Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 1/22/2022 6:20:57 pm • Time spent: 02:05

Score: 100% Passing Score: 80%

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?

○ Availability

➡ ● Confidentiality

○ Integrity

○ Non-repudiation

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 it with unauthorized users.

Availability ensures that data is available when it is needed. Copying files to a server that includes malware could threaten the data's availability if the malware deletes or corrupts the data.

Integrity ensures that data is not modified or tampered with.

Non-repudiation provides validation of a message's origin.

Question 2: ✓ Correct

Which of the following BEST describes a cyber terrorist?

○ Downloads and runs attacks available on the internet

○ Exploits internal vulnerabilities to steal information

○ Desires some kind of financial reward or revenge

➡ ● Disrupts network-dependent institutions

EXPLANATION

Cyber terrorists generally use the internet to carry out terrorist activities such as disrupting network-dependent institutions.

Downloading and running attacks available on the internet is usually a script kiddie activity.

Cybercriminals are after some kind of financial reward or revenge.

A spy applies for a job with a commercial competitor and then exploits internal vulnerabilities to steal information.

Question 3: ✓ 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, which protection does the hashing activity provide?

○ Non-repudiation

○ Availability

○ Confidentiality

➡ ● Integrity

EXPLANATION

Hashing of any sort, 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 cleartext.

No form of cryptography provides protection for availability.

▾ Question 4: ✓ 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 user accidentally deletes the new product designs.

○ A server backdoor allows an attacker on the internet to gain access to the intranet site.

○ A water pipe in the server room breaks.

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 through 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.

▾ Question 5: ✓ Correct

Which of the following could an employee also be known as?

- ○ Exploit
- ➡ ● Internal threat
- ○ Script kiddie
- ○ Cybercriminal

EXPLANATION

Employees are also known as internal threats. Employees can be the most overlooked, yet most dangerous, threat agent because they have greater access to information assets than anyone on the outside trying to break in.

An exploit is a procedure or product that takes advantage of a vulnerability to carry out a threat.

Script kiddies download and run attacks available on the internet.

Cybercriminals usually seek to exploit security vulnerabilities for some kind of financial reward or revenge.

▾ Question 6: ✓ Correct

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

- ○ Integrity
- ➡ ● Non-repudiation
- ○ Authentication
- ○ Privacy

EXPLANATION

The ability to prove that a sender undeniably sent a message is known as non-repudiation. By various mechanisms in different cryptographic solutions, you can prove that only the sender would be able to have initiated a certain 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.

Question 7: ✓ Correct

Which of the following includes all hardware and software necessary to secure data, such as firewalls and antivirus software?

○ Policies

○ Assets

➡ ◉ Physical security

○ Users and administrators

EXPLANATION

Physical security includes all hardware and software necessary to secure data, such as firewalls and antivirus software.

Users and administrators are the people who use the software and the people who manage the software, respectively.

Policies are the rules an organization implements to protect information.

An asset is something that has value to a person or organization, such as sensitive information in a database.

Question 8: ✓ Correct

Which of the following are often identified as the three main goals of security? (Select three.)

- □ Employees
- ➡ ☑ Availability
- □ Non-repudiation
- □ Policies
- ➡ ☑ Integrity
- ➡ ☑ Confidentiality
- □ Assets

EXPLANATION

The acronym CIA refers to confidentiality, integrity, and availability in respect to security. These are often identified as the three main goals of any security-oriented task.

Non-repudiation provides validation of a message's origin.

Policies are the rules an organization implements to protect information.

Employees can be the most overlooked, yet most dangerous, threat agent because they have greater access to information assets than anyone on the outside trying to break in.

An asset is something that has value to a person or organization, such as sensitive information in a database.

▼ Question 9: ✓ Correct

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

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

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.

▼ Question 10: ✓ Correct

Which of the following is an example of a vulnerability?

- ○ Denial-of-service attack
- ➡ ◉ Misconfigured server
- ○ Virus infection
- ○ Unauthorized access to confidential resources

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.