Exam Report: 3.2.5 Practice Questions

Date: 4/4/29 5:18:05 pm
Time Spent: 1:26

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 55%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Correct

You are a security consultant and have been hired to evaluate an organization's physical security practices. All employees must pass through a locked door to enter the main work area. Access is restricted using a biometric fingerprint lock.

A receptionist is located next to the locked door in the reception area. She uses an iPad application to log any security events that may occur. She also uses her iPad to complete work tasks as assigned by the organization's CEO.

What could you do to add an additional layer of security to this organization?

○ Require users to use workstation screensaver passwords.

➡ ● Train the receptionist to keep her iPad in a locked drawer.

○ Move the receptionist's desk into the secured area.

○ Replace the biometric locks with smart cards.

Explanation

In this scenario, the best option to add an additional layer of security is to train the receptionist to keep her iPad in a locked drawer.

In this scenario, moving the receptionist's desk into the secured area would defeat the purpose; only employees would have to access the receptionist.

Biometrics are already in place in this scenario.

All companies should require users to use workstation screensaver passwords. In this scenario, the receptionist does not have a workstation.

References

TestOut Ethical Hacker Pro - 3.2 Physical Security
[e_physical_security_eh1.exam.xml Q_PHYSICAL_SECURITY_LAYER_DEF_01_EH1]

Question 2: Correct

While reviewing video files from your organization's security cameras, you notice a suspicious person using piggybacking to gain access to your building. The individual in question did not have a security badge.

Which of the following would you most likely implement to keep this from happening in the future?

○ Cable locks

○ Anti-passback

○ Scrubbing

➡ ● Mantraps

Explanation

You could implement mantraps at each entrance to the facility to mitigate piggybacking. 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. If authentication is not provided, the intruder is kept in the mantrap until authorities arrive.

Scrubbing involves holding a lock with a tension wrench and quickly scraping the lock pins with a pick.

Cable locks are used to secure computer hardware.

An anti-passback system prevents a cardholder from passing their card back to someone else.

References

TestOut Ethical Hacker Pro - 3.2 Physical Security
[e_physical_security_eh1.exam.xml Q_PHYSICAL_SECURITY_PHYS_CONTROL_01_EH1]

Question 3: Incorrect

Implementing emergency lighting that runs on protected power and automatically switches on when the main power goes off is part of which physical control?

➡ ○ Employee and visitor safety

○ Perimeter barriers

○ Physical access controls

● ~~Physical access logs~~

Explanation

As you implement physical security, be sure to keep the safety of employees and visitors in mind. Consider the importance of the following actions:

- Implement adequate lighting in parking lots and around employee entrances.
- Implement emergency lighting that runs on protected power and automatically switches on when the main power goes off.
- Implement fail-open locking systems that allow employees to exit your facility quickly in the event of an emergency.
- Devise escape plans that utilize the best escape routes for each area in your organization. Post these escape plans in prominent locations.
- Conduct emergency drills to verify that the physical safety and security measures you have implemented function correctly.

You can implement physical access controls inside the facility as follows:

- Physical controls may include key fobs, swipe cards, or badges.
- Physical controls may include biometric factors such as fingerprint scanners, retinal scanners, iris scanners, voice recognition, and facial recognition.
- To control access to sensitive areas within the facility, require a card swipe or reader.
- Some systems can track personnel movement within a facility and proactively lock or unlock doors based on the access token device.
- An anti-passback system prevents a card holder from passing a card back to someone else.
- Physical controls are often implemented along with sensors and alarms to detect unauthorized access.

Perimeter barriers physically secure a building's perimeter and restrict access to only secure entry points.

Physical access logs are implemented by facility guards and require everyone gaining access to the facility to sign in upon entry.

