Exam Report: C.4 Domain 3: Security, All Questions

Date: 7/30/2017 5:06:21 am Candidate: Stangl, Thomas (Email: tstangl@ciat.edu)
Time Spent: 3:54

Overall Performance

Your Score: 0%

View results by: ○ Objective Analysis ◉ Individual Responses

Individual Responses

Question 1: Incorrect

A user has a problem accessing several shared folders on the network. After determining the issue is not from his computer's IP configuration, you suspect the shared folders are not currently connected. Which of the following commands will confirm your suspicions?

- ○ tracert
- ○ nslookup
- ○ ipconfig
- ➡ ○ net use

Explanation

Use the net use command to list the current connected shared folders and drive letters. Ipconfig displays the TCP/IP configuration of network interfaces. Netstat displays protocol connections that have been established by the system, as well as what incoming TCP/IP ports are in use by the system. Tracert displays information on the route that a packet takes as it traverses the network to a remote host.

References

LabSim for PC Pro, Section 11.4.
[pcpro2016_all_questions_en.exm SHARED_01]

Question 2: Incorrect

How can you see a list of valid command parameters for the **net use** command?

- ○ net use -h
- ○ help net use
- ➡ ○ net use /?
- ○ net use help

Explanation

Type net use /? to see a list of the valid parameters for the net use command.

References

LabSim for PC Pro, Section 11.4.
[pcpro2016_all_questions_en.exm SHARED_02]

Question 3: Incorrect

You have a folder that you would like members of your development team to access. You want to

restrict network and local access to only specific users. All other users must not be able to view or modify the files in the folder. What should you do? (Select two.)

- [ ] Configure both share and NTFS permissions.
- [ ] Place the files on an NTFS partition.
- [ ] Configure NTFS permissions.
- [ ] Configure share permissions.
- [ ] Place the files on a FAT32 partition.

Explanation

To control both local and network access, you will need to use both NTFS and share permissions. The folder must be located on an NTFS partition to be able to configure NTFS permissions. Configuring only NTFS permissions will not allow network access. Configuring only shared permissions with the files on a FAT32 partition will not control local access.

References

LabSim for PC Pro, Section 11.4.
[pcpro2016_all_questions_en.exm SHARED_03]

Question 4: Incorrect

You want to use the Universal Naming Convention (UNC) format to access a shared folder called Pictures on a computer named Home1. Which format would you use?

- ( ) \\Home1\Pictures
- ( ) Home1:\\Pictures
- ( ) Home1:Pictures
- ( ) .Home1:Pictures

Explanation

Use \\Home1\Pictures to access the shared folder. The format is \\Servername\sharename.

References

LabSim for PC Pro, Section 11.4.
[pcpro2016_all_questions_en.exm SHARED_04]

Question 5: Incorrect

Which of the following statements are true regarding administrative shares? (Select two.)

- [ ] If you are a member of the Administrators group, the administrative shares are visible when browsing the network.
- [ ] By default, Windows automatically creates an administrative share for every volume.
- [ ] To connect to an administrative share, you must use the UNC path.
- [ ] Default administrative shares are accessed by members of the Administrators or Power Users group.

Explanation

By default, Windows automatically creates an administrative share for every volume, with the share name being the volume letter plus the dollar sign (such as C$). Because administrative

shares are not visible when browsing the network, you must use the UNC path to connect to an administrative share. Default administrative shares can only be accessed by a member of the Administrators group.

References

LabSim for PC Pro, Section 11.4.
[pcpro2016_all_questions_en.exm SHARED_05]

Question 6: Incorrect

Which of the following permissions are not available when sharing a folder on a Windows 7 workstation? (Select two.)

- [ ] Modify
- [ ] Write
- [ ] Read
- [ ] Read/write

Explanation

Modify and Write are NTFS permissions, not share permissions. With Windows 7, there are two separate share permission sets:

- Read
- Read/write

References

LabSim for PC Pro, Section 11.4.
[pcpro2016_all_questions_en.exm SHARED_06]

Question 7: Incorrect

Bob is a member of the Accounting group. The Accounting group has been granted the Read and Write NTFS permissions to the WeeklyReport.xls file. Bob is attempting to access the report through a share with the Full Control permission assigned to the Everyone group. Which of the following statements correctly describes Bob's ability to access the WeeklyReport.xls file?

- ( ) Bob cannot search for or open the file.
- ( ) Bob can open and read the file, but cannot write changes to the file.
- ( ) Bob can open, read, and write changes to the file
- ( ) Bob can find the file in a search, but cannot open the file.
- ( ) Bob has Full Access to the file, and can open, read, write changes, delete, and change permissions on the file.

Explanation

When evaluating the interaction between Share and NTFS permissions, remember that the most restrictive set of permissions takes precedence. In this case, the NTFS permissions (Read and Write) are more restrictive than the Full Control granted through the share, so the effective permissions are Read and Write.

References

LabSim for PC Pro, Section 11.4.
[pcpro2016_all_questions_en.exm SHARED_07]

Question 8: Incorrect

You have a folder on your Windows 7 computer that you would like to share with members of your development team. Users should be able to view and edit any file in the shared folder. You share the folder and give Everyone Full Control permission to the shared folder. Users connect to the shared folder and report that they can open the files, but they cannot modify any of the files. What should you do?

- Create new user accounts for each user and assign the necessary folder permissions.
- Install Samba on your workstation, then configure permissions using Samba.
- Create a group and make all user accounts members of the group. Grant Full Control share permissions to the group.
- Modify the NTFS permissions on the folder.

Explanation

Access to shared folders on a Windows system are controlled through the combination of share and NTFS permissions. Even though the necessary share permissions have been granted, you need to verify that the NTFS permissions also allow access. Modifying users and groups will not affect the ability to access the files unless the NTFS permissions are also modified. Use Samba on a Linux system to share folders.

References

LabSim for PC Pro, Section 11.4.
[pcpro2016_all_questions_en.exm SHARED_08]

Question 9: Incorrect

Which tool in Windows 10 would you use to browse all networks and shared folders to which a user has access? (Select three.)

- [x] File Explorer
- [ ] Windows Explorer
- [x] Network
- [ ] Network Neighborhood
- [x] Computer
- [ ] Computer Management

Explanation

In Windows 10, *Network* acts as a built-in network browser showing all networks and shared folders to which the user has access. This same information can be viewed in *Computer* and *File Explorer*. Network Neighborhood was used in previous Windows versions, but was replaced by My Network Places in Windows 2000, Me, and XP and by Network in Windows Vista, Windows 7, and Windows 8. Computer Management and Device Manager are used to manage hardware and software in the Windows system and can't be used to browse the network.

Windows Explorer was replaced by File Explorer in Windows 10.

References

LabSim for PC Pro, Section 11.4.
[pcpro2016_all_questions_en.exm SHARED_09]

Question 10: Incorrect

If your anti-malware software does not detect and remove a virus, what should you try first?

- Update your malware definitions.

- ◯ Scan the computer using another virus detection program.
- ◯ Search for and delete the file you believe to be infected.
- ◯ Set the read-only attribute of the file you believe to be infected.

Explanation

Malware detection software can search only for malware listed in its malware definitions file. An outdated file can prevent the anti-malware software from recognizing a new virus.

References

LabSim for PC Pro, Section 12.6.
[pcpro2016_all_questions_en.exm MALWARE_01]

Question 11: Incorrect

You have just installed anti-malware software on all computers on your company's network. Which additional actions should you take to help protect systems from malicious software? (Select two.)

- ➡ ☐ Configure the software to automatically update its definition files.
- ☐ Disconnect all computers from the Internet.
- ☐ Configure e-mail servers to block all attachments.
- ➡ ☐ Train users to scan removable storage devices before copying files.
- ☐ Require strong passwords in the local security policy.
- ☐ Configure all computers with a screen saver password.

Explanation

Configuring the anti-malware software to automatically update its definition files and to scan removable storage devices before copying files will help protect systems from malicious software.

Configuring e-mail servers to block all attachments might prevent some viruses, but will also prevent users from receiving necessary files through e-mail. Disconnecting all computers from the Internet will impede a productive work environment. Requiring strong passwords and configuring all computers with a screen saver password are important aspects of a security policy, but they won't prevent the transfer of malicious software.

References

LabSim for PC Pro, Section 12.6.
[pcpro2016_all_questions_en.exm MALWARE_02]

Question 12: Incorrect

You discover that a system on your network has been infected with a worm. What is the best way to prevent the spread of the worm to other systems while you work on removing the worm?

- ➡ ◯ Quarantine the computer
- ◯ Update the anti-malware definition files on all computers
- ◯ Close the firewall ports that the worm uses
- ◯ Run a system scan on other computers

Explanation

The best means to prevent a worm (or any other type of malicious code) from spreading is to quarantine the system. Quarantine places the computer in an isolated network, or removes the computer from the network completely, so that it cannot interact with other computers.

Updating the definition files and scanning other computers should be done to make sure that they have not been affected. However, if the definition file does not identify the worm, it will have no effect on stopping its spread. Closing firewall ports might help, but is not as sure a method of protecting your system as quarantining the infected computer.

References

LabSim for PC Pro, Section 12.13.
[pcpro2016_all_questions_en.exm TRB_SECURITY_04]

Question 13: 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
- Low system memory
- Malware infection
- Faulty network card

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 14: Incorrect

Which of the following actions adds new features and fixes bugs for anti-malware software?

- Quarantining infected files and systems
- Remediating unhealthy computers
- Automatically downloading definition file updates
- Updating the anti-malware engine

Explanation

Updating the anti-malware engine adds new features and fixes bugs.

Downloading definition file updates allows the engine to scan for the most recent threats. Quarantining infected files moves a file to a secure folder where it cannot be opened or run normally. Remediating unhealthy computers is the process of correcting any problems that are found.

References

LabSim for PC Pro, Section 12.6.

[pcpro2016_all_questions_en.exm MALWARE_04]

Question 15: Incorrect

To tightly control the anti-malware settings on your computer, you elect to update the signature file manually. Even though you vigilantly update the signature file, the machine becomes infected with a new type of malware.

Which of the following actions would best prevent this scenario from occurring again?

- Configure the software to automatically download the definition file updates as soon as they become available.
- Carefully review open firewall ports and close any unneeded ports.
- Switch to a more reliable anti-malware software.
- Create a scheduled task to run sfc.exe daily.

Explanation

Anti-malware software is most effective against new threats if it has the latest definition files installed. Instead of manually updating the signature files, you should configure the software to automatically download updated definition files as soon as they become available.

Use sfc.exe to repair infected files after malware has caused the damage. Using different anti-malware software will not resolve the problem if you don't apply the latest definition files.

References

LabSim for PC Pro, Section 12.6.
[pcpro2016_all_questions_en.exm MALWARE_03]

Question 16: Incorrect

A user reports that his machine will no longer boot properly. After asking several questions to determine the problem, you suspect the user unknowingly downloaded malware from the Internet, and that the malware corrupted the boot block.

Based on your suspicions, what actions could you take to correct the problem? (Select two.)

- Boot into Safe Mode and try removing the malware.
- Reimage the machine.
- Boot from the Windows 7 installation DVD and use the Recovery Environment to run a startup repair.
- Run sfc.exe.
- Have the user attend an internal Internet safety training course.

Explanation

From the Recovery Environment, run a startup repair operation. If you have an existing image of the computer, you could also reimage the system. However, all data and applications added to the system since the image was created will be lost. Reimaging the system will typically get Windows back up and running on the computer more quickly than manually re-installing the operating system.

User training is a preventative measure against malware infections; however, the training will not repair the current damage. Sfc.exe scans every system file in the operating system for altered files, but does not scan the master boot record or the volume boot record. Since the machine no longer boots properly, booting into Safe Mode is not an option in this scenario.

References

LabSim for PC Pro, Section 12.13.
[pcpro2016_all_questions_en.exm TRB_SECURITY_02]

Question 17: Incorrect

Your anti-malware software has detected a virus on your Windows 10 system. However, the anti-malware software is unable to remove it, and when you try to delete the files, you can't because they are in use.

