlined version of the software which requires a local installation. After downloading, Don tried to install the application, but the operating system will not allow it. Out of

frustration, he called the Help Desk. The Help Desk personnel came to Don's machine and installed the application without issue.
Which of the following is the most likely reason Don could not install the application?

- ○ Insufficient system RAM
- ➡ ○ Insufficient permissions
- ○ Insufficient disk space
- ○ Incorrect service pack level
- ○ Failed device driver

Explanation

Most likely, Don cannot install the application because his user account has insufficient permissions. The Help Desk technician's user account has permissions to install applications, but Don does not.

Insufficient space would keep an application from installing if it required more space than what is available, but in this case the Help Desk personnel was able to install it without issue. Device drivers are only needed for devices connecting to the computer. Service packs generally contain security-related hotfixes and do not affect the ability to install legitimate applications.

References

LabSim for PC Pro, Section 9.6.
[pcpro2016_all_questions_en.exm WINDOWS_APP_12]

▼ **Question 53:**   Incorrect

Which of the following measures will make your wireless network less visible to the casual attacker performing war driving?

- ○ Implement WPA2 Personal
- ○ Implement MAC address filtering
- ➡ ○ Disable SSID broadcast
- ○ Change the default SSID
- ○ Use a form of authentication other than Open authentication

Explanation

Wireless access points are transceivers which transmit and receive radio signals on a wireless network. Each access point has a service set ID (SSID) which identifies the wireless network. By default, access points broadcast the SSID to announce their presence and make it easy for clients to find and connect to the wireless network. You can turn off the SSID broadcast to keep a wireless 802.11 network from being automatically discovered. When SSID broadcasting is turned off, users must know the SSID to connect to the wireless network. This helps to prevent casual attackers from connecting to the network, but any serious hacker with the right tools can still connect to the wireless network.

Using authentication with WPA2 helps prevent attackers from connecting to your wireless network, but does not hide the network. Changing the default SSID to a different value does not disable the SSID broadcast. Implementing MAC address filtering prevents unauthorized hosts from connecting to your WAP, but it doesn't disable the SSID broadcast.

References

LabSim for PC Pro, Section 12.9.
[pcpro2016_all_questions_en.exm NET_SEC_WIRELESS_03]

▼ **Question 54:**   Incorrect

A user needs to copy a file from an NTFS partition to a FAT32 partition. The file has NTFS permissions and the following attributes: Read only (R) and Encryption. When the folder is copied, which of the following is true?

- ○ None of the NTFS permissions or attributes are retained on the file.
- ➡ ○ The R attribute is retained on the file.
- ○ The R and encryption attribute are retained on the file.
- ○ Only the NTFS permissions are retained on the file.
- ○ The attributes and NTFS permissions are retained on the file.

Explanation

Only the Read only (R) attribute is retained, and not the encryption attribute, nor the NTFS permissions. The FAT32 file system only supports the following attributes: R, H, S, and A. When you copy files from an NTFS partition to a FAT32 partition, attributes not available under FAT32 do not remain with the file. Moving NTFS files to a non-NTFS partition removes the permissions.

References

LabSim for PC Pro, Section 11.3.
[pcpro2016_all_questions_en.exm NTFS_01]

▼ **Question 55:**   Incorrect

A user reports that her machine is behaving erratically. She suspects something is wrong because lately a firewall alert keeps indicating programs are trying to access the Internet, and several files have disappeared or have been renamed. What do you suspect is causing these problems?

○ Incorrect drivers

○ Faulty network card

➡ ○ Malware infection

○ Low system memory

Explanation

A firewall alert indicating programs are trying to access the Internet, and missing and renamed files are symptoms of a malware infection. Low system memory may also indicate a malware infection, but is not the cause of the symptoms. An incorrect driver may be to blame if a device does not work properly. A faulty network card would affect network communications, but would not affect files on the computer.

References

LabSim for PC Pro, Section 12.13.
[pcpro2016_all_questions_en.exm TRB_SECURITY_03]

▼ **Question 56:**   Incorrect

A user calls to report a problem. She is trying to install an application on a Windows 10 system, but cannot. In the past, she installed applications on her Windows XP system without any issues. Her user account has always been a member of the Power Users group. What do you suspect is causing the installation issue?

○ The operating system always denies changes to the registry settings.

➡ ○ Her group membership denies program installation on this operating system.

○ Her group membership must include the Users group.

○ The program is incompatible with this operating system.

Explanation

Users must have the correct permissions or rights to install applications. On Windows 2000 and XP, users who were members of the Power Users group could install applications as long as they didn't modify any system files. On Windows Vista and later, Power Users cannot install applications. In fact, the Power Users group is only included in modern versions of Windows for backwards compatibility. Users who are members of the Administrators group can install applications. The additional membership in the Users group is insufficient to install programs. All operating systems allow the modification of the registry settings if the user has sufficient permissions or rights.

