Exam Report: 15.4.7 Practice Questions

Date: 12/6/2019 5:05:29 pm
Time Spent: 6:17

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 54%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

You are considering using Wi-Fi triangulation to track the location of wireless devices within your organization. However, you have read on the internet that this type of tracking can produce inaccurate results.

What is the most important consideration for getting reliable results when implementing this type of system?

- Signal strength
- Wireless encryption in use
- Wireless standard in use
- WAP placement

Explanation

Wi-Fi triangulation works by configuring wireless devices to sniff for wireless networks in range and then measuring each network's signal strength. The results are compared with a signal strength database, and basic geometry identifies the device's location. The wireless device doesn't actually have to connect to any of these networks; it simply scans them to determine their signal strength. For this to work, the administrators of all Wi-Fi networks used for triangulation must perform periodic site surveys to populate and maintain the signal strength database.
WAP placement is a consideration in Wi-Fi triangulation, but the signal strength database is the key to determining a device's location. Only a small amount of physical displacement between access points is necessary to triangulate. The wireless standard or encryption in use has little effect on Wi-Fi triangulation.

References

LabSim for Network Pro, Section 15.4.
[netpro18v5_all_questions_en.exm MCS8]

Question 2: Incorrect

Match each bring your own device (BYOD) security concern on the right with a possible remedy on the left. Each remedy may be used once, more than once, or not at all.

Users take pictures of proprietary processes and procedures.	✓ Specify where and when mobile devices can be possessed in your acceptable use policy.
Devices with a data plan can email stolen data.	~~Enroll devices in a mobile device management system.~~ Specify where and when mobile devices can be possessed in your acceptable use policy.
Devices have no PIN or password configured.	✓ Enroll devices in a mobile device management system.
Anti-malware software is not installed.	~~Enroll devices in a mobile device management system.~~ Implement a network access control (NAC) solution.
A device containing sensitive data may be lost.	~~Implement a network access control (NAC) solution.~~ Enroll devices in a mobile device management system.

Explanation

Even though it entails a host of security risks, bring your own device (BYOD) is a very common practice in modern work environments. Security administrators need to keep the following BYOD security issues in mind:

- If a user is so inclined, they could use their mobile device to conduct a malicious insider attack. For example, they could use the built-in camera, which nearly all modern mobile devices have, to take pictures of sensitive internal information. They could also use the device's mobile broadband connection to transfer stolen data to parties outside the organization, bypassing the organization's network security mechanisms. To defend against this, implement an acceptable use policy that specifies where and when mobile devices can be possessed within the organization. For example, the possession of mobile devices may be prohibited in high security areas.
- If a user copies sensitive data to their device, your organization could potentially lose control of that information. For example, the user may not have implemented appropriate security settings on their device, allowing anyone who gains access to the device to view the sensitive data. In addition, the user may lose the device, allowing anyone who finds it to access the sensitive data. To address these issues, require personal devices to be enrolled with a mobile device management infrastructure, such as Windows Intune, to enforce mobile device security policies.
- To ensure anti-malware software is installed, consider implementing a network access control (NAC) solution that remediates devices before allowing them to connect to your network.

References

LabSim for Network Pro, Section 15.4.
[netpro18v5_all_questions_en.exm RT-5.4-5]

Question 3: Incorrect

Your organization recently purchased 30 tablet devices for your traveling sales force. These devices have Windows RT preinstalled on them.

To increase the security of these devices, you want to apply a default set of security-related configuration settings.

What is the best approach to take to accomplish this? (Select two. Each option is part of a complete solution.)

- [ ] Link the Group Policy object to the container where the tablets' computer objects reside.
- [x] ~~Configure security settings in a Group Policy object.~~
- [x] Enroll the devices in a mobile device management system.
- [ ] Configure and apply security policy settings in a mobile device management system.
- [ ] Join the tablets to your domain.
- [ ] Manually configure security settings using the Local Group Policy Editor program.

Explanation

You can implement a mobile device management (MDM) solution that pushes security policies directly to each tablet device over a network connection. This option enables policies to be remotely enforced and updated without any action by the end user. The tablet devices must be enrolled in the MDM system before the policy settings can be applied.