What should you try first?

- Reset the operating system
- Update the anti-malware definition files
- Boot into Safe Mode and try removing the malware
- Run Sfc.exe

Explanation

If a malware process is running and you are unable to stop it, try booting into Safe Mode, then run the scanning software to locate and remove the malware (or delete the files manually). Safe Mode loads only the required drivers and processes.

Anti-malware definition files are used to identify a virus; in this case, the anti-malware software has already detected the virus so the files are sufficiently up-to-date to detect the virus. Resetting the operating system might be necessary, but should only be tried after all other measures have failed. Sfc.exe checks and repairs system files.

References

LabSim for PC Pro, Section 12.13.
[pcpro2016_all_questions_en.exm TRB_SECURITY_01]

Question 18: Incorrect

You have installed anti-malware software on computers at your business. Within a few days, however, you notice that one computer has a virus. When you question the user, she says she did install some software a few days ago, but it was supposed to be a file compression utility. She admits she did not scan the file before running it.

What should you add to your security measures to help prevent this from happening again?

- Account lockout
- User awareness training
- Close unused firewall ports
- Proxy server

Explanation

Many anti-malware prevention measures are ineffective if users take actions that put their computers at risk (such as downloading and running files or copying unscanned files to their computers). If users are educated about malware and about the dangers of downloading software, the overall security of the environment improves.

A proxy server controls access to the Internet based on username, URL, or other criteria. Account lockout helps prevent attackers from guessing passwords. Firewall ports might be used by some malware, but will not prevent malware introduced by downloading and installing a file.

References

LabSim for PC Pro, Section 12.13.
[pcpro2016_all_questions_en.exm TRB_SECURITY_05]

Question 19: Incorrect

Which of the following is the process of fixing problems detected by anti-virus software so that the computer is restored to its original state?

- Quarantine
- Scanning
- Remediation
- Isolation

Explanation

Remediation is the process of correcting any problems that are found. Most antivirus software remediates problems automatically or semi-automatically (i.e. you are prompted to identify the action to take).

Quarantine is the process of moving an infected file or computer to a safe location so that the problem cannot affect or spread to other files or computers. Isolation is one method of performing quarantine. Scanning is the process of checking a system for infected files.

References

LabSim for PC Pro, Section 12.13.
[pcpro2016_all_questions_en.exm TRB_SECURITY_06]

Question 20: Incorrect

You have installed anti-malware software that checks for viruses in e-mail attachments. You configure the software to quarantine any files with problems. You receive an e-mail with an important attachment, but the attachment is not there. Instead, you see a message that the file has been quarantined by the anti-malware software. What has happened to the file?

- It has been deleted from your system.
- The file extension has been changed to prevent it from running.
- The infection has been removed, and the file has been saved to a different location.
- It has been moved to a folder on your computer.

Explanation

Quarantine moves the infected file to a secure folder where it cannot be opened or run normally. By configuring the software to quarantine any problem files, you can view, scan, and possibly repair those files. Quarantine does not automatically repair files. Deleting a file is one possible action to take, but this action removes the file from your system.

References

LabSim for PC Pro, Section 12.6.
[pcpro2016_all_questions_en.exm MALWARE_05]

Question 21: Incorrect

You have installed anti-malware software on a computer that only you use. You want to protect the computer from files that you download from the Internet.

What should you do next to make sure that there aren't any existing files on your system that are infected? (Select two.)

- [ ] Manually create a restore point
- [ ] Encrypt the hard disk drive

- [ ] Run a full scan
- [ ] Download the latest definition files
- [ ] Quarantine your computer

Explanation

Run a full system scan to check files already on your computer. In addition, you should schedule full system scans to run periodically. You should also update the engine and definition files.

Quarantining the system isn't necessary unless malware is discovered that could spread to other systems over a network connection. Manually creating a restore point isn't necessary in this scenario, nor is encrypting the hard disk drive.

References

LabSim for PC Pro, Section 12.6.
[pcpro2016_all_questions_en.exm MALWARE_06]

Question 22: 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?

- ( ) Rename the files
- ( ) Delete the files
- ( ) Quarantine 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 23: 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?

- ( ) Security and Maintenance
- ( ) System
- ( ) Network and Sharing Center
- ( ) Windows Firewall

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 24: Incorrect

Which of the following is not a form of biometrics?

- Token device
- Retina scan
- Face recognition
- Fingerprint

Explanation

A token device is not a form of biometrics. Biometrics rely on personal characteristics (such as fingerprints, facial recognition, or a retina scan) to prove identity. A token device is an example of the authentication factor of Something You Have. A token device is a small device that you type in a code or a pin and the token produces a response. The response is used on a secured system along with your name and password to gain access to that system.

References

LabSim for PC Pro, Section 12.7.
[pcpro2016_all_questions_en.exm AUTHORIZATION_01]

Question 25: Incorrect

What do biometrics use to perform authentication of identity?

- Human characteristics
- Knowledge of passwords
- Possession of a device
- Ability to perform tasks

Explanation

Biometrics is based on human characteristics. Biometrics is a strong form of authentication because each person has unique characteristics. When these unique characteristics are used for authentication, they are more reliable and stronger than the best passwords. For example, no two people have the exact same fingerprint or retina pattern.

References

LabSim for PC Pro, Section 12.7.
[pcpro2016_all_questions_en.exm AUTHORIZATION_02]

Question 26: Incorrect

Which of the following security technologies stores identification information in either a magnetic strip, radio frequency transmitter, or hardware contacts to authorize access to a computer?

- SSID
- ID badge
- Biometric
- Smart card
- Key fob

Explanation

A smart card contains identification information stored on a magnetic strip, radio frequency transmitter, or hardware contacts that allow it to interact with a smart card reader to authorize access. The reader uses information on the card to allow or deny access.

A biometric is a physical characteristic of a human that can be scanned to control access. A key fob can be used for accessing an automobile, but is not used for computer access. An ID badge can be just a picture with a name on it and may or may not also be a smart card. In Windows, the Local Security Policy is a collection of settings that control how the system behaves. The SSID is the name of a wireless network.

References

LabSim for PC Pro, Section 12.7.
[pcpro2016_all_questions_en.exm AUTHORIZATION_03]

Question 27: Incorrect

Which of the following is the most common form of authentication?

- Username and password
- Photo ID
- Digital certificate on a smart card
- Fingerprint

Explanation

Passwords are the most common form of authentication. Most secure systems require only a username and password to provide users with access to the computing environment. Many forms of online intrusion attacks focus on stealing passwords. This makes using strong passwords very important. Without a strong password policy and properly trained users, the reliability of your security system is greatly diminished. Photo ID, fingerprint, and digital certificate on a smart card are not the most common forms of authentication.

References

LabSim for PC Pro, Section 12.7.
[pcpro2016_all_questions_en.exm AUTHORIZATION_04]

Question 28: Incorrect

Which type of biometric authentication uses the ridges of your skin?

- Retina scan
- Face scan
- Keystroke dynamics
- Fingerprint

Explanation

Fingerprint biometrics use the ridges of your skin known as ridge minutiae. Retina scans use blood vein patters, facial scans use a facial pattern, and keystroke dynamics use a behavioral system.

References

LabSim for PC Pro, Section 12.7.
[pcpro2016_all_questions_en.exm AUTHORIZATION_05]

Question 29: Incorrect

Which of the following is an example of a strong password?

- desktop#7
- a8bT11$yi
- Robert694
- at9iov45a

Explanation

A strong password should not contain dictionary words or any part of the login name. They should include upper- and lower-case letters, numbers, and symbols. In addition, longer passwords are stronger than shorter passwords.

References

LabSim for PC Pro, Section 12.7.
[pcpro2016_all_questions_en.exm AUTHORIZATION_06]

Question 30: Incorrect

Which of the following security measures is a form of biometrics?

- Fingerprint scanner
- BIOS password
- TPM
- Chassis intrusion detection

Explanation

A fingerprint scanner is a type of biometrics. The fingerprint scanner uses the ridges of your skin known as ridge minutiae. A Trusted Platform Module (TPM) is a special chip on the motherboard that generates and stores cryptographic keys to verify that the hardware has not changed. This value can be used to prevent the system from booting if the hardware has changed. Chassis intrusion detection helps you identify when a system case has been opened. A BIOS password controls access to the BIOS setup program.

References

LabSim for PC Pro, Section 12.7.
[pcpro2016_all_questions_en.exm AUTHORIZATION_07]

Question 31: Incorrect

You are configuring a network firewall to allow SMTP outbound email traffic, and POP3 inbound email traffic. Which of the following IP ports should you open on the firewall? (Select two.)

- 143

- [ ] 443
- [x] 110
- [x] 25
- [ ] 21

Explanation

The Simple Mail Transfer Protocol (SMTP) uses IP port 25. The Post Office Protocol version 3 (POP3) uses IP port 110. The File Transfer Protocol (FTP) uses IP Ports 20 and 21. The Internet Message Access Protocol (IMAP) uses IP port 143. IP port 443 is used by the Secure Sockets Layer (SSL) protocol.

References

LabSim for PC Pro, Section 12.10.
[pcpro2016_all_questions_en.exm FIREWALL_02]

Question 32: 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?

- [x] 443
- [ ] 69
- [ ] 23
- [ ] 80
- [ ] 21

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 33: Incorrect

You are configuring a firewall to allow access to a server hosted in the demilitarized zone of your network. You open IP ports 80, 25, 110 and 143. Assuming that no other ports on the firewall need to be configured to provide access, what applications are most likely to be hosted on the server?

- [x] Web server, email server
- [ ] Web server, DNS server, DHCP server
- [ ] Web server, DNS server, email server
- [ ] email server, Newsgroup server, DNS server

Explanation

TCP/IP port 80 is associated with accessing Web pages from a Web server using the Hypertext Transfer Protocol (HTTP). Email can be accessed using a number of protocols including the Simple Mail Transfer Protocol (SMTP), the Post Office Protocol version 3 (POP3) and the Internet Message Access Protocol version 4 (IMAP4). SMTP uses TCP/IP port 25, while POP3 uses TCP/IP port 110, and IMAP4 uses TCP/IP port 143. Domain Name Service (DNS) traffic uses TCP/IP port 53. Newsgroup servers are accessed using the Network News Transfer (NNTP) protocol on TCP/IP port 119. Dynamic Host Configuration Protocol (DHCP) traffic uses the BOOTP protocol on TCP/IP ports 67 and 68.

References

LabSim for PC Pro, Section 12.10.
[pcpro2016_all_questions_en.exm FIREWALL_04]

Question 34: Incorrect

Which of the following is the best device to deploy to protect your private network from a public untrusted network?

- Router
- Firewall
- Gateway
- Hub

Explanation

A firewall is the best device to deploy to protect your private network from a public untrusted network. Firewalls are used to control traffic entering and leaving your trusted network environment. Firewalls can manage traffic based on source or destination IP address, port number, service protocol, application or service type, user account, and even traffic content. Routers offer some packet-based access control, but not as extensive as that of a full-fledged firewall. Hubs and gateways are not sufficient for managing the interface between a trusted and an untrusted network.

References

LabSim for PC Pro, Section 12.10.
[pcpro2016_all_questions_en.exm FIREWALL_05]

Question 35: Incorrect

Which of the following is a firewall function?

- Packet filtering
- Packet rearranging
- Protocol converting
- Encrypting
- FTP hosting

Explanation

Firewalls often filter packets by checking each packet against a set of administrator-defined criteria. If the packet is not accepted, it is simply dropped.

References

LabSim for PC Pro, Section 12.10.
[pcpro2016_all_questions_en.exm FIREWALL_06]

Question 36: Incorrect

In which of the following situations should you install a firewall?

