Exam Report: 4.1.5 Practice Questions

Date: 1/20/2020 8:20:39 am
Time Spent: 6:25

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 47%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Correct

You are about to enter your office building through a back entrance. A man dressed as a plumber asks you to let him in so he can fix the restroom. What should you do?

○ Let him in and help him find the restroom, then let him work.

○ Let him in.

○ Tell him no and quickly close the door.

➡ ● Direct him to the front entrance and instruct him to check in with the receptionist.

Explanation

You should direct him to the front entrance, where he can check in with the proper people at your organization. Letting him in without knowing if he should be there can compromise security. Turning him away would be unprofessional.

References

LabSim for Security Pro, Section 4.1.
[All Questions SecPro2017_v6.exm PHYS_THREAT_01]

Question 2: Correct

Which of the following are solutions that address physical security? (Select two.)

➡ ☑ Require identification and name badges for all employees

□ Disable guest accounts on computers

□ Scan all floppy disks before use

➡ ☑ Escort visitors at all times

□ Implement complex passwords

Explanation

Physical security controls physical access to the network or its components. Physical security controls include:

- Requiring identification or key cards before entry is permitted
- Escorting visitors at all times
- Keeping doors and windows locked
- Keeping devices with sensitive information out of view of public users
- Keeping the server room locked (locking computers to racks or tables to prevent theft)

References

LabSim for Security Pro, Section 4.1.
[All Questions SecPro2017_v6.exm PHYS_THREAT_02]

▼ **Question 3:** Correct

Which of the following is **not** an example of a physical barrier access control mechanism?

○ Fences

➡ ◉ One-time passwords

○ Biometric locks

○ Mantrap

Explanation

A one-time password is a logical or technical access control mechanism, not a physical barrier access control mechanism.

A biometric lock is an entryway security device that keeps a door or gate locked until an authorized individual provides a valid biometric, such as a hand scan. A mantrap is a small room with two doors. Authorized users must authenticate to enter the room and then further authenticate to exit the room into the secured environment. If the second authentication fails, the intruder is retained in the room until authorities respond. A fence is a perimeter protection device designed to deter intruders and define the boundary of protection employed by an organization.

References

LabSim for Security Pro, Section 4.1.
[All Questions SecPro2017_v6.exm PHYS_THREAT_03]

▼ **Question 4:** Incorrect

Which of the following can be used to stop piggybacking at a front entrance where employees should swipe smart cards to gain entry?

○ Use key locks rather than electronic locks

○ Use weight scales

◉ ~~Install security cameras~~

➡ ○ Deploy a mantrap

Explanation

Piggybacking is when an authorized or unauthorized individual gains entry into a secured area by exploiting the credentials of a prior person. Often, the first person will authenticate, unlock the door, and then hold it open for the next person to enter without forcing them to authenticate separately. Piggybacking can be stopped by a mantrap. A mantrap is a single-person room with two doors. It often includes a scale to prevent piggybacking. Mantraps requires proper authentication before the inner door unlocks to allow authorized personal into a secured area. Those who fail to properly authenticate are held captive until authorities respond.

A security camera may deter piggybacking, but it does not directly stop piggybacking. Using weight scales inside a mantrap will stop piggybacking, but they are not useful or effective without the mantrap. The use of conventional keys as opposed to electronic locks has little effect on preventing piggybacking and may actually make piggybacking more prevalent.

References

LabSim for Security Pro, Section 4.1.
[All Questions SecPro2017_v6.exm PHYS_THREAT_04]

▼ **Question 5:** Correct

Which option is a secure doorway that can be used in coordination with a mantrap to allow easy egress from a secured environment while actively preventing re-entrance through the exit portal?

○ Egress mantraps

○ Locked doors with interior unlock push bars

➡ ● Turnstiles

○ Electronic access control doors

Explanation

Turnstiles allow easy egress from a secured environment but actively prevent re-entrance through the exit portal. Turnstiles are a common exit portal used in conjunction with entrance portal mantraps. A turnstile cannot be used to enter into a secured facility, as it only functions in one direction.

Egress mantraps are not easy egress portals. Plus, they are a tremendous unnecessary expense and administrative burden. Any form of door, including self-locking doors with push bars or credential readers, can be hijacked to allow an outsider to enter.

References

LabSim for Security Pro, Section 4.1.
[All Questions SecPro2017_v6.exm PHYS_THREAT_05]

▼ **Question 6:** Correct

What is the primary benefit of CCTV?

