INTI International University & Colleges

FINAL
Examination Paper

(COVER PAGE)

Session	:	**AUGUST 2018**
Programme	:	Diploma In Information And Communication Technology (DICTN)
Course	:	**ICT2106: Fundamentals of Trustworthy Computing**
Date of Examination	:	7 December 2018, (Friday)
Time	:	11:00am – 1:00pm 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 Kavitha Thamadharan

Moderator : Richard Tham

*This paper consists of **6** printed pages, including the cover page*

DIPLOMA IN INFORMATION AND COMMUNICATION TECHNOLOGY PROGRAMME (DICTN)
DIPLOMA IN INFORMATION TECHNOLOGY PROGRAMME (DITN)
ICT2106: FUNDAMENTALS OF TRUSTWORTHY COMPUTING
FINAL EXAMINATION: AUGUST 2018 SESSION

SECTION A

Instructions: 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 of the following is **NOT** a typical component of an Information Security program?

   A. The consequences for the person breaking the security policies
   B. The policies and protective measures that will be used
   C. The responsibilities of individuals involved in maintaining security
   D. The responsibilities of those who abide by established security policies

   (2 marks)

3. The likelihood of a threat source taking advantage of a vulnerability is called?

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

   (2 marks)

4. Jack wishes to conduct an Information Security vulnerability research. Following are vulnerability databases that you would recommend **EXCEPT**

   A. Common Vulnerabilities and Exposures
   B. Github
   C. Microsoft Security Bulletins
   D. NIST Vulnerability Database

   (2 marks)

5. The threat of embedding a message in a document, image, video or sound recording so that its very existence is hidden is called?

   A. Anonymity
   B. Data diddling
   C. Shielding
   D. Steganography

(2 marks)

6. Using a vulnerable file system in Windows operating system should always be avoided. Which of the following is the **MOST** secure file system for use with today's Windows?

   A. APFS
   B. FAT
   C. FAT32
   D. NTFS

(2 marks)

7. Which of the following ports would be blocked if Victor, a security administrator, wants to deny access to web sites?

   A. 21
   B. 25
   C. 80
   D. 3389

(2 marks)

8. Password are vulnerable for attack in Microsoft Windows operating system because it store the password hashes information in a specific database file referred to as _____.

   A. DLL
   B. PWD
   C. SAM
   D. VXD

(2 marks)

9. Following are ways to harden the operating system **EXCEPT**

   A. Making alterations to common accounts
   B. Making use of logging and auditing functions
   C. Removing unnecessary software
   D. Utilize the use of open source software whenever possible

(2 marks)

10. "**X**" replaces bits, characters, or blocks of characters with different bits, characters or blocks. What **BEST** represents "**X**"?

    A. Autokey cipher
    B. Chaocipher
    C. Substitution cipher
    D. Transposition cipher

(2 marks)

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

    A. AES
    B. Blowfish
    C. RSA
    D. Triple DES

(2 marks)

12. In asymmetric encryption _____.

    A. Different keys are used encryption and decryption
    B. No key is required for encryption and decryption
    C. Same key is used for encryption and decryption
    D. None of the mentioned

(2 marks)

13. What provides digital fingerprints used to identify the integrity of files?

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

(2 marks)

14. In 2000, the U.S. Department of Defense published the _____ to replace the Trusted Computer System Evaluation Criteria document which established a metric against which computers systems can be evaluated for security.

    A. Common Criteria (CC)
    B. Federal Information Processing Standard (FIPS) 140-2
    C. Information Technology Security Evaluation Criteria (ITSEC)
    D. ISO/IEC 27001

(2 marks)

15. The second step in creating a security metric according to Payne is?

    A. Establish benchmark and targets
    B. Decide which metrics to generate
    C. Define the metrics program goals and objectives
    D. Create an action plan and act on it

(2 marks)

16. Which of the following is used to send secure messages from one location to another using a public network such as the Internet?

A. Physical public network
B. Virtual public network
C. Physical private network
D. Virtual private network

(2 marks)

17. Which of the following is the **MOST** suitable deep web browser that anonymizes web traffic using a proxy network, making it easy to protect your identity online.

A. Chrome
B. Firefox
C. Opera
D. Tor

(2 marks)

18. The major difference between pentesters and blackhat hackers is the consent of conducting the ethical hacking activities to find the security posture after a signed document known as _____.

A. NDA
B. MOU
C. RFP
D. SLA

(2 marks)

19. Select the important factors of considerations when choosing a penetration testing tool.

I. Documentation
II. Licensing
III. Tool has an active community
IV. Versions

A. I, II, III
B. II, III, IV
C. I, II, IV
D. I, II, III, and IV

(2 marks)

20. Choose the following that are exploit tools.

I. Burp suite
II. Maltego
III. Metasploit
IV. VMWare

A. I, II, III
B. II, III, IV
C. I, II, IV
D. I, II, III, and IV

(2 marks)

SECTION B

Instructions: 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) List and describe **THREE (3)** trustworthy computing goals.

(6 marks)

b) Name any **SIX (6)** types of malware threats.

(6 marks)

c) Identify and briefly explain **FOUR (4)** classifications of Information Security vulnerabilities.

(8 marks)

Question 2

a) Identify and describe **FIVE (5)** common password policies.

(10 marks)

b) Determine and explain **FIVE (5)** security threats of a web server.

(10 marks)

Question 3

a) Name and explain **FIVE (5)** categories of Information security metrics.

(10 marks)

b) Identify and briefly explain **FIVE (5)** security design principles.

(10 marks)

Question 4

a) Name **FOUR (4)** ways an Intrusion Detection System detects an intrusion.

(4 marks)

b) List **FIVE (5)** types of hardware-based firewall.

(5 marks)

c) With the use of a diagram, identify and explain the **FIVE (5)** phases of ethical hacking.

(11 marks)

--THE END—

(ICT2106 (final)/August2018/ formatted)