- You want to restrict Internet users from accessing private data on your network.
- You want to improve Internet performance by saving popular websites locally.
- You want to implement a password system for Internet users who access your private website.
- You want Internet users to see a single IP address when accessing your company network.

Explanation

Firewalls limit traffic by blocking connections that are initiated from an untrusted network, such as the Internet, unless the traffic matches rules you configure in the firewall's access control list (ACL).

References

LabSim for PC Pro, Section 12.10.
[pcpro2016_all_questions_en.exm FIREWALL_07]

Question 37: Incorrect

Which of the following actions directly improves system security on Windows systems? (Select two.)

- [ ] Use Backup and Restore in Control Panel to schedule regular backups.
- [ ] Use File History to back up user files.
- [ ] Install anti-malware software.
- [ ] Enable the Windows firewall.
- [ ] Disable automatic updates.
- [ ] Configure 802.11n networking.

Explanation

Two actions that directly improve system security are enabling the Windows firewall and installing anti-malware software. The firewall restricts incoming network traffic to block attacks. Anti-malware software scans files for malicious code.

802.11n is a wireless networking standard. Making regular backups protects data from loss. Turning off automatic updates decreases security as bugs and security holes in the operating system will not be fixed in a timely manner.

References

LabSim for PC Pro, Section 12.1.
[pcpro2016_all_questions_en.exm SECURITY_BEST_02]

Question 38: Incorrect

You want to be able to access your home computer using Remote Desktop while traveling. You enable Remote Desktop, but you find that you cannot access your computer outside of your home network. What should you do?

- Configure a VPN connection to your computer.
-

Move your home computer outside of the firewall.

Open the Telnet and SSH ports in your firewall.

➡ Open the firewall port for the Remote Desktop protocol.

Explanation

You need to open the firewall port for the Remote Desktop program. Firewalls prevent all but authorized traffic. To allow a specific program, open the port that corresponds to the port used by that application.

Placing your computer outside of the firewall leaves it open to attack. A VPN encrypts communications between two computers through the Internet. However, the VPN will not allow a Remote Desktop connection. The Telnet and SSH ports do not apply to this scenario.

References

LabSim for PC Pro, Section 12.10.
[pcpro2016_all_questions_en.exm FIREWALL_01]

Question 39: Incorrect

To access your company's internal network from home, you use Secure Shell (SSH). The administrator has recently implemented a new firewall at the network perimeter and disabled as many ports as possible.

Which port needs to remain open so you can still work from home?

443

80

23

21

➡ 22

Explanation

SSH uses port 22. This port would need to remain open for you to access your company's internal network from home.

SSL uses port 443, FTP uses port 21, and HTTP uses port 80. Telnet uses port 23.

References

LabSim for PC Pro, Section 12.10.
[pcpro2016_all_questions_en.exm FIREWALL_08]

Question 40: 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.

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

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

Autorun has been disabled on a Windows workstation.

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 41: Incorrect

What is a program that appears to be a legitimate application, utility, game, or screensaver, but performs malicious activities surreptitiously?

- Worm
- Ransomware
- Scareware
- Trojan horse

Explanation

A Trojan horse is a program that appears to be a legitimate application, utility, game, or screensaver but which performs malicious activities surreptitiously. Trojan horses are very common on the Internet. To keep your systems secure and free from such malicious code, you need to take extreme caution when downloading any type of file from just about any site on the Internet. If you don't fully trust the site or service that is offering a file, don't download it.

A worm is a type of malicious code, similar to a virus, whose primary purpose is to duplicate itself and spread, while not necessarily intentionally damaging or destroying resources. Ransomware is a form of malware that denies access to an infected computer system until the user pays a ransom. Scareware is a scam that fools users into thinking they have some form of malware on their system. The intent of the scam is to sell the user fake antivirus software to remove malware they don't have.

References

LabSim for PC Pro, Section 12.6.
[pcpro2016_all_questions_en.exm MALWARE_09]

Question 42: Incorrect

Which of the following best describes spyware?

- It is a malicious program that is disguised as legitimate software.
- It monitors the actions of the user, then sends pop-up ads to the user that match their tastes.
- It monitors the actions you take on your machine and sends the information back to its originating source.
- It is a program that attempts to damage a computer system and replicate itself to other computer systems.

Explanation

Spyware monitors the actions you take on your machine and sends the information back to its originating source. Adware monitors the actions of the user that would denote their personal preferences, then sends pop-ups and ads to the user that match their tastes. A virus is a program that attempts to damage a computer system and replicate itself to other computer systems. A Trojan horse is a malicious program that is disguised as legitimate software.

References

LabSim for PC Pro, Section 12.6.
[pcpro2016_all_questions_en.exm MALWARE_11]

Question 43: Incorrect

What is a cookie?

- An executable file that runs in the background and tracks Internet use.
- A malicious program that runs when you read an e-mail attachment.
- A file saved on your hard drive that tracks Web site preferences and use.
- A malicious program that disguises itself as a useful program.

Explanation

A cookie is a file saved on your hard drive that tracks Web site preferences and use. Many legitimate Web sites use cookies to remember your preferences and make the Web sites easier to use. However, other sites can use cookies to track personal information. Spyware is a program that runs in the background and reports Internet use to servers on the Internet. A Trojan horse is a malicious program that disguises itself as a useful program. Programs do not run when you simply read an e-mail attachment. However, many malicious script programs are disguised as simple text files and can cause damage if you run the script file.

References

LabSim for PC Pro, Section 12.6.
[pcpro2016_all_questions_en.exm MALWARE_12]

Question 44: Incorrect

Which type of malicious activity can be described as numerous unwanted and unsolicited e-mail messages sent to a wide range of victims?

- E-mail hijacking
- Crimeware
- Spamming
- Trojan horse

Explanation

Spamming is a type of malicious activity in which numerous unwanted and unsolicited e-mail messages are sent to a wide range of victims. Spam itself may or may not be malicious in nature. Unfortunately, spam accounts for 40% to 60% of the e-mail traffic on the Internet. Most of this activity is unsolicited.

References

LabSim for PC Pro, Section 12.6.
[pcpro2016_all_questions_en.exm MALWARE_14]

Question 45: Incorrect

While browsing the Internet, you notice that your browser displays pop-ups containing advertisements that are related to recent keyword searches you have performed.

What is this an example of?

- Trojan horse

- Worm
- Grayware
- Adware

Explanation

Adware monitors actions that denote personal preferences, then sends pop-ups and ads that match those preferences. Adware is:

- Usually passive.
- Invasive.
- Installed on your machine by visiting a particular Web site or running an application.
- Usually more annoying than harmful.

A worm is a self-replicating virus. Grayware is software that might offer a legitimate service, but which also includes features that you aren't aware of or features that could be used for malicious purposes. A Trojan horse is a malicious program that is disguised as legitimate or desirable software.

References

LabSim for PC Pro, Section 12.6.
[pcpro2016_all_questions_en.exm MALWARE_15]

Question 46: Incorrect

You've just received an e-mail message that indicates a new serious malicious code threat is ravaging across the Internet. The message contains detailed information about the threat, its source code, and the damage it can inflict. The message states that you can easily detect whether or not you have already been a victim of this threat by the presence of three files in the \Windows\System32 folder. As a countermeasure, the message suggests that you delete these three files from your system to prevent further spread of the threat.

What should your first action based on this message be? (Select two.)

- [ ] Run a full anti-malware scan.
- [ ] Perform a complete system backup.
- [ ] Reboot the system.
- [ ] Distribute the message to everyone in your address book.
- [ ] Delete the indicated files if present.
- [ ] Verify the information on well-known malicious code threat management Web sites.

Explanation

The best first step to take after receiving an e-mail message about a new malicious code threat is to verify the information it contains. You can easily verify information by visiting two or more well-known malicious threat management Web sites. These sites can be your anti-malware vendor or a well-known and well-regarded Internet security watch group. All too often, messages of this type are hoaxes. It is important not to fall prey to e-mail hoaxes or spread them to others. If you are still concerned, you could run a full anti-malware scan on your system.

Your first step should not be to follow any directions included in the e-mail, especially deleting files. You should never forward e-mail warnings until you have firmly established the authenticity and validity of such information. Making a full backup is often a good idea, but it is not necessary in this instance.

References

LabSim for PC Pro, Section 12.6.
[pcpro2016_all_questions_en.exm MALWARE_16]

Question 47: Incorrect

You are a security consultant and have been hired to evaluate an organization's physical security practices. All employees must pass through a locked door to enter the main work area. Access is restricted using a biometric fingerprint lock. A receptionist is located next to the locked door in the reception area. She uses an iPad application to log any security events that may occur. She also uses her iPad to complete work tasks as assigned by the organization's CEO. Network jacks are provided in the reception area such that employees and vendors can access the company network for work-related purposes. Users within the secured work area have been trained to lock their workstations if they will be leaving them for any period of time.

What recommendations would you make to this organization to increase their security? (Select two.)

- [ ] Move the receptionist's desk into the secured area.
- [ ] Disable the network jacks in the reception area.
- [ ] Require users to use screensaver passwords
- [ ] Replace the biometric locks with smart cards.
- [ ] Train the receptionist to keep her iPad in a locked drawer when not in use.

Explanation

You should recommend the following:

- Disable the network jacks in the reception area. Having these jacks in an unsecured area allows anyone who comes into the building to connect to the company's network.
- Train the receptionist to keep her iPad in a locked drawer when not in use. Tablet devices are small and easily stolen if left unattended.

The receptionist's desk should remain where it is currently located because it allows her to visually verify each employee as they access the secured area. Biometric locks are generally considered more secure than smart cards because cards can be easily stolen. Training users to lock their workstations is more secure than screensaver passwords, although this may be a good idea as a safeguard in case a user forgets.

References

LabSim for PC Pro, Section 12.3.
[pcpro2016_all_questions_en.exm PHYSICAL_SECURITY_01]

Question 48: Incorrect

You have 5 salespersons who work out of your office and who frequently leave their laptops laying on their desk in their cubicles. You are concerned that someone might walk by and take one of these laptops. Which of the following is the best protection to implement to address your concerns?

- ( ) Implement screen saver passwords.
- ( ) Require strong passwords in the local security policy.
- ( ) Use cable locks to chain the laptops to the desks.
- ( ) Encrypt all company data on the hard drives.

Explanation

The main concern in this case is with laptops being stolen. The best protection against physical

theft is to secure the laptops in place using a cable lock. Requiring strong passwords or using encryption might prevent unauthorized users from accessing data on the laptops, but does not prevent physical theft.

References

LabSim for PC Pro, Section 12.3.
[pcpro2016_all_questions_en.exm PHYSICAL_SECURITY_02]

Question 49: Incorrect

You need to enable a screen saver password on the Windows workstations in your organization. Which Control Panel option should you use to do this?

- System and Security
- Windows Firewall
- Personalization
- Power Options
- Ease of Access

Explanation

Use the Personalization option in Control Panel to enable a screen saver password on a Windows 7 workstation.

References

LabSim for PC Pro, Section 12.3.
[pcpro2016_all_questions_en.exm PHYSICAL_SECURITY_03]

Question 50: Incorrect

You are responsible for disposing of several old workstations formerly used by accountants in your organization's Finance department. Before being shipped to a computer recycler, you decide to make sure any old data on the hard drives is erased. To do this, you use the Windows XP Installation CDs that came with these systems to delete all partitions from the hard drives. Have you properly prepared theses systems for disposal?

- Yes, the systems are ready to be recycled.
- No, you need to also repartition and reformat the drives before disposal.
- No, you should use disk wiping software to fully erase the drives.
- No, the Windows XP installer doesn't completely remove disk partitions. You need to use a Linux fdisk utility to completely remove them.

Explanation

No, you should use disk wiping software to fully erase the drives. The problem here is that partitioning and even reformatting doesn't completely remove old data from the drive. Data could potentially be recovered from the drive. To keep this from happening, you should use disk wiping software to erase the drive and write random characters multiple times to the drive to completely destroy any old data.

