Introduction to security hardening
OS hardening
Network hardening
Cloud hardening
Review: Security hardening
Video: Wrap-up
58 sec
Reading: Glossary terms from week 4
10 min
Quiz: Weekly challenge 4
10 questions
Quiz: Portfolio Activity: Use the NIST Cybersecurity Framework to respond to a security incident
6 questions
Reading: Portfolio Activity Exemplar: Use the NIST Cybersecurity Framework to respond to a security incident
10 min
Congratulations on completing Course 3!

Congratulations! You passed!

Grade received 92.50%

Weekly challenge 4

Latest Submission Grade 92.50%

To pass 80% or higher

Quiz • 50 min

Go to next item

Review Learning Objectives

1. What are the purposes of performing a patch update for security hardening? Select all that apply. **0.5 / 1 point**

Fixing known security vulnerabilities in a network or services.

Correct

Upgrading an operating system to the latest software version.

Correct

Requiring a user to verify their identity to access a system or network.

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

This should not be selected
Please review the video about security hardening.

Preventing malicious actors from flooding a network.

This should not be selected
Please review the video about security hardening.

Submit your assignment **Try again**

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

Receive grade **Your grade** 92.50% **View Feedback**

To Pass 80% or higher

We keep your highest score

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

- Security challenge
- Risk
- Attack surface
- Security architecture

Correct

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

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

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

Correct

5. What are some methods for hardening operating systems? Select three answers. **0.75 / 1 point**

Keeping an up-to-date list of authorized users.

Correct

Implementing an intrusion detection system (IDS)

This should not be selected
Please review the video about security hardening.

Removing unused software to limit unnecessary vulnerabilities

Correct

Configuring a device setting to fit a secure encryption standard

Correct

6. A security analyst notices something unusual affecting their company's OS. To confirm that no changes have been made to the system, the analyst compares the current configuration to existing documentation about the OS. What does this scenario describe? **1 / 1 point**

- Responsibly managing applications
- Checking baseline configuration
- 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 _____ requires a user to verify their identity in two or more ways to access a system or network. **1 / 1 point**

- password policy
- network log analysis
- baseline configuration
- multifactor authentication (MFA)

Correct

8. Which of the following statements accurately describes port filtering? **1 / 1 point**

- A security protocol that provides an encrypted tunnel for issuing commands from a remote server
- A process performed by a VPN service that protects data by wrapping it in other data packets
- A security technique that divides a network into segments
- A firewall function that blocks or allows certain port numbers in order to limit unwanted network traffic

Correct

9. A security team works to ensure that an issue in one area of the business does not spread to others and create more problems. They design subnets for each department, such as one for research and another for finance. What does this scenario describe? **1 / 1 point**

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

Correct

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

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

Correct