One of the key problems associated with managing mobile devices is the fact that they can't be joined to a Windows domain. This means Group Policy can't be used to automatically push security settings to mobile devices. Security settings could be manually configured on each individual device. However, this would be a time-consuming task for the administrator, especially given the number of mobile devices in this scenario. In addition, any changes that need to be made in the future will have to be manually applied to one device at a time.

References

LabSim for Network Pro, Section 15.4.
[netpro18v5_all_questions_en.exm RT-5.5-1]

Question 4: Incorrect

Your organization recently purchased 18 iPad tablets for use by the organization's management team. These devices have iOS pre-installed on them.

To increase the security of these devices, you want to apply a default set of security-related configuration settings.

What is the best approach to take to accomplish this? (Select two. Each option is a part of a complete solution.)

- [ ] Join the tablets to a Windows domain.
- [ ] Configure and apply security policy settings in a mobile device management system.
- [ ] Require uses to install the configuration profile.
- [x] Enroll the devices in a mobile device management system.
- [ ] Configure security settings in a Group Policy object.
- [x] ~~Configure and distribute security settings in a configuration profile.~~

Explanation

You can implement a mobile device management (MDM) solution that pushes security policies directly to each tablet device over a network connection. This option enables policies to be remotely enforced and updated without any action by the end user. The tablet devices must be enrolled in the MDM system before the policy settings can be applied.

One of the key problems associated with managing mobile devices is the fact that they can't be joined to a Windows domain. This means Group Policy can't be used to automatically push security settings to mobile devices. For devices running Apple's iOS operating system, security settings can be distributed in a configuration profile. The profile can be defined such that only an administrator can delete the profile, or you can lock the profile to the device so that it cannot be removed without completely erasing the device. However, this option relies on the end user to install the profile, which can be problematic. It's also not a dynamic strategy; even the smallest change to your mobile device security policies would require a great deal of effort to implement.

References

LabSim for Network Pro, Section 15.4.
[netpro18v5_all_questions_en.exm RT-5.5-2]

Question 5: Incorrect

Your organization's security policy specifies that, regardless of ownership, any mobile device that connects to your internal network must have remote wipe enabled. If the device is lost or stolen, then it must be wiped to remove any sensitive data from it.

Which of the following should you implement to ensure organizational data can be remote wiped while preserving personal data?

- Asset tracking and inventory control
- ~~Lockout or screen Lock~~
- Storage segmentation
- Reporting system

Explanation

Storage segmentation for mobile devices lets you segment the personal data from the organization's data. Storage segmentation also allows:

- Encryption to be applied only to sensitive organizational data on the device.
- Only organizational data to be removed during a remote wipe, preserving personal data.

Asset tracking and inventory control only track devices owned by the organization. Lockout or screen lock only protect the device access and do not have remote wipe capability. Reporting systems provide a way to disable the device, but not remote wipe only organization data.

References

LabSim for Network Pro, Section 15.4.
[netpro18v5_all_questions_en.exm RT-5.5-6]

Question 6: Correct

Most mobile device management (MDM) systems can be configured to track the physical location of enrolled mobile devices. Arrange the location technology on the left in order of accuracy on the right, from most accurate to least accurate.

Most accurate
- GPS

More accurate
- Wi-Fi triangulation

Less accurate
- Cell phone tower triangulation

Least accurate
- IP address resolution

Explanation

Most mobile device management (MDM) solutions can leverage the following technologies on enrolled mobile devices to track their physical location:

- The Global Position System (GPS) can track the location of GPS-enabled devices to within a meter.
- Wi-Fi triangulation can track the location of devices in heavily-populated urban areas to within a few meters, depending on the number of networks in range and the accuracy of their signal strength data.
- Cell phone tower triangulation can track the location of devices to within a kilometer, depending on the signal strength and number of cell towers within range.
- IP address resolution is much less accurate than the other options, tracking the location of devices to within roughly 20 kilometers.