References

LabSim for PC Pro, Section 12.3.
[pcpro2016_all_questions_en.exm PHYSICAL_SECURITY_04]

Question 51: Incorrect

You have purchased new computers and will be disposing of your old computers. Instead of

recycling the computers, you decide to resell them by placing an ad on the Internet. These computers were previously used for storing sensitive information. What should you do prior to getting rid of the computers?

- Reformat the hard drives
- Use data wiping software to clear the hard drives
- Delete user data and applications from the hard drives
- Include the original operating system discs and product keys with the computers

Explanation

Data wiping software will sanitize or clean a device by removing all data remnants. Sanitization is necessary because deleting, overwriting, and reformatting (even multiple times) does not remove all data remnants. Sanitization securely removes sensitive data from storage media and is designed to solve the data remanence problem for devices that will be reused. It is the best way to remove Personally Identifiable Information (PII) from a hard disk before reuse.

Deleting data and applications from the hard drives or reformatting the drive will not permanently remove data from the system. Many tools can recover deleted files.

References

LabSim for PC Pro, Section 12.3.
[pcpro2016_all_questions_en.exm PHYSICAL_SECURITY_05]

Question 52: Incorrect

You have a set of DVD-RW discs that have been used to archive files for your latest development project. You need to dispose of the discs. Which of the following methods should you use to best prevent extracting data from the discs?

- Write junk data over the discs 7 times
- Delete the data on the discs
- Shredding
- Degaussing

Explanation

To completely prevent reading data from discs, destroy them using a DVD shredder or crushing. Degaussing only works for magnetic media such as floppy and hard disk drives. Simply deleting data offers little protection. Overwriting the data multiple times is not efficient in this scenario as the discs can simply be destroyed.

References

LabSim for PC Pro, Section 12.3.
[pcpro2016_all_questions_en.exm PHYSICAL_SECURITY_06]

Question 53: Incorrect

Which of the following are common forms of social engineering attack?

- Using a sniffer to capture network traffic.
- Distributing false information about your organization's financial status.
- Hoax virus information e-mails.
- Stealing the key card of an employee and using that to enter a secured building.

Explanation

Hoax virus information e-mails are a form of social engineering attack. This type of attack preys on e-mail recipients who are fearful and will believe most information if it is presented in a professional manner. All too often, the victims of these attacks fail to double check the information or instructions with a reputable third party anti-virus software vendor before implementing the recommendations. Usually these hoax messages instruct the reader to delete key system files or download Trojan horses. Social engineering relies on the trusting nature of individuals to take an action or allow unauthorized action.

References

LabSim for PC Pro, Section 12.4.
[pcpro2016_all_questions_en.exm SOCMED_SECURITY_01]

Question 54: Incorrect

Which of the following is a form of attack that tricks victims into providing confidential information, such as identity information or logon credentials, through emails or Websites that impersonate an online entity that the victim trusts, such as a financial institution or well-known e-commerce site?

- Phishing
- Session hijacking
- Fraggle attack
- Social engineering

Explanation

Phishing tricks victims into providing confidential information, such as identity information or logon credentials, through emails or Websites that impersonate an online entity that the victim trusts, such as a financial institution or well-known e-commerce site. Phishing is a specific form of social engineering. A fraggle attack uses spoofed UDP packets to flood a victim with echo requests using a bounce network, thus it is similar to Smurf. Session hijacking takes over a logon session from a legitimate client, thus impersonating the user and taking advantage of their established communication link.

References

LabSim for PC Pro, Section 12.4.
[pcpro2016_all_questions_en.exm SOCMED_SECURITY_02]

Question 55: Incorrect

Question 56: Incorrect

What is the best countermeasure against social engineering?

- Access auditing
- Strong passwords
- User awareness training
- Acceptable use policy

Explanation

The best countermeasure to social engineering is user awareness training. If users understand the importance of security and the restrictions on types of information, they are less likely to

reveal confidential information or perform unauthorized activities at the prompting of a stranger or a claimed identity over the phone.

References

LabSim for PC Pro, Section 12.4.
[pcpro2016_all_questions_en.exm SOCMED_SECURITY_04]

Question 57: Incorrect

You are a security consultant and an organization has hired you to review their security measures. They are chiefly concerned that they could become the victim of a social engineering attack.

What should you recommend they do to mitigate the risk?

- Train managers to monitor user activity.
- Implement a border firewall to filter inbound network traffic.
- Teach users how to recognize and respond to social engineering attacks.
- Establish a written security policy.

Explanation

The best way to combat social engineering is to train users how to recognize and respond to social engineering attacks. For example, most organizations train employees to forward any calls or e-mails requesting a password or other network information to their help desk.

Filtering network traffic with a firewall fails to address the human element involved in social engineering. While a written security policy is a necessary measure, it will do little to defend your network if your users don't know how to recognize social engineering attempts. Management oversight is expensive and unlikely to detect a social engineering attempt until it is too late. Raising user awareness of the issue tends to be much more effective.

References

LabSim for PC Pro, Section 12.4.
[pcpro2016_all_questions_en.exm SOCMED_SECURITY_05]

Question 58: Incorrect

Several users have forwarded you an e-mail stating that your company's health insurance provider has just launched a new web site for all employees. To access the site they are told in the e-mail to click a link and provide their personal information. Upon investigation, you discover that your company's health insurance provider did not send this e-mail.

What kind of attack just occurred?

- Piggybacking
- Smurf
- Phishing
- Denial of service

Explanation

A phishing attack has occurred. In a phishing attack, a spoofed email containing a link to a fake website is used to trick users into revealing sensitive information, such as a username, password, bank account number, or credit card number. Both the email and the website used in the attack appear on the surface to be legitimate.

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. A

denial of service (DoS) attack involves using network mechanisms to flood a particular host with so many bogus requests that it can no longer respond to legitimate network requests. A Smurf attack is a distributed type of DoS attack that inserts a target system's IP address for the source address of ICMP echo request packets, causing a flood of ICMP echo response packets to be sent to a victim system.

References

LabSim for PC Pro, Section 12.4.
[pcpro2016_all_questions_en.exm SOCMED_SECURITY_06]

Question 59: Incorrect

An intruder waits near an organization's secured entrance until an employee approaches the entrance and unlocks it with a security badge. The intruder falls in line behind the employee, who assumes the intruder is another employee and holds the door open for her.

What kind of attack just occurred?

- Smurf
- Phishing
- Tailgating
- Denial of service

Explanation

A tailgating attack has occurred. Tailgating occurs when an unauthorized person follows behind an authorized person to enter a secured building or area within a building. Tailgating is also sometimes called piggybacking.

In a phishing attack, a spoofed email containing a link to a fake website is used to trick users into revealing sensitive information, such as a username, password, bank account number, or credit card number. Both the email and the website used in the attack appear on the surface to be legitimate. A denial of service (DoS) attack involves using network mechanisms to flood a particular host with so many bogus requests that it can no longer respond to legitimate network requests. A Smurf attack is a distributed type of DoS attack that inserts a target system's IP address for the source address of ICMP echo request packets, causing a flood of ICMP echo response packets to be sent to a victim system.

References

LabSim for PC Pro, Section 12.4.
[pcpro2016_all_questions_en.exm SOCMED_SECURITY_07]

Question 60: Incorrect

Which security measure can be used to generate and store cryptographic keys?

- Trusted Platform Module (TPM)
- DriveLock
- Chassis intrusion detection
- BIOS/UEFI password

Explanation

A Trusted Platform Module (TPM) is a special chip on the motherboard that generates and stores cryptographic keys. The TPM can be used by applications (such as Bitlocker on Windows systems) to generate and save keys that are used for encryption.

DriveLock is a disk encryption solution. Chassis intrusion detection helps you identify when a

system case has been opened. A BIOS/UEFI password controls access to the BIOS/UEFI setup program.

References

LabSim for PC Pro, Section 12.5.
[pcpro2016_all_questions_en.exm BIOSSEC_01]

Question 61: Incorrect

Which of the following functions are performed by the TPM?

- Encrypt data on the hard disk drive
- Generate authentication credentials
- Perform bulk encryption
- Create a hash based on installed system components

Explanation

A Trusted Platform Module (TPM) is a hardware cryptoprocessor that resides on the motherboard that stores and generates cryptographic keys. Using these keys, the TPM can generate a hash value based on the components installed in the system. The hash value can be used to verify that system components have not been modified when the system boots. Because each system will have a unique hash value, the hash can also be used as a form of identification for the system. Keys generated by the TPM can be used for encryption and authentication, but the TPM does not perform the actual encryption.

References

LabSim for PC Pro, Section 12.5.
[pcpro2016_all_questions_en.exm BIOSSEC_02]

Question 62: Incorrect

You want to configure your computer so that a password is required before the operating system will load.

What should you do?

- Configure chassis instruction detection
- Require complex passwords in the local security policy
- Configure an administrator password in the BIOS/UEFI
- Configure a user password in the BIOS/UEFI

Explanation

Configuring a user password in the BIOS/UEFI requires that a valid password is entered before the operating system will load.

When an administrative password is set, it must be entered in order to access the firmware setup program. Chassis intrusion detection helps you identify when a system case has been opened. Password settings in the local security policy controls passwords associated with user accounts that are configured within the operating system. These passwords are used after the system loads the operating system, not before.

References

LabSim for PC Pro, Section 12.5.
[pcpro2016_all_questions_en.exm BIOSSEC_03]

Question 63: Incorrect

You have purchased a used computer from a computer liquidator. When you boot the computer, you find that there has been a password set on the BIOS. You need to clear the password so that you can edit the CMOS settings.

What should you do?

- Press Ctrl + Alt + Del while booting the computer.
- Flash the BIOS.
- Press F2 while booting the computer.
- Move the motherboard jumper.

Explanation

To reset the BIOS password, most motherboards have a jumper labeled *RTC Clear* or *CMOS Clear*. Removing the jumper or moving it to a different setting for a short period of time resets all CMOS settings to their default values.

Flashing the BIOS probably will not remove the password.

References

LabSim for PC Pro, Section 12.5.
[pcpro2016_all_questions_en.exm BIOSSEC_04]

Question 64: Incorrect

Which of the following would indicate when a system case cover is removed?

- Chassis intrusion detection
- BIOS password
- DriveLock
- Trusted Platform Module (TPM)

Explanation

Chassis intrusion detection helps you identify when a system case has been opened. When the case cover is removed, an alert is recorded in the BIOS. A BIOS password controls access to the system. If set, the administrator (or supervisor or setup) password is required to enter the CMOS program to make changes to BIOS settings. A Trusted Platform Module (TPM) is a special chip on the motherboard that generates and stores cryptographic keys to verify that the hardware has not changed. This value can be used to prevent the system from booting if the hardware has changed. DriveLock is a disk encryption solution.

References

LabSim for PC Pro, Section 12.5.
[pcpro2016_all_questions_en.exm BIOSSEC_05]

Question 65: Incorrect

What is the common name for a program that has no useful purpose, but attempts to spread itself to other systems and often damages resources on the systems where it is found?

- Buffer overflow
- Virus
- Trojan horse
- Password attack

Explanation

A virus is the common name for a program that has no useful purpose, but attempts to spread itself to other systems and often damages resources on the systems where it is found. Viruses are a serious threat to computer systems, especially if they are connected to the Internet. You should install anti-malware software on every computer in your network to protect against viruses.

Trojan horses are programs that claim to serve a useful purpose but hide a malicious purpose or activity. A buffer overflow is partially correct in that a buffer overflow may be used as an insertion vector for a virus. A password attack attempts to identify the password used by a user account.

References

LabSim for PC Pro, Section 12.6.
[pcpro2016_all_questions_en.exm MALWARE_17]

Question 66: Incorrect

What are the most common means of virus distribution? (Select two.)