References

LabSim for PC Pro, Section 9.14.
[pcpro2016_all_questions_en.exm TRB_OS_02]

▼ **Question 57:**   Incorrect

You have a compiler that compiles applications used in your business. You want to make sure that the compiler continues to receive adequate processor time, even if you open other applications. How can you adjust the amount of CPU attention given to that application?

○ Use Task Manager to modify the processor affinity.

➡ ○ Use Task Manager to modify the process priority.

○ Use the Services console to change the startup type to Automatic.

○

Use Task Manager to switch to the running application.

Explanation

Use Task Manager to configure the process priority. The priority controls how the system can delay or switch between processes. By default, the system typically gives a higher priority to a process that has active user input or interaction. Processes can continue to run in the background (i.e. when the user is not actively interacting with the application). Virus scanners, video compression, compilers, and backups are examples of processes that run in the background while you can continue working in a different application. If a background process has a priority that is too high, the system might seem slow and unresponsive when running other programs. The affinity identifies which processors or processor cores that the process can use. For example, you can configure a process to run only on one of the cores in a quad-core CPU. Switching to an application simply brings that application to the front where you can work with it. The service startup type identifies whether a service starts automatically when the system boots.

References

LabSim for PC Pro, Section 9.14.
[pcpro2016_all_questions_en.exm TRB_OS_08]

▼ **Question 58:**   Incorrect

Which command would you use to copy all files in a directory, including all subdirectories (as well as empty ones)?

   ○ copy /v

➡ ○ xcopy /e

   ○ copy /n

   ○ xcopy /s

Explanation

Use xcopy /e to copy directories and subdirectories, including empty ones. xcopy /s copies directories and subdirectories, but not empty ones. Use copy /n to copy a single directory with the short filenames. Use copy /v to verify the files after the copy.

References

LabSim for PC Pro, Section 11.2.
[pcpro2016_all_questions_en.exm FILEMAN_04]

▼ **Question 59:**   Incorrect

A security incident is currently occurring on the company network. You discover that the attack involves a computer system that is attached to the network. You're not sure yet exactly what kind of damage is being done to the network systems or data. What action should you take first?

➡ ○ Stop the attack and contain the damage by disconnecting the system from the network.

   ○ Document and photograph the entire scene of the crime including the current state of the attached computer system.

   ○ Examine the active computer system to analyze the live network connection, memory contents, and running programs.

   ○ Determine whether you have the expertise to conduct an investigation, or whether you need to call in additional help.

Explanation

The first step in responding to an incident should be to take actions to stop the attack and contain the damage. If the attack involves a computer system attached to the network, the first step might be to disconnect it from the network. Although you want to preserve as much information as possible to assist in later investigations, it is better to stop the attack, even if doing so alerts the attacker or results in the loss of evidence regarding the attack.

After containing the damage, subsequent steps you can take include, but are not limited to, the following:

   • Examine the active computer system to analyze the live network connection, memory contents, and running programs.
   • Document and photograph the entire scene of the crime including the current state of the attached computer system.
   • Determine whether you have the expertise to conduct an investigation, or whether you need to call in additional help.

References

LabSim for PC Pro, Section 12.2.
[pcpro2016_all_questions_en.exm FIRST STEP]

▼ Question 60:   Incorrect

Where are fonts stored on a Windows 7 system?

➡️ ⭕ %systemroot%\Fonts\

⭕ %systemroot%\Documents and Settings\Fonts\

⭕ %systemdrive%\Fonts\

⭕ %systemdrive%\Documents and Settings\Fonts\

Explanation

On all versions of Windows, fonts are stored in the %systemroot%\Fonts\ directory. For Windows 7, %systemroot% is C:\Windows by default. The %systemdrive% variable identifies the drive where Windows is installed (by default the C:\ drive). The %systemdrive%\Documents and Settings\ folder holds user profiles for Windows 2000 and XP.

References

LabSim for PC Pro, Section 11.1.
[pcpro2016_all_questions_en.exm FILELOC_11]

▼ Question 61:   Incorrect

Which of the following provides security for wireless networks?

