UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER I
SESSION 2014/2015

COURSE NAME	:	CORPORATE SECURITY ENGINEERING
COURSE CODE	:	BIS 33103
PROGRAMME	:	3 BIS
EXAMINATION DATE	:	DECEMBER 2014/ JANUARY 2015
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER **ALL** QUESTIONS

THIS QUESTION PAPER CONSISTS OF **FOUR (4)** PAGES

Q1 (a) Explain the concept of **security engineering**.

(3 marks)

(b) Suggest a scenario that will achieve the following security objectives.

(i) Confidentiality

(4 marks)

(ii) Availability

(4 marks)

(iii) Integrity

(4 marks)

(c) Company Solution has four main systems for daily operation; OS, Accounting Program, Accounting data, Insurance Data and Payroll data. Rina, Ali and Amin have different roles in the company. The management has provide access to each of them according to their roles. Rina is the IT staff and has full access (read (r), write (w) and execute (x) to OS and accounting program. She can only read the accounting data but can both read write to insurance data and payroll data. Ali can read and execute the OS and accounting program and can only read accounting data but does not has access to insurance data and payroll Data. Amin can execute and read the OS and accounting program, read the accounting data but can both read and write to payroll data and insurance data.

(i) Draw the Access Control Matrix for Rina, Ali and Amin.

(8 marks)

(ii) Ali want to add a module of new accounting calculation to the accounting program. By considering the Access Control Matrix, who should Ali consult?

(2 marks)

Q2 (a) Copyright is an issue in the past and present. Compare the copyright implementation in the past (before the Internet) and the present.

(6 marks)

(b) Music Inc. are preparing to launch new songs for a new artist. The songs are planned to be uploaded online. The management worried of the copyright issue.

   (i) State **TWO (2)** methods to properly do the copyright for digital material on the Internet.

   (3 marks)

   (ii) Compare the two methods that have stated in **Q2(b)(i).**

   (6 marks)

(c) Company Dzen is a new company in Kedah. The management plan to draft new security policies for the company. You are asked by the manager to take the responsibilities.

   (i) Differentiate between a corporate security policy and a major security policy.

   (4 marks)

   (ii) Provide **THREE (3)** major security policies required for the company

   (6 marks)

Q3 (a) Differentiate between the concept of **defense in depth** and **weakest-link**.

   (4 marks)

(b) The management of Company Hacko consult you to plan the technical security for the company.

   (i) Outline **FOUR (4)** classes of technical countermeasures used by most companies to defend from the threats.

   (8 marks)

   (ii) Determine the countermeasures for each class as mentioned in **Q3 (b)(i).**

   (4 marks)

(c) Compare **THREE (3)** password cracking techniques with an example.

   (9 marks)

Q4   (a)   You are a network administrator for Company ABC. The company has been attacked by the DDoS attack. Due to this, the company has lost RM5 millions. To prevent future lost, you have been asked to come out with relevance security goals. Each goal exists for a reason.

(i)   Outline **FOUR (4)** goals for creating secure network.

(8 marks)

(ii)   Justify the need of each goal in securing the network using an example.

(12 marks)

(b)   Compare between **Bell La Padula Model** and **Information-flow Model**.

(5 marks)

- END OF QUESTION -