Exam Report: 1.1.4 Practice Questions

Date: 1/8/2020 2:08:15 pm
Time Spent: 8:07

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 70%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

A user copies files from her desktop computer to a USB flash device and puts the device into her pocket. Which of the following security risks is most pressing?

- Integrity
- Availability
- Non-repudiation
- Confidentiality

Explanation

Confidentiality ensures that data is not disclosed to unintended persons. Removable media poses a big threat to confidentiality because it makes it easy to remove data and share data with unauthorized users.

Availability ensures that data is available when it is needed. Copying files to a server that includes malware could threaten data's availability if the malware deletes or corrupts data. *Integrity* ensures that data is not modified or tampered with. *Non-repudiation* provides validation of a message's origin.

References

LabSim for Security Pro, Section 1.1.
[All Questions SecPro2017_v6.exm SEC_OVW_01]

Question 2: Correct

Smart phones with cameras and internet capabilities pose a risk to which security concept?

- Integrity
- Confidentiality
- Availability
- Non-repudiation

Explanation

Smart phones with cameras and data transfer capabilities pose a risk to confidentiality. Users can take pictures of computer screens or save data to cell phones and make that information available to non-authorized users.

Availability ensures that data is available when it is needed. Copying files to a server that includes malware could threaten data's availability if the malware deletes or corrupts data. *Integrity* ensures that data is not modified or tampered with. *Non-repudiation* provides validation for a message's origin.

References

LabSim for Security Pro, Section 1.1.
[All Questions SecPro2017_v6.exm SEC_OVW_02]

Question 3: Incorrect

By definition, which security concept ensures that only authorized parties can access data?

- Integrity
- Authentication
- Confidentiality
- ~~Non-repudiation~~

Explanation

Confidentiality ensures that only authorized parties can access data. When a cryptographic system protects data confidentiality, unauthorized users cannot view the resource.

Non-repudiation is the ability to prove that a sender sent a message. Integrity is protection against alteration. Authentication is the assignment of access privileges to users.

References

LabSim for Security Pro, Section 1.1.
[All Questions SecPro2017_v6.exm SEC_OVW_03]

Question 4: Correct

Your computer system is a participant in an asymmetric cryptography system. You've created a message to send to another user. Before transmission, you hash the message and encrypt the hash using your private key. You then attach this encrypted hash to your message as a digital signature before sending it to the other user.

In this example, what protection does the hashing activity provide?

- Confidentiality
- Non-repudiation
- Availability
- Integrity

Explanation

Hashing of any sort at any time, including within a digital signature, provides data integrity.

Signing the message with the private key creates non-repudiation. A digital signature activity, as a whole, does not provide protection for confidentiality because the original message is sent in clear form. No form of cryptography provides protection for availability.

References

LabSim for Security Pro, Section 1.1.
[All Questions SecPro2017_v6.exm SEC_OVW_04]

Question 5: Correct

Which of the following is an example of an *internal* threat?

- A delivery man is able to walk into a controlled area and steal a laptop.
- A water pipe in the server room breaks.
- A server back door allows an attacker on the internet to gain access to the intranet site.
- A user accidentally deletes the new product designs.

Explanation

Internal threats are intentional or accidental acts by employees, including:

- Malicious acts such as theft, fraud, or sabotage
- Intentional or unintentional actions that destroy or alter data
- Disclosing sensitive information by snooping or espionage

External threats are events that originate outside of the organization. They typically focus on compromising the organization's information assets. Examples of external threats include hackers, fraud perpetrators, and viruses. *Natural events* are events that may reasonably be expected to occur over time, such as a fire or a broken water pipe.

References

LabSim for Security Pro, Section 1.1.
[All Questions SecPro2017_v6.exm SEC_OVW_05]

Question 6: Incorrect

What is the *greatest* threat to the confidentiality of data in most secure organizations?

- USB devices
- Hacker intrusion
- ~~Operator error~~
- Malware

Explanation

The greatest threat to data confidentiality in most secure organizations is portable devices (including USB devices). There are so many devices that can support file storage that stealing data has become easy, and preventing data theft is difficult.

References

LabSim for Security Pro, Section 1.1.
[All Questions SecPro2017_v6.exm SEC_OVW_06]

Question 7: Correct

Which of the following is the correct definition of a *threat*?

- Any potential danger to the confidentiality, integrity, or availability of information or systems
- Instance of exposure to losses from an attacker
- The likelihood of an attack taking advantage of a vulnerability
- Absence or weakness of a safeguard that could be exploited

Explanation

A threat is any potential danger to the confidentiality, integrity, or availability of information or systems.

Risk is the likelihood of a threat taking advantage of a vulnerability. A vulnerability is the absence or weakness of a safeguard that could be exploited. An exposure is an instance of exposure to losses from a threat agent.

References

LabSim for Security Pro, Section 1.1.
[All Questions SecPro2017_v6.exm SEC_OVW_07]

Question 8: Correct

Which of the following is an example of a *vulnerability*?

- Virus infection
- Unauthorized access to confidential resources
- A misconfigured server
- Denial of service attack

Explanation

A misconfigured server is a vulnerability. A vulnerability is the absence or weakness of a safeguard that could be exploited, such as a USB port that is enabled on the server hosting the database.
All of the other selections are examples of exposures. An exposure is an instance of exposure to losses from a threat agent.

References

LabSim for Security Pro, Section 1.1.
[All Questions SecPro2017_v6.exm SEC_OVW_08]

Question 9: Correct

By definition, which security concept uses the ability to prove that a sender sent an encrypted message?

- Authentication
- Integrity
- Privacy
- Non-repudiation

Explanation

The ability to prove that a sender sent a message is known as *non-repudiation*. By various mechanisms in different cryptographic solutions, you can prove that only the sender is able to initiate a communication. Therefore, the sender cannot repute that they originated a message.

Integrity is protection against alteration. Authentication is the assignment of access privileges to users. Privacy is the protection and confidentiality of personal information.

References

LabSim for Security Pro, Section 1.1.
[All Questions SecPro2017_v6.exm SEC_OVW_09]

Question 10: Incorrect

Which of the following is not a valid concept to associate with integrity?

- Prevent the unauthorized change of data
- Control access to resources to prevent unwanted access
- Ensure that your systems record the real information when collecting data
- ~~Protect your environment so it maintains the highest source of truth~~

Explanation

To control access to resources and prevent unwanted access is to protect of confidentiality, not integrity.

Integrity concepts include preventing unauthorized change, ensuring that your data is a true reflection of reality (meaning that it recording real information), and maintaining the highest source of truth.

References

LabSim for Security Pro, Section 1.1.
[All Questions SecPro2017_v6.exm SEC_OVW_10]