Exam Report: 13.1.4 Practice Questions

Date: 12/2/2019 9:39:50 am
Time Spent: 24:02

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 33%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

You've just deployed a new Cisco router that connects several network segments in your organization.

The router is physically located in a cubicle near your office. You've backed up the router configuration to a remote location in an encrypted file. You access the router configuration interface from your notebook computer using an SSH client with a username of **admin01** and a password of **P@ssW0rd**. You have used the MD5 hashing algorithm to protect the password.

What should you do to increase the security of this device?

- ~~Change the default administrative username and password.~~
- Use a Telnet client to access the router configuration.
- Move the router to a secure server room.
- Use TFTP to back up the router configuration to a remote location.
- Use encrypted type 7 passwords.

Explanation

In this scenario, the router is not physically secure. Anyone with access to the area could gain access to the router and manipulate its configuration by plugging into the console port. The device should be moved to a secure location, such as a server room, that requires an ID badge for access.

You should not use a Telnet client to access the router configuration. Telnet transfers data in clear text over the network connection, exposing sensitive data to sniffing. The user name and password used to access the router configuration are reasonably strong. Encrypted type 7 passwords on a Cisco device are less secure than those protected with MD5. Using TFTP to manage the router configuration could expose sensitive information to sniffers, as it transmits data in clear text.

References

LabSim for Network Pro, Section 13.1.
[netpro18v5_all_questions_en.exm RT-7.4-2]

Question 2: Incorrect

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

Explanation

In this scenario, you should recommend 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 for preventing 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 will control 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 would be unlikely to increase the security of the network.

References

LabSim for Network Pro, Section 13.1.
[netpro18v5_all_questions_en.exm RT-5.2-1]

Question 3: Incorrect

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

- [ ] Require identification and name badges for all employees.
- [ ] Implement complex passwords.
- [ ] Disable guest accounts on computers.
- [x] ~~Scan all floppy disks before use.~~
- [x] Escort visitors at all times.

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 and locking computers to racks or tables to prevent theft.

References

LabSim for Network Pro, Section 13.1.
[netpro18v5_all_questions_en.exm NP09 6-5 MCM2]

Question 4: Correct

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

- Use key locks rather than electronic locks
- Use weight scales
- Deploy a mantrap
- Install security cameras

Explanation

Piggybacking is the activity where 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. It requires proper authentication before unlocking the inner door 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 does little to prevent piggybacking and may actually make piggybacking more prevalent.

References

LabSim for Network Pro, Section 13.1.
[netpro18v5_all_questions_en.exm SP02_5-1 [116]]

Question 5: Correct

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

- Biometric locks
- Mantraps
- One-time passwords
- Fences

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 entry way 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 and enter 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 Network Pro, Section 13.1.

[netpro18v5_all_questions_en.exm SP02_5-1 [5]]

Question 6: Incorrect

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

- ~~Dome~~
- C-mount
- Bullet
- PTZ

Explanation

A pan tilt zoom (PTZ) camera lets you dynamically move the camera and zoom in on specific areas (cameras without PTZ capabilities are manually set looking a specific direction). Automatic PTZ mode automatically moves the camera between several preset locations; manual PTZ lets an operator remotely control the camera positon.

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 and is typically rectangular in shape. 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.

PTZ cameras can be bullet, c-mount, or dome cameras.

References

LabSim for Network Pro, Section 13.1.
[netpro18v5_all_questions_en.exm SP08_3-9 1]

Question 7: Incorrect

You want to use CCTV as a preventative security measure. Which of the following is a requirement for your plan?

- Low LUX or infrared camera
- ~~Sufficient lighting~~
- PTZ camera
- Security guards

Explanation

When used in a preventative way, you must have a guard or other person available who monitors one or more cameras. Only a security guard can interpret what the camera sees to make appropriate security decisions.

