Exam Report: 4.2.4 Practice Questions

Date: 1/20/2020 8:29:31 am
Time Spent: 8:40

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 20%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

Which of the following is the most important thing to do to prevent console access to the router?

- Keep the router in a locked room
- ~~Implement an access list to prevent console connections~~
- Set console and enable secret passwords
- Disconnect the console cable when not in use

Explanation

To control access to the router console, you must keep the router in a locked room. A console connection can only be established with a direct physical connection to the router. If the router is in a locked room, only those with access are able to make a console connection. In addition, even if you had set console passwords, users with physical access to the router could perform router password recovery and gain access.

References

LabSim for Security Pro, Section 4.2.
[All Questions SecPro2017_v6.exm DEV_PROTECT_01]

Question 2: Correct

Your company has five salesmen who work out of the office and frequently leave their laptops laying on their desks 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?

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

Explanation

In this case, your main concern is that someone might steal the laptops. 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 Security Pro, Section 4.2.
[All Questions SecPro2017_v6.exm DEV_PROTECT_02]

Question 3: Incorrect

You are an IT consultant. You are visiting a new client's site to become familiar with their network. As you walk around their facility, you note the following:

- When you enter the facility, a receptionist greets you and directs you down the hallway to the office manager's cubicle. The receptionist uses a notebook system that is secured to her desk with a cable lock.
- The office manager informs you that the organization's servers are kept in a locked closet. Only she has the key to the closet. When you arrive on site, you will be required to get the key from her to access the closet.
- She informs you that server backups are configured to run each night. A rotation of external USB hard disks are used as the backup media.
- You notice that the organization's network switch is kept in an empty cubicle adjacent to the office manager's workspace.
- You notice that a router/firewall/content filter all-in-one device has been implemented in the server closet to protect the internal network from external attacks.

Which security-related recommendations should you make to this client? (Select two.)

- [ ] Replace the USB hard disks used for server backups with a tape drive
- [ ] Use separate dedicated network perimeter security devices instead of an all-in-one device
- [x] Relocate the switch to the locked server closet
- [x] ~~Replace the key lock on the server closet with a card reader~~
- [ ] Control access to the work area with locking doors and card readers

Explanation

In this scenario, you should recommend that the client make the following changes:

- Relocate the switch to the locked server closet. Keeping it in a cubicle could allow an attacker to configure port mirroring on the switch and capture network traffic.
- Control access to the work area with locking doors and card readers. Controlling access to the building is critical to prevent unauthorized people from gaining access to computers. In this scenario, you were able to walk unescorted into the work area without any kind of physical access control other than the receptionist.

Because the office manager controls who has access to the server closet key, it isn't necessary to implement a card reader on the server closet door. Using tape drives instead of hard disks wouldn't increase the security of the backups. Using separate perimeter security devices instead of an all-in-one device probably wouldn't increase network security.

References

LabSim for Security Pro, Section 4.2.
[All Questions SecPro2017_v6.exm DEV_PROTECT_03]

Question 4: Incorrect

You are an IT consultant. You are visiting a new client's site to become familiar with their network. As you walk around their facility, you note the following:

- When you enter the facility, a receptionist greets you and escorts you through a locked door to the work area, where the office manager sits.
- The office manager informs you that the organization's servers are kept in a locked closet. An access card is required to enter the server closet.
- She informs you that server backups are configured to run each night. A rotation of tapes are used as the backup media.
- You notice the organization's network switch is kept in the server closet.
- You notice that a router/firewall/content filter all-in-one device has been implemented in the server closet to protect the internal network from external attacks.
- The office manager informs you that her desktop system will no longer boot and asks you to repair or replace it, recovering as much data as possible in the process. You take the workstation back to your office to work on it.

What security-related recommendations should you make to this client?

- Replace the tape drive used for backups with external USB hard disks.
- Upgrade the server closet lock to a biometric authentication system.
- ~~Keep the network infrastructure devices (switch and all-in-one device) in a locked room separate from network servers.~~
- Implement a hardware checkout policy.

Explanation

In this scenario, you should recommend the client implement a hardware checkout policy. A checkout policy ensures that hardware containing sensitive data does not leave the organization's premises without approval and without recording the device's serial number, make, and model number.

A biometric server room lock is probably not necessary in this scenario. It is acceptable to keep servers and network devices, such as routers and switches, in the same room, as long as that room is kept secure. There's no security advantage to using external hard drives instead of tape backup media.

References

LabSim for Security Pro, Section 4.2.
[All Questions SecPro2017_v6.exm DEV_PROTECT_04]

Question 5: Incorrect

A malicious user in your organization was able to use the Trinity Rescue Kit to change the password on a department manager's computer in the finance department. The user was able to copy data containing bank account information and social security numbers. The user then destroyed the data by resetting the computer.

The department manager was at lunch at the time and had enabled the lock screen to require a password to gain access to the computer.

Which additional measure should the manager have taken to prevent data theft?

- The computer should have been bolted to the desk.
- The data should have been backed up so it could be restored after it was destroyed.
- ~~The sensitive data on the computer should have been encrypted.~~
- The computer should have been kept in a physically secure location.

Explanation

To prevent the theft of this sensitive data, the computer should have been kept in a physically secure location, such as a locked office. If the user was able to use the Trinity Rescue Kit, they must have gained physical access to the machine.

Encrypting the data would not have prevented it from being stolen. The user could still use decryption tools to get to the sensitive information. Bolting the computer to the desk would not have made any difference because the thief did not steal the computer. Backing up the data is a good practice so that the computer can be restored to the state it was in before it was attacked, but data backups don't prevent data theft.

References

LabSim for Security Pro, Section 4.2.
[All Questions SecPro2017_v6.exm DEV_PROTECT_05]