UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2022/2023

COURSE NAME	:	INFORMATION SECURITY FUNDAMENTALS
COURSE CODE	:	BIS 10103
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	JULY / AUGUST 2023
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.

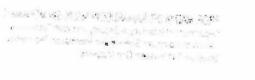THIS QUESTION PAPER CONSISTS OF **SEVEN (7)** PAGES

TERBUKA

SECTION A

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

Q1   When the original cover-object and stego-object are both available, this attack is known as _____.

A.   known message attack
B.   known cover attack
C.   known stego attack
D.   chosen stego attack

(2 marks)

Q2   A virus software can do dynamic analysis which means _____.

A.   it checks the virus codes without trying to execute it
B.   it checks the the virus codes by running it inside a sandbox
C.   it checks binary code to understand if it is an executable
D.   none of the above

(2 marks)

Q3   The image used for steganography is called _____.

A.   stego image
B.   cover image
C.   output image
D.   last image

(2 marks)

Q4   Some documents need to be opened with correct password, denying access to unauthorized users. This action supports _____.

A.   integrity
B.   availability
C.   recovery
D.   confidentiality

(2 marks)

TERBUKA

Q5 _____ is an example of a passive attack.

     A.   Man-in-the-middle (MITM)
     B.   Replay attack
     C.   Data sniffing
     D.   Distributed Denial of Service (DDoS)

                                                    (2 marks)

Q6 In Information Security, _____ is much preferred.

     A.   detection
     B.   prevention
     C.   recovery
     D.   discovery

                                                    (2 marks)

Q7 A database can be protected from inference attack **EXCEPT** using _____.

     A.   cell suppression
     B.   generalization
     C.   noise addition
     D.   table deletion

                                                    (2 marks)

Q8 Electronic online payment system security goals includes the following **EXCEPT** _____.

     A.   integrity
     B.   privacy
     C.   availability
     D.   accountability

                                                    (2 marks)

Q9 Electronic Payment Schemes includes the following **EXCEPT** _____.

     A.   customer
     B.   merchant
     C.   bank
     D.   system

                                                    (2 marks)

Q10 Which of the following is considered as ethical?

    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.

(2 marks)

SECTION B

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

Q11   A worm spreads and activates itself, whereas a bot is controlled from a central location.

(1 mark)

Q12   A popular application of watermarking techniques is to provide a proof of ownership of digital data by embedding hidden message in video or image digital products.

(1 mark)

Q13   Leakage of data from Universal Serial Bus (USB) pendrive can be avoided using TrueCrypt.

(1 mark)

Q14   Bitlocker can be used to encrypt NTFS volume of Windows operating system (OS) only.

(1 mark)

Q15   Recovery is one of the goal of information security.

(1 mark)

Q16   Gait recognition cannot be used for biometrics.

(1 mark)

Q17   Trojan horse can self-replicate.

(1 mark)

Q18   Computer virus needs human assistance to propagate.

(1 mark)

Q19 Malware can turn a computer into a zombie, which is a machine that is controlled externally to perform malicious attacks, usually as a part of a botnet.

(1 mark)

Q20 Digital rights management (DRM) is the management of legal access to digital content using various tools to restrict the use of copyrighted and open-source works.

(1 mark)

TERBUKA

SECTION C

Q21 (a)   Explain the Chinese wall access control model.

(5 marks)

(b)   Explain the file permission granted to user, group and others using `chmod 761 file.txt` command in Linux.

(5 marks)

(c)   Explain the term Identity Federation.

(5 marks)

Q22 Discuss on how brute-force birthday attack is used to find collision for a hash `function h`. Justify your answer.

(10 marks)

Q23 Compare Symmetric Key Cryptography and Public Key Cryptography by using **Table Q23**. Justify your answer.

Table Q23

	Symmetric Key Cryptography	Public Key Cryptography
Key used in encryption and decryption		
Key distribution		

(10 marks)

Q24 Discuss on how a database uses two-phase commit protocol to cope with consistency and reliability issues when performing updates.

(15 marks)

- END OF QUESTIONS -

TERBUKA