



**INTI**

International College Subang

LAUREATE INTERNATIONAL UNIVERSITIES®

**FINAL**  
Examination Paper

(COVER PAGE)

Session : April 2014

Programme : Diploma In Information And Communication Technology (DICTN)

Course : ICT2106: Fundamentals Of Trustworthy Computing

Date of Examination : July 23, 2014

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) questions.

Materials permitted : Nil

Materials provided : OMR sheets

Examiner (s) : Mr. Andrew Ho Mun Wah, Mugunthan Kandasamy.

Moderator : Mr. Victor Raj Kolintiar

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

## INTI INTERNATIONAL COLLEGE SUBANG

DIPLOMA IN INFORMATION AND COMMUNICATION TECHNOLOGY (DICTN)  
ICT2106: FUNDAMENTALS OF TRUSTWORTHY COMPUTING  
FINAL EXAMINATION: APRIL 2014 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.

(40 marks)

- 1) \_\_\_\_\_ is the notion used by hackers to express that something is worth doing or is interesting.
  - (A) Asset
  - (B) Big data
  - (C) Hack value
  - (D) Exploit
  - (E) Payload
  
- 2) "*Keep the design, as simple and small as possible*" is one of the security design principle recommended by \_\_\_\_\_.
  - (A) Phil Zimmerman
  - (B) Jason Andress
  - (C) Caroline Wong
  - (D) Saltzer and Schroeder
  - (E) Alan Turing
  
- 3) \_\_\_\_\_ refers to the technique to separate the code in different parts, so that each part runs with least privilege.
  - (A) Abstraction
  - (B) Compartmentalization
  - (C) Encapsulation
  - (D) Inheritance
  - (E) Sanitization
  
- 4) Microsoft uses the term \_\_\_\_\_ to refer to the computer security professionals they invited to find the vulnerability of their products such as Windows.
  - (A) Black hat hacker
  - (B) Blue hat hacker
  - (C) Grey hat hacker
  - (D) Red hat hacker
  - (E) White hat hacker

- 5) An NMAP scan of a server shows port 3306 is open. What risk could this pose?
- (A) Active mail relay
  - (B) Clear text authentication
  - (C) Database exposure
  - (D) Open printer sharing
  - (E) Web portal risk
- 6) The Regional Internet Register which provides management of the public IP address space for countries in Europe such as France is \_\_\_\_\_.
- (A) AfriNIC
  - (B) APNIC
  - (C) ARIN
  - (D) LACNIC
  - (E) RIPE
- 7) A hacker, upon scanning a company's network discovered vulnerability in one of the applications running on that particular company's network. He then, immediately grabs the opportunity and penetrates the company's network and steals all the company's classified information. This particular attack can be described as?
- (A) Cyber attack
  - (B) Internal attack
  - (C) External attack
  - (D) Stealth attack
  - (E) Zero-day attack
- 8) Which is the correct order of the ethical hacking phases?
- (A) Scanning, Reconnaissance, Gaining Access, Maintaining Access, Covering Tracks
  - (B) Reconnaissance, Scanning, Gaining Access, Maintaining Access, Covering Tracks
  - (C) Reconnaissance, Scanning, Gaining Access, Covering Tracks, Maintaining Access
  - (D) Reconnaissance, Gaining Access, Scanning, Maintaining Access, Covering Tracks
  - (E) Scanning, Reconnaissance, Gaining Access, Maintaining Access, Covering Tracks
- 9) \_\_\_\_\_ refers to the detailed guidelines and constraints regarding the execution of information security testing. It is established before the start of a security test, and gives the test team authority to conduct defined activities without the need for additional permissions.
- (A) BYOD
  - (B) ROE
  - (C) RFP
  - (D) SETA
  - (E) SLA