⭕ CSMA/CD

⭕ 802.11a

⭕ WAP

➡️ ⭕ WPA2

⭕ 802.3u

Explanation

Wi-Fi Protected Access (WPA) provides encryption and user authentication for wireless networks. Wired Equivalent Privacy (WEP) also provides security, but WPA is considered more secure than WEP. A wireless access point (WAP) is a hardware device, like a switch, that provides access to the wireless network. 802.11a is a wireless networking standard that defines the signal characteristics for communicating on the wireless network. CSMA/CD is a media access control method that controls when a device can communicate on the network.
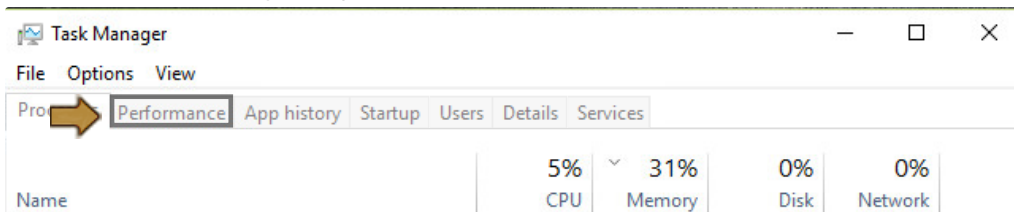
References

LabSim for PC Pro, Section 12.8.
[pcpro2016_all_questions_en.exm ENCRYPT_07]

▼ Question 62:   Incorrect

You need to use Task Manager to analyze memory utilization on a Windows system. For example, you need to see how much system RAM is currently in use and how much is available.

Click on the tab in Task Manager that you would use to do this.

Explanation

In this scenario, you would access the Performance tab and then select the Memory graph. When you do, various memory utilization statistics are displayed.

The Processes tab displays a list of running applications on the system. The App History tab displays performance statistics for apps from the Microsoft Store that are running on the system. The Startup tab displays a list of applications that are automatically launched at system boot. The Users tab displays utilization statistics for each user logged into the system. The Details tab displays extended information about each process running on the system. The Services tab is used to view information about the services configured on the system.

References

LabSim for PC Pro, Section 9.3.

[pcpro2016_all_questions_en.exm RT PERF MON 01-PB]
Question 63:   Incorrect

Which tool lets you automatically start an application or run a script based on triggers?

○ Event Viewer

➡ ○ Task Scheduler

○ Device Manager

○ Task Manager

Explanation

Use Task Scheduler to automatically start an application or run a script based on triggers. A trigger identifies conditions that start a task. Triggers include day and time, logon, and system events. Common tasks that are scheduled to run at regular intervals include backups, system virus scans, and system updates.

Use Task Manager to view current operating statistics such as the running processes and CPU and memory usage. Use Device Manager to manage hardware devices. Use Event Viewer to view logs about programs, system events, and security.

References

LabSim for PC Pro, Section 9.1.
[pcpro2016_all_questions_en.exm WINDOWS_SYSTOOLS_20]

Question 64:   Incorrect

Which file attribute identifies the file as having been modified since the last backup?

➡ ○ Archive

○ Hidden

○ Read only

○ Encrypted

Explanation

The Archive (A) attribute identifies if a file has been modified since the last backup. A file attribute is metadata that gives certain qualities to a file after the attribute has been assigned. The Read only (R) attribute marks a file as read-only meaning that the file cannot be altered by subsequent users. The encrypted attribute encrypts a file. The Hidden (H) attribute hides a file within the file system so it cannot be viewed or accessed by users that do not have access to its specific filename.

References

LabSim for PC Pro, Section 11.2.
[pcpro2016_all_questions_en.exm FILEMAN_14]

Question 65:   Incorrect

One of the Windows workstations you manage has three user accounts defined on it. Two of the users are limited users while the third (your account) is an administrative user. Each limited and administrative user has been assigned a strong password. File and folder permissions have been assigned to prevent users from accessing each other's files. What else could you do to increase the security of this system? (Select two.)

➡ ☐ Set a screensaver password.

➡ ☐ Disable autorun on the system.

☐ Change the two limited user accounts to restricted users.

☐ Enable the Guest account.

☐ Assign each user a simple password so they won't be tempted to write it down.

Explanation

You could increase the overall security of this system by:

- Disabling autorun on the system
- Setting a screensaver password

Enabling the Guest user account would decrease the security of the system as would assigning simple passwords to user accounts. There's no such thing as a restricted user on Windows

operating systems.
References

LabSim for PC Pro, Section 12.1.
[pcpro2016_all_questions_en.exm SECURITY_BEST_05]

▼ **Question 66:**   Incorrect

Which command will display a list of files and subdirectories in a directory?

- ○ list

- ○ md

- ○ cd

➡ ○ dir

- ○ ls

- ○ attrib

Explanation

Use the *dir* command to display a list of files and subdirectories in a directory.

You use the cd command to work with the current directory. You use the md (and mkdir) command to create a directory. You use the attrib command to change or view the attributes of one or more files. The ls command is used on Linux systems. List is not a command line command.

References

LabSim for PC Pro, Section 11.2.
[pcpro2016_all_questions_en.exm FILEMAN_20]

▼ **Question 67:**   Incorrect

Which of the following features is supplied by WPA2 on a wireless network? (Select two.)

