INTI International University & Colleges

FINAL
Examination Paper

(COVER PAGE)

Session	:	August 2016
Programme	:	Diploma In Information And Communication Technology (DICTN)
Course	:	**ICT2106: Fundamentals of Trustworthy Computing**
Date of Examination	:	09 December, 2016 (Friday)
Time	:	8:00am – 10:00am 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 2016 SESSION

Instruction: This paper consists of **TWO (2) SECTIONS.** Answer **ALL** questions in **SECTIONA** and any **THREE (3)** questions in **SECTION B.**

SECTION A: Answer **ALL** questions in the OMR sheet provided. **(40 marks)**

1. What are the three fundamental principles of Information Security?

   A. confidentiality, integrity, and availability
   B. integrity, availability, and accountability
   C. availability, accountability, and confidentiality
   D. trustworthy, integrity, and availability

2. Hacking for a cause is called _____.

   A. Activism
   B. Blue-hat hacking
   C. Hacktivism
   D. Passive hacking

3. A _____ is a term for a person who floods a web site with data packets, creating a DoS.

   A. Cracker
   B. Dox hacker
   C. Packet monkey
   D. Violentacrez

4. DoS in **question 3** stands for _____.

   A. Daemons of Shadow
   B. Dead on Scene
   C. Denial of Service
   D. Date of Separation

5. Following are examples of DoS **EXCEPT**

   A. ICMP flood
   B. Ping of death
   C. Salami slicing
   D. Teardrop attack

6. A scan of a server shows port TCP 143 is open. What risk could this pose?

   A. Active mail relay
   B. Database exposure
   C. Open printer sharing
   D. Remote unauthenticated attack

7. **X** is a malware that hides its presence on the computer, using some of the lower layers of the operating system (such as the kernel), which makes it almost undetectable by common anti-malware software. What is **X**?

   A. Beetroot
   B. Dicotroot
   C. Kingoroot
   D. Rootkit

8. Which of the following virus program is usually targeted at Microsoft Office products?

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

9. An information system resource that is expressly set up to attract and trap people who attempt to penetrate an organization's network is called a _____.

   A. DMZ
   B. Honeypot
   C. Trapper
   D. Zapper

10. The intent of "Least privilege" is to enforce the most restrictive user rights required?

    A. To execute system processes
    B. By their job description
    C. To execute authorized tasks
    D. By their security role

11. Access rights are completely validated every time an access occurs. Systems should rely as little as possible on access decisions retrieved from a cache. In reference to Saltzer and Schroeder list, this principle is known as _____.

    A. Complete mediation
    B. Fail-safe defaults
    C. Least privilege
    D. Least common mechanism

12. Following are examples of established metric standard which computers systems can be evaluated for security **EXCEPT**

    A. Common Criteria
    B. ISO 27001
    C. Orange Book
    D. TCSEC

13. Which of the following is an example of symmetric encryption standard?

    A. AES
    B. HMAC
    C. MD-5
    D. SHA-1

14. Digital signature attached to certificate's container file to certify file is from entity it claims to be from and to ensure _____.

    A. availability
    B. confidentiality
    C. non-repudiation
    D. scarcity

15. **X** is an algorithm based on the use of a random permutation and is commonly used for the encryption of traffic to and from secure Web sites using the SSL protocol. What is **X**?

    A. DES
    B. Blowfish
    C. IDEA
    D. RC4

16. Pretty Good Privacy (PGP) is used in _____ security.

    A. browser
    B. email
    C. operating system
    D. web site

17. _____ is an attack which systematically checks all possible keys or passwords.

    A. Brute force attack
    B. Cognitive attack
    C. Dictionary attack
    D. Rainbow table attack

18. Victor would like to check the integrity of an application file that he just downloaded. Which of the following tool can Victor use?

A. Havij
B. Netcraft
C. Tripwire
D. Silica

19. Which of the following is **BEST** used for footprinting social networking profiles?

A. Maltego
B. Loki
C. Passive Recon
D. Whois

20. _____ is the process of hiding the data, for instance in images and sound files.

A. Pantography
B. Radiography
C. Sonography
D. Steganography

SECTION B: Answer any **THREE (3)** questions in the answer booklet provided. **(60 marks)**

Question 1

(a) Expand the following information security management related acronyms.

(i) CVE
(ii) EoP

(2 marks)

(b) What are the **THREE (3)** classifications of multi-factor authentication? For *each* classification identified, name **TWO (2)** examples.

(9 marks)

(c) Identify and briefly explain **THREE (3)** categories of "threat sources" for Information Security. For *each* category identified, list **ONE (1)** example.

(9 marks)

(Total: 20 marks)

Question 2

(a)

Restaurant Sehati Sejiwa free Wi-Fi
SSID: malaysia
Password: 123cat

(i) Identify **FIVE (5)** poor password design mistake for the above free Wi-Fi service.
(5 marks)

(ii) For *each* poor password design mistake identified in Q2(a)(i), recommend **ONE (1)** improvement to redesign the password to be more secure.
(5 marks)

(b) Name and explain **FOUR (4)** examples of human-based social engineering attacks.
(10 marks)

(Total: 20 marks)

Question 3

(a) Identify **FIVE (5)** examples of website attacks.
(5 marks)

(b) For *each* of the following, name **ONE (1)** example of tool:-

(i) Vulnerability scanning
(ii) Port scanning
(iii) Network scanning

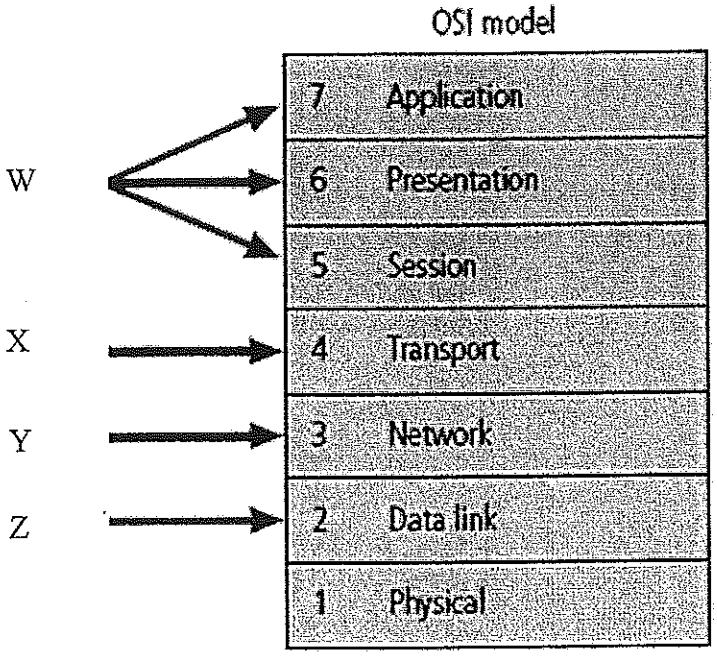
(3 marks)

(c) With the use of suitable examples, identify and briefly explain **SIX (6)** types of countermeasures for Information Security.
(12 marks)

(Total: 20 marks)

Question 4

(a) Define firewall. Determine "W", "X", "Y", and "Z" firewalls for the OSI model diagram below, and briefly explain each of them.



(10 marks)

(b) State and briefly explain any **FIVE (5)** clusters of security metrics for an Information Technology department.

(10 marks)

(Total: 20 marks)

~ The End ~

ict2106(f)/aug16/formatted