Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 1/22/2022 6:32:42 pm • Time spent: 03:32

Score: 100%

Passing Score: 80%

Question 1: ✓ Correct

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

- □ Log management
- ➡ ☑ User management
- □ User education
- □ Environmental controls
- ➡ ☑ 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 2: ✓ 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.)

- □ Usage policies
- □ Encryption policies
- ➡ ☑ Clean desk policies
- ➡ ☑ Password policies
- □ Group 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 3: ✓ Correct

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

➡ ● Countermeasures

○ Manageable network plans

○ 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 4: ✓ Correct

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

○ Auditing

○ Authentication

○ Group policies

➡ ● Cryptography

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 5:** ✓ Correct

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

➡ ● Firewalls

○ VLANs

○ Routers

○ Switches

EXPLANATION

Firewalls using ACLs are secured in the Perimeter layer.

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

▾ **Question 6:** ✓ Correct

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

○ Email phishing

○ Unsecure physical access to network resources

➡ ● 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 7: ✓ Correct

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

- ○ Perimeter security
- ➡ ● Layered security
- ○ Cumulative security
- ○ Network security
- ○ Countermeasure 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 8: ✓ 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 9: ✓ Correct

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

○ Password attack

○ Remote attack

➡ ● Phishing attack

○ DNS 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 10: ✓ Correct

The Policies, Procedures, and Awareness layer of the security model includes which of the following? (Select two.)

□ Environmental controls

□ Server cages

➡ ☑ User education

➡ ☑ Employee onboarding

□ Motion detectors

EXPLANATION

User education and employee onboarding and off-boarding procedures are included in the Policies, Procedures, and Awareness layer.

The Physical layer deals with server cages, motion detectors, and environmental controls.