References

LabSim for Network Pro, Section 15.4.
[netpro18v5_all_questions_en.exm RT-5.4-1]

Question 7: Incorrect

Your organization has recently purchased 20 tablet devices for the Human Resource department to use for training sessions.

You are concerned that these devices could represent a security risk to your network and want to strengthen their security profile as much as possible.

Which actions should you take? (Select two. Each response is a separate solution.)

- [ ] Implement storage segmentation.
- [ ] Configure a Group Policy object (GPO) containing mobile device-specific security settings.
- [x] Enable device encryption.
- [ ] Join the devices to your organization's domain.
- [x] ~~Install the devices in your organization's directory services tree.~~

Explanation

When deploying new mobile devices, there are many things you should do to increase their overall security, including the following:

- Enable device encryption. Data encryption ensures data confidentiality on the device.
- Segment personal data from organizational data on mobile devices. This storage strategy allows encryption to be applied only to sensitive organizational data on the device. It also allows only organizational data to be removed during a remote wipe, preserving personal data.

Mobile devices can't be joined to a domain, so there is no way to apply Group Policy settings from a GPO to a mobile device. Most directory services, such as OpenLDAP, do not support mobile devices, so it probably isn't possible to install the new tablets in your organization's directory services tree.

References

LabSim for Network Pro, Section 15.4.
[netpro18v5_all_questions_en.exm RT-5.4-2]

Question 8: Correct

Which of the following mobile device security consideration disables the ability to use the device after a short period of inactivity?

- [x] Screen lock
- [ ] Remote wipe
- [ ] GPS
- [ ] TPM

Explanation

A lockout (or screen lock) disables the ability to use the device after a short period of inactivity. The correct password or personal identification number (PIN) unlocks the device.

Remote wipe, also known as sanitization, remotely clears specific, sensitive data on the mobile device. This task is also useful if you are assigning the device to another user, or after multiple incorrect entries of the password or PIN. Data encryption also ensures data confidentiality on the device. Voice encryption (on mobile phones) ensures data confidentiality during transit. Global Positioning System (GPS) tracking can assist in the recovery of the device by displaying its current location. The Trusted Platform Module (TPM) is a hardware chip on the motherboard that can generate and store cryptographic keys to check the integrity of of startup files and components.

References

LabSim for Network Pro, Section 15.4.
[netpro18v5_all_questions_en.exm GS2]

Question 9: Correct

Which of the following are not reasons to remote wipe a mobile device?

- [x] The device is inactive for a period of time.
- [ ] The device is locked, and someone has entered multiple incorrect entries of the password or PIN.
- [ ] The device is stolen or lost.
- [ ] The device is being assigned to another user.

Explanation

Device inactivity is not a reason to remotely wipe a mobile device.

Remote wipe, also known as sanitization, remotely clears specific sensitive data on stolen, misplaced, or lost mobile devices. This ensures that whoever has the device is not able to see the sensitive data. This task is also useful if you are assigning the device to another user or after multiple incorrect entries of the password or PIN.

References

LabSim for Network Pro, Section 15.4.
[netpro18v5_all_questions_en.exm GS3]

Question 10: Correct

A smart phone was lost at the airport. There is no way to recover the device. Which if the following will ensure data confidentiality on the device?

- [ ] GPS
- [ ] Screen lock
- [ ] TPM
- [x] Remote wipe

Explanation

Remote wipe, also known as sanitization, remotely clears specific sensitive data on the mobile device. This ensures that whoever has the device is not able to see the sensitive data. This task is also useful if you are assigning the device to another user or after multiple incorrect entries of the password or PIN. Data encryption also ensures data confidentiality on the device. Voice encryption on mobile phones ensures data confidentiality during transit.

Global Positioning System (GPS) tracking can assist in the recovery of the device by displaying its current location. A lockout (or screen lock) disables the ability to use the device after a short period of inactivity. The correct password or personal identification number (PIN) unlocks the device. The Trusted Platform Module (TPM) is a hardware chip on the motherboard that can generate and store cryptographic keys for integrity checking startup files and components.

