Congratulations! You passed!

Grade received 100%
Latest Submission Grade 100%
To pass 80% or higher

Retake the assignment in **23h 56m**

Go to next item

Weekly challenge 4

Quiz • 50 min

Review Learning Objectives

1. What are the purposes of performing a patch update for security hardening? Select all that apply. **1 / 1 point**

Fixing known security vulnerabilities in a network or services.

Submit your assignment **Try again**

Due Jul 2, 11:59 PM +08 **Attempts** 3 every 24 hours

Correct

Retake the quiz in **23h 56m**

Preventing malicious actors from flooding a network.
Requiring a user to verify their identity to access a system or network.
Upgrading an operating system to the latest software version.

Receive grade

To Pass 80% or higher

Your grade 100%

View Feedback

We keep your highest score

Correct

Like **Dislike** **Report an issue**

2. What is the term for all the potential system vulnerabilities that a threat actor could exploit? **1 / 1 point**

- Security architecture
- Security challenge
- Attack surface
- Risk

Correct

3. Fill in the blank: Hiring a security guard is an example of a _____ security hardening practice. **1 / 1 point**

- network-focused
- virtual
- physical
- software-based

Correct

4. To help improve the security of a business, its in-house security team is approved to simulate an attack that will identify vulnerabilities in business processes. What does this scenario describe? **1 / 1 point**

- The Ping of Death
- A Distributed Denial of Service (DDoS) attack
- Packet sniffing
- Penetration testing

Correct

5. Which of the following statements accurately describe OS hardening tasks? Select three answers. **1 / 1 point**

Multi-factor authentication is a security measure requiring users to change passwords every month.
When disposing of software, it is a best practice to delete any unused applications.

Correct

Some OS hardening tasks are performed at regular intervals, while others are performed only once.

Correct

OS hardening is a set of procedures that maintain and improve OS security.

Correct

6. A security analyst reviews documentation about a firewall rule that includes a list of allowed and disallowed network ports. They compare it to the current firewall to ensure no changes have been made. What does this scenario describe? **1 / 1 point**

- Checking baseline configuration
- Responsibly managing applications
- Upgrading the interface between computer hardware and the user
- Verifying user identity when accessing an OS

Correct

7. Fill in the blank: The security measure multi-factor authentication (MFA) requires a user to verify their identity _____ before accessing a system or network. **1 / 1 point**

- at least once
- within 60 seconds
- in two or more ways
- every day

Correct

8. In what way might port filtering be used to protect a network from an attack? **1 / 1 point**

- To create isolated subnets for different departments in an organization
- To increase the attack surface in a network
- To inspect, analyze, and react to security events based on their priority
- To disable unused ports in order to reduce the attack surface

Correct

9. A security team considers the best way to handle the different security zones within their network. They prioritize protecting the restricted zone by separating from the rest of the network and ensuring it has much higher encryption standards. What does this scenario describe? **1 / 1 point**

- Network segmentation
- Patch updating
- Cloud hardening
- Penetration testing

Correct

10. How can a security professional confirm that no unverified changes have occurred within a cloud server? **1 / 1 point**

- Perform a penetration test
- Compare the server baseline image to the data in cloud servers
- Use port filtering to block or allow certain updates
- Establish multifactor authentication (MFA)

Correct