Congratulations! You passed!

Grade received 80%
Latest Submission Grade 80%
To pass 80% or higher
Go to next item

Weekly challenge 4

Quiz • 50 min

Review Learning Objectives

1. Which of the following could be examples of social engineering attacks? Select three answers. **0.75 / 1 point**

Submit your assignment
Try again
Due Jul 2, 11:59 PM +08
Attempts 3 every 24 hours

- [x] A pop-up advertisement promising a large cash reward in return for sensitive information
  - Correct
- [x] A lost record of important customer information
  - Receive grade
  - This should not be selected
    Please review the video on social engineering.
- [x] An unfamiliar employee asking you to hold the door open to a restricted area
  - Correct
- [x] An email urgently asking you to send money to help a friend who is stuck in a foreign country
  - Correct

Your grade 80%
To Pass 80% or higher
View Feedback
We keep your highest score
Like
Dislike
Report an issue

2. What is the main difference between a vishing attack and a smishing attack? **1 / 1 point**

- (•) Vishing makes use of voice calls to trick targets.
- ( ) Vishing is used to target executives at an organization.
- ( ) Vishing exploits social media posts to identify targets.
- ( ) Vishing involves a widespread email campaign to steal information.

Correct

3. A digital artist receives a free version of professional editing software online that has been infected with malware. After installing the program, their computer begins to freeze and crash repeatedly. **1 / 1 point**

The malware hidden in this editing software is an example of which type of malware?

- ( ) scareware
- ( ) spyware
- ( ) adware
- (•) trojan

Correct

4. Which type of malware requires the user to make a payment to the attacker to regain access to their device? **1 / 1 point**

- ( ) Spyware
- (•) Ransomware
- ( ) Cryptojacking
- ( ) Botnets

Correct

5. Fill in the blank: Cryptojacking is a type of malware that uses someone's device to _____ cryptocurrencies. **1 / 1 point**

- ( ) earn
- ( ) collect
- (•) mine
- ( ) invest

Correct

6. Security researchers inserted malicious code into the web-applications of various organizations. This allowed them to obtain the personally identifiable information (PII) of various users across multiple databases. **1 / 1 point**

What type of attack did the researchers perform?

- ( ) Ransomware
- (•) Injection
- ( ) Malware
- ( ) Social engineering

Correct

7. An attacker sends a malicious link to subscribers of a sports news site. If someone clicks the link, a malicious script is sent to the site's server and activated during the server's response. **1 / 1 point**

This is an example of what type of injection attack?

- (•) Reflected
- ( ) DOM-based
- ( ) SQL injection
- ( ) Stored

Correct

8. Which of the following are areas of a website that are vulnerable to SQL injection? Select two answers. **0.5 / 1 point**

- [x] User login pages
  - Correct
- [x] Pop-up advertisements
  - This should not be selected
    Please review the video about SQL injection attacks.
- [x] Social media feeds
  - This should not be selected
    Please review the video about SQL injection attacks.
- [x] Credit card payment forms
  - Correct

9. What are some key benefits of the threat modeling process? Select all that apply. **0.75 / 1 point**

- [x] Remediate all vulnerabilities
  - This should not be selected
    Please review the video about threat modeling.
- [x] Reduce an attack surface
  - Correct
- [x] Help prioritize threats
  - Correct
- [x] Identify points of failure
  - Correct

10. Which stage of the PASTA framework is related to identifying the application components that must be evaluated? **0 / 1 point**

- ( ) Perform a vulnerability analysis
- ( ) Conduct attack modeling
- ( ) Define the technical scope
- (•) Decompose the application

Incorrect
Please review the video about PASTA threat modeling.