Even with sufficient lighting on a low-lux or infrared camera, a camera is not a useful preventative measure without a security guard present to interpret images and make security decisions.

A pan tilt zoom (PTZ) camera lets you dynamically move the camera and zoom in on specific areas.

References

LabSim for Network Pro, Section 13.1.
[netpro18v5_all_questions_en.exm SP08_3-9 5]

Question 8: Correct

Which of the following CCTV types would you use in areas with little or no light?

- C-mount

- Infrared
- A camera with a high LUX rating
- PTZ

Explanation

Infrared cameras can record images in little or no light.

LUX is a measure of sensitivity to light. The lower the number, the less light needed for a clear image. Infrared cameras have a low LUX rating, meaning that little light is needed.

A c-mount camera has interchangeable lenses and is typically rectangular in shape. A pan tilt zoom (PTZ) camera lets you dynamically move the camera and zoom in on specific areas.

References

LabSim for Network Pro, Section 13.1.
[netpro18v5_all_questions_en.exm SP08_3-9 4]

Question 9: Incorrect

Which of the following CCTV camera types lets zoom the focus in and out?

- ~~C-mount~~
- Infrared
- Varifocal
- Fixed

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 and is typically rectangular in shape. You can change the focal length of a c-mount camera by changing the lens, but you can't zoom the focus unless the lens is a varifocal lens.

References

LabSim for Network Pro, Section 13.1.
[netpro18v5_all_questions_en.exm SP08_3-9 3]

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.)

- [ ] Turnstile
- [x] Double-entry door
- [x] ~~Mantrap~~
- [ ] Anti-passback system
- [ ] PTZ CCTV

Explanation

A *double entry door* has two doors that are locked from the outside but with crash bars on the inside that allow easy 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 to monitor.

References

LabSim for Network Pro, Section 13.1.
[netpro18v5_all_questions_en.exm SP08_3-9 6]

Question 11: Incorrect

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

- Hiring background checks
- Locks on doors
- Passwords
- ~~Access control lists with permissions~~
- Smart cards

Explanation

Locks on doors is 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 a 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 Network Pro, Section 13.1.
[netpro18v5_all_questions_en.exm SSCP-1 NEW [39]]

Question 12: Correct

Five salesmen who work out of your office. They frequently leave their laptops laying on the desk in their cubicles. You are concerned that someone might walk by and take one of these laptops.

Which of the following is the best way to address your concerns?

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

Explanation

The main concern in this case is with laptops being stolen. 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 Network Pro, Section 13.1
[netpro18v5_all_questions_en.exm APESS_6-2 MC [39]]

Question 13: 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
~~Physical access control~~	~~Physical access control~~	~~Physical access control~~
Protected cable distribution	Door locks	Perimeter barrier
Emergency escape plans	Alarmed carrier	Anti-passback system
✓ Safety	~~Perimeter barrier~~	✓ Physical access control
	Protected cable distribution	
Emergency lighting	Exterior floodlights	
✓ Safety	✓ Perimeter barrier	

Explanation

Physical security controls and their functions include the following:

- 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 a door is unlocked.
- 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 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 Network Pro, Section 13.1.
[netpro18v5_all_questions_en.exm RT-5.1-1]

Question 14: Incorrect

You are an IT consultant and 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 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 UTM 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.)

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

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 proximity 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 will control 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 would be unlikely to increase the security of the network.

References

LabSim for Network Pro, Section 13.1.
[netpro18v5_all_questions_en.exm RT NP15_3.4-1]

Question 15: Correct

Which of the following is the most important way to prevent console access to a network switch?

- (•) Keep the switch in a room that is locked by a keypad.
- ( ) Set console and enable secret passwords.
- ( ) Disconnect the console cable when not in use.
- ( ) Implement an access list to prevent console connections.

Explanation

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

References

LabSim for Network Pro, Section 13.1.
[netpro18v5_all_questions_en.exm RT NP15_3.4-2]