INTI
International College Subang
LAUREATE INTERNATIONAL UNIVERSITIES

FINAL
Examination Paper

(COVER PAGE)

Session	:	**April 2015**
Programme	:	Diploma In Information And Communication Technology (DICTN)
Course	:	**ICT2106: Fundamentals Of Trustworthy Computing**
Date of Examination	:	August 4, 2015
Time	:	2:00pm – 4:00pm Reading Time: Nil
Duration	:	2 Hours
Special Instructions	:	

Section A: Answer **ALL** Multiple Choice questions.

Section B: Answer any **THREE (3)** questions.

Materials permitted : Nil

Materials provided : OMR sheets

Examiner (s)	:	**Mr. Andrew Ho Mun Wah,** Shahriman Mohd Said.
Moderator	:	Mr. Richard Tham

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

INTI INTERNATIONAL COLLEGE SUBANG

DIPLOMA IN INFORMATION AND COMMUNICATION TECHNOLOGY
ICT2106: FUNDAMENTALS OF TRUSTWORTHY COMPUTING
FINAL EXAMINATION: APRIL 2015 SESSION

SECTION A : 40 marks

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) _____ is the anti-hacking statute law that prohibits unauthorized access to computers and networks.
   (A) CFAA
   (B) ISA
   (C) POTA
   (D) PDPA
   (E) SOSMA

(2 marks)

2) The security, functionality, and ease-of-use triangle illustrates which concept?
   (A) As security increases, functionality and ease of use increase
   (B) As security decreases, functionality and ease of use increase
   (C) As security decreases, functionality and ease of use decrease
   (D) Security does not affect functionality and ease of use
   (E) None of the above

(2 marks)

3) 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) ACL
   (B) DMZ
   (C) Firewall
   (D) Mantrap
   (E) Honeypot

(2 marks)

4) A _____ team consists of a group of ethical hackers that works together to perform a full-scale test covering all aspects of network, physical, and systems intrusion.
   (A) Dragon
   (B) Snake
   (C) Tiger
   (D) Phoenix
   (E) Unicorn

(2 marks)

5) An NMAP scan of a server shows port TCP 6000 is open. Following are risks that it could pose EXCEPT
(A) Active mail relay
(B) Denial of service
(C) Remote access control
(D) Trojan attack
(E) X11 attack

(2 marks)

6) The Regional Internet Register (RIRs) provides management of the public IP address space for countries. Iran is listed in _____ of RIRs service region.
(A) AfriNIC
(B) APNIC
(C) ARIN
(D) LACNIC
(E) RIPE

(2 marks)

7) _____ is a dedicated computer which is used to test files on removable media for viruses before they are allowed to be used with other computers.
(A) Bastion host
(B) Gateway
(C) Proxy
(D) Sheep dip
(E) Web marshal

(2 marks)

8) Which of the following is capable of altering its form in order to avoid discovery by certain virus detection programs?
(A) Auto-run virus
(B) Boot virus
(C) Camouflage virus
(D) Macro virus
(E) Polymorphic virus

(2 marks)

9) Which of the following term best describes the weakness in a system that may possibly be exploited?
(A) Exposure
(B) Exploit
(C) Risk
(D) Threat
(E) Vulnerability

(2 marks)

10) A set of step-by-step instructions used to satisfy information system security control requirements is called _____.
(A) guidelines
(B) policy
(C) principles
(D) protocol
(E) standard

(2 marks)

11) The purpose of_____ is to make attack less likely.
(A) avoidance control
(B) detection control
(C) deterrence control
(D) mitigation control
(E) transference control

(2 marks)

12) _____ describe a category of security appliances which integrates a range of security features such as firewall, gateway anti-virus, and intrusion detection and prevention capabilities into a single appliance or platform.
(A) UM
(B) UKM
(C) UPM
(D) UTM
(E) UUM

(2 marks)

13) Which of the following is a classic cipher that uses simple substitution algorithm?
(A) AES
(B) Blowfish
(C) Caesar
(D) DES
(E) RSA

(2 marks)

14) Which of the following encryption standard is the strongest?
(A) AES
(B) DES
(C) IDEA
(D) RC
(E) Twofish

(2 marks)

15) Following are examples of asymmetric algorithms for encryption EXCEPT
(A) 3DES
(B) Diffie-Hellman
(C) ECC
(D) El Gamal
(E) RSA

(2 marks)

16) What do you call a pre-computed hash?
(A) Deimos tables
(B) Europa tables
(C) Luna tables
(D) Oberon tables
(E) Rainbow tables

(2 marks)

17) Which of the following is an example of a password sniffing tool?
(A) Cain & Abel
(B) Jack the ripper
(C) Lastpass
(D) Password Gorilla
(E) TrueCrypt

(2 marks)

18) Following are examples of scanner tool EXCEPT
(A) Fullz
(B) Nessus
(C) SATAN
(D) SAINT
(E) Zenmap

(2 marks)

19) **X** is a lightweight network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. What is **X**?
(A) Hping2
(B) Dsniff
(C) Ettercap
(D) Kismet
(E) Snort

(2 marks)

20) In order to show improvement of information security over time in a business organization, what must be developed?
(A) Metrics
(B) Patches
(C) Reports
(D) Taxonomy of vulnerabilities
(E) Testing tools

(2 marks)

SECTION B : 60 marks

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) Determine and briefly explain the **THREE (3)** classic security attributes of the CIA triad model for Information Security.

(6 marks)

(b) An Information Security awareness program can help ensure the CIA triad model is implemented successfully for the IT system assets and its information. List and describe **SEVEN (7)** recommendations for an InfoSec awareness program for your college.

(14 marks)

Question 2

(a) Name **FOUR (4)** authentication alternatives to replace text-based passwords in an information system.

(4 marks)

(b)

CHONG CAFE
FREE WIFI
SSID: chong
Password: cafe

Recommend **SIX (6)** guidelines for improving the effectiveness of the above text-based password to improve security measure.

(6 marks)

(c) Human threats may be intentional or accidental (Harris, 2002). List and briefly explain **FIVE (5)** examples of human threats in regards to Information Security.

(10 marks)

Question 3

(a) Define the terminology "hacktivism". Name **THREE (3)** hacktivism groups.

(5 marks)

(b) What is the main different between passive footprinting and active footprinting? Name **TWO (2)** passive footprinting tools and **TWO (2)** active footprinting tools.

(6 marks)

(C) Identify and briefly explain **THREE (3)** techniques a hacker would conduct human-based social engineering attack. For *each* of the technique identified, describe **ONE (1)** way to countermeasure against the attack.

(9 marks)

Question 4

(a) The incident response team must learn from the incident by determining what caused it and what lessons can be drawn from the incident to prevent its happening again. Determine **FOUR (4)** incident management metrics.

(4 marks)

(b) List **SIX (6)** specific web services and web application exploit.

(6 marks)

(c) What are **FOUR (4)** Saltzer and Schroeder design principles for Information Security would you recommend for the redesign of today's business organization web services and web application? Explain your recommendations.

(10 marks)

--THE END--

(ICT2106 (F)/Apr15/ Andrew/ 180515)