References

TestOut Ethical Hacker Pro - 3.2 Physical Security
[e_physical_security_eh1.exam.xml Q_PHYSICAL_SECURITY_PHYS_CONTROL_02_EH1]

Question 4: Incorrect

Closed-circuit television can be used as both a preventative tool (to monitor live events) or as an investigative tool (to record events for later playback). Which camera is more vandal-resistant than other cameras?

○ A Pan Tilt Zoom camera

● ~~A c-mount camera~~

➡ ○ A dome camera

○ A bullet camera

Explanation

A dome camera, which is a camera protected with a plastic or glass dome, is more vandal-resistant than other cameras.

A c-mount camera has interchangeable lenses and is typically rectangle in shape with the lens on the end. Most c-mount cameras require a special housing to be used outdoors.

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 toward a specific direction).

A bullet camera has a built-in lens and is long and round in shape. Most bullet cameras can be used indoors or outdoors.

References

TestOut Ethical Hacker Pro - 3.2 Physical Security
[e_physical_security_eh1.exam.xml Q_PHYSICAL_SECURITY_PHYS_CONTROL_03_EH1]

▼ **Question 5:** Incorrect

Important aspects of physical security include which of the following?

○ Identifying what was broken into, what is missing, and the extent of the damage.

○ Implementing adequate lighting in parking lots and around employee entrances.

➡ ○ Preventing interruptions of computer services caused by problems such as fire.

● ~~Influencing the target's thoughts, opinions, and emotions before something happens.~~

Explanation

Important aspects of physical security include:

- Restricting physical access to facilities and computer systems.
- Preventing interruptions of computer services caused by problems such as loss of power or fire.
- Preventing unauthorized disclosure of information.
- Disposing of sensitive material.
- Protecting the interior and exterior of your facility.

Detection is identifying what was broken into, what is missing, and the extent of the damage.

Preloading is influencing the target's thoughts, opinions, and emotions before something happens.

Implement adequate lighting in parking lots and around employee entrances are control measures for employee and visitor safety.

References

TestOut Ethical Hacker Pro - 3.2 Physical Security
[e_physical_security_eh1.exam.xml Q_PHYSICAL_SECURITY_SECUR_ASPECTS_01_EH1]

▼ **Question 6:** Incorrect

What are the three factors to keep in mind with physical security?

● ~~Detection, prevention, and implementation~~

➡ ○ Prevention, detection, and recovery

○

○ Implementation, detection, and recovery

○ Detection, implementation, and prevention

Explanation

There are three factors to keep in mind with physical security:

- Prevention is making the location less appealing to hackers.
- Detection is identifying what was broken into, what is missing, and the extent of the damage.
- Recovery is reviewing the physical security procedures, repairing any damage, and hardening the physical security of the company against future problems.

References

TestOut Ethical Hacker Pro - 3.2 Physical Security
[e_physical_security_eh1.exam.xml Q_PHYSICAL_SECURITY_SECUR_FACTOR_01_EH1]

Question 7: Correct

A person in a dark grey hoodie has jumped the fence at your research center. A security guard has detained this person, denying him physical access. Which of the following areas of physical security is the security guard currently in?

○ Security factors

➡ ● Security sequence

○ Physical control

○ Layered defense

Explanation

The security sequence area of physical security should be deployed in the following sequence. If a step in the sequence fails, the next step should implement itself automatically.

1. Deter initial access attempts.
2. Deny direct physical access.
3. Detect the intrusion.
4. Delay the violator to allow for response.

When designing physical security, implement a layered defense system. A layered defense system is one in which controls are implemented at each layer to ensure that defeating one level of security does not allow an attacker subsequent access.

There are three security factors to keep in mind with physical security: prevention, detection, and recovery.

Physical controls are measures you take to physical secure a building, secure the perimeter, and restrict access to only secure entry points.

References

TestOut Ethical Hacker Pro - 3.2 Physical Security
[e_physical_security_eh1.exam.xml Q_PHYSICAL_SECURITY_SECUR_SEQ_01_EH1]

Question 8: Incorrect

Which of the following best describes a lock shim?

