INTI International University & Colleges

FINAL
Examination Paper

(COVER PAGE)

Session	:	**AUGUST 2017**
Programme	:	Diploma In Information And Communication Technology (DICTN)
Course	:	**ICT2106: Fundamentals of Trustworthy Computing**
Date of Examination	:	9 December, 2017 (Saturday)
Time	:	8:00 am – 10:00 am Reading Time : Nil
Duration	:	2 Hours
Special Instructions	:	

SECTION A: Answer **ALL** multiple choice questions.

SECTION B: Answer any **THREE (3)** essay questions.

IMPORTANT NOTE : **THIS PAPER SHOULD NOT BE TAKEN OUT OF THE EXAMINATION HALL**

Materials permitted : Nil

Materials provided : OMR Sheets

Examiner(s) : **Andrew Ho Mun Wah** and Shahriman Mohd Said

Moderator : Richard Tham

This paper consists of 7 printed pages, including the cover page

DIPLOMA IN INFORMATION AND COMMUNICATION TECHNOLOGY PROGRAMME (DICTN)
ICT2106: FUNDAMENTALS OF TRUSTWORTHY COMPUTING
FINAL EXAMINATION: AUGUST 2017 SESSION

SECTION A
Instruction: This section consists of **TWENTY (20)** multiple-choice questions. Answer **TWENTY (20)** questions in the OMR sheet provided. All questions carry equal marks.

1. Information security is generally considered to be the responsibility of _____ in the organization.

   A. Everyone in the organization
   B. The corporate security staff
   C. IT staff
   D. Everyone with computer access

   (2 marks)

2. Which one of the following Information Security terms characterizes the absence or weakness of a risk-reducing safeguard?

   A. Exposure
   B. Risk
   C. Vulnerability
   D. Danger

   (2 marks)

3. Which of the following is an example of logical control?

   A. Access control list
   B. Backup generators
   C. Fire suppression systems
   D. Locks

   (2 marks)

4. What security implementation principle recommends division of responsibilities so that one person cannot commit an undetected fraud?

   A. Access enforcement
   B. Account management
   C. Least privilege
   D. Separation of duties

   (2 marks)

5. What security implementation principle is used for granting users only the rights that are necessary for them to perform their work?

A. Discretionary Access
B. Least Privilege
C. Mandatory Access
D. Separation of Duties

(2 marks)

6. Which of the following mechanism process is used by a computer worm?

A. Fake process
B. Spawn process
C. Stealth process
D. VAX process

(2 marks)

7. _____ can modify the operating system's kernel and can intercept system calls while remaining hidden to the computer users.

A. Ransomware
B. Rootkit
C. Scareware
D. Trojan Horse

(2 marks)

8. The first step in establishing a security metrics program is to define its_____.

A. Action plans
B. Benchmark
C. Goals and objectives
D. Rubrics

(2 marks)

9. In the case of a DoS attack on a mail server, we would classify this as _____.

A. Interception
B. Interruption
C. Fabrication
D. Modification

(2 marks)

10. Which of the following password is considered to be the **MOST** secure?

A. `godismysavior`
B. `P@s$w07D`
C. `1234abcd!@#$`
D. `%$#edc973PWA`

(2 marks)

11. A _____ computer is commonly used for computer virus checking.

A. bastion
B. gateway
C. proxy
D. sheepdip

(2 marks)

12. _____ is a type of computer virus that contains a variety of mechanisms specifically coded to make its detection and decryption very difficult.

A. Armored virus
B. Cavity virus
C. Macro virus
D. Phage virus

(2 marks)

13. Michelle, a system administrator is trying to secure the Lightweight Directory Access protocol which is used to access the directory listings within Active Directory or from the other directory services. Which of the following TCP port should she engage for this task?

A. 53
B. 161
C. 389
D. 636

(2 marks)

14. Which of the following is the solution for sending an encrypted e-mail message?

A. IMAP
B. PGP
C. POP
D. SMTP

(2 marks)

15. The strength of the encryption method comes from the following **EXCEPT**

A. Algorithm
B. Initialization Vectors
C. Length of the key
D. Reputation of the encryption standard

(2 marks)

16. Which of the following utilizes a stream-based cipher for encryption?

A. MD5
B. RC4
C. RIPEMD
D. SHA

(2 marks)

17. Following are Symmetric Key Algorithms **EXCEPT**

A. AES
B. DES
C. IDEA
D. RSA

(2 marks)

18. _____ provides digital fingerprints used to identify the integrity of files.

A. Hash
B. Private key
C. Public key
D. Secret key

(2 marks)

19. _____ heavily rely on its database to match well-known attack signatures.

A. Captcha
B. Firewall
C. Intrusion Detection System
D. Virtual Private Network

(2 marks)

20. The purpose of Honeypot is _____.

A. controls the incoming and outgoing network traffic based on applied rule set
B. gathers information regarding an attacker or intruder into your system
C. prevents, search for, detect, and remove software viruses, and other malicious software
D. transfer computer files from one host to another host over a TCP-based network

(2 marks)

SECTION B
Instruction: This section consists of **FOUR (4)** questions. Answer any **THREE (3)** out of **FOUR (4)** questions in the answer booklet provided. All questions carry equal marks.

Question 1

(a) Name **FOUR (4)** techniques of human-based social engineering attacks.
(4 marks)

(b) List the **SIX (6)** security elements of Information Security according to the Parkerian Hexad model.
(6 marks)

(c) Discuss the **FIVE (5)** classifications of security metrics that can be implemented for network security management? For *each* category identified, state **ONE (1)** example.
(10 marks)

Question 2

(a) Name any **FOUR (4)** cybersecurity attack techniques.
(4 marks)

(b) List and explain **FOUR (4)** reasons on why it is getting more difficult to defend against cybersecurity attacks.
(10 marks)

(c) Your college is considering to implement a Multi-Factor Authentication (MFA) system for students and staffs who uses the lab computers. As the information security officer in your college, recommend and discuss **TWO (2)** practical implementation for 2FA for the college lab computers.
(6 marks)

Question 3

(a) For *each* of the following threats to Information Security, name **TWO (2)** examples:-

(i) Human
(ii) Nature
(iii) Environment

(6 marks)

(b) (i) Identify and briefly explain **FIVE (5)** types of passwords that can be enforced in a computing device.

(10 marks)

(ii) List and describe **TWO (2)** ways that passwords are attacked.

(4 marks)

Question 4

Hackers commonly perform "hacking cycle" to ensure safe hacks. Charles is not sure of what "hacking cycle" means. Elaborate the following questions for Charles.

(a) Draw and label the phases of a "hacking cycle".

(5 marks)

(b) Explain *each* phases of the "hacking cycle".

(10 marks)

(c) List **FIVE (5)** negative impacts of hacking for a business organization.

(5 marks)

~The End~

ict2106 (f)/aug17/formatted