○ Increase security protection throughout an environment

○ Provide a corrective control

➡ ● Expand the area visible by security guards

○ Reduce the need for locks and sensors on doors

Explanation

A primary benefit of CCTV is that it expands the area visible by security guards. This helps few guards oversee and monitor a larger area.

CCTV does not reduce the need for locks and sensors on doors. CCTV does not provide a corrective control (it is a preventative, deterrent, or detective control). CCTV does not increase security protection throughout an environment; it only does so over those environments where the CCTV is aimed.

References

LabSim for Security Pro, Section 4.1.
[All Questions SecPro2017_v6.exm PHYS_THREAT_06]

▼ **Question 7:** Incorrect

You want to use CCTV to increase your physical security. You want the ability to remotely control the camera position. Which camera type should you choose?

○ Dome

○ Bullet

➡ ○ PTZ

● ~~C mount~~

Explanation

A Pan Tilt Zoom (PTZ) camera lets you dynamically move the camera and zoom in on specific areas (cameras without PTZ capabilities are set looking a specific direction). Automatic PTZ mode automatically moves the camera between several preset locations. Manual PTZ lets an operator remotely control the position of the camera.

A *bullet* camera has a built-in lens and is long and round in shape. Most bullet cameras can be used indoors or outdoors. A *c-mount* camera has interchangeable lenses, is typically rectangle in shape, and carries the lens on its end. Most c-mount cameras require a special housing to be used outdoors. A *dome* camera is a camera protected with a plastic or glass dome. These cameras are more vandal-resistant than other cameras.

Bullet, c-mount, or dome cameras can also be PTZ cameras.

References

LabSim for Security Pro, Section 4.1.
[All Questions SecPro2017_v6.exm PHYS_THREAT_07]

Question 8: Incorrect

You want to use CCTV to increase the physical security of your building. Which of the following camera types would offer the sharpest image at the greatest distance under the lowest lighting conditions?

○ 400 resolution, 10mm, 2 LUX

○ 500 resolution, 50mm, 2 LUX

➡ ○ 500 resolution, 50mm, .05 LUX

● ~~400 resolution, 10mm, .05 LUX~~

Explanation

When you select cameras, be aware of the following characteristics:

- The resolution is rated in the number of lines included in the image. In general, the higher the resolution, the sharper the image.
- The focal length measures the magnification power of a lens. The focal length controls the distance that the camera can see, as well as how much detail can be seen at a specific range. A higher focal length lets you see more detail at a greater distance.
- LUX is a measure of the sensitivity to light. The lower the number, the less light is necessary for a clear image.

References

LabSim for Security Pro, Section 4.1.
[All Questions SecPro2017_v6.exm PHYS_THREAT_08]

Question 9: Incorrect

Which of the following CCTV camera types lets you adjust the distance that the camera can see (in other words, zoom in or out)?

● ~~C-mount~~

○ Fixed

○ Infrared

➡ ○ Varifocal

Explanation

A *varifocal* camera lens lets you adjust the focus (zoom).

A *fixed* lens camera has a set focal length. Infrared cameras can record images in little or no light. A *c-mount* camera has interchangeable lenses, is typically rectangle in shape, and carries the lens on its end. You can change the focal length of a c-mount camera by changing the lens, but you can't change the focus unless the lens is a varifocal lens.

References

LabSim for Security Pro, Section 4.1.
[All Questions SecPro2017_v6.exm PHYS_THREAT_09]

Question 10: Incorrect

Which of the following allows for easy exit of an area in the event of an emergency, but prevents entry? (Select two.)

□ PTZ CCTV

☑ ~~Mantrap~~

☐ Anti-passback system

➡ ☐ Turnstile

➡ ☐ Double-entry door

Explanation

A *double-entry door* has two doors that are locked from the outside and have crash bars on the inside, which make it easy to exit. Double-entry doors are typically used only for emergency exits, and alarms sound when the doors are opened. A *turnstile* is a barrier that permits entry in only one direction. Turnstiles are often used to permit easy exit from a secure area. Entry is controlled through a mantrap or other system that requires authentication for entry.

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. This may include visual identification and identification credentials.

An anti-passback system is used when a physical access token is required for entry and prevents a card holder from passing their card back to someone else. A Pan Tilt Zoom (PTZ) camera lets you dynamically move the camera and zoom in on specific areas.

References

LabSim for Security Pro, Section 4.1.
[All Questions SecPro2017_v6.exm PHYS_THREAT_10]

Question 11: Correct

Which of the following controls is an example of a physical access control method?