➡ ○ A thin, stiff piece of metal.

○ A cut to the number nine position.

● ~~A small, angled, and pointed tool.~~

○ When the pins are scraped quickly.

Explanation

A lock shim is a tool that is, basically, a thin, stiff piece of metal that can be inserted into the latch of a

padlock.
A bump key is cut to the number nine position, which is the lowest possible cut.

A pick is a small, angled, and pointed tool kind of like a dentist pick.

One of the most common ways to pick a lock is called scrubbing. This method involves holding the lock with a tension wrench while the pins are scraped quickly with the pick.

References

TestOut Ethical Hacker Pro - 3.2 Physical Security
[e_physical_security_eh1.exam.xml Q_PHYS_SEC_ATTACKS_LOCK_PICK_01_EH1]

▼ Question 9: Correct

On her way to work, Angela accidentally left her backpack with a company laptop at the coffee shop. What type of threat has she caused the company?

➡ ● Man-made threat

○ External threat

○ Cloud threat

○ Environmental threat

Explanation

Human threats can be outsiders or insiders, so it can be tricky to safeguard against them all. Man-made threats include:

- Theft
- Vandalism
- Destruction

Environmental threats are natural disasters such as floods, fires, hurricanes, and other types of extreme weather.

An external threat is a threat originating outside a company, government agency, or institution.

Cloud threats are against the cloud services. The cloud is susceptible to many threats.

References

TestOut Ethical Hacker Pro - 3.2 Physical Security
[e_physical_security_eh1.exam.xml Q_PHYS_SEC_ATTACKS_MAN_MADE_01_EH1]

▼ Question 10: Correct

The U.S. Department of Commerce has an agency with the goal of protecting organizational operations, assets, and individuals from threats such as malicious cyber-attacks, natural disasters, structural failures, and human errors. Which of the following agencies was created for this purpose?

○ NVD

○ JPCERT

○ CAPEC

➡ ● NIST

Explanation

To protect data from threats and attacks, the U.S. Department of Commerce created the National Institute of Standards and Technology (NIST). NIST has released a special publication referred to as the NIST SP 800-53, which details security controls and assessment procedures that companies and organizations should implement to protect the integrity of their information systems. This document's goal is to protect organizational operations, assets, and individuals from many different kinds of threats, such as malicious cyberattacks, natural disasters, structural failures, and human errors.

The National Vulnerability Database (NVD) was originally created in 2000 and is a government-sponsored, detailed database of known vulnerabilities.

JPCERT is Japan's CERT organization. It provides security alerts and Japanese Vulnerability Notes (JVN).

CAPEC is a dictionary of known patterns of cyberattacks used by hackers.

References

TestOut Ethical Hacker Pro - 3.2 Physical Security
[e_physical_security_eh1.exam.xml Q_PHYS_SEC_ATTACKS_NIST_01_EH1]

Question 11: Correct

Which type of attack involves changing the boot order on a PC so that the hacker can gain access to the computer by bypassing the install operating system?

○ Opportunistic attack

➡ ● Physical attack

○ Environmental attack

○ Man-made attack

Explanation

Physical security is the protection of corporate assets including property, facilities, equipment, and personnel from damage, theft, or harm. Physical attacks include items such as cold boot attacks, badge cloning, and BIOS access attacks.

An opportunistic attack is typically automated and involves scanning a wide range of systems for known vulnerabilities such as old software, exposed ports, poorly secured networks, and default configurations.

One thing to remember is that human threats can be outsiders or insiders, so it can be tricky to safeguard against them all. Man-made threats include theft, vandalism, and destruction.

Environmental threats are natural disasters such as floods, fires, hurricanes, and other types of extreme weather.

References

TestOut Ethical Hacker Pro - 3.2 Physical Security
[e_physical_security_eh1.exam.xml Q_PHYS_SEC_ATTACKS_OTHER_ATTACKS_01_EH1]