References

LabSim for Network Pro, Section 15.4.
[netpro18v5_all_questions_en.exm GS1]

Question 11: Incorrect

Many of the end users in your organization are bringing their own personal mobile devices to work and are storing sensitive data on them. To prevent the data from being compromised, you create a cloud-based Microsoft Intune account and configure mobile device security policies.

You now need to apply those security policies to the end users' mobile devices.

What should you do? (Select two. Each response is a part of the complete solution.)

- [ ] Enroll the devices with the Intune service.
- [ ] Download and install the Intune client software on the mobile device.
- [x] ~~Join each device to your organization's domain.~~
- [x] ~~Perform a clean install of the mobile operating system on each user's device.~~
- [ ] Configure mobile device security policies using gpedit.msc.

Explanation

To manage mobile devices with Windows Intune, you must complete the following:

- Create a user account for each user who has a managed mobile device.
- Enroll the devices with the Intune service. The enrollment process will copy down and install the Intune management agent to the device.

It is not necessary to reinstall the mobile operation system on each device. Most mobile devices, with the exception of Windows-based notebooks, cannot be joined to a Windows domain; therefore, Group Policy cannot be used to apply security settings.

References

LabSim for Network Pro, Section 15.4.
[netpro18v5_all_questions_en.exm NP15_MOBILE_DEVICE_MANAGEMENT_02]

Question 12: Correct

Which of the following enterprise wireless configuration strategies best keeps public wireless access separate from private wireless access?

- ( ) Implement MAC address filtering to restrict connections to the private access point only to MAC addresses that are explicitly allowed.
- (•) Configure a guest access WLAN that uses open authentication and isolates guest WLAN traffic from other clients on the same access point.
- ( ) Establish shared key authentication that uses one passphrase for guest users and another passphrase for private users.
- ( ) Deploy independent stand-alone access points throughout your enterprise and configure each to use the same SSID, the same channel, and the same IP subnet.

Explanation

Configuring a guest access WLAN that uses open authentication and isolates guest WLAN traffic from other clients on the same access point is the best solution.

Using MAC address filtering would be very difficult to manage, especially if dozens of devices need to be connected. In addition, MAC filtering can be easily bypassed using MAC spoofing techniques. Deploying independent APs would require manual configuration and management of each device. Devices could also have issues when roaming between APs. Using two different shared keys only provides separate authentication and does not properly separate the two networks.

References

LabSim for Network Pro, Section 15.4.
[netpro18v5_all_questions_en.exm *NP15_OPTIMIZATION_11]

Question 13: Correct

The owner of a hotel has contracted you to implement a wireless network to provide internet access for patrons.

The owner has asked that you implement security controls so that only paying patrons are allowed to use the wireless network. She wants them to be presented with a login page when they initially connect to the wireless network. After entering a code provided by the concierge at check-in, they should then be allowed full access to the internet. If a patron does not provide the correct code, they should not be allowed to access the internet.

Under no circumstances should patrons be able to access the internal hotel network where sensitive data is stored.

What should you do?

- (•) Implement a guest network.
- ( ) Implement 802.1x authentication using a RADIUS server.
- ( ) Implement MAC address filtering.
- ( ) Implement pre-shared key authentication.

Explanation

A guest network that is isolated from the hotel's network would be the best choice in this scenario. The guest network could be configured to require wireless network users to abide by certain conditions before they are allowed access to the wireless network using a captive portal. For example, it could require them to:

- Agree to an acceptable use policy.
- Provide a PIN or password.
- Pay for access to the wireless network.
- View information or advertisements about the organization providing the wireless network (such as an airport or hotel).

When a wireless device initially connects to the wireless network, all traffic to or from that device is blocked until the user opens a browser and accesses the captive portal web page. After providing the appropriate code, traffic is unblocked and the host can access the guest network.

MAC address filtering and 802.1x authentication would work from a technical standpoint, but would be completely unmanageable in a hotel scenario where guests constantly come and go every day. Using a pre-shared key would require a degree of technical expertise on the part of the hotel guests. It could also become problematic if the key were to be leaked, allowing non-guests to use the wireless network.

References

LabSim for Network Pro, Section 15.4.
[netpro18v5_all_questions_en.exm RT NP15_3.6-2]