UNIVERSITI TEKNOLOGI MARA
FINAL EXAMINATION

COURSE	**:**	**COMPUTER SECURITY**
COURSE CODE	**:**	**CSC662**
EXAMINATION	**:**	**JULY 2023**
TIME	**:**	**3 HOURS**

INSTRUCTIONS TO CANDIDATES

1. This question paper consists of two (2) part: PART A (10 Question)
   PART B (2 Question)

2. Answer ALL questions in the Answer Booklet. Start each answer on a new page.

3. Do not bring any material into the examination room unless permission is given by the invigilator.

4. Please check to make sure that this examination pack consists of:

   i) the Question Paper
   ii) an Answer Booklet – provided by the Faculty

5. Answer ALL questions in English.

DO NOT TURN THIS PAGE UNTIL YOU ARE TOLD TO DO SO

This examination paper consists of 5 printed pages

PART A

Answer ALL questions

QUESTION 1

Security Identifiers (SID), access tokens, and access control entries are the building blocks to implementing access control mechanisms in Windows operating system.

a) What is an access token?

(2 marks)

b) Using these terminologies, explain how Windows operating system implements its access control.

(6 marks)

QUESTION 2

One of the two most critical lines of defense that Linux networks and systems rely on is authentication.

a) Where does Linux keep its passwords?

(2 marks)

b) Modern Linux operating systems use 'salt' in managing passwords. Explain,

i. What is 'salt'?
ii. Its advantage and disadvantages.

(6 marks)

QUESTION 3

Cross-site scripting (XSS) is a security vulnerability that is more prevalent in web applications. The Open Web Application Security Project® (OWASP) Top Ten document even lists XSS flaws as one of the critical threats to web application security.

a) What is XSS attack?

(2 marks)

b) Describe **THREE(3)** strategies can be taken by end user to minimize this attack.

(6 marks)

QUESTION 4

Generally, digital watermarking uses two techniques to secure digital objects. These techniques are spatial and frequency domain analysis.

a) What is the purpose of these techniques?

(2 marks)

b) Explain **THREE (3)** characteristics these techniques must possess to secure digital objects.

(6 marks)

QUESTION 5

The Secure Sockets Layer (SSL) and Transport Layer Security (TLS) provide network security at the Transport Layer of TCP/IP.

a) What is the protocol used to securing the Transport Layer of TCP/IP?

(2 marks)

b) Differentiate SSL and TLS in terms of security level.

(6 marks)

QUESTION 6

An Intrusion Detection System (IDS) is a network security component to detect vulnerabilities against a target application or computer system. The detection results can be categorized as true positive, true negative, false positive, and false negative.

a) Why we are more concerned about the false negative detection results?

(2 marks)

b) Explain **THREE (3)** remedy actions that can be taken to resolve the above issue.

(6 marks)

QUESTION 7

Physiological and behavioral biometrics are the classification of biometrics.

a) State **TWO (2)** examples of behavioral biometrics.

(2 marks)

b) Explain with example **TWO (2)** behavioral biometrics usage in securing the system.

(6 marks)

QUESTION 8

a) What is Next Generation Secure Computing Base (NGSCB) ?

(2 marks)

b) List and explain the two primary system components of Next Generation Secure Computing Base(NGSCB).

(6 marks)

QUESTION 9

a) One of the common ethical issues is Software Piracy. What is Software Piracy?

(2 marks)

b) Describe **THREE** examples of inappropriate sharing of information among organization and employees.

(6 marks)

QUESTION 10

Blockchain technology uses highly sophisticated algorithms (smart contracts) to speed up processes and increase efficiency in business processes.

a) List **TWO (2)** Blockchain applications.

(2 marks)

b) Discuss from computer security perspective, **THREE (3)** benefits of using Blockchain technology with these applications.

(6 marks)

PART B

Answer ALL questions

QUESTION 1

One of the main criteria in operating systems development is security and protection.

a) Using **ONE (1)** example, explain what security in operating systems is.

(5 marks)

b) Using **ONE (1)** example, explain what protection in operating systems is.

(5 marks)

QUESTION 2

For the two real-life scenarios below, you need to determine whether there is an ethical element or not. Provides **ONE (1)** reason to justify your answer.

If your answer is yes, explain **ONE (1)** method to improve the security of the action. If your answer is no, describe how to make it an ethical scenario.

a) A student has conducted a penetration test on the i-Student Portal and reported the findings to the system administrator.

(5 marks)

b) The academic computing department implements a printing quota for every student. Therefore, the students must log into the system before using the printing service. Sometimes students complain that their printing quota is empty, although they hardly use the service.

(5 marks)

END OF QUESTION PAPER