- [x] Malicious web sites
- [ ] Downloading music files from the Internet
- [ ] Floppy disks
- [ ] Commercial software CDs
- [x] E-mail

Explanation

E-mail is the most common means of virus distribution. Often viruses will employ self-contained SMTP servers to facilitate self-replication and distribution over the Internet. Viruses are able to spread quickly and broadly by exploiting the communication infrastructure of Internet e-mail. Malicious web sites are also frequently used for virus distribution. For this reason, it is important to keep your anti-virus software updated so as to block any possible attempt of viruses to infect your systems or to spread to other systems from your system.

Downloaded music files and commercial software CDs all have the potential to spread viruses, but they are not as commonly employed.

References

LabSim for PC Pro, Section 12.6.
[pcpro2016_all_questions_en.exm MALWARE_18]

Question 67: Incorrect

After installing new software a few days ago, your DVD drive tray randomly began to open and close. Today, you were called into your boss's office to discuss why you are calling 900 numbers while at work. Which type of malware would create these symptoms?

- (x) Grayware
- ( ) Spyware
- ( ) Crimeware
- ( ) Adware

Explanation

Grayware is software that might offer a legitimate service, but which also includes features that you aren't aware of or features that could be used for malicious purposes. Most classifications of

grayware include:

- Joke programs that perform annoying yet harmless actions (such as displaying messages or opening/closing the optical drive tray)
- Dialer programs that automatically dial long-distance or 900 numbers
- Adware and spyware programs

Adware monitors actions that denote personal preferences, then sends pop-ups and ads that match those preferences. Spyware is software that is installed without the user's consent or knowledge, designed to intercept or take partial control over the user's interaction with the computer. Crimeware is designed to facilitate identity theft by gaining access to a user's online financial accounts, such as banks and online retailers.

References

LabSim for PC Pro, Section 12.6.
[pcpro2016_all_questions_en.exm MALWARE_20]

Question 68: 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.)

- [ ] Enforce password history
- [x] Minimum password length
- [ ] Account lockout duration
- [ ] Maximum password age
- [ ] Password complexity
- [x] Account lockout threshold

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 69: 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?

- ( ) Enable the account
- ( ) Have the user wait for the account to be unlocked automatically

- Unlock the account
- Change the password for 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, manually unlock the account.

A disabled account cannot be used for logon. 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 70: Incorrect

You manage two computers with the following user accounts:

- Wrk1 has user accounts Mary and Admin. The Mary account does not have a password set; the Admin account does.
- Wrk2 has user accounts Mary and Julia. The Mary account has a password set; the Julia account does not.

You are working from Wrk2 and would like to access a shared folder on Wrk1. What credentials should you use to access the shared folder?

- Type Mary for the username and leave the password blank
- Type Mary for the username and specify the password
- Type Julia for the username and leave the password blank
- Type Admin for the username and specify the password

Explanation

Type Admin for the username and specify the password. To access a shared folder or use Remote Desktop for a workgroup computer, you must supply a username and password that matches a user account configured on the computer you are trying to access. For Wrk1, you would use either Mary or Admin for the user account name. You cannot use the Mary account to access Wrk1 over the network. 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.

References

LabSim for PC Pro, Section 12.7.
[pcpro2016_all_questions_en.exm AUTHORIZATION_11]

Question 71: Incorrect

A user is trying to log into her notebook computer. She enters the correct password for her user account, but the system won't let her authenticate, claiming the wrong password has been entered. What's causing the problem?

- The Scroll Lock key has been pressed, locking all input from the keyboard.
- She has entered the wrong password too many times, causing Intruder Detection in

Windows to lock the system.

- The keyboard must be replaced.
- The CPU is in power-save mode causing all login attempts to be denied.
- She has enabled Num Lock, causing numbers to be sent from the keyboard instead of letters.

Explanation

The most likely cause of this user's problem is that the Num Lock key sequence for the notebook system has been pressed causing the keyboard to send numbers in the place of letters. Turning Num Lock off should fix the problem.

References

LabSim for PC Pro, Section 12.7.
[pcpro2016_all_questions_en.exm AUTHORIZATION_12]

Question 72: 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?

- Configure a password for the Administrator account
- Make the Administrator account a member of the Remote Desktop Users group
- Disable fast user switching on the computer
- Unlock the Administrator account

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 73: Incorrect

You are configuring the local security policy of a Windows system. You want to prevent users from reusing old passwords. You also want to force them to use a new password for at least 5 days before changing it again. Which policies should you configure? (Select two.)

- [ ] Password complexity
- [ ] Maximum password age
- [ ] Minimum password age
- [ ] Enforce password history

Explanation

Set the Enforce password history policy to prevent users from reusing old passwords. Set the Minimum password age policy to prevent users from changing passwords too soon. Passwords must remain the same for at least the time period specified. Use the Maximum password age policy to force periodic changes to the password. After the maximum password age has been reached, the user must change the password. Use the Password complexity to require that passwords include letters, numbers, and symbols. This makes it harder for hackers to guess or crack passwords.

References

LabSim for PC Pro, Section 12.7.
[pcpro2016_all_questions_en.exm AUTHORIZATION_14]

Question 74: Incorrect

Which are examples of a strong password? (Select two.)

- [ ] Morganstern
- [ ] skippy
- [x] il0ve2EatIceCr3am
- [x] TuxP3nguinsRn0v3l
- [ ] NewYork

Explanation

A strong password is one that:

- Is at least 6 characters long (longer is better)
- Is not based on a word found in a dictionary
- Contains both upper-case and lower-case characters
- Contains numbers
- Does not contain words that can be associated with you personally
- Is changed frequently

The passwords *il0ve2EatIceCr3am* and *TuxP3nguinsRn0v3l* both meet the above criteria.

The password *NewYork* is long enough and includes upper- and lower-case letters, however it doesn't contain numbers and could be easily dissected into a dictionary word. The password *skippy* is probably a pet name. The password *Morganstern* is probably someone's last name (e.g. a spouse's name or perhaps someone's maiden name).

References

LabSim for PC Pro, Section 12.1.
[pcpro2016_all_questions_en.exm SECURITY_BEST_03]

Question 75: Incorrect

One of the Windows workstations you manage has four user accounts defined on it. Two of the users are limited users while the third (your account) is an administrative user. The fourth account is the Guest user account, which has been enabled to allow management employees convenient workstation access. 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. Autorun has been disabled on the system. What should you do to increase the security of this system?

- (x) Disable the Guest account.
- ( ) Enable autorun on the system.

- ◯ Change the two limited user accounts to administrative users.
- ◯ Change your user account to a limited user.

Explanation

The Guest user account has no password and provides too much access to the system. Unless you have an overriding reason to do so, the Guest user account should remain disabled.

Changing your administrative user account to a limited user would prevent you from completing management tasks on the workstation. Changing the two limited user accounts to administrative users would decrease the security of the system as would enabling autorun functionality.

References

LabSim for PC Pro, Section 12.1.
[pcpro2016_all_questions_en.exm SECURITY_BEST_04]

Question 76: 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.
- ☐ Enable the Guest account.
- ☐ Assign each user a simple password so they won't be tempted to write it down.
- ➡ ☐ Disable autorun on the system.
- ☐ Change the two limited user accounts to restricted users.

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 77: Incorrect

Which TCP/IP protocol is a secure form of HTTP that uses SSL as a sublayer for security?

- ◯ DNS
- ◯ SSH
- ◯ SMTP
- ➡ ◯ HTTPS

Explanation

HTTPS is a secure form of HTTP that uses SSL as a sublayer for security. SMTP is used to route electronic mail through the internetwork. SSH allows for secure interactive control of remote systems. DNS is a system that is distributed throughout the internetwork to provide address/name resolution.

References

LabSim for PC Pro, Section 12.8.
[pcpro2016_all_questions_en.exm ENCRYPT_01]

Question 78: Incorrect

You want a security solution that protects the entire hard drive, preventing access even when it is moved to another system. Which solution would you choose?

- EFS
- BitLocker
- IPSec
- VPN

Explanation

BitLocker is a Microsoft security solution which encrypts the entire contents of a hard drive, protecting all files on the disk. BitLocker uses a special key which is required to unlock the hard disk. You cannot unlock/decrypt a drive simply by moving it to another computer. EFS is a Windows file encryption option, but only encrypts individual files. Encryption and decryption is automatic and dependent upon the file's creator and whether other uses have read permissions. A virtual private network (VPN) uses an encryption protocol (such as IPSec, PPTP, or L2TP) to establish a secure communication channel between two hosts, or between one site and another site. Data that passes through the unsecured network is encrypted and protected.

References

LabSim for PC Pro, Section 12.8.
[pcpro2016_all_questions_en.exm ENCRYPT_02]

Question 79: Incorrect

Which of the following security solutions would prevent a user from reading a file which she did not create?

- EFS
- IPSec
- BitLocker
- VPN

Explanation

EFS is a Windows file encryption option that encrypts individual files so that only the user who created the file can open it. Decryption is automatic when the file owner opens it. Other users cannot open the encrypted file unless specifically authorized. BitLocker is a Microsoft security solution which encrypts the entire contents of a hard drive, protecting all files on the disk. BitLocker uses a special key which is required to unlock the hard disk. You cannot unlock/decrypt a drive simply by moving it to another computer. A virtual private network (VPN) uses an encryption protocol (such as IPSec, PPTP, or L2TP) to establish a secure communication channel between two hosts, or between one site and another site. Data that passes through the unsecured network is encrypted and protected.

References

LabSim for PC Pro, Section 12.8.
[pcpro2016_all_questions_en.exm ENCRYPT_03]

Question 80: Incorrect

Which of the following protocols establish a secure connection and encrypt data for a VPN? (Select three.)

- [x] PPTP
- [ ] RDP
- [x] L2TP
- [x] IPSec
- [ ] FTP

Explanation

A virtual private network (VPN) uses an encryption protocol (such as IPSec, PPTP, or L2TP) to establish a secure communication channel between two hosts, or between one site and another site. Data that passes through the unsecured network is encrypted and protected. The Remote Desktop Protocol (RDP) is used by Windows Terminal Services based applications, including Remote Desktop. FTP is used for transferring files and will not establish a secure connection.

References

LabSim for PC Pro, Section 12.8.
[pcpro2016_all_questions_en.exm ENCRYPT_04]

Question 81: Incorrect

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

- ( ) ISDN
- (x) Wireless
- ( ) DSL
- ( ) Satellite
- ( ) Dial-up

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 82: Incorrect

Which of the following components, used with BitLocker, is a special hardware chip included on the computer motherboard that contains software in firmware that generates and stores cryptographic keys. ?

- (x) Trusted Platform Module (TPM)

- BitLocker partition
- BIOS/UEFI
- USB device

Explanation

A Trusted Platform Module (TPM) is a special hardware chip included on the computer motherboard that contains software in firmware that generates and stores cryptographic keys.

The TPM chip must be enabled in the BIOS/UEFI. A USB device is used to save the BitLocker key on a system that does not have a TPM chip. Implementing BitLocker requires two NTFS partitions.

References

LabSim for PC Pro, Section 12.8.
[pcpro2016_all_questions_en.exm ENCRYPT_06]

Question 83: Incorrect

Which of the following provides security for wireless networks?

- 802.11a
- WPA2
- WAP
- 802.3u
- CSMA/CD

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 84: Incorrect

Which of the following wireless security methods uses a common shared key configured on the wireless access point and all wireless clients?

- WPA Personal and WPA2 Personal
- WEP, WPA Personal, and WPA2 Personal
- WPA Enterprise and WPA2 Enterprise
- WEP, WPA Personal, WPA Enterprise, WPA2 Personal, and WPA2 Enterprise
- WEP

Explanation

Shared key authentication can be used with WEP, WPA, and WPA2. Shared key authentication

used with WPA and WPA2 is often called WPA Personal or WPA2 Personal. WPA Enterprise and WPA2 Enterprise use 802.1x for authentication. 802.1x authentication uses usernames and passwords, certificates, or devices such as smart cards to authenticate wireless clients.

