INTI International University & Colleges

**FINAL**
Examination Paper

(COVER PAGE)

| | | |
|---|---|---|
| Session | : | April 2016 |
| Programme | : | Diploma In Information And Communication Technology (DICTN) |
| Course | : | **ICT2106: Fundamentals of Trustworthy Computing** |
| Date of Examination | : | 26 July, 2016 (Tuesday) |
| 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)** essay questions.

**IMPORTANT NOTE** : **THIS PAPER SHOULD NOT BE TAKEN OUT OF THE EXAMINATION HALL**

Materials permitted :
Nil

Materials provided :
OMR Sheets

Examiner(s) : **Shahriman Mohd Said** and Andrew Ho Mun Wah

Moderator : Richard Tham

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

DIPLOMA IN INFORMATION AND COMMUNICATION TECHNOLOGY (DICTN)
ICT2106: FUNDAMENTALS OF TRUSTWORTHY COMPUTING
FINAL EXAMINATION: APRIL 2016 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. The information in a computer system can only be accessible for reading by authorized personnel. This is categorized as _____.
   A. Authenticity
   B. Assurance
   C. Non-disclosure
   D. Non-repudiation

(2 marks)

2. Which of the following describes elements that create reliability and stability in networks and systems and which assure that connectivity is accessible when needed?
   A. Availability
   B. Acceptability
   C. Accountability
   D. Integrity

(2 marks)

3. 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. Overt channels

(2 marks)

4. 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

(2 marks)

5. In order to show improvement of information security over time in a business organization, what must be developed?
   A. Metrics
   B. Reports
   C. Patches
   D. Taxonomy of vulnerabilities

(2 marks)

6. _____ Management can be defined as "*the cyclical practice of identifying, classifying, remediating, and mitigating weaknesses in an information system.*"
   A. Payload
   B. Risk
   C. Threat
   D. Vulnerability

(2 marks)

7. A security exploit in which the attacker seeks to compromise a specific group of users by infecting websites that members of the group are known to visit is known as _____
   A. Spear phishing
   B. Man in the middle
   C. Watering hole attack
   D. Passive hacking

(2 marks)

8. The payroll department was targeted by an isolated email phishing scam in which a scammer impersonated the CEO and asked for employee payroll information. This phishing technique is known as _____
   A. Spear phishing
   B. Whaling
   C. Link manipulation
   D. Vishing

(2 marks)

9. Non repudiation _____.
   A. Protects against the disclosure of information to unauthorised users
   B. Assures that a person or system is who or what they claim to be
   C. Protects against unauthorised changes in data whether intentional or accidental
   D. Protects against a person denying later that a communication or transaction took place

(2 marks)

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

(2 marks)

11. Which of the following is a Public Key Encryption algorithm?
   A. Twofish
   B. Serpent
   C. RSA
   D. All of the above

(2 marks)

12. Which of the following encryption standard is the weakest?
    A. AES
    B. Blowfish
    C. DES
    D. IDEA

(2 marks)

13. Which version of RC is use in SSL/ TLS and HTTPS protocol?
    A. 2
    B. 3
    C. 4
    D. 5

(2 marks)

14. The major difference between penetration test and hacking is the consent of conducting the ethical hacking activities to find the security posture after a signed document known as _____.
    A. Non-disclosure agreement
    B. Memorandum of understanding
    C. Request for proposal
    D. Service level agreement

(2 marks)

15. When designing a company's web application, Victor 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

(2 marks)

16. Which of the following computer virus cannot be detectable by signature-based anti-virus scanner?
    A. Companion virus
    B. Cavity virus
    C. Macro virus
    D. Polymorphic virus

(2 marks)

17. _____ is an apparently useful program containing hidden functions that can exploit the privileges of the user (running the program), with a resulting security threat.
    A. Rootkit
    B. Torrent
    C. Trojan
    D. Worm

(2 marks)

18. Which of the following is a password cracking tool?
    A. Lastpass
    B. John the Ripper
    C. TrueCrypt
    D. Zenmap

(2 marks)

19. Following are examples of scanning tools EXCEPT
    A. Nessus
    B. MBSA
    C. Metasploit
    D. Wireshark

(2 marks)

20. Which of the following correctly describes Tripwire?
    A. Integrity verification tool
    B. Exploit tool
    C. Malware remover tool
    D. Password manager

(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) Name **FOUR (4)** motivations of Information Security attacks.

(4 marks)

(b) Authentication system proves the genuine identity of an information system end-user. List and briefly explain **THREE (3)** biometric authentication systems.

(6 marks)

(c) Identify and explain **FOUR (4)** reasons on why it is difficult to defend against hacking attacks.

(10 marks)

**Question 2**

(a) Identify and explain **FIVE (5)** examples of Network Security Metrics for an IT department.

(10 marks)

(b) Identify and briefly explain **FIVE (5)** types of passwords that can be found in computing devices.

(10 marks)

**Question 3**

(a) Identify and explain any **FOUR (4)** Saltzer and Schroeder secure design principles for application or web site development.

(10 marks)

(b) State and briefly explain any **FIVE (5)** techniques of using Social Engineering.

(10 marks)

**Question 4**

Hackers commonly perform "hacking cycle" to ensure safe hacks. Jane is not sure of what "hacking cycle" means. Elaborate the following questions for Jane:-

(a) Draw and label the phases of a "hacking cycle".

(5 marks)

(b) Explain each of the phases of a "hacking cycle".

(10 marks)

(c) Name **FIVE (5)** categories of countermeasures she may encounter if she performs the "hacking cycle"

(5 marks)

**~THE END~**