Try again once you are ready

Grade received 72.50%
Latest Submission Grade 72.50%
To pass 80% or higher

Try again

Weekly challenge 3

Quiz • 50 min

Review Learning Objectives

Submit your assignment
Due Jun 25, 11:59 PM +08 **Attempts** 3 every 8 hours

Receive grade
To Pass 80% or higher

Your grade
72.50%

View Feedback
We keep your highest score

Try again

1. An application has broken access controls that fail to restrict any user from creating new accounts. This allows anyone to add new accounts with full admin privileges. **1 / 1 point**

The application's broken access controls are an example of what?

- A security control
- (●) A vulnerability
- An exploit
- A threat

Correct

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

2. Why do organizations use the defense in depth model to protect information? Select two answers. **0.5 / 1 point**

- [x] Security teams can easily determine the "who, what, when, and how" of an attack.

This should not be selected
Please review the video on defense in depth.

- [x] Layered defenses reduce risk by addressing multiple vulnerabilities.

Correct

- [x] Threats that penetrate one level can be contained in another.

Correct

- [x] Each layer uses unique technologies that communicate with each other.

This should not be selected
Please review the video on defense in depth.

3. Which layer of the defense in depth model is a user authentication layer that can include usernames and passwords? **0 / 1 point**

- (●) Application
- Endpoint
- Network
- Perimeter

Incorrect
Please review the video about the controls used in defense in depth.

4. Fill in the blank: According to the CVE® list, a vulnerability with a score of _____ or above is considered to be a critical risk to company assets that should be addressed right away. **1 / 1 point**

- 11
- (●) 9
- 1
- 4

Correct

5. What is the purpose of vulnerability management? Select three answers. **0.75 / 1 point**

- [x] To review an organization's internal security systems

Correct

- [x] To identify exposures to internal and external threats

Correct

- [x] To uncover vulnerabilities and reduce their exploitation

Correct

- [x] To track assets and the risks that affect them

This should not be selected
Please review the video about vulnerability management.

6. A security team is conducting a periodic vulnerability assessment on their security procedures. Their objective is to review gaps in their current procedures that could lead to a data breach. After identifying and analyzing current procedures, the team conducts a risk assessment. **1 / 1 point**

What is the purpose of performing a risk assessment?

- To simulate attacks that could be performed against each vulnerability
- To adjust current security procedures
- To fix vulnerabilities that have been identified
- (●) To score vulnerabilities based on their severity and impact

Correct

7. Which of the following are types of attack surfaces? Select three answers. **0.75 / 1 point**

- [x] Malicious software

This should not be selected
Please review the video about attack surfaces.

- [x] Computer workstations

Correct

- [x] Cloud servers

Correct

- [x] Network routers

Correct

8. A project manager at a utility company receives a suspicious email that contains a file attachment. They open the attachment and it installs malicious software on their laptop. **0.5 / 1 point**

What are the attack vectors used in this situation? Select two answers.

- [x] The malicious software

This should not be selected
Please review the video about identifying attack vectors.

- [x] The infected workstation

This should not be selected
Please review the video about identifying attack vectors.

- [x] The suspicious email

Correct

- [x] The file attachment

Correct

9. A security team is performing a vulnerability assessment on a banking app that is about to be released. Their objective is to identify the tools and methods that an attacker might use. **0.75 / 1 point**

Which steps of an attacker mindset should the team perform to figure this out? Select three answers.

- [x] Determine how the target can be accessed.

Correct

- [x] Evaluate attack vectors that can be exploited.

Correct

- [x] Identify a target.

Correct

- [x] Consider potential threat actors.

This should not be selected
Please review the video about an attacker mindset.

10. What are ways to protect an organization from common attack vectors? Select three answers. **0.75 / 1 point**

- [x] By not practicing an attacker mindset

This should not be selected
Please review the video about defending attack vectors.

- [x] By keeping software and systems updated

Correct

- [x] By educating employees about security vulnerabilities

Correct

- [x] By implementing effective password policies

Correct