- 10) A mantrap is a type of \_\_\_\_\_.
- (A) Firewall
  - (B) Physical Security
  - (C) Logical Security
  - (D) IDS
  - (E) IPS
- 11) A machine that has been cracked and is being used as part of a second-stage attack by miscreants trying to mask their home IP address is known as a \_\_\_\_\_ machine.
- (A) Jaguar
  - (B) Snake
  - (C) Tiger
  - (D) Unicorn
  - (E) Zombie
- 12) \_\_\_\_\_ imitates the actual production system that host variety of services.
- (A) Pure Honeypots
  - (B) High Interaction Honeypots
  - (C) Low Interaction Honeypots
  - (D) Production Honeypots
  - (E) Research Honeypots
- 13) When designing a company's web application Steve did not filter out special characters such as \*, %, ,, and /. By doing so what attack is the web application susceptible to \_\_\_\_\_?
- (A) Click-jacking attack
  - (B) Cross-site request forgery attack
  - (C) Cross-site scripting attack
  - (D) SQL injection attack
  - (E) Cryptographic attack
- 14) Which of the following is a Public Key Encryption algorithm?
- (A) AES
  - (B) Twofish
  - (C) Serpent
  - (D) RSA
  - (E) All of the above
- 15) Which of the following reasons are NOT listed in the password policy?
- (A) Change your passwords every 3 months
  - (B) Use long passwords
  - (C) Mix your password characters with alpha numeric characters
  - (D) Use hard to guess passwords, and write it down so that you will not forget them
  - (E) Do not share your passwords with anyone

- 16) Which of the following is a scanner tool?
- (A) AeroDump
  - (B) Nessus
  - (C) TrueCrypt
  - (D) Comodo
  - (E) Ophcrack
- 17) Which of the following is a password cracking tool?
- (A) TrueCrypt
  - (B) KeePass
  - (C) John the Ripper
  - (D) Wireshark
  - (E) Zmap
- 18) \_\_\_\_\_ is a tool that can be used to query DNS servers and potentially obtain records about the various host of which it is aware.
- (A) Google Alerts
  - (B) NSLookup
  - (C) Maltego
  - (D) Monitter
  - (E) Serph
- 19) Which of the following is a web server vulnerability scanner tool that automates the process of scanning web servers for out-of-date and unpatched software as well as searching for dangerous file's that may resides on the web server?
- (A) NeoTrace
  - (B) Nikto
  - (C) Reamweaver
  - (D) SubSeven
  - (E) TraceRoute
- 20) \_\_\_\_\_ programs take a programs executable binary as input and generate textual files that contain the assembly language code for the entire program or parts of it to conduct code analysis.
- (A) Assemblers
  - (B) Compilers
  - (C) Disassemblers
  - (D) Wrappers
  - (E) Interpreter

**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.

(60 marks)

**Question 1**

(a) List any **FOUR (4)** factors that influence the trustworthiness of computing resources.

(4 marks)

(b) Name the **SIX (6)** elements of the Parkarian Hexad theory for information security management:

(6 marks)

(c) State and describe **FIVE (5)** categories of threats in information system.

(10 marks)

**Question 2**

(a) Explain the distinct characteristics of the following symmetric encryption standards:-

- (i) DES
- (ii) AES
- (iii) Blowfish
- (iv) RC4

(8 marks)

(b) (i) Identify and briefly explain **THREE (3)** examples of human-based social engineering attack techniques.

(6 marks)

(ii) For *each* examples of human-based social engineering attack techniques identified in Q2 (b)(i), state and briefly explain an appropriate countermeasure.

(6 marks)

**Question 3**

(a) Name and describe **FIVE (5)** types of computer viruses.

(10 marks)

(b) List and briefly explain **FIVE (5)** reasons for the increase cases of attack among business enterprise users of mobile devices.

(10 marks)

**Question 4**

(a) Identify and describe **THREE (3)** types of firewall.

(6 marks)

(b) List and briefly explain the **SEVEN (7)** key steps to establish a security metrics program.

(14 marks)

**-THE END-**  
*ICT2106 (F)/Apr2014*