

CONFIDENTIAL



UTHM

Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

**FINAL EXAMINATION
SEMESTER II
SESSION 2021/2022**

COURSE NAME : FUNDAMENTALS OF INFORMATION SECURITY

COURSE CODE : BIS 10103

PROGRAMME CODE : BIS

EXAMINATION DATE : JULY 2022

DURATION : 3 HOURS

INSTRUCTION :

1. ANSWER ALL QUESTIONS
2. THIS FINAL EXAMINATION IS CONDUCTED VIA **CLOSED BOOK**.
3. STUDENTS ARE **PROHIBITED** TO CONSULT THEIR OWN MATERIAL OR ANY EXTERNAL RESOURCES DURING THE EXAMINATION CONDUCTED VIA CLOSED BOOK.

THIS QUESTION PAPER CONSISTS OF SEVEN (7) PAGES

CONFIDENTIAL

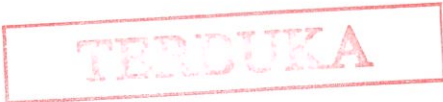
TERBUKA

SECTION A

Choose the **BEST** answer for each of the following questions.

- Q1** Which of the following is a way of a virus infects a device?
- A. Listening online to music.
 - B. An attachment in an email.
 - C. Streaming video or music.
 - D. None of above.
- Q2** What is the common things of a phishing email?
- A. Spelling errors.
 - B. Images in them.
 - C. Symbols that they want you to click on.
 - D. No spelling errors.
- Q3** The image obtained after steganography is called as _____.
- A. stego image
 - B. cover image
 - C. output image
 - D. last image
- Q4** Which of the following statement is **TRUE** about steganography and watermarking?
- A. Steganography is not an information hiding technique.
 - B. Watermarking is not an information hiding technique.
 - C. Both techniques belong to information hiding domain.
 - D. None of the above.

- Q5** When you choose credit/debit card as a payment method, what information is requested at the beginning?
- A. CCV number.
 - B. PIN number.
 - C. Date of birth.
 - D. All of the above.
- Q6** _____ forwards the transaction detail to their payment gateway.
- A. Customer's browser
 - B. Merchant's browser
 - C. Merchant's Server
 - D. None of the above
- Q7** A(n) _____ is a user who has administrative responsibility for part or all of the database.
- A. end user other than application owner
 - B. application owner
 - C. database relations manager
 - D. administrator
- Q8** Network security is extremely important in a facility in which such a large collection of assets is concentrated in a _____ place and accessible by _____ network connections.
- A. multiple, external
 - B. single, external
 - C. single, internal
 - D. multiple, internal

A red rectangular stamp with the word "TERBUKA" written in capital letters inside.

- Q9** The success of cybercriminals and the relative failure of law enforcement influence _____.
- A. cyber detectives
 - B. cybercrime acts
 - C. cybercrime victims
 - D. cyber thieves
- Q10** Which of the following is not considered as unethical?
- A. Using an idea in a journal and citing the source.
 - B. Using software that a friend purchased for your personal use.
 - C. Pretending to be a college student in a chat room.
 - D. Posting fake information about a lecturer.

(20 marks)

SECTION B

State **TRUE** or **FALSE** for each of the following statements.

- Q11** A bot spreads and activates itself, whereas a worm is initially controlled from a central location.
- Q12** Programmers use backdoors to debug and test programs.
- Q13** Term for concealing sensitive data inside of another file is called as watermarking.
- Q14** Masking is a technology that protects software from unauthorized modification.
- Q15** The communication by gateway is always in the form of computer codes.

TERBUKA

- Q16** Using anti-skimming device is an effective way to prevent card skimming.
- Q17** Malware can exploit vulnerabilities and cause damage to database.
- Q18** In database security, encryption becomes the final line of protection.
- Q19** To acknowledge, or give credit to, the person who actually created the content you're using can be called ascopyright.
- Q20** It is ethical to use peoples' computer resources with authorization or proper compensation.
- (10 marks)

SECTION C

- Q21** Assume you have found a USB memory stick in FSKTM's parking area.

Based on the given scenario, answer the following questions.

- (a) Explain **TWO (2)** threats to your computer if you just plug in the memory stick and examine its contents.
- (5 marks)
- (b) Suggest **TWO (2)** steps that can be taken to mitigate these threats in order to safely determine the contents of the memory stick.
- (5 marks)

TERBUKA

Q22 (a) Explain **TWO (2)** differences between steganography and cryptography. (4 marks)

(b) Discuss how malicious hackers use steganography in social media. (3 marks)

(c) Discuss **ONE (1)** technique to detect steganography. (3 marks)

Q23 Define each of the following terms.

(a) Ciphertext. (2 marks)

(b) Authentication. (2 marks)

(c) Non-repudiation. (2 marks)

(d) Inside attack. (2 marks)

(e) Vulnerability. (2 marks)

Q24 (a) Define a drive-by-download. (2 marks)

(b) Describe **FOUR (4)** malware countermeasures. (8 marks)

TERBUKA

- (c) Assuming that you receive an e-mail containing official logo of your bank with the following contents:

"Dear Customer. Our records show that your Internet Banking access has been blocked due to too many login attempts with invalid information such as incorrect access number, password and identification card number. We urge you to restore your account access immediately and avoid permanent closure of your account, by clicking on this [link to restore your account](#). Thank you from your banking customer service team."

- (i) State the form of attack this e-mail is attempting. (2 marks)
- (ii) Explain the most likely mechanism used to distribute this email. (4 marks)
- (iii) How should you respond to such emails? (4 marks)

- Q25** (a) List **FIVE (5)** acts related to Malaysian Cyber Laws. (5 marks)
- (b) Explain **THREE (3)** classifications of computer crime based on the role that the computer plays in the criminal activity. Include **ONE (1)** example of the criminal activity in each of classification. (15 marks)

- END OF QUESTIONS -

TERBUKA