Exam Report: 7.12.9 Practice Questions

Date: 1/23/2020 2:39:52 pm
Time Spent: 4:22

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 38%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: 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.)

➡ □ Configure and apply security policy settings in a mobile device management system.

□ Join the tablets to your domain.

☑ ~~Manually configure security settings using Local Group Policy Editor.~~

□ Link the Group Policy object to the container where the tablets' computer objects reside.

□ Configure security settings in a Group Policy object.

➡ □ Enroll the devices in a mobile device management system.

Explanation

A mobile device management (MDM) solution can be implemented 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 needed to be made in the future would have to be manually applied to one device at a time.

References

LabSim for Security Pro, Section 7.12.
[All Questions SecPro2017_v6.exm MOB_DEV_MGMT_01]

Question 2: 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.)

☑ ~~Configure and distribute security settings in a configuration profile~~

➡ ☐ Enroll the devices in a mobile device management system

➡ ☐ Configure and apply security policy settings in a mobile device management system

☑ ~~Configure security settings in a Group Policy object~~

☐ Join the tablets to a Windows domain

☐ Require uses to install the configuration profile

Explanation

A mobile device management (MDM) solution can be implemented 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 so 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; making even the smallest change to your mobile device security policies requires a great deal of effort.

References

LabSim for Security Pro, Section 7.12.
[All Questions SecPro2017_v6.exm MOB_DEV_MGMT_02]

▼ Question 3: Incorrect

Match each mobile device application control term on the right with the appropriate description on the left. Each description may be used once, more than once, or not at all.

Jailbreaking

✓ Allows apps to be installed from sources other than the App Store

Sideloading

✓ Allows apps to be installed from sources other than the Windows Store

Sandboxing

~~Embeds GPS coordinates within mobile device files~~

Prevents a running app from accessing data stored by other running apps

Assigned Access

~~Prevents a running app from accessing data stored by other running apps~~

Defines a whitelist of Windows Store applications

Explanation

All apps that come from Apple's App Store run in a *sandbox*, which means they cannot access data stored by other running apps, nor can they access system files and resources.

iOS devices can be *jailbroken*, allowing apps to be installed from sources other than the App Store. Non-Windows Store apps can be installed on Windows RT devices using a process called *sideloading*.

Windows RT provides a feature called *Assigned Access*, which allows you to define a whitelist of Windows Store applications.

References

LabSim for Security Pro, Section 7.12.
[All Questions SecPro2017_v6.exm MOB_DEV_MGMT_03]

▼ **Question 4:** Correct

Recently, a serious security breach occurred in your organization. An attacker was able to log in to the internal network and steal data through a VPN connection using the credentials assigned to a vice president in your organization.

For security reasons, all individuals in upper management in your organization have unlisted home phone numbers and addresses. However, security camera footage from the vice president's home recorded someone rummaging through her garbage cans prior to the attack. The vice president admitted to writing her VPN login credentials on a sticky note that she subsequently threw away in her household trash. You suspect the attacker found the sticky note in the trash and used the credentials to log in to the network.

You've reviewed the vice president's social media pages. You found pictures of her home posted, but you didn't notice anything in the photos that would give away her home address. She assured you that her smart phone was never misplaced prior to the attack.

Which security weakness is the most likely cause of the security breach?

➡ ● Geo-tagging was enabled on her smart phone.

○ Weak passwords were used on her smart phone.

○ Sideloaded apps were installed on her smart phone.

○ An Xmas Tree attack was executed on her smart phone.

Explanation

Geo-tagging embeds GPS coordinates within mobile device files (such as image or video files) created with the device's camera. While this feature can be useful in some circumstances, it can also create security concerns. In this scenario, the vice president probably posted geo-tagged images to her social media accounts. The attacker likely analyzed the images to discover where she lives and then conducted a dumpster dive attack that yielded the sticky note with the vice president's VPN credentials. The best way to remedy this weakness is to simply disable this functionality in the mobile devices you manage.