References

LabSim for PC Pro, Section 12.8.
[pcpro2016_all_questions_en.exm ENCRYPT_08]

Question 85: Incorrect

Question 86: Incorrect

While browsing the Internet, a pop-up browser window is displayed warning you that your system is infected with a virus. You are directed to click a link to remove the virus.

What should you do? (Select two.)

- [ ] Click on the link provided to scan for and remove the virus.
- [ ] Run a full system scan using the anti-malware software installed on your system.
- [ ] Update the virus definitions for your locally-installed anti-malware software.
- [ ] Close the pop-up window and ignore the warning.
- [ ] Use a search engine on the Internet to learn how to manually remove the virus.

Explanation

This is an example of a rogue anti-virus attack. As such, you should assume that your system may have been infected by some time of malware, possibly by one of the sites you visited recently.

You should first close your browser window and then update the virus definitions for your locally-installed anti-virus software. Once done, you should Run a full system scan using the anti-virus software installed on your system.

Clicking the link provided would be the worst choice as it will most likely install a host of malware on your system. Ignoring the message is unwise as your system has probably been infected with malware that should be removed. You shouldn't try to manually remove the virus as the message displayed by the rogue anti-virus attack is probably fictitious.

References

LabSim for PC Pro, Section 12.13.
[pcpro2016_all_questions_en.exm MALWARE_23]

Question 87: Incorrect

Which techniques are used in a pharming attack to redirect legitimate web traffic to malicious websites? (Select two.)

- [ ] Changing the hosts file of a user's computer
- [ ] Exploiting DHCP servers to deliver the IP address of poisoned DNS servers
- [ ] Dictionary attack
- [ ] Man-in-the-middle attack
- [ ] Search engine results poisoning

Explanation

Pharming redirects one website's traffic to another, bogus website that is designed to look like the

real website. Once there, the attacker tricks the user into supplying personal information, such as bank account and PIN numbers. Pharming works by resolving legitimate URLs to the IP address of malicious websites. This is typically done using one of the following techniques:

- Changing the hosts file of a user's computer
- Poisoning a DNS server
- Exploiting DHCP servers to deliver the IP address of malicious DNS servers in DHCP leases

Search engine results poisoning is not typically associated with pharming attacks. A man-in-the-middle attack occurs when the attacker intercepts legitimate network traffic and then poses as one of the parties involved in the network communication. A dictionary attack is used to crack passwords by guessing the password from a list of likely words.

References

LabSim for PC Pro, Section 12.13.
[pcpro2016_all_questions_en.exm MALWARE_24]

Question 88: Incorrect

Which of the following are likely symptoms of malware infection? (Select two.)

- [ ] Receipt of phishing emails in your inbox
- [ ] Renamed system files
- [ ] Changed file permissions
- [ ] Operating system updates that were installed without your knowledge
- [ ] Cookies placed by a website recently visited

Explanation

Common symptoms of a malware infection include the following:

- Slow computer performance
- Internet connectivity issues
- Operating system lock ups
- Windows update failures
- Renamed system files
- Disappearing files
- Changed file permissions
- Access denied errors

Cookies are commonly placed by legitimate websites and aren't considered a major security threat. Windows operating systems automatically install updates by default. Receiving phishing emails doesn't necessarily indicate that the system is infected with malware. It's more likely your email address has been picked up and included on a list.

References

LabSim for PC Pro, Section 12.13.
[pcpro2016_all_questions_en.exm MALWARE_25]

Question 89: Incorrect

Which of the following is the most secure security protocol for wireless networks?

- ( ) BitLocker
- ( ) 802.11n
- ( )

- WPA2
- WEP
- WPA

Explanation

WEP, WPA, and WPA2 are all security protocols for wireless networks. However, WPA2 provides much stronger security than WEP or WPA.

802.11n is a wireless standard with specific parameters for wireless data transmission. BitLocker is a Microsoft solution that provides hard drive disk encryption.

References

LabSim for PC Pro, Section 12.9.
[pcpro2016_all_questions_en.exm NET_SEC_WIRELESS_01]

Question 90: Incorrect

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

- [ ] Refusal of client connections based on MAC address
- [x] Authentication
- [x] Encryption
- [ ] Filtering of traffic based on packet characteristics
- [ ] Identification of the network
- [ ] Centralized access for clients

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 91: Incorrect

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

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

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 92: Incorrect

What is the least secure place to locate an omnidirectional access point when creating a wireless network?

- In the center of the building
- In common or community work areas
- Above the 3rd floor
- Near a window

Explanation

The least secure location for an omnidirectional wireless access point is against a perimeter wall. So, placement near a window would be the worst option from this list of selections.

For the best security, omnidirectional wireless access points should be located in the center of the. This will reduce the likelihood that the wireless network's access radius will extend outside of the physical borders of your environment (i.e. building). It is important to place wireless access points where they are needed, such as in a common or community work area.

References

LabSim for PC Pro, Section 12.9.
[pcpro2016_all_questions_en.exm NET_SEC_WIRELESS_05]

Question 93: Incorrect

You've just finished installing a wireless access point for a client. Which action best protects the access point from unauthorized tampering with its configuration settings?

- Disabling DHCP
- Implementing MAC address filtering
- Changing the administrative password
- Disabling SSID broadcast

Explanation

To prevent administrative access to the access point, change the default administrator password. If you do not change the password, users can search the Internet for the default password and use it to gain access to the access point and make configuration changes.

Disabling SSID broadcast, disabling DHCP, and using MAC address filtering helps prevent

unauthorized access to the wireless network.

References

LabSim for PC Pro, Section 12.9.
[pcpro2016_all_questions_en.exm NET_SEC_WIRELESS_06]

Question 94: Incorrect

You've just installed a wireless access point (WAP) for your organization's network. You know that the radio signals used by the WAP extend beyond your organization's building and are concerned that unauthorized users outside may be able to access your internal network. What can you do to protect the wireless network? (Select two.)

- [ ] Disable SSID broadcast on the WAP.
- [ ] Disable the spread-spectrum radio signal feature on the WAP.
- [ ] Implement a WAP with a shorter range.
- [ ] Install a radio signal jammer at the perimeter of your organization's property.
- [ ] Configure the WAP to filter out unauthorized MAC addresses.
- [ ] Use the WAP's configuration utility to reduce the radio signal strength.

Explanation

To increase the security of the wireless network, you can use the WAP's configuration utility to reduce the radio signal strength. This will reduce or even eliminate signal emanation outside of your building. You can also configure the WAP to filter out unauthorized MAC addresses. Enabling MAC address filtering denies access to unauthorized systems.

References

LabSim for PC Pro, Section 12.9.
[pcpro2016_all_questions_en.exm NET_SEC_WIRELESS_07]

Question 95: Incorrect

You are implementing a wireless access point for a small business. To secure the access point, you decide to implement WPA2 using AES to encrypt the data. The access point's configuration interface asks you to specify the AES key size.

The business owner needs the access point to be as secure as possible.

Which key size is the largest valid key size that AES can be configured to use?

- ( ) 64
- ( ) 128
- (•) 256
- ( ) 192

Explanation

When working with encryption, the general rule is that the longer the key used, the more complex the encryption and the more secure the data will be. The largest key size that can be used by AES is 256 bits.

AES doesn't support 64-bit keys. AES does support 128- and 192-bit key lengths, but they are less secure than a 256-bit key.

References

LabSim for PC Pro, Section 12.9.
[pcpro2016_all_questions_en.exm NET_SEC_WIRELESS_08]

Question 96: Incorrect

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

- They use an 802.11n wireless network.
- The wireless network is broadcasting an SSID of Linksys.
- The wireless network uses WPA2 with AES security.
- 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? (Select two.)

- [ ] Implement omni-directional access points.
- [ ] Change the SSID to something other than the default.
- [ ] Disable SSID broadcast.
- [ ] Upgrade to an 802.11g wireless network.
- [ ] Configure the wireless network to use WPA with TKIP security.

Explanation

You should recommend the following:

- Disable SSID broadcast. This makes the network harder (but not impossible) to locate.
- Change the SSID to something other than the default. This obscures what type of AP is in use.

Using WPA instead of WPA2 would decrease the security of the wireless network as would implementing omni-directional APs. Switching to an 802.11g network would dramatically reduce the speed of the network without providing any security enhancements.

References

LabSim for PC Pro, Section 12.9.
[pcpro2016_all_questions_en.exm SECURITY_BEST_06]

Question 97: Incorrect

Question 98: Incorrect

Your organization is frequently visited by sales reps. While on-site, they frequently plug their notebook systems into any available wall jack, hoping to get Internet connectivity. You are concerned that allowing them to do this could result in the spread of malware throughout your network. What should you do? (Select two.)

- [ ] Implement SNMP traps on your network switch.
- [ ] Implement MAC address filtering.
- [ ] Enable port analysis on your network switch.
- [ ] Implement private IP addressing with a Network Address Translation (NAT) router facing the Internet.
- [ ] Implement static IP addressing.

Explanation

You should consider enabling MAC address filtering. MAC filtering is configured on your network switches and is used to restrict network access to only systems with specific MAC addresses. You could also consider assigning static IP addresses to your network hosts. By not using DHCP, visitor laptops connected to a wired Ethernet jack won't receive a valid IP address and won't be able to communicate with other hosts on your network.

Implementing SNMP traps, port analysis, or a NAT router will not prevent visitors from connecting to your network.

References

LabSim for PC Pro, Section 12.9.
[pcpro2016_all_questions_en.exm SECURITY_BEST_08]

Question 99: Incorrect

Your client has hired you to evaluate their wired network security posture. As you tour their facility, you note the following:

- Server systems are kept in a locked server room.
- User accounts on desktop systems have strong passwords assigned.
- A locked door is used to control access to the work area. Users must use ID badges to enter the area.
- Users connect their personal mobile devices to their computers using USB cables.
- Users work in three 8-hour shifts per day. Each computer is shared by three users. Each user has a limited account on the computer they use.

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

- ○ Move the server systems to an empty cubicle in the work area.
- ○ Assign users easy-to-remember simple passwords so they won't be tempted to write them down.
- ○ Provision each employee with their own computer system.
- ➡ ○ Disable the USB ports on user's workstations.

Explanation

Users connecting their personal mobile devices to their computers using USB cables represents a significant security risk. Malware could be spread throughout the network. They could also copy sensitive information from the network to the device. Disabling all USB ports on all workstations will prevent this from happening. You should configure the BIOS/UEFI firmware with a password to prevent users from re-enabling the ports.

Moving the server to an empty cubicle and assigning simple passwords will decrease the overall security of the network. It isn't necessary for each employee to have their own dedicated computer system.

References

LabSim for PC Pro, Section 12.1.
[pcpro2016_all_questions_en.exm SECURITY_BEST_09]

Question 100: Incorrect

You would like to control Internet access based on users, time of day, and Web sites visited. How can you do this?

- ○ Configure Internet zones using the Internet Options.
- ○ Configure a packet-filtering firewall. Add rules to allow or deny access based on time of day and content.

- Install a proxy server. Allow Internet access only through the proxy server.
- Configure the Local Security Policy of each system to add access restrictions based on time of day and content.
- Enable Windows Firewall on each system. Add or remove exceptions to control access based on time of day and content.

Explanation

Use a proxy server to control Internet access based on users, time of day, and websites visited. You configure these rules on the proxy server, and all Internet access requests are routed through the proxy server. Use a packet filtering firewall, such as Windows Firewall, to allow or deny individual packets based on characteristics such as source or destination address and port number. Configure Internet zones to identify trusted or restricted websites and to control the types of actions that can be performed when going to those sites.

References

LabSim for PC Pro, Section 12.11.
[pcpro2016_all_questions_en.exm PROXY_01]

Question 101: Incorrect

Which of the following functions are performed by proxy servers? (Select two.)

