INTI International University & Colleges

FINAL
Examination Paper

(COVER PAGE)

Session	:	**August 2015**
Programme	:	Diploma In Information And Communication Technology (DICTN)
Course	:	**ICT2106: Fundamentals Of Trustworthy Computing**
Date of Examination	:	December 8, 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)** essay questions.

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

Materials permitted : Nil

Materials provided : OMR Sheets

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

Moderator : Mr. Richard Tham

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

DIPLOMA IN INFORMATION AND COMMUNICATION TECHNOLOGY (DICTN)
ICT2106: FUNDAMENTALS OF TRUSTWORTHY COMPUTING
FINAL EXAMINATION: AUGUST 2015 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. What are the three fundamental principles of Information Security?

   A. accountability, confidentiality, and integrity
   B. confidentiality, integrity, and availability
   C. integrity, availability, and accountability
   D. availability, accountability, and confidentiality
   E. trustworthy, integrity, and availability

(2 marks)

2. Hacking for a cause is called _____.

   A. Active hacking
   B. Activism
   C. Blue-hat hacking
   D. Hacktivism
   E. Passive hacking

(2 marks)

3. What is the objective of ethical hacking from the hacker's prospective?

   A. Determine the security posture of the organization
   B. Find and penetrate invalid parameters
   C. Find and steal available system resources
   D. Leave marks on the network to prove they gained access
   E. All of the above

(2 marks)

4. _____ = (threat * vulnerabilities * probability * impact) / countermeasures

   A. Breach
   B. Exposure
   C. Exploit
   D. Loss
   E. Risk

(2 marks)

5. A scan of a server shows port TCP 139 and 445 are 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

(2 marks)

6. The Regional Internet Register (RIRs) provides management of the public IP address space for countries. Brazil is listed in _____ of RIRs service region.

A. AfriNIC
B. APNIC
C. ARIN
D. LACNIC
E. RIPE

(2 marks)

7. A _____ is a program that secretly takes over another networked computer and then uses that computer to launch attacks.

A. Botnet
B. Trap doors
C. Rootkit
D. Worm
E. Zombie

(2 marks)

8. Which of the following programs is usually targeted at Microsoft Office products?

A. Boot virus
B. Cavity virus
C. Macro virus
D. Multipartite virus
E. Polymorphic virus

(2 marks)

9. The intent of least privilege is to enforce the most restrictive user rights required?

A. To execute system processes
B. By their job description
C. To execute authorized tasks
D. By their security role
E. By their ranks

(2 marks)

10. Access rights are completely validated every time an access occurs. Systems should rely as little as possible on access decisions retrieved from a cache. In reference to Saltzer and Schroeder list, this principle is known as _____.

A. Complete mediation
B. Economy of mechanism
C. Fail-safe defaults
D. Least privilege
E. Least common mechanism

(2 marks)

11. Which of the following is NOT a typical component of an Information Security program?

A. The consequences for the person breaking the security policies
B. The policies that will be used
C. The protective measures that will be used
D. The responsibilities of individuals involved in maintaining security
E. The responsibilities of those who abide by established security policies

(2 marks)

12. 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. Black Book
B. Grey Book
C. Orange Book
D. Purple Book
E. White Book

(2 marks)

13. Which of the following encryption standard is the weakest?
A. AES
B. DES
C. IDEA
D. RC
E. Twofish

(2 marks)

14. The strength of the encryption method comes from the following EXCEPT
A. The Algorithm
B. Secrecy of the Key
C. Length of the Key
D. Initialization Vectors
E. Reputation of the encyption standard

(2 marks)

15. PGP is an example of a

A. Digital signature
B. Hybrid cryptosystem
C. Public-key cryptography
D. Private- key cryptography
E. Secret-key cryptography

(2 marks)

16. Which of the following is a stream cipher?

A. 3DES
B. Blowfish
C. IDEA
D. RC4
E. RC5

(2 marks)

17. Following are examples of hashing algorithm EXCEPT

A. Keccak
B. MD-5
C. HMAC
D. SHA-1
E. Sudo

(2 marks)

18. An organization wants to select the most appropriate hashing method that can be used to secure Windows authentication. Which of the following should the organization choose?

A. MD4
B. MD5
C. LM
D. NTLM
E. NTLMv2

(2 marks)

19. Which of the following is FALSE?

A. Footprinting speeds up the hacking process
B. Footprinting involves publically available and accessible resources
C. Footprinting enable determining the network range
D. Footprinting assist in identifying system users
E. Footprinting is an active process that connects to the targets' machine

(2 marks)

20. Following are examples of tools commonly uses for footprinting EXCEPT

A. Havij
B. NSlookup
C. Sam Spade
D. Traceroute
E. Whois

(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) Expand the following information security management related acronyms.

(i) EoP
(ii) DoS
(iii) RCE

(3 marks)

(b) Define the terminology "vulnerability" in computer security. Name and briefly explain **THREE (3)** examples of Web application vulnerabilities.

(5 marks)

(c) Identify and briefly explain **FOUR (4)** categories of "threat sources" in managing Information Security. For *each* category identified, list **ONE (1)** example.

(12 marks)

Question 2

(a)

Restaurant 1Kawan
Free Wi-Fi
SSID: r1kawan
Password: 12345

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

(5 marks)

(b) Explain the term "script-kiddie". Determine **THREE (3)** reasons that help grow the numbers of "script-kiddie".

(5 marks)

(c) List and explain **FOUR (4)** examples of computer-based social engineering attacks.
(10 marks)

Question 3

(a) Identify and briefly explain **THREE (3)** categories of countermeasures for Information Security.
(6 marks)

(b) For *each* of the following types of scanning, name **ONE (1)** example of scanning tool:-

(i) Vulnerability scanning
(ii) Port scanning
(iii) Network scanning
(iv) War dialing

(4 marks)

(c) List and explain **FOUR (4)** methods of gaining access among penetration testers.
(10 marks)

Question 4

(a) Briefly explain **TWO (2)** objectives of utilizing a honeypot in a computer network. Name **ONE (1)** high interaction honeypot.
(3 marks)

(b) List the **SEVEN (7)** steps in a bottom up approach in building a security metrics.
(7 marks)

(c) State and briefly explain any **FIVE (5)** categories of security metrics recommended for Information Security management.
(10 marks)

~THE END~