○ Passwords

➡ ● Locks on doors

○ Smart cards

○ Hiring background checks

○ Access control lists with permissions

Explanation

Locks on doors are an example of a physical access control method. Physical controls restrict or control physical access.

Passwords, access control lists, and smart cards are all examples of technical controls. Even though the smart card is a physical object, the card by itself is part of a technical implementation. Requiring background checks for hiring is an example of a policy or an administrative control.

References

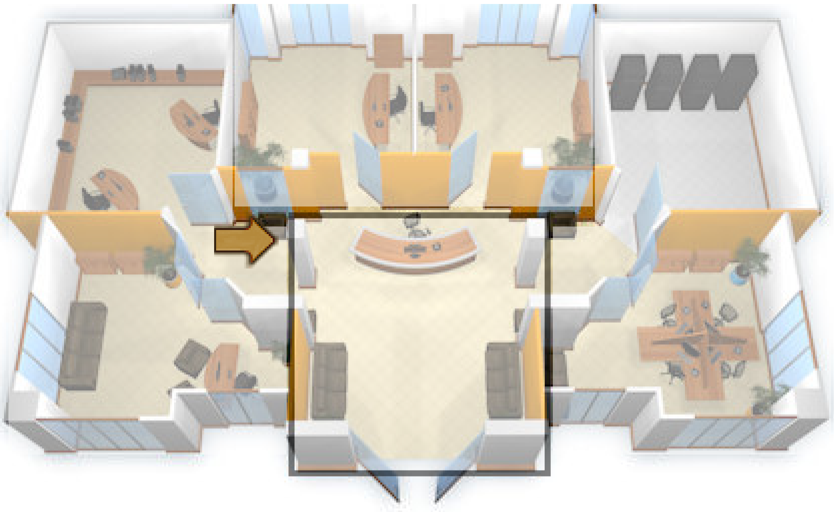
LabSim for Security Pro, Section 4.1.
[All Questions SecPro2017_v6.exm PHYS_THREAT_11]

Question 12: Correct

You are the security administrator for a small business. The floor plan for your organization is shown in the figure below.

You've hired a third-party security consultant to review your organization's security measures. She has discovered multiple instances where unauthorized individuals have gained access to your facility, even to very sensitive areas. She recommends that you implement mantraps to prevent this from happening in the future.

Click on the office location where a mantrap would be most appropriate.



Explanation

By implementing a mantrap at the lobby entrance, two doors must be unlocked in sequence for an individual to gain access to this facility. A mantrap allows both doors to lock, detaining a suspicious individual between doors.

References

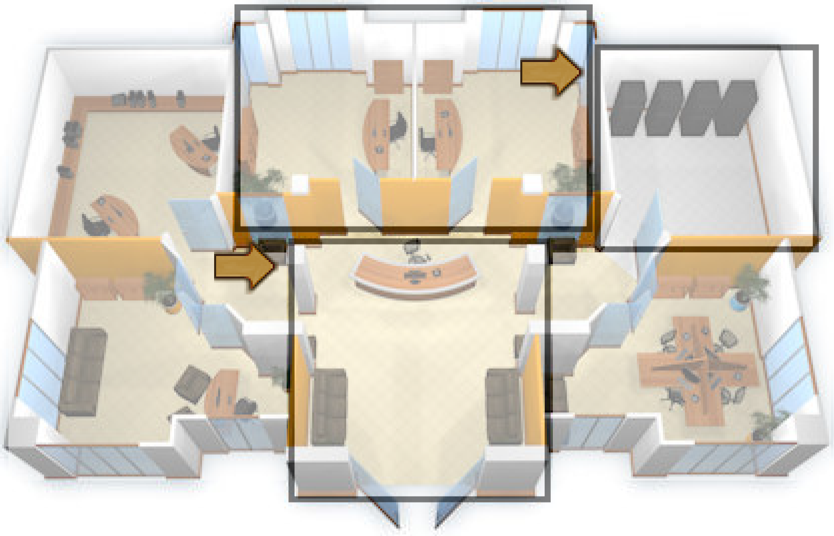
LabSim for Security Pro, Section 4.1.
[All Questions SecPro2017_v6.exm PHYS_THREAT_12]

Question 13: Incorrect

You are the security administrator for a small business. The floor plan for your organization is shown in the figure below.

You've hired a third-party security consultant to review your organization's security measures. She has discovered multiple instances where unauthorized individuals have gained access to your facility, even to very sensitive areas. She recommends that you provide employees with access badges and implement access badge readers to prevent this from happening in the future.

Click on the office locations where access badge readers would be most appropriate.