- [x] Cache web pages
- [ ] Filter unwanted email
- [x] Block employees from accessing certain websites
- [ ] Block unwanted packets from entering your private network
- [ ] Store client files

Explanation

A proxy, or proxy server, stands between client computers and Internet Web servers. You can use a proxy server to prevent access to specific websites, or to cache (save) frequently-used web pages. When a proxy receives a request from the client, it checks to verify that the client is allowed access to the website. If allowed, it then checks its cache to see if the requested page is in the cache. If the page is already cached, then the proxy server fulfills the request by displaying the requested page from the cache rather than retrieving it from the Internet. Receiving a web page from a local proxy server is much faster than downloading the page from the Internet.

References

LabSim for PC Pro, Section 12.11.
[pcpro2016_all_questions_en.exm PROXY_02]

Question 102: Incorrect

Two employees cannot access any websites on the Internet, but can still access servers on the local network, including those residing on other subnets. Other employees are not experiencing the same problem.

What should you do?

- Use ipconfig to confirm APIPA has not assigned an IP address.
- Identify the filtering settings on the proxy server for specific Internet sites.
- Reconfigure the clients to send all traffic directly to the ISP, bypassing the proxy server.

Identify the proxy server name and port number in Internet Options.

Explanation

In this case, you should identify the proxy server name and port number in Internet Options. Windows automatically detects and uses a proxy server if one is on the network. However, if the proxy server is not detected you should manually configure the proxy settings.

If you bypass the proxy server, the clients are no longer managed by the proxy server. This is not a recommended solution. Because other users are not experiencing the same problems, the filtering settings on the proxy server for specific Internet sites are probably not the cause of the problem. IP addresses assigned by APIPA force the client to the 169.254.0.0 subnet. This would prevent the client form accessing internal servers that use static IP addresses, especially those on different subnets.

References

LabSim for PC Pro, Section 12.11.
[pcpro2016_all_questions_en.exm PROXY_03]

Question 103: Incorrect

You connect your computer to a wireless network available at the local library. You find that you can't access several websites you need to on the Internet.

What might be causing the problem?

- A firewall is blocking ports 80 and 443.
- The router has not been configured to perform port forwarding.
- Port triggering is redirecting traffic to the wrong IP address.
- A proxy server is filtering access to websites.

Explanation

A proxy server can be configured to block Internet access based on website or URL. Many schools and public networks use proxy servers to prevent access to websites with objectionable content. Ports 80 and 443 are used by HTTP to retrieve all Web content. If a firewall were blocking these ports, access would be denied to all websites. Port forwarding directs incoming connections to a host on the private network. Port triggering dynamically opens firewall ports based on applications that initiate contact from the private network.

References

LabSim for PC Pro, Section 12.11.
[pcpro2016_all_questions_en.exm PROXY_04]

Question 104: Incorrect

A VPN is used primarily for what purpose?

- Allow remote systems to save on long distance charges
- Allow the use of network-attached printers
- Support secured communications over an untrusted network
- Support the distribution of public web documents

Explanation

A VPN (Virtual Private Network) is used primarily to support secured communications over an untrusted network. A VPN can be used over a local area network, across a WAN connection, over

the Internet, and even between a client and a server over a dial-up connection through the Internet. All of the other items listed in this question are benefits or capabilities that are secondary to this primary purpose.

References

LabSim for PC Pro, Section 12.12.
[pcpro2016_all_questions_en.exm VPN_01]

Question 105: 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. 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.)

- [ ] Enable the Guest account.
- [ ] Secure the system to the desk with a cable lock.
- [ ] Assign each user a simple password so they won't be tempted to write it down.
- [ ] Install a privacy filter on the monitor.
- [ ] Make user accounts members of the Administrators group.

Explanation

Because this system is used in close proximity to customers, you should install a privacy filter on the monitor and secure it to the desk with a cable lock. The privacy filter prevents customers from viewing sensitive information displayed on the monitor (such as usernames, passwords, and account numbers). Securing the computer to the desk prevents a malicious person from stealing the computer and all of the sensitive information it contains.

Enabling the Guest user account would decrease the security of the system as would assigning simple passwords to user accounts and making all users members of the Administrators group.

References

LabSim for PC Pro, Section 12.1.
[pcpro2016_all_questions_en.exm SECURITY_BEST_10]

Question 106: Incorrect

Match each security policy on the left with the appropriate description on the right. Each security policy may be used once, more than once, or not at all.

Provides a high-level overview of the organization's security program.
Organizational Security Policy

Defines an employee's rights to use company property.
Acceptable Use Policy

Identifies the requirements for credentials used to authenticate to company-owned systems.
Password Policy

Identifies a set of rules or standards that define personal behaviors.
Code of Ethics

Sets expectations for user privacy when using company resources.

Acceptable Use Policy

Specifies that user accounts should be locked after a certain number of failed login attempts.

Password Policy

Explanation

An Organizational Security Policy is a high-level overview of the organization's security program. An Acceptable use Policy (AUP) defines an employee's rights to use company property. The AUP should also set expectations for user privacy when using company resources. Password Policy identifies the requirements for passwords used to authenticate to company-owned systems. For example, this policy may specify that user accounts should be disabled or locked out after a certain number of failed login attempts.

References

LabSim for PC Pro, Section 12.1.
[pcpro2016_all_questions_en.exm SECURITY_BEST_11]

Question 107: Incorrect

You have purchased new computers and will be disposing of your old computers. These computers were previously used for storing highly-sensitive customer order information, including credit card numbers.

What should you do prior to getting rid of the computers?

- Repartition the hard drives.
- Reinstall a fresh copy of Windows on the drives.
- Physically destroy the hard drives with a hammer.
- Reformat the hard drives.
- Delete user data and applications from the hard drives.

Explanation

Because the hard drives contained very sensitive information (such as credit card numbers), the best solution in this scenario is to physically destroy the drives. For example, they could be rendered useless with a hammer or hard disk shredder.

Reinstalling Windows, repartitioning the drives, or even reformatting them will not remove all data remnants. Deleting data and applications from the hard drives also will not permanently remove data from the system.

References

LabSim for PC Pro, Section 12.3.
[pcpro2016_all_questions_en.exm PHYSICAL_SECURITY_07]

Question 108: Incorrect

While reviewing video files from your organization’s security cameras, you notice a suspicious person using piggy-backing to gain access to your building. The individual in question did not have a security badge.

Which security measure could you implement to keep this from happening in the future?

- Lo-jack recovery service
- Cable locks
- Door locks with card readers

Mantraps

Explanation

You could implement mantraps at each entrance to the facility. A mantrap is a specialized entrance with two doors that creates a security buffer zone between two areas. Once a person enters into the space between the doors, both doors are locked. To enter the facility, authentication must be provided. If authentication is not provided, the intruder is kept in the mantrap until authorities arrive.

Cable locks are used to secure computer hardware. Lo-jack recovery services are used to locate stolen or misplaced computer hardware. Door locks with card readers were already circumvented in this scenario using the piggy-backing technique.

References

LabSim for PC Pro, Section 12.3.
[pcpro2016_all_questions_en.exm PHYSICAL_SECURITY_08]

Question 109: 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
- [x] Remove the optical drive
- [x] Disable all USB ports in the BIOS/UEFI firmware configuration
- [ ] Disable the network jack to which the system is connected
- [ ] 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 110: Incorrect

A malicious person calls an employee from a cell phone. She tells the employee that she is the vice president over the Accounting department in the employee's company. She relates that she has forgotten her password demands that the employee give her his password so that she can access the reports she needs for an upcoming presentation. She threatens to fire the employee if he does not comply.

What kind of attack has occurred in this scenario?

- Eavesdropping

- Phishing
- Piggybacking
- Masquerading

Explanation

A masquerading attack has occurred. Masquerading involves an attacker convincing authorized personnel to grant them access to protected information by pretending to be someone who is authorized and/or requires that access. Usually, the attacker poses as a member of senior management. A sense of urgency is typically fabricated to motivate the user to act quickly.

References

LabSim for PC Pro, Section 12.4.
[pcpro2016_all_questions_en.exm SOCMED_SECURITY_08]

Question 111: 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?

- Eavesdropping
- Piggybacking
- Man-in-the-Middle
- Phishing

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 112: Incorrect

You just bought a new notebook. This system uses UEFI firmware and comes with Windows 10 preinstalled. However, you want to use Linux on this system. You download your favorite distribution and install it on the system, removing all Windows partitions on the hard disk in the process. When the installation is complete, you find that the operating system won't load when the system is rebooted.

What should you do?

- Enable the TPM chip on the motherboard.
-

Disable SecureBoot in the UEFI configuration.

Enable SecureBoot in the UEFI configuration.

Set the boot order to boot from the hard disk first in the UEFI configuration.

Reinstall Windows 10 on the system.

Explanation

You should disable the SecureBoot option in the UEFI configuration. SecureBoot requires the operating system installed on the hard drive to be digitally signed. If it isn't digitally signed, then the UEFI firmware will not boot it by default.

Reinstalling Windows 10 doesn't meet the requirements of the scenario. If SecureBoot is already enabled, then the TPM chip on the motherboard must already be enabled. The boot order configuration is not preventing the system from booting in this scenario.

References

LabSim for PC Pro, Section 12.5.
[pcpro2016_all_questions_en.exm BIOSSEC_06]

Question 113: Incorrect

You just bought a new computer. This system uses UEFI firmware and comes with Windows 10 preinstalled. You recently accessed the manufacturer's support website and saw that a UEFI firmware update has been released. You download the update. However, when you try to install the update, an error message is displayed indicating the digital signature on the update file is invalid.

Why did this happen?

Interim UEFI updates released since the system was manufactured need to be installed before installing the latest update.

SecureBoot has been enabled in the UEFI firmware configuration.

The system has a rootkit malware infection.

The update file has been tampered with.

Explanation

UEFI requires firmware updates to be digitally signed by the hardware vendor. Using digital signatures, unauthorized changes to firmware updates (such as the insertion of malware) can be detected.

The SecureBoot feature requires that operating systems be digitally signed before they can be booted on the system. The latest UEFI update most likely includes all of the changes implemented in early updates. There is no indication that the system has been infected with rootkit malware in this scenario.

References

LabSim for PC Pro, Section 12.5.
[pcpro2016_all_questions_en.exm BIOSSEC_07]

Question 114: Incorrect

A local dentist has contracted with you to implement a network in her new office. Because of security concerns related to patient privacy laws, she has asked that the new network meet the following criteria:

- No one from the Internet should be able to access her internal network.
- Email messages should be scanned for spam, phishing attacks, and malware before they

• Each users' workstations should be blocked from accessing non-work related web sites, especially sites that contain inappropriate content.
• A system should be put in place to detect and prevent external attacks on her network.

What should you do?

- Implement a firewall.
- Implement an email security appliance.
- Implement a content filter.
- Implement an all-in-one security appliance.
- Implement an intrusion prevention system (IPS).

Explanation

You should implement an all-in-one security appliance. The network criteria specified by your client requires several different network devices to be implemented, including a firewall, an email scanner, a content filter, and an intrusion prevention system.

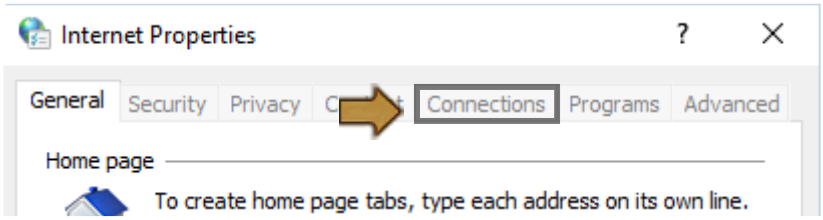
While you could purchase each device separately, the cost of doing so would probably be quite high. Because you are working with a small business, an all-in-one security appliance that includes all of these functions in a single device would be more cost-effective and easier for you to manage.

References

LabSim for PC Pro, Section 12.10.
[pcpro2016_all_questions_en.exm FIREWALL_09]

Question 115: 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 116: Incorrect

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

- Router
- Switch
- NAT

- Firewall

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 117: Incorrect

Your organization employs a group of traveling salespeople who need to access the corporate home network through the Internet while they are on the road. You want to funnel remote access to the internal network through a single server. Which solution should you implement?

