Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2016/2017

COURSE NAME	:	SPECIAL TOPICS IN INFORMATION SECURITY
COURSE CODE	:	BIS 33403
PROGRAMME CODE	:	3 BIS
EXAMINATION DATE	:	JUNE 2017
DURATION	:	2 HOURS 30 MINUTES
INSTRUCTION	:	ANSWER **ALL** QUESTIONS

THIS QUESTION PAPER CONSISTS OF **THREE (3)** PAGES

Q1 (a) Describe avalanche effect in cryptography.

(5 marks)

(b) (i) Give **ONE (1)** example of Internet of Things application.

(1 mark)

(ii) Discuss **THREE (3)** information security challenges posed by **Q1(b)(i)** to users.

(9 marks)

(iii) Discuss **TWO (2)** best practices to prevent IoT Botnet.

(5 marks)

Q2 (a) Differentiate the following terms:

(i) Incident response and incident handling.

(4 marks)

(ii) Preparation phase and detection phase.

(4 marks)

(b) Consider the following scenario.

Alice uploads a malicious file on her cloud storage account. Applying social engineering technique, Alice sent an email invitation to Bob indicating that there is an important file that has been shared on his corporate cloud storage account. Bob download the file using his mobile device and install it. Suspicious events are consequently detected which subsequently bring to incident assessment, respond, and evaluation.

Based on the above scenario, answer the following questions.

(i) Discuss the responsibility boundaries between cloud providers and cloud users in handling the incident?

(6 marks)

(ii) Explain **THREE (3)** lesson-learnt issues for the cloud users.

(6 marks)

Q3 (a) State **ONE (1)** topic of current issues in information security.

(1 mark)

(b) Describe the information security domain in **Q3(a)**.

(4 marks)

(c) Discuss **THREE (3)** security challenges and its potential mitigation approaches in **Q3 (a)**.

(15 marks)

Q4 (a) Distinguish between ransomware and spyware.

(4 marks)

(b) Identify potential incident handling strategies that include Preparation, Detection, Analysis, Response, and Post-incident, for the ransomware threat.

(10 marks)

(c) Distinguish between mass-scale phishing, spear phishing, and whaling.

(6 marks)

- END OF QUESTION -