Explanation

Access badge readers are typically implemented at building entrances to control access to a facility. Only individuals who have an authorized access badge are allowed to enter the facility. Individuals who do not have an access badge must be cleared and admitted by security personnel. Additional access badge readers can be implemented within the facility to further restrict access to sensitive areas, such as the server room.

References

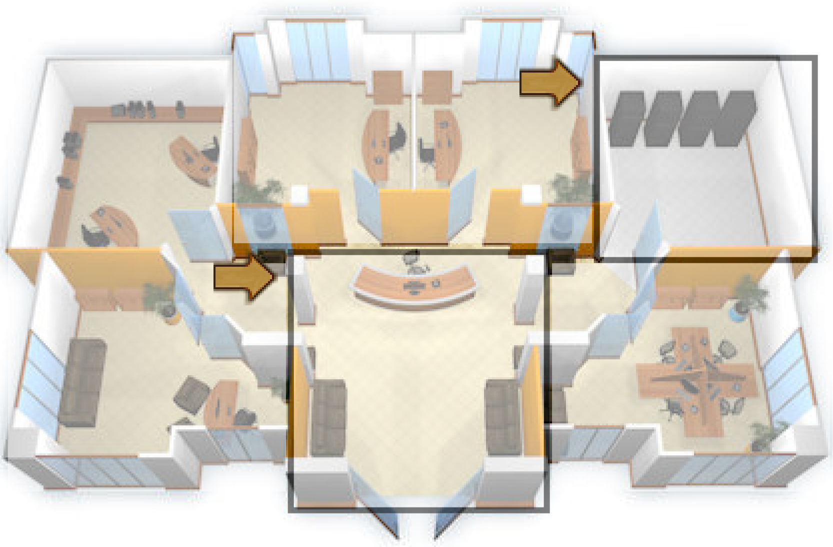
LabSim for Security Pro, Section 4.1.
[All Questions SecPro2017_v6.exm PHYS_THREAT_13]

Question 14: Incorrect

You are the security administrator for a small business. The floor plan for your organization is shown in the figure below.

You've hired a third-party security consultant to review your organization's security measures. She has discovered multiple instances where unauthorized individuals have gained access to your facility, even to very sensitive areas. She recommends that you implement closed-circuit TV (CCTV) surveillance cameras to prevent this from happening in the future.

Click on the office locations where surveillance cameras would be most appropriate.



Explanation

Video surveillance cameras are typically implemented at building entrances to monitor access to a facility. If a security breach occurs, video recordings can be reviewed to identify the individual(s) involved. Additional video surveillance cameras can be implemented within the facility to further monitor access to sensitive areas, such as the server room.

References

LabSim for Security Pro, Section 4.1.
[All Questions SecPro2017_v6.exm PHYS_THREAT_14]

Question 15: Incorrect

Match each physical security control on the left with an appropriate example of that control on the right. Each security control may be used once, more than once, or not at all.

Hardened carrier	Biometric authentication	Barricades
~~Door locks~~ Protected cable distribution	~~Physical access control~~ Door locks	✓ Perimeter barrier
Emergency escape plans	Alarmed carrier	Anti-passback system
✓ Safety	~~Door locks~~ Protected cable distribution	✓ Physical access control
Emergency lighting	Exterior floodlights	
✓ Safety	~~Safety~~	

Perimeter barrier

Explanation

Following are several physical security controls and functions you should be familiar with:

- *Perimeter barriers* secure the building perimeter and restrict access to only secure entry points. Examples include *barricades* and *floodlights*.
- *Door locks* allow access only to those with the proper key. For example, a *biometric authentication system* requires an individual to submit to a finger print or retina scan before unlocking a door.
- *Physical access controls* are implemented inside the facility to control who can go where. For example, an *anti-passback system* prevents a card holder from passing their card back to someone else.
- *Safety controls* help employees and visitors remain safe while on site. For example, consider devising *escape plans* that utilize the best escape routes for each area in your organization. In addition, *emergency lighting* should be implemented that runs on protected power and automatically switches on when the main power goes off.
- A *protected distribution system* (PDS) encases network cabling within a carrier. This enables data to be securely transferred directly between two high-security areas through an area of lower security. In a *hardened carrier PDS*, network cabling is run within metal conduit. In an *alarmed carrier PDS,* an electronic alarm system is used to detect attempts to compromise the carrier and access the cable within it.

References

LabSim for Security Pro, Section 4.1.
[All Questions SecPro2017_v6.exm PHYS_THREAT_15]