Sideloaded apps can only be installed if the device administrator has specifically configured the device to allow them, so this is an unlikely cause. A weak smart phone password is a concern, but would not be the cause of the exploit if the device was always in the vice president's possession. An Xmas Tree attack is used to fingerprint network devices, not to gather personally identifying information.

References

LabSim for Security Pro, Section 7.12.
[All Questions SecPro2017_v6.exm MOB_DEV_MGMT_04]

▼ **Question 5:** Incorrect

Your organization is formulating a bring your own device (BYOD) security policy for mobile devices.

Which of the following statements should be considered as you formulate your policy?

➡ ○ You can't use domain-based group policies to enforce security settings on mobile devices.

○ Anti-malware software isn't available for most mobile device operating systems.

● ~~It is difficult for users to connect personal mobile devices to your organization's corporate network.~~

○ Mobile devices are immune to malware threats.

Explanation

A mobile device running Windows RT, Android, or iOS cannot join a domain for centralized security enforcement. In a Windows environment, this means that you cannot use group policies to enforce security settings.

Mobile devices are susceptible to malware threats, just like notebook and desktop systems. Depending on the security configuration of your network, it is typically quite easy to connect personal mobile devices to an organization's internal network. Anti-malware solutions are available for most mobile device operating systems.

References

LabSim for Security Pro, Section 7.12.
[All Questions SecPro2017_v6.exm MOB_DEV_MGMT_05]

▼ **Question 6:** Incorrect

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

Your organization recently purchased several Windows RT tablets. Which should you do?

➡ ○ Sign up for a Windows Intune account to manage the tablets.

● ~~Go to **Settings Charm** > **Change PC settings** > **Privacy** and enable the **Remote Wipe** setting.~~

○ Enable Remote Wipe local group policies on each device.

○ Implement Remote Wipe group policies in your domain.

Explanation

You can use Windows Intune to remotely wipe a Windows RT device if it is reported lost or stolen. You can selectively wipe data or wipe the entire device.

Windows RT devices can't be joined to a domain, so domain-based group polices can't be used to manage its configuration. There are no local policies for managing Remote Wipe functionality, either. Remote Wipe can't be enabled from Change PC settings.

References

LabSim for Security Pro, Section 7.12.
[All Questions SecPro2017_v6.exm MOB_DEV_MGMT_06]

▼ **Question 7:** Correct

Your organization provides its sales force with Windows RT 8.1 tablets to use while visiting customer sites. You manage these devices by enrolling them in your cloud-based Windows Intune account.

One of your sales representatives left her tablet at an airport. The device contains sensitive information, and you need to remove it in case the device is compromised.

Which Intune portal should you use to perform a remote wipe?

○ Account portal

➡ ● Admin portal

○ Security portal

○ Company portal

Explanation

The Admin portal in Windows Intune is used to manage enrolled devices, including sending remote wipe commands.

The Account portal in Windows Intune is used to manage subscriptions, users, groups, and domains. End users can also use the Account portal to manage their passwords. The Company portal in Windows Intune is used by end users to manage their own account and enroll devices. Windows Intune does not provide a security portal.

References

LabSim for Security Pro, Section 7.12.
[All Questions SecPro2017_v6.exm MOB_DEV_MGMT_07]

▼ **Question 8:** Correct

Your organization provides its sales force with Windows 8.1 tablets to use while visiting customer sites. You manage these devices by enrolling them in a cloud-based Windows Intune account.
One of your sales representatives left his notebook at a customer's site. The device contains sensitive information, and you want to change the password to prevent the data from being compromised.

Which Intune portal should you use to remotely change the password?

○ Account portal

○ Company portal

○ Security portal

➡ ● Admin portal

Explanation

The Admin portal in Windows Intune is used to manage enrolled devices, including sending password change commands.

The Account portal in Windows Intune is used to manage subscriptions, users, groups, and domains. End users can also use the Account portal to manage their passwords. The Company portal in Windows Intune is used by end users to manage their own account and enroll devices. Windows Intune does not provide a security portal.

References

LabSim for Security Pro, Section 7.12.
[All Questions SecPro2017_v6.exm MOB_DEV_MGMT_08]