➡ ☐ Authentication

- ☐ Refusal of client connections based on MAC address

- ☐ Identification of the network

- ☐ Filtering of traffic based on packet characteristics

- ☐ Centralized access for clients

➡ ☐ Encryption

Explanation

Wi-Fi Protected Access 2 (WPA2) provides encryption and authentication for wireless networks.

MAC address filtering allows or rejects client connections based on the hardware address. The SSID is the network name or identifier. A wireless access point (called an AP or WAP) is the central connection point for wireless clients. A firewall allows or rejects packets based on packet characteristics (such as address, port, or protocol type).

References

LabSim for PC Pro, Section 12.9.
[pcpro2016_all_questions_en.exm NET_SEC_WIRELESS_02]

▼ **Question 68:**   Incorrect

You need to protect the user data on a Windows 7 system.

Which tools could you use to do this? (Select two.)

- ☐ Bitlocker

- ☐ NTBackup

➡ ☐ Previous Versions

- ☐ File History

➡ ☐ Backup and Restore

Explanation

User data on a Windows 7 system can be protected using the following tools:

- Backup and Restore in Control Panel can be used to configure backups that run automatically on a specified schedule.
- Previous Versions works in conjunction with System Protection to store previous versions of user files within restore points.

File History is not available on Windows 7. Bitlocker is used to encrypt data, not back it up. NTBackup is an older backup utility that was provided on earlier versions of Windows. It is not available on Windows 7 or later.

References

LabSim for PC Pro, Section 9.10.
[pcpro2016_all_questions_en.exm RT WINDOWS BACKUP 05]

▼ **Question 69:**   Incorrect

Match each cloud computing definition on the left with the appropriate characteristic on the right. Each characteristic may be used once, more than once, or not at all.

Provides resources to a single organization

| Private cloud |

Combines public, private, and community cloud resources from different service providers

| Hybrid cloud |

Designed to be shared by several organizations

| Community cloud |

Provides computing resources that are accessible by the general public

| Public cloud |

Keeps one organization data separate and secure from any other organization using the same service provider

| Private cloud |

Explanation

In a public cloud, computing resources such as platforms, applications, and storage are made available to the general public by a cloud service provider.

A private cloud provides resources to a single organization. The cloud service provider ensures the organization's data is kept separate and secure from any other organization using the same service provider.

A community cloud is designed to be shared by several organizations.

A hybrid cloud combines public, private, and community cloud resources from different service providers.

References

LabSim for PC Pro, Section 10.5.
[pcpro2016_all_questions_en.exm VIRTUAL_MACHINE_06]

▼ **Question 70:**   Incorrect

Where is Disk Management located within Windows 7?

○ Control Panel

○ Administrative Tools

○ Device Manager

➡ ○ Computer Management

Explanation

Within Windows 7, Disk Management is found under Storage in Computer Management.

Within Windows 10, Disk Management is found in the list of utilities that appear when you right-click the Start Menu.

References

LabSim for PC Pro, Section 5.7.
[pcpro2016_all_questions_en.exm DISK MANAGEMENT_01]

▼

Question 71:   Incorrect

ESD is most likely to occur:

- ○ In a warm, humid atmosphere.

➡ ○ In a cool, dry atmosphere.

- ○ In a cool, humid atmosphere.

- ○ In a warm, dry atmosphere.

Explanation

Electrostatic discharge (ESD) is most likely to occur in a cool, dry atmosphere. A warm and humid atmosphere helps dissipate the buildup of static electricity, hence ESD is less likely to occur.

References

LabSim for PC Pro, Section 2.1.
[pcpro2016_all_questions_en.exm PC 2016 ESD COOL DRY]

▼ **Question 72:**   Incorrect

A small business named BigBikes, Inc. has hired you to evaluate their wireless network security practices. As you analyze their facility, you note the following:

- They use an 802.11a wireless network.
- The wireless network SSID is set to BWLAN.
- The wireless network is not broadcasting the network SSID.
- The wireless network uses WPA2 with AES security.
- Omnidirectional access points are positioned around the periphery of the building.

Based on this information, what should you recommend your client do to increase their wireless network security?

- ○ Upgrade to an 802.11g wireless network.

➡ ○ Implement directional access points.

- ○ Enable SSID broadcast.

- ○ Change the SSID to something similar to BigBikeInc.

- ○ Configure the wireless network to use WEP security.

Explanation

You should recommend that they implement directional access points along the periphery of the building. Using omnidirectional APs in these locations can cause the wireless network radio signal to emanate outside the building, making it readily available to malicious individuals.

Enabling SSID broadcasts and using an SSID that is easily identifiable reduces the security of the wireless network; as would switching to WEP security. Switching to an 802.11g network offers no speed or security benefits and would require retrofitting all wireless equipment in the organization.

