## Congratulations! You passed!

Grade received 90%

Latest Submission Grade 90%

To pass 80% or higher

Go to next item

# Weekly challenge 3

Quiz • 50 min

Review Learning Objectives

Submit your assignment

Due Jun 25, 11:59 PM +08 Attempts 3 every 8 hours

Try again

Receive grade

To Pass 80% or higher

Your grade 90%

View Feedback

We keep your highest score

**1.** Consider the following scenario:

A cloud service provider has misconfigured a cloud drive. They've forgotten to change the default sharing permissions. This allows all of their customers to access any data that is stored on the drive.

This misconfigured cloud drive is an example of what?

1 / 1 point

- ○ A security control
- ○ A threat
- ○ An exploit
- ◉ A vulnerability

Correct

Like Dislike Report an issue

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

1 / 1 point

- ☑ Layered defenses reduce risk by addressing multiple vulnerabilities.

  Correct
- ☑ Threats that penetrate one level can be contained in another.

  Correct
- ☐ Security teams can easily determine the “who, what, when, and how” of an attack.
- ☐ Each layer uses unique technologies that communicate with each other.

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

0 / 1 point

- ○ Application
- ○ Network
- ○ Perimeter
- ◉ Endpoint

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
- ○ 4
- ◉ 9
- ○ 1

Correct

**5.** What is the purpose of vulnerability management? Select three answers.

1 / 1 point

- ☑ To uncover vulnerabilities and reduce their exploitation

  Correct
- ☑ To review an organization's internal security systems

  Correct
- ☑ To identify exposures to internal and external threats

  Correct
- ☐ To track assets and the risks that affect them

**6.** What are some of the goals of performing vulnerability assessments? Select two answers.

1 / 1 point

- ☑ To identify weaknesses and prevent attacks

  Correct
- ☐ To pass remediation responsibilities over to the IT department
- ☐ To catalog assets that need to be protected
- ☑ To perform an audit that measures regulatory compliance

  Correct

**7.** What are the two types of attack surfaces that security professionals defend? Select two answers.

1 / 1 point

- ☑ Physical

  Correct
- ☐ Brand reputation
- ☑ Digital

  Correct
- ☐ Intellectual property

**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.

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

1 / 1 point

- ☑ The file attachment

  Correct
- ☐ The malicious software
- ☐ The infected workstation
- ☑ The suspicious email

  Correct

**9.** What phase comes after identifying a target when practicing an attacker mindset?

1 / 1 point

- ○ Prepare defenses against threats.
- ○ Find the tools and methods of attack.
- ◉ Determine how the target can be accessed.
- ○ Evaluate the target's attack vectors.

Correct

**10.** What is *not* a step of practicing an attacker mindset?

1 / 1 point

- ◉ Identify ways to fix existing vulnerabilities.
- ○ Evaluate attack vectors that can be exploited.
- ○ Find the tools and methods of attack.
- ○ Determine how a target can be accessed.

Correct