- Site-to-site VPN
- Host-to-host VPN
- VPN concentrator
- DMZ

Explanation

With a remote access VPN, a server on the edge of a network (called a VPN concentrator) is configured to accept VPN connections from individual hosts. Hosts that are allowed to connect using the VPN connection are granted access to resources on the VPN server or the private network.

A demilitarized zone (DMZ), also called a screened subnet, is a buffer network (or subnet) that sits between the private network and an untrusted network (such as the Internet). With a host-to-host VPN, two hosts establish a secure channel and communicate directly with each other. With a site-to-site VPN, the routers on the edge of each site establish a VPN connection with the router at the other location.

References

LabSim for PC Pro, Section 12.12.
[pcpro2016_all_questions_en.exm VPN_03]

Question 118: Incorrect

A salesperson in your organization spends most of her time traveling between customer sites. After a customer visit, she must complete various managerial tasks, such as updating your organization's order database. Because she rarely comes back to your home office, she usually accesses the network from her notebook computer using Wi-Fi access provided by hotels, restaurants, and airports.

Many of these locations provide unencrypted public Wi-Fi access, and you are concerned that sensitive data could be exposed. To remedy this situation, you decide to configure her notebook to use a VPN when accessing the home network over an open wireless connection.

Which key steps should you take when implementing this configuration? (Select two.)

- [ ] Configure the browser to send HTTPS requests directly to the Wi-Fi network without going through the VPN connection.
- [ ] Configure the VPN connection to use PPTP.
- [ ] Configure the VPN connection to use MS-CHAPv2.

- [ ] Configure the VPN connection to use IPsec.
- [ ] Configure the browser to send HTTPS requests through the VPN connection.

Explanation

It is generally considered acceptable to use a VPN connection to securely transfer data over an open Wi-Fi network. As long as strong tunneling ciphers and protocols are used, the VPN provides sufficient encryption to secure the connection, even though the wireless network itself is not encrypted. It is recommended that you use IPsec or SSL to secure the VPN, as these protocols are relatively secure. You should also configure the browser's HTTPS requests to go through the VPN connection.

To conserve VPN bandwidth and to improve latency, many VPN solutions automatically reroute web browsing traffic through the client's default network connection instead of through the VPN tunnel. This behavior would result in HTTP/HTTPS traffic being transmitted over the unsecure open wireless network instead of through the secure VPN tunnel. Avoid using PPTP with MS-CHAPv2 in a VPN over open wireless configuration as these protocols are no longer considered secure.

References

LabSim for PC Pro, Section 12.12.
[pcpro2016_all_questions_en.exm VPN_04]

Question 119: Incorrect

You want to use a protocol that can encapsulate other LAN protocols and carry the data securely over an IP network. Which of the following protocols is suitable for this task?

- ( ) PPP
- ( ) PPTP
- ( ) NetBEUI
- ( ) SLIP

Explanation

PPTP is used with VPNs, which allow you to send data securely over a public network.

References

LabSim for PC Pro, Section 12.12.
[pcpro2016_all_questions_en.exm VPN_05]

Question 120: Incorrect

Which of the following protocols can your portable computer use to connect to your company's network via a virtual tunnel through the Internet? (Select two.)

- [ ] VNC
- [ ] PPPoE
- [ ] Remote Desktop Protocol (RDP)
- [ ] L2TP
- [ ] PPTP

Explanation

PPTP (Point-to-Point Tunneling Protocol) and L2TP (Layer Two Tunneling Protocol) are two VPN

(Virtual Private Networking) protocols that let you access your company's network through a public network, such as the Internet.

PPPoE is used for connecting to the Internet through an Ethernet connection to include authentication and accounting. VNC and RDP are remote desktop protocols used for remote administration or remote access of devices.

References

LabSim for PC Pro, Section 12.12.
[pcpro2016_all_questions_en.exm VPN_06]

Question 121: Incorrect

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

- TCP
- L2TP
- SSL
- 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 122: Incorrect

Which of the following statements about an SSL VPN are true? (Select two.)

- [ ] Uses port 443
- [ ] Uses UDP port 500
- [ ] Provides message integrity using HMAC
- [ ] Encapsulates packets by adding a GRE header
- [ ] Uses pre-shared keys for authentication
- [ ] Encrypts the entire communication session

Explanation

SSL VPN uses the SSL protocol to secure communications. SSL VPN:

- Authenticates the server to the client using public key cryptography and digital certificates.
- Encrypts the entire communication session.
- Uses port 443, which is already open on most firewalls.

Pre-shared keys are used by IPsec to provide authentication with other protocols. IPsec also uses HMAC to provide message integrity checks. GRE headers are used exclusively by the GRE tunneling protocol. UDP port 500 is used by the Layer Two Tunneling Protocol (L2TP).

References

LabSim for PC Pro, Section 12.12.
[pcpro2016_all_questions_en.exm VPN_08]

Question 123: Incorrect

You are a security consultant and have been hired to evaluate an organization's physical security practices. All employees must pass through a locked door to enter the main work area. Access is restricted using a smart card reader. Network jacks are provided in the reception area such that employees and vendors can access the company network for work-related purposes. Users within the secured work area have been trained to lock their workstations if they will be leaving them for any period of time.

What recommendations would you make to this organization to increase their security?

- ○ Replace the smart card reader with a key code lock.
- ○ Move the receptionist's desk into the secured area.
- ➡ ○ Disable the switch ports connected to the network jacks in the reception area.
- ○ Require users to use screensaver passwords.

Explanation

You should recommend the company disable the switch ports connected to the network jacks in the reception area. Having active network jacks in an unsecured area allows anyone who comes into the building to connect to the company's network.

Smart card readers are generally considered more secure than key code locks because access codes can be easily shared or observed. Training users to lock their workstations is more secure than screensaver passwords, although this may be a good idea as a safeguard in case a user forgets.

References

LabSim for PC Pro, Section 12.9.
[pcpro2016_all_questions_en.exm NET_SEC_WIRED_01]

Question 124: Incorrect

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

- They use an 802.11n wireless network.
- The wireless network is broadcasting an SSID of Linksys.
- The wireless network uses WPA2 with AES security.
- 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? (Select two.)

- ☐ Upgrade to an 802.11g wireless network.
- ➡ ☐ Change the SSID to something other than the default.
- ➡ ☐ Disable SSID broadcast.

- [ ] Implement omnidirectional access points.
- [ ] Configure the wireless network to use WPA with TKIP security.

Explanation

You should recommend the following:

- Disable SSID broadcast. This makes the network harder (but not impossible) to locate.
- Change the SSID to something other than the default. This obscures what type of AP is in use.

Using WPA instead of WPA2 would decrease the security of the wireless network as would implementing omnidirectional APs. Switching to an 802.11g network would dramatically reduce the speed of the network without providing any security enhancements.

References

LabSim for PC Pro, Section 12.9.
[pcpro2016_all_questions_en.exm NET_SEC_WIRELESS_09]

Question 125: 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?

- ( ) Change the SSID to something similar to BigBikeInc.
- ( ) Configure the wireless network to use WEP security.
- (→) Implement directional access points.
- ( ) Upgrade to an 802.11g wireless network.
- ( ) Enable SSID broadcast.

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 126: Incorrect

Your organization is frequently visited by sales reps. While on-site, they frequently plug their notebook systems into any available wall jack, hoping to get Internet connectivity. You are

concerned that allowing them to do this could result in the spread of malware throughout your network.
What should you do? (Select two.)

- [ ] Enable port analysis on your network switch.
- [ ] Implement MAC address filtering.
- [ ] Implement static IP addressing.
- [ ] Implement private IP addressing with a Network Address Translation (NAT) router facing the Internet.
- [ ] Implement SNMP traps on your network switch.

Explanation

You should consider enabling MAC address filtering. MAC filtering is configured on your network switches and is used to restrict network access to only systems with specific MAC addresses. You could also consider assigning static IP addresses to your network hosts. By not using DHCP, visitor laptops connected to a wired Ethernet jack won't receive a valid IP address and won't be able to communicate with other hosts on your network.

Implementing SNMP traps, port analysis, or a NAT router will not prevent visitors from connecting to your network.

References

LabSim for PC Pro, Section 12.9.
[pcpro2016_all_questions_en.exm NET_SEC_WIRED_02]

Question 127: Incorrect

A user reports that his machine will no longer boot properly. After asking several questions to determine the problem, you suspect the user unknowingly downloaded malware from the Internet, and that the malware has infected the system.

Based on your suspicions, what actions could you take to correct the problem? (Select two.)

- [ ] Use an anti-malware scanner to scan for and remove the infection.
- [ ] Reinstall Windows on the system.
- [ ] Revert the system to a restore point created before the malware infection occurred.
- [ ] Have the user attend an internal Internet safety training course.
- [ ] Run sfc.exe.

Explanation

The first step would be to run an anti-malware scan on the system to see if it can located and remove the malware infection. If that doesn't work, you could also revert the system to a restore point that was created before the malware infection occurred.

User training is a preventative measure against malware infections; however, the training will not repair the current damage. Sfc.exe scans every system file in the operating system for altered files. This may or may not help remediate the malware infection. Reinstalling Windows should occur only as a last resort after every other option has been exhausted.

References

LabSim for PC Pro, Section 12.13.
[pcpro2016_all_questions_en.exm TRB_SECURITY_07]

Question 128: 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 Middle Eastern 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 and was instructed to wire $5,000 to the sender to facilitate the transfer. She complied, but has not heard from the sender since.

What type of attack occurred in this scenario?

- Man-in-the-Middle
- Eavesdropping
- Vishing
- Nigerian 419 scam

Explanation

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

Vishing is similar to phishing but instead of an email, the attacker uses Voice over IP (VoIP) to gain sensitive information. 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 12.13.
[pcpro2016_all_questions_en.exm TRB_SECURITY_08]

Question 129: Incorrect

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

- A person over the phone convinces an employee to reveal their logon credentials.
- An attacker intercepts communications between two network hosts by impersonating each host.
- 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 130: Incorrect

A router on the border of your network receives a packet with a source address that shows it originating from a client on the internal network. However, the packet was received on the router's external interface, which means it originated somewhere on the Internet.
What form of attack has occurred in this scenario?

- Sniffing
- Snooping
- Session hijacking
- Spoofing
- Man-in-the-Middle

Explanation

This is an example of spoofing. Spoofing involves changing or falsifying information in order to mislead or re-direct traffic. In this scenario, the router's external interface cannot receive a valid packet with a source address from the internal network. One must assume that the source address of the packet was faked.

Snooping is the act of spying into private information or communications. One type of snooping is sniffing. Sniffing is the act of capturing network packets in order to examine the contents of communications. 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. Session hijacking is an extension of a Man-in-the-Middle attack where the attacker hijacks an active communication session.

References

LabSim for PC Pro, Section 12.13.
[pcpro2016_all_questions_en.exm TRB_SECURITY_10]

Question 131: Incorrect

The TCP/IP session state between two computers on a network is being manipulated by an attacker such that she is able to insert tampered packets into the communication stream.

What type of attack has occurred in this scenario?

- Hijacking
- Spear phishing
- Whaling
- Phishing

Explanation

A hijacking attack has occurred. Hijacking happens when the TCP/IP session state is manipulated such that a third party is able to insert alternate packets into the communication stream.

A phishing scam employs an email pretending to be from a trusted organization, asking to verify personal information or send a credit card number. In spear phishing, attackers gather information about the victim, such as identifying which online banks they use. They then send phishing emails for the specific bank that the victim uses. Whaling is another form of phishing that is targeted to senior executives and high profile victims.

References

LabSim for PC Pro, Section 12.13.
[pcpro2016_all_questions_en.exm TRB_SECURITY_11]

Question 132: 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 133: 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 134: 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]