References

LabSim for PC Pro, Section 12.9.
[pcpro2016_all_questions_en.exm NET_SEC_WIRELESS_10]

▼ **Question 73:**   Incorrect

While trying to log on, a user accidentally typed the wrong password three times, and now the system is locked because he entered too many incorrect passwords. He still remembers his password, but he just typed it wrong. He needs access as quickly as possible. What should you do?

- ○ Change the password for the account

- ○ Have the user wait for the account to be unlocked automatically

➡ ○ Unlock the account

- ○ Enable the account

Explanation

With the account lockout policy configured, an account will be locked (and cannot be used for logon) when a specified number of incorrect passwords are entered. You can unlock a locked account by editing the account properties in Local Users and Groups. Depending on the policy

settings, locked accounts might be unlocked automatically after a period of time. However, to
~~Allow immediate access, or be used to log in. Accounts~~ are not disabled automatically, and
enabling an account does not unlock it. Changing the password is not required because the user
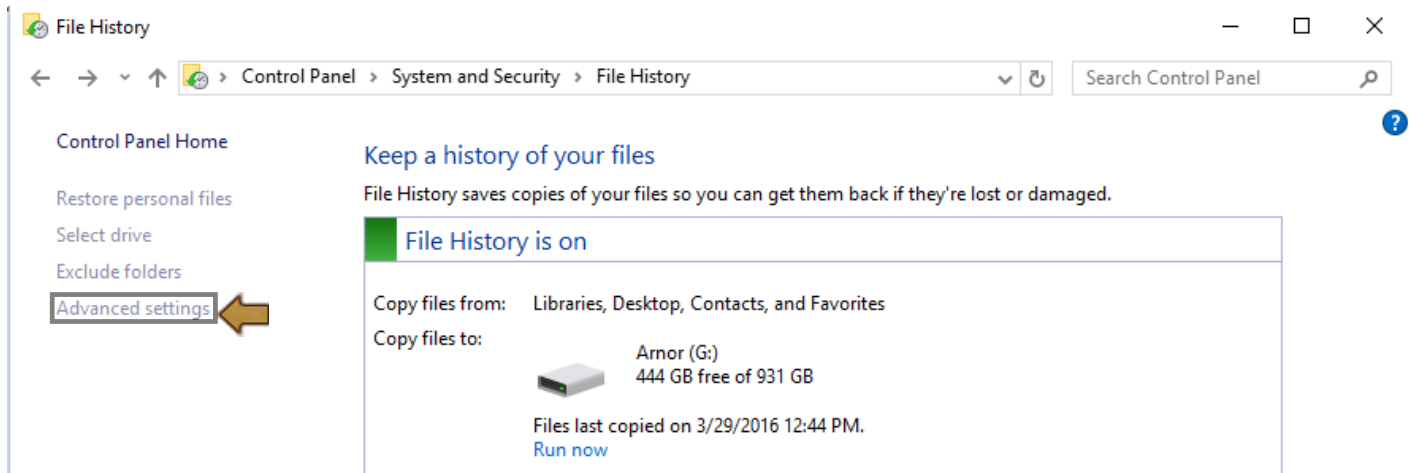still remembers the correct password.

References

LabSim for PC Pro, Section 12.7.
[pcpro2016_all_questions_en.exm AUTHORIZATION_10]

▼ **Question 74:**   Incorrect

You need to configure File History to automatically delete any stored snapshots that are older
than 1 month.

Click the option you would use in Control Panel to do this.

Explanation

To clean up old versions, select the **Advanced Settings** option. Then select the appropriate
clean up interval from the Keep Saved Versions drop-down list.

The Exclude Folders option is used to prevent certain folders from being protected by File History.
The Select Drive option is used to specify which hard disk is used to store File History data. The
Restore Personal Files option is used to retrieve previous versions of files protected by File
History.

References

LabSim for PC Pro, Section 9.10.
[pcpro2016_all_questions_en.exm RT WINDOWS BACKUP 11-PB]

▼ **Question 75:**   Incorrect

Which port must be opened in the firewall of a Windows system in order Remote Desktop
connections to be established with it?

- ○ 22

- ○ 123

➡ ○ 3389

- ○ 23

Explanation

The firewall on a Windows system must be configured to allow Remote Desktop traffic through.
This is done by opening TCP port 3389 (by default). This port is opened automatically on the
Remote Desktop host when remote connections are enabled.

Port 22 is used by the SSH protocol. Port 23 is used by the Telnet protocol. Port 123 is used by
the Network Time Protocol.

References

LabSim for PC Pro, Section 9.5.
[pcpro2016_all_questions_en.exm RT REMOTE CON 03]

▼ **Question 76:**   Incorrect

Your supervisor recently purchased 100 desktop computer systems and 100 new Windows 10
licenses for your organization's Accounting department. She received a single Windows 10
installation disc with the licenses.

