INTI International University & Colleges

FINAL
Examination Paper

(COVER PAGE)

Session	:	**APRIL 2018**
Programme	:	Diploma In Information And Communication Technology (DICTN) Diploma In Information Technology (DITN)
Course	:	**ICT2106: Fundamentals of Trustworthy Computing**
Date of Examination	:	July 30, 2018 (Monday)
Time	:	5.00pm - 7.00pm 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 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)
DIPLOMA IN INFORMATION TECHNOLOGY PROGRAMME (DITN)
ICT2106: FUNDAMENTALS OF TRUSTWORTHY COMPUTING
FINAL EXAMINATION: APRIL 2018 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. Which security strategy requires using several, varying methods to protect IT systems against attacks?
   A. Covert channels
   B. Defense-in-depth
   C. Exponential back-off algorithm
   D. Three-way handshake

2. Which of the following web site should Seymour, a security technician visit to complete the task of vulnerability research?
   A. cve.mitre.org
   B. comptia.org
   C. eccouncil.org
   D. isc2.org

3. A vulnerability exists in the Remote Desktop Protocol (RDP), where an attacker could send a specially crafted sequence of packets to TCP port _____ which can result in RDP to accessing an object in memory after it has been deleted. Which of the following port should be blocked by Edward, a security administrator?
   A. 23
   B. 5353
   C. 3389
   D. 8080

4. Password are vulnerable for attack in Microsoft Windows operating system because it stores the password hashes information in a specific database file referred as _____.
   A. DLL
   B. PWD
   C. SAM
   D. VXD

5. Older versions of operating system such as Microsoft XP and Vista are commonly patched with bundled security updates known as _____.
   A. bugfix
   B. hotfix
   C. service pack
   D. x-fix

6. An Operating Systems' kernel is often a target of attack for which type of malware?
   A. Adware
   B. Keylogger
   C. Rootkit
   D. Worm

7. Which of the following scanning tools is specifically designed to find potential vulnerabilities in Microsoft Windows products?
   A. MBAS
   B. MBJB
   C. MBPJ
   D. MBSA

8. What do you call a pre-computed hash?
   A. Moon tables
   B. Rainbow tables
   C. Star tables
   D. Sun tables

9. Where are encrypted passwords hashes kept in Linux operating system?
   A. /bin/password
   B. /bin/shadow
   C. /etc/profile
   D. /etc/shadow

10. _____ has three fixed 128-bit block ciphers with cryptographic key sizes of 128, 192 and 256-bits. It is a symmetric algorithm requiring only one encryption and decryption key.
   A. AES
   B. DES
   C. IDEA
   D. Twofish

11. Which of the following is the preferred way of encryption for web site?
   A. Pre-shared Secret key
   B. Public key-encryption
   C. Symmetric key-encryption
   D. Using Key Distribution Center (KDC)

12. Which of the following is the **MOST** common web server vulnerability?
   A. Default installation
   B. Limited user accounts
   C. No directory access
   D. Private shares

13. In 1985, the U.S. Department of Defense published the Trusted Computer System Evaluation Criteria, popularly known as the_____. This document established a metric against which computers systems can be evaluated for security.
    A. Green Book
    B. Orange Book
    C. Red Book
    D. White Book

14. Without establishing a _____, it is hard to demonstrate that information security efforts had more than assumed success.
    A. baseline
    B. metanoia
    C. scintilla
    D. taxonomy

15. "**X**" is a part of a information system that, if it fails, will stop the entire system from working. "**X**" are undesirable in any information system with a goal of high availability. Conclude what is "**X**".
    A. BPOF
    B. EPOF
    C. SPOF
    D. VPOF

16. Following are examples of exploit tools **EXCEPT**
    A. EnCase
    B. John the Ripper
    C. Metasploit
    D. Social-Engineer Toolkit

17. Identifying the target, finding out the target's network address range, banner grabbing, identifying DNS records, etc. is which phase in the ethical hacking methodology?
    A. Reconnaissance
    B. Scanning
    C. Gaining access
    D. Escalation of privilege

18. Select the important factors of considerations when choosing an exploit 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

19. Choose the following that are footprinting tools.

I. Maltego
II. GHDB
III. Nessus
IV. Netcraft

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

20. Choose the countermeasures such as detecting and blocking traffic when suspected traffic flow is detected.

I. IBS
II. ICS
III. IDS
IV. IPS

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

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. Expand the following information security management related acronyms:-

i. NDA
ii. DoS

(2 marks)

b. Name the **SIX (6)** elements of Information Security from the Parkerian Hexad model.

(6 marks)

c. What are the **FOUR (4)** categories of threats as classified by NIST? For *each* category identified, explain using **ONE (1)** example.

(12 marks)

Question 2

a. List and describe **FIVE (5)** examples of web site attacks.

(10 marks)

b. Determine and explain **FOUR (4)** classifications of security metrics that can be implemented for Information Security management.

(10 marks)

Question 3

a.

Alliance Cafe free Wi-Fi
SSID: hope
Password: abchope

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

(5 marks)

ii. For *each* poor password design mistake identified in Question 3(a)(i), recommend **ONE (1)** improvement to redesign the password to be more secure.

(5 marks)

b. Identify and briefly explain any **THREE (3)** security design principles.

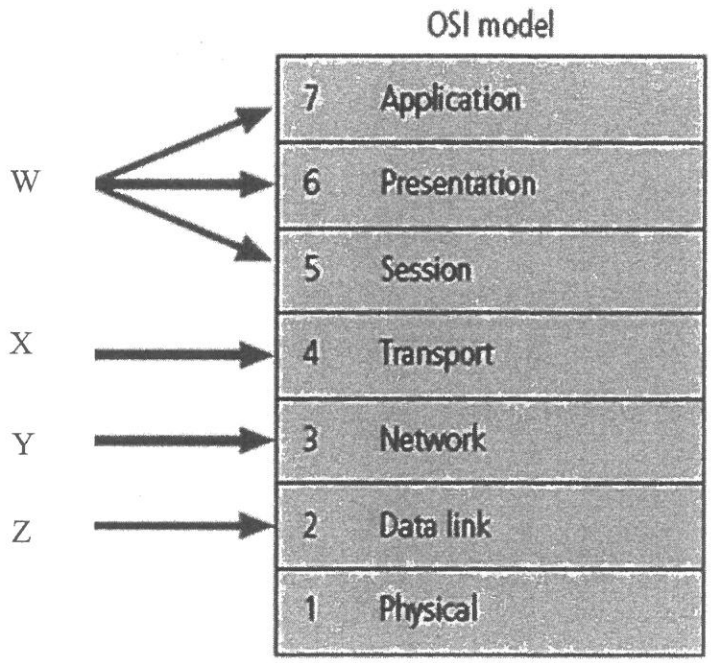
(6 marks)

c. Name **FOUR (4)** types of Intrusion Detection System.

(4 marks)

Question 4

a. Define firewall. Determine the appropriate W, X, Y and Z firewalls for the OSI model and explain each of them.



(10 marks)

b. Cecil would like to conduct ethical hacking in the gaining access phase. Suggest and discuss **FOUR (4)** ethical hacking approaches to Cecil.

(10 marks)

~ The End ~

ICT2106 (F)/Apr18