FINAL
Examination Paper

(COVER PAGE)

Session : August 2014

Programme : Diploma In Information And Communication Technology (DICTN)

Course : ICT2106: Fundamentals Of Trustworthy Computing

Date of Examination : December 12, 2014

Time : 8:00am – 10:00am  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 : Ms. Noor Hasrina

This paper consists of 6 printed pages, including the cover page.
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) Information in a computer system is only accessible for reading by authorized personnel. This is categorized as ________________.
   (A) Admissibility
   (B) Availability
   (C) Authenticity
   (D) Confidentiality
   (E) Integrity

2) The Parkerian Hexad model adds three additional attributes to the existing three classic security attributes of the CIA triad model. This newer model was proposed in 2002 by

   (A) Bruce Schneier
   (B) George Kurtz
   (C) Gene Spafford
   (D) Donn Parker
   (E) Winn Schwartau

3) The cyclical practice of identifying, classifying, remediating, and mitigating weaknesses in an information system is best described as ________________ Management.
   (A) Exploit
   (B) Payload
   (C) Risk
   (D) Threat
   (E) Vulnerability

4) An attack on port 53 is known as ________________.
   (A) CSRF attack
   (B) DNS zone transfer attack
   (C) LDAP injection attack
   (D) SQL injection attack
   (E) XSS attack
5) Ports to block and avoid SMB session hijacking are _______ and _______.
(A) 25, 110
(B) 80, 443
(C) 139, 445
(D) 143, 993
(E) 515, 9100

6) The Regional Internet Register which provides management of the public IP address space for countries in Europe such as Germany is _____________.
(A) AfriNIC
(B) APNIC
(C) ARIN
(D) LACNIC
(E) RIPE

7) Followings are examples of Denial of Service (DoS) attacks EXCEPT
(A) Ping of Death
(B) Smurf attack
(C) Slowloris attack
(D) REST attack
(E) SYN attack

8) Mr. X uses existing computer scripts or codes to hack into others computers. He is lacking the expertise to write his own scripts or code. Mr. X is known as ________________.
(A) Cracker
(B) ID10T
(C) Luzzer
(D) Phreaker
(E) Script kiddie

9) A virus places an identical copy of itself into other programs or into certain system areas on the disk. This is done at the ____________ phase.
(A) Dormant
(B) Execution
(C) Mature
(D) Propagation
(E) Triggering

10) A virus explicitly designed to hide itself from detection by antivirus software is known as _____________.
(A) Boot virus
(B) Cavity virus
(C) Macro virus
(D) Multipartite virus
(E) Polymorphic virus
11) __________ attack would exploit company telephone and private branch exchange (PBX) systems, breaking inside the organization to steal data or map the internal networks.
   (A) Butt dialing
   (B) Drunk dialing
   (C) Rogue dialing
   (D) Rotary dialing
   (E) War dialing

12) A pre-computed look up table for reversing cryptographic hash functions is known as __________ table.
   (A) Hacking
   (B) Moon
   (C) Rainbow
   (D) Sun
   (E) Star

13) A password of P@SSWORD can be cracked using which type of attack?
   (A) Brute force
   (B) Dictionary
   (C) Harakiri
   (D) Kamikaze
   (E) Zero-day exploit

14) The process of replacing some characters in an encryption key is called __________.
   (A) Elimination
   (B) Subtraction
   (C) Substitution
   (D) Transposition
   (E) Transrelation

15) Group or network of compromised systems used for attacks is called as __________.
   (A) Botnet
   (B) Extranet
   (C) Honeynet
   (D) TORnet
   (E) Zombie

16) Following are examples of scanner tool EXCEPT
   (A) IPscan
   (B) Netcraft
   (C) Nmap
   (D) Nessus
   (E) Zenmap
17) Which of the following is able to automate finding of a database table to perform an SQL injection attack?
   (A) Havij
   (B) Nemesis
   (C) SARA
   (D) SAINT
   (E) SATAN

18) Certain types of SQL injection vulnerabilities in a website can be identified by using
   (A) Ethereal
   (B) Hping2
   (C) Scrawlr
   (D) Tripwire
   (E) Wireshark

19) Following are examples of banner grabbing tools EXCEPT
   (A) Netcat
   (B) Netcraft
   (C) Samspade
   (D) SmartWhois
   (E) Traceroute

20) The process of hiding the data, for instance in images and sound files is known as
   (A) Cryptography
   (B) Deception
   (C) Encryption
   (D) Sonography
   (E) Steganography

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) Name FOUR (4) examples for forces of nature threats. (4 marks)

(b) Identify FOUR (4) categories of vulnerability for information system. Briefly explain your answers. (8 marks)
(c) Suggest **FOUR (4)** password policy. Describe each policy suggested. **(8 marks)**

**Question 2**

Hackers commonly perform “hacking cycle” to ensure safe hacks. Donnie is not sure of what “hacking cycle” means. Elaborate the following questions to help Donnie understand the “hacking cycle”.

(a) Draw the phases of a “hacking cycle”. Label your drawing appropriately. **(5 marks)**

(b) Explain each of the phases of a “hacking cycle”. **(10 marks)**

(c) Name **FIVE (5)** types of countermeasures he may encounter if he performs the “hacking cycle”. **(5 marks)**

**Question 3**

(a) Name **FIVE (5)** types of Trojan. Elaborate your answers. **(10 marks)**

(b) List **FIVE (5)** ways to increase security of web server. For each ways listed, briefly provide the explanation. **(10 marks)**

**Question 4**

(a) Name **FOUR (4)** types of phishing. **(4 marks)**

(b) State **FOUR (4)** examples of symmetric encryption standards. **(4 marks)**

(c) List and briefly explain **SIX (6)** categories of a security metrics program. **(12 marks)**