Exam Report: 3.8.3 Practice Questions

Date: 1/16/2020 4:52:30 pm
Time Spent: 4:52

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 50%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: 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?

- Screen lock
- Remote wipe
- GPS
- TPM

Explanation

Remote wipe, also known as *sanitization*, remotely clears specific, sensitive data on the mobile device. This ensures that whoever has the device cannot 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 device's interface 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 to check the integrity of startup files and components.

References

LabSim for Security Pro, Section 3.8.
[All Questions SecPro2017_v6.exm MOB_POLI_01]

Question 2: Incorrect

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

- The device is inactive for a period of time.
- The device is stolen or lost.
- ~~The device is locked and someone has entered multiple incorrect passwords or PINs.~~
- 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 cannot see the sensitive data. This task is also useful if you are assigning the device to another user, or after multiple incorrect password or PIN entries.

References

LabSim for Security Pro, Section 3.8.
[All Questions SecPro2017_v6.exm MOB_POLI_02]

Question 3: Correct

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

- TPM
- Screen lock
- Remote wipe
- GPS

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 password or PIN entries. 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 a device's recovery 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 startup files and components.

References

LabSim for Security Pro, Section 3.8.
[All Questions SecPro2017_v6.exm MOB_POLI_03]

Question 4: 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 Security Pro, Section 3.8.
[All Questions SecPro2017_v6.exm MOB_POLI_04]

Question 5: Incorrect

Over the last several years, the use of mobile devices within your organization has increased dramatically.

Unfortunately, many department heads circumvented your information systems procurement policies and directly purchased tablets and smartphones for their employees without authorization. As a result, there is a proliferation of devices within your organization without accountability.

You need to get things under control and begin tracking your organization's devices.

How should you do this?

- ~~Require users to sign an acceptable use policy before allowing them to use mobile devices for work-related tasks.~~
- Join the devices to your organization's domain.
- Implement a mobile device management (MDM) solution.
- Apply security-related Group Policy settings to the devices using a Group Policy object.
- Implement a mobile endpoint management (MEM) solution.

Explanation

Because mobile devices are not tied to a physical location, asset tracking and inventory control are very important. At a minimum, you should track the following for each device owned by your organization:

- The make and model number of the device
- The device serial number
- The operating system version number
- The date the device was purchased and the vendor it was purchased from
- The end-of-warranty date for the device
- The vendor providing support for the device
- The employee the device has been issued to

To accomplish this goal, you should implement a *mobile endpoint management* (MEM) solution to automate asset tracking and inventory control processes.

A mobile device management (MDM) solution is a valuable administration tool, but devices have to be enrolled in the service before they can be managed. Until an accurate device inventory is available, this won't be possible. Mobile devices can't be joined to a Windows domain; therefore you can't use Group Policy to apply security settings.

References

LabSim for Security Pro, Section 3.8.
[All Questions SecPro2017_v6.exm MOB_POLI_05]

Question 6: 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.)

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

- [ ] Implement storage segmentation.
- [ ] Enable device encryption.

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 them. 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 Security Pro, Section 3.8.
[All Questions SecPro2017_v6.exm BYOD_SEC_01]