Which of the following would be the best installation methods to use? (Select two.)

➡ ☐ Use a network installation.

☐ Copy the installation media to 10 flash drives and install 10 systems at a time.

☐ Install Window on each system one at a time using the installation disc.

☐ Burn 50 copies of the installation disc and install 50 systems at a time.

➡ ☐ Install one system and image it to the other systems.

Explanation

The best installation options in this scenario would be to perform either a network installation or use imaging. In a network installation you would copy the installation media to a Windows Deployment Services (WDS) server, configure each new workstation to use a PXE boot, boot them from the WDS server over the network, and then run the install.

Alternatively, you could install Windows on one of the systems and then use imaging software to take an image of that system and copy it to the remaining 99 systems over a network connection.

Installing one system at a time from the installation disc would take a considerable amount of time. Burning multiple copies of the installation disc or create multiple flash drives and then installing 100 systems from them would be time-consuming.

References

LabSim for PC Pro, Section 10.3.
[pcpro2016_all_questions_en.exm WINDOWS_INSTALL_02]

▼ **Question 77:**   Incorrect

You have a Windows system shared by three shift workers. Files that are used by all users are stored on the D:\ drive in various folders. The users have created hundreds of files on this drive and sometimes experience difficulty finding the files they need.

What should you do?

○ Configure Work Folders for the folders on the D:\ drive

○ Configure visual settings to optimize performance

➡ ○ Configure indexing to include the D:\ drive

○ Add an additional drive to the system and configure a new Storage Space using the files from the old D:\ drive

Explanation

The Windows file search tool runs relatively quickly because it does not search the entire storage device. Instead, it searches for file within an index that is maintained by the operating system. You can use the Indexing Options in the Control Panel to customize what file locations are included in the index.

Storage Spaces are used to pool available storage space from multiple storage devices in the system. You use Work Folders to make files on the system available across all devices used by users, even when the system is offline. Visual effects controls how window contents and fonts appear on the screen.

References

LabSim for PC Pro, Section 9.2.
[pcpro2016_all_questions_en.exm WINDOWS_PREFS_03]

▼ **Question 78:**   Incorrect

If you want to boot from a hard drive, what must it have?

➡ ○ Active partition

○ Extended partition

○ Dynamic partition

○ Passive partition

Explanation

The active partition contains the boot sector, which is required to load an operating system. An extended partition is a partition type on a basic disk. An extended partition can exist, but is not required to boot.

References

LabSim for PC Pro, Section 5.5.

[pcpro2016_all_questions_en.exm DRIVE STATUS_01]

▼ **Question 79:**   Incorrect

A user within your organization received an email relating how an account containing a large sum of money has been frozen by the government of a small African nation. The user was offered a 25% share of this account if she would help the sender transfer it to a bank in the United States. The user responded to the sender and was instructed to send her bank account number so that it could be used to facilitate the transfer. She complied, and then the sender used the information to drain her bank account.

What type of attack occurred?

○ Man-in-the-Middle

➡ ○ Phishing

○ Eavesdropping

○ Piggybacking

Explanation

A phishing attack has occurred in this scenario. This particular attack is sometimes referred to as a Nigerian 419 attack and is very common.

Piggybacking occurs when an unauthorized person follows behind an authorized person to enter a secured building or area within a building. Piggybacking is also sometimes called tailgating. Eavesdropping refers to an unauthorized person listening to conversations of employees or other authorized personnel discussing sensitive topics. A man-in-the-middle attack is a technological attack where a malicious person intercepts network communications between two hosts, posing as the sender to the receiver and as the receiver to the sender.

References

LabSim for PC Pro, Section 12.4.

[pcpro2016_all_questions_en.exm SOCMED_SECURITY_09]

▼ **Question 80:**   Incorrect

To answer this question, complete the lab using information below.   **Launch Lab**

You did not complete the lab correctly.

You work as the IT Administrator for a small corporate network. A user has inadvertently allowed his Local Area Network settings to be changed during the installation of a free software package. He reports that his browser no longer goes to his usual home page when he opens it and an error sometimes appears in his browser window saying that the proxy server isn't responding. Your company network does not use a proxy server, so the free software installation might have configured his Internet options to use a malicious proxy server.

Your tasks in this lab are to do the following:

▪ Deselect the option to use a proxy server for your LAN.
▪ Configure **www.testout.com** as the home page for Internet Explorer.

References

LabSim for PC Pro, Section 12.11.

