Chp 1 NS

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 1/22/2022 7:02:48 pm • Time spent: 02:55

Score: 90% Passing Score: 80%

Question 1: ✔ Correct

Which of the following reduces the risk of a threat agent being able to exploit a vulnerability?

- Manageable network plans
- Countermeasures
- Secure data transmissions
- Implementation of VLANs

EXPLANATION

A countermeasure is a means of mitigating potential risk. Countermeasures reduce the risk of a threat agent being able to exploit a vulnerability. An appropriate countermeasure:

- Must provide a security solution to an identified problem
- Should not depend on secrecy
- Must be testable and verifiable
- Must provide uniform or consistent protection for all assets and users
- Should be independent of other safeguards
- Should require minimal human intervention
- Should be tamper-proof
- Should have overrides and fail-safe defaults

Question 2: ✔ Correct

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

- [ ] Non-repudiation
- [ ] Employees
- [ ] Assets
- [x] Integrity
- [ ] Policies
- [x] Availability
- [x] Confidentiality

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 3: ✔ Correct

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

- Authentication
- Privacy
- Integrity
- ➡ Non-repudiation

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 4: ✔ 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?

- ➡ Confidentiality
- Integrity
- Availability
- 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 5: ✔ Correct

When training your employees on how to identify various attacks, which of the following policies should you be sure to have and enforce? (Select two.)

- [ ] Group policies
- [ ] Usage policies
- [x] Clean desk policies
- [ ] Encryption policies
- [x] Password policies

EXPLANATION

Be sure to have an effective password policy and clean desk policy in place, and don't forget to enforce them. Be sure to train your employees on how to identify all the various attacks that could target them. Train them on how to spot suspicious emails, instant messages, downloads, attachments, and websites.

Encryption policies should protect you in the event you experience a physical security breach. For example, if a hard drive were stolen, the thief wouldn't be able to access the information stored on it.

An Acceptable Use Policy (AUP) determines the rules for using a website or internet service.

You can use Windows group policies to administer your Windows systems.

Question 6: ✔ Correct

Which of the following items would be implemented at the Data layer of the security model?

- (•) Cryptography
- ( ) Authentication
- ( ) Group policies
- ( ) Auditing

EXPLANATION

Cryptography is implemented at the Data layer.

Authentication, authorization, and group policies are implemented at the Application layer.

Auditing is implemented at the Host layer.

Question 7: ✗ Incorrect

You create a new document and save it to a hard drive on a file server on your company's network. Then you employ an encryption tool to encrypt the file using AES. This activity is an example of accomplishing which security goal?

- ~~Integrity~~
- ➡ Confidentiality
- Non-repudiation
- Availability

EXPLANATION

Encrypting a file while it is stored on a hard drive is usually done to provide protection for the object's confidentiality.

Hashing is used to provide integrity. Using mechanisms like backups and avoiding single points of failure provide availability protection. Non-repudiation is usually provided for during a secured communication, not while a file is stored on a hard drive.

Question 8: ✓ Correct

Which of the following is one of the MOST common attacks on employees?

- Password attack
- DNS attack
- ➡ Phishing attack
- Remote attack

EXPLANATION

Phishing attacks are one of the most common attacks directed at employees. In most cases, employees are lured into clicking a link or downloading an attachment from a seemingly legitimate email.

Question 9: ✔ Correct

Which of the following is the single greatest threat to network security?

- Unsecure physical access to network resources
- Email phishing
- Employees
- Weak passwords

EXPLANATION

Employees are the single greatest threat to network security. Therefore, user education is very important.

- Employees need to be aware that they are the primary targets in most attacks.
- Phishing attacks are one of the most common attacks directed toward employees.
- Employees should be able to identify attacks through email, instant messages, downloads, and websites.
- Effective password policies should be enforced, and passwords should not be written down.
- Employees should be able to identify both internal and external threats.
- Employees need to be aware of the company's security policies.

Question 10: ✔ Correct

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

- A server backdoor allows an attacker on the internet to gain access to the intranet site.
- A delivery man is able to walk into a controlled area and steal a laptop.
- A water pipe in the server room breaks.
- 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 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 11: ✔ 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?

- Availability
- ➡ Integrity
- Confidentiality
- Non-repudiation

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 12: ✔ Correct

Which of the following items would be implemented at the Network layer of the security model?

- Network plans
- Firewalls using ACLs
- Wireless networks
- ➡ Penetration testing

EXPLANATION

The installation and configuration of switches and routers, the implementation of VLANs, penetration testing, and virtualization are implemented at the Network layer.

Firewalls with ACLs and wireless networks are secured in the Perimeter layer.

Network plans are implemented at the Policies, Procedures, and Awareness layer.

Question 13: ✕ Incorrect

The Application layer of the security model includes which of the following? (Select two.)

- ➡ ☐ User management
- ☐ Log management
- ☐ Environmental controls
- ☑ ~~User education~~
- ➡ ☑ Web application security

EXPLANATION

The Application layer includes user management and web application security.

The Policies, Procedures, and Awareness layer includes user education.

The Physical layer includes environmental controls.

The Host layer includes log management.

Question 14: ✓ Correct

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

- ➡ ◉ Physical security
- ○ Assets
- ○ Users and administrators
- ○ Policies

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 15: ✔ Correct

Which of the following BEST describes a cyber terrorist?

- Desires some kind of financial reward or revenge
- Exploits internal vulnerabilities to steal information
- Downloads and runs attacks available on the internet
- ➡ 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 16: ✔ Correct

Which of the following is a security approach that combines multiple security controls and defenses?

- Cumulative security
- Countermeasure security
- Network security
- Perimeter security
- ➡ Layered security

EXPLANATION

Layered security, sometimes called defense in depth security, is a security approach that combines multiple security controls and defenses to create a cumulative effect.

Perimeter security includes firewalls with ACLs and a wireless network. Network security includes the installation and configuration of switches and routers, the implementation of VLANs, penetration testing, and the utilization of virtualization. A countermeasure is a means of mitigating a potential risk. Countermeasures reduce the risk of a threat agent exploiting a vulnerability.

Question 17: ✔ Correct

Which of the following items would you secure in the Perimeter layer of the security model?

- ➡ Firewalls
- Routers
- VLANs
- Switches

EXPLANATION

Firewalls using ACLs are secured in the Perimeter layer.

Switches, routers, and VLANs are secured in the Network layer.

Question 18: ✔ Correct

Which of the following is an example of a vulnerability?

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

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.

Question 19: ✔ Correct

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

- Script kiddie
- ➡ Internal threat
- Cybercriminal
- Exploit

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 20: ✔ Correct

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

- The likelihood of an attack taking advantage of a vulnerability
- Instance of exposure to losses from an attacker
- ➡ Any potential danger to the confidentiality, integrity, or availability of information or systems
- 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.