INTI International University & Colleges

FINAL
Examination Paper

(COVER PAGE)

Session : APRIL 2017

Programme : Diploma In Information And Communication Technology (DICTN)

Course : **ICT2106: Fundamentals of Trustworthy Computing**

Date of Examination : 31 July, 2017 (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) : **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 PROGRAMME
(DICTN)
ICT2106: FUNDAMENTALS OF TRUSTWORTHY COMPUTING
FINAL EXAMINATION: APRIL 2017 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. What is breach of confidentiality?
   A This type of violation involves unauthorized disclosure of data
   B This type of violation involves unauthorized modification of data
   C This type of violation involves unauthorized destruction of data
   D This type of violation involves unauthorized use of resources

(2 marks)

2. Petya and WannaCry are two examples of
   A Ransomware
   B Buffer overflow
   C Sniffer
   D Keylogger

(2 marks)

3. Which of the following ports would be blocked if Alex, a security administrator, wants to deny access to web sites?
   A 21
   B 25
   C 80
   D 3389

(2 marks)

4. Which of the following is **NOT** a web site attack technique?
   A Cross-Site Request Forgery
   B SQL injection
   C eXtensible Markup Language
   D Cross-Site Scripting

(2 marks)

5. Which of the following **BEST** describe a DoS attack?
   A It is attack to block traffic of network
   B It is attack to harm contents stored in storage devices by deploying malware processes
   C It is an attempt to make a machine or network resource unavailable
   D It is an attack where malicious scripts are injected into otherwise benign and trusted web sites

(2 marks)

6. Which of the following describes Physical Separation in security of Operating Systems?
   A Separation in which process use different physical objects like separate printers
   B Separation in which process having different security requirement at different times
   C Separation in which users operate under illusion that no other processes exist
   D Separation in which processes conceal their data and computations

(2 marks)

7. A user is required to not only provide a password to gain access to the system, but also a another security code, like a unique one-time access code generated from a token device or secure mobile app on their smartphone. This technique is known as
   A Password salting
   B Captcha
   C Multifactor authentication
   D Password hashing

(2 marks)

8. Which of the following is the **STRONGEST** password?
   A 31stAugust57
   B Delta2o17
   C P@assw0rd
   D !augustdelta

(2 marks)

9. What is **NOT** a best practice for a password policy?
   A Deciding maximum age of password
   B Having change password every 1 year
   C Password encryption
   D Restriction on password reuse and history

(2 marks)

10. What is **NOT** a role of encryption?
   A It is used to protect data from unauthorized access during transmission
   B It is used to ensure user authentication
   C It is used to ensure data integrity
   D It is used to ensure data corruption doesn't happens

(2 marks)

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)

(2 marks)

12. A kind of phishing scam and CEO fraud that targets high profile executives with access to highly valuable information. Try to trick users into divulging bank account data, employee personnel details, customer information or credit card numbers, or even to make wire transfers to someone they believe is the CEO or CFO of the company. This technique is known as
    A Whaling attack
    B Link manipulation
    C Teardrop attack
    D Covert Redirect

(2 marks)

13. What is a Hash function?
    A It creates an encrypted block of data
    B It creates a small flexible block of data
    C It creates a small fixed block of data
    D None of the mentioned

(2 marks)

14. Any alert that should have happened but didn't are considered
    A False negative
    B False positive
    C True negative
    D True positive

(2 marks)

15. When an administrator can configure and modify access controls on files and resources but cannot administer auditing functions, we would call that which of the following?
    A Access enforcement
    B Account management
    C Least privilege
    D Separation of duties

(2 marks)

16. What is trap door?
    A It is a secure doorway used in a server room
    B It is a security hole inserted at programming time in the system for later use
    C It is a Trojan horse
    D It is a computer virus which traps and locks user terminal

(2 marks)

17. By default, *https* uses port
    A 80
    B 443
    C 8080
    D 55

(2 marks)

18. Multipartite viruses attack on
    A Boot sector
    B Files
    C Memory
    D All of the mentioned

(2 marks)

19. Following are ways to classify an Intrusion Detection System (IDS) **EXCEPT**
    A Anomaly detection
    B Signature based misuse
    C Stack based
    D Zone based

(2 marks)

20. Which choice listed below describes the deployment of a network device in order to conduct research and analysis of attackers inside the organization's network perimeter?
    A Demilitarized zone
    B Honeypot
    C Intrusion detection system
    D Simultaneous Iterative Reconstruction Technique

(2 marks)

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) What are the **FOUR (4)** categories of Information system vulnerabilities? For *each* category identified, name **ONE (1)** example.

(8 marks)

(b) Identify and briefly explain **SIX (6)** classifications of security metrics that can be implemented for network security management.

(12 marks)

Question 2

(a) Identify the **TWO (2)** categories of firewall based on its location. Explain **FOUR (4)** types of firewall based on the way it provides protection.

(10 marks)

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

(10 marks)

Question 3

(a) For *each* of the following, name **TWO (2)** examples of authentication implementation:-

(i) What you are
(ii) What you have
(iii) What you know

(6 marks)

(b) With the use of suitable examples, identify and briefly explain **SEVEN (7)** categories of countermeasures for Information Security.

(14 marks)

Question 4

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

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

(5 marks)

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

(10 marks)

(c) One type of hacker is known as *script-kiddies*. Explain the term *script-kiddies* and why is it easy to become one.

(5 marks)

~THE END~

ict2106 (f)/apr17/ formatted