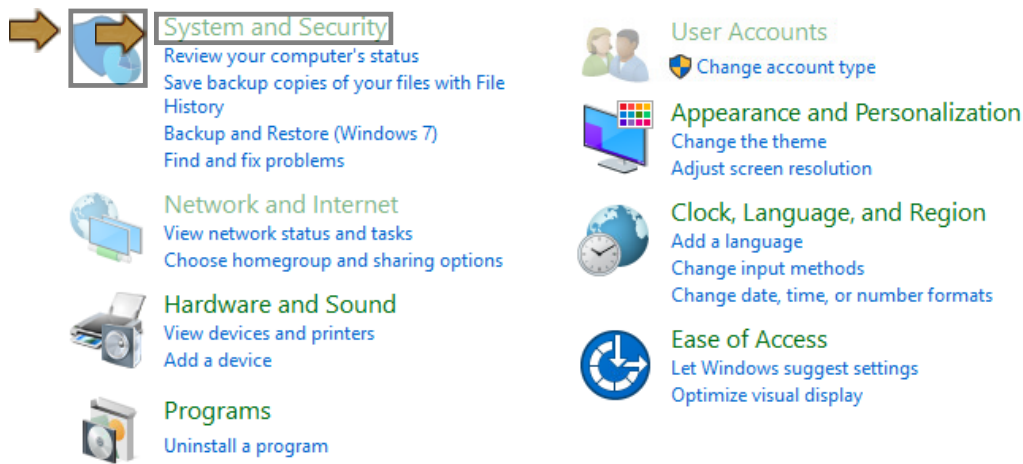[pcpro2016_all_questions_en.exm PROXY1HOMEPAGE SECURITY]

▼ **Question 81:**   Incorrect

You need to enable Remote Desktop on a user's Windows 10 system so that you can manage it over the network from your office.

Click the option you would use in Control Panel to do this.

Adjust your computer's settings   View by: Category ▼

System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)
Find and fix problems

Network and Internet
View network status and tasks
Choose homegroup and sharing options

Hardware and Sound
View devices and printers
Add a device

Programs
Uninstall a program

User Accounts
Change account type

Appearance and Personalization
Change the theme
Adjust screen resolution

Clock, Language, and Region
Add a language
Change input methods
Change date, time, or number formats

Ease of Access
Let Windows suggest settings
Optimize visual display

Explanation

To enable Remote Desktop on a Windows 10 system, you access Control Panel and select **System and Security** > **Allow remote access**.

The Network and Internet option in Control Panel is used to manage network connections. The User Accounts option is used to manage user accounts.

References

LabSim for PC Pro, Section 9.5.
[pcpro2016_all_questions_en.exm RT REMOTE CON 01-PB]

▼ **Question 82:**   Incorrect

Good documentation will:

➡ ⚪ Save you time and money in troubleshooting problems.

⚪ Eliminate the need to troubleshoot problems.

⚪ Reduce hardware maintenance.

⚪ All of the above.

Explanation

By keeping adequate documentation, you can reduce the time and money spent troubleshooting. While documentation can help reduce troubleshooting, it can never completely eliminate it. Documentation helps you know when regular maintenance of hardware is required, but does not eliminate maintenance.

References

LabSim for PC Pro, Section 2.5.
[pcpro2016_all_questions_en.exm PC 2016 DOCUMENTATION]

▼ **Question 83:**   Incorrect

You have just installed a new USB card reader in your Windows computer. Every time you perform a certain action using the card reader, you get an error message that you've never seen before.

What should you do first?

⚪ Install the device on another computer.

➡ ⚪ Check the manufacturer's website for information about the error.

⚪ Uninstall the device, then reinstall it.

⚪ Replace the card reader with a new device.

Explanation

For information about a specific error, check the manufacturer's website. Taking any other action might fix the problem, but would most likely just waste time. In most cases, device-specific problems can be corrected with a new driver or other software update.

References

LabSim for PC Pro, Section 2.5
[pcpro2016_all_questions_en.exm PC 2016 MANUFACTURER REF]

▼ **Question 84:**   Incorrect

While running a full system scan using your anti-malware software, three files have been
identified as possible problems. You want to keep the files intact so you can review them later,
but you also need to ensure they can't harm anything else on your computer.

What action should you take?

     ◯ Delete the files

➡ ◯ Quarantine the files

     ◯ Rename the files

     ◯ Repair the infected files

Explanation

Quarantine moves the infected file to a secure folder where it cannot be opened or run normally.
You might quarantine an infected file that cannot be repaired to see if another tool or utility might
be able to recover important data from the file.

During a repair, the virus is removed and the file is placed back in its original state (if possible).
Deleting the file removes the file from your system. Renaming the file might not offer sufficient
protection because the virus might be able to still run, or it might be able to rename or replace
the infected files.

References

LabSim for PC Pro, Section 12.6.
[pcpro2016_all_questions_en.exm MALWARE_07]

▼ **Question 85:**   Incorrect

Which security practice is an example of the Principle of Least Privilege?

➡ ◯ All users on a Windows workstation are limited users except for one user who is
       responsible for maintaining the system.

     ◯ Autorun has been disabled on a Windows workstation.

     ◯ All users on a Windows workstation have been assigned strong passwords.

     ◯ The Guest user account on a Windows workstation has been disabled.

Explanation

The Principle of Least Privilege specifies that users should have only the degree of access to the
workstation necessary for them to complete their work and no more. Making all users limited
users except for those who need administrative access is an example of the Principle of Least
Privilege.

The other practices listed are workstation security best practices, but are not necessarily
examples of the Principle of Least Privilege.

References

LabSim for PC Pro, Section 12.1.
[pcpro2016_all_questions_en.exm SECURITY_BEST_01]

▼ **Question 86:**   Incorrect

     🖥 To answer this question, complete the lab using information below. | Launch Lab |

You did not complete the lab correctly.

You work as the IT Administrator for a small corporate network. A user
accidentally installed an adware application on his laptop computer. He realized
his mistake and used Programs and Features to uninstall it. However, whenever
he starts Internet Explorer, it still automatically goes to a shopping site that
appears to be dubious in nature.

Your task in this lab is to correct the system configuration parameter that was
modified by the adware.

References

LabSim for PC Pro, Section 12.11.
[pcpro2016_all_questions_en.exm HOMEPAGE SECURITY]

▼ **Question 87:**   Incorrect

Which of the following should be handled with caution due to high operating temperatures?
(Select two.)

☐ External hard disk drive

☐ System RAM modules

➡ ☐ Components within a laser printer

➡ ☐ Printing head in a dot matrix printer

☐ Inkjet printer tractor feed

Explanation

Components such as the printing head of a dot matrix printer or components inside a laser printer
can be hot, and should be handled with caution. You should allow components to cool sufficiently
before servicing to prevent burns. Typically, other components such as RAM and external hard
disk drives do not operate at a high enough temperature to cause injury. The same is true of the
tractor feed mechanism in an inkjet printer.

References

LabSim for PC Pro, Section 2.1.
[pcpro2016_all_questions_en.exm PC 2016 HIGH TEMP COMPONENTS]

▼ **Question 88:**   Incorrect

While working on your Windows 7 system, the system encounters a critical error. For a brief
second you see the Blue screen indicating the error. Before you can read the error, however, the
system reboots. After rebooting and logging back on, the same thing happens again. What
should you do so that you can read the error message next time it happens without the system
rebooting?

○ Access Startup Repair in the Recovery Environment.

○ When the error occurs, quickly press the Spacebar to pause the information on the
screen.

○ In the Control Panel, use the Power Options to disable automatic rebooting.

➡ ○ Reboot the system. Press F8 and disable the automatic restart feature.

○ Edit the CMOS settings. Select Stay Off for the Restart on Power Fail option.

Explanation

Windows 7 has an automatic restart feature. To turn this off, press F8 during startup, then select
the Disable automatic restart on system failure option. Use Startup Repair to correct system boot
errors. The Restart on Power Fail setting in the BIOS determines what the system does after
power is restored when the power is unexpectedly lost. It does not control what happens when a
system error is encountered (that is controlled by the operating system).

References

LabSim for PC Pro, Section 9.14.
[pcpro2016_all_questions_en.exm TRB_OS_19]

▼ **Question 89:**   Incorrect

You need to configure when Windows checks for and downloads updates from Microsoft's update
servers on a Windows 7 system. Which option in Control Panel should you use to do this?

➡ ○ System and Security

○ Appearance and Personalization

○ Hardware and Sound

○ Network and Internet

Explanation

You can configure Windows updates under System and Security in Control Panel on Windows 7.

You can use Hardware and Sound in Control Panel to configure printers and other hardware devices. Network and Internet is used to manage network connections. Appearance and Personalization is used to configure desktop themes and screen resolution.

References

LabSim for PC Pro, Section 9.1.
[pcpro2016_all_questions_en.exm WINDOWS_PREFS_09]

▼ **Question 90:**   Incorrect

🖥 To answer this question, complete the lab using information below.   [**Launch Lab**]

You did not complete the lab correctly.

You work as the IT Administrator for a small corporate network. A user inadvertently installed an adware application on his laptop computer. He realized his mistake and used Programs and Features to uninstall it. However, whenever he starts his web browser, his home page is a shopping website of a dubious nature. When he tries to go to a different website, he gets a message that "the proxy server is refusing connections."

The proxy server on your network is functioning properly and the user's laptop should be configured to automatically detect the proxy server settings.

Your task in this lab is to correct the system configuration parameters that were modified by the malware.

References

LabSim for PC Pro, Section 12.11.
[pcpro2016_all_questions_en.exm BADPROXY_EXM]