UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2013/2014

COURSE NAME	:	FUNDAMENTAL OF INFORMATION SECURITY
COURSE CODE	:	BIS 10103
PROGRAMME	:	1 BIS
EXAMINATION DATE	:	JUNE 2014
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER **ALL** QUESTIONS

THIS QUESTION PAPER CONSISTS OF **NINE (9)** PAGES

SECTION A

Q1 Confidentiality ensures that ______________________________.

(A) our physical assets are safe from attackers
(B) only unauthorized parties can modify the data
(C) computer-related assets are accessed only by authorized parties
(D) only administrator can gain physical access to the computer resources

Q2 What are the **THREE (3)** primary goals of information security?

i. Confidentiality
ii. Redundancy
iii. Integrity
iv. Availability
v. Privacy

(A) i, ii and iii
(B) i, iii and iv
(C) ii, iii and iv
(D) i, iii and v

Q3 "*Precise, accurate, unmodified, modified only in acceptable ways and consistent*" are example of terms related with ____________.

(A) confidentiality
(B) integrity
(C) availability
(D) authorization

Q4 Which of the following statement is related to threat?

(A) Attacking a new web sites
(B) Phishing a web site
(C) Finding a new weakness in any network or systems
(D) Deleting files in a server

Q5 "*Controlled concurrency, simultaneous access, deadlock management and exclusive access as required.*" are examples of services related to __________.

(A) integrity
(B) confidentiality
(C) availability
(D) threat

Q6 "*Alteration of data without permission of data owner*" is an example of attack against ___________.

(A) confidentiality
(B) integrity
(C) availability
(D) threat

Q7 "*Deletion of files or records without permission of data owner*" is an example of attack against ___________.

(A) integrity
(B) confidentiality
(C) availability
(D) threat

Q8 "*Non availability of wireless network due to failure of access points*" is an example of attack against ___________.

(A) integrity
(B) confidentiality
(C) availability
(D) threat

Q9 What is a possible cipher text for the following plain text "*You are the best*" if the algorithm used is Caesar Cipher?

(A) Qwy abe cbi wik
(B) Csy evi xli fiwx
(C) Bwy tce wim wicn
(D) Cti wer nei cdtu

Q10 Malicious programs such as viruses, worms, Trojan horse programs and backdoors are example of ________.

(A) trapdoor
(B) malware
(C) hacker code
(D) super code

Q11 Tools or technique that takes advantages of vulnerability in order to exceed the user's authorized level of access is called _________.

(A) Exploits
(B) Spyware
(C) Backtrack 5
(D) Anti Virus

Q12 Reconnaissance is also known as ___________.

(A) backup of critical data
(B) information gathering
(C) strategic planning
(D) Disaster Recovery Plan

Q13 A _________ has the skill to break into computer systems and do damage. However, he uses his skill to help organizations.

(A) white hat hacker
(B) black Hat hacker
(C) gray hat hacker
(D) phreaker

Q14 A _______ can be thought of as a white hat hacker who occasionally strays and acts unethically.

(A) white hat hacker
(B) black hat hacker
(C) gray hat hacker
(D) phreaker

Q15 A ________, also known as a "*cracker*", uses his skills for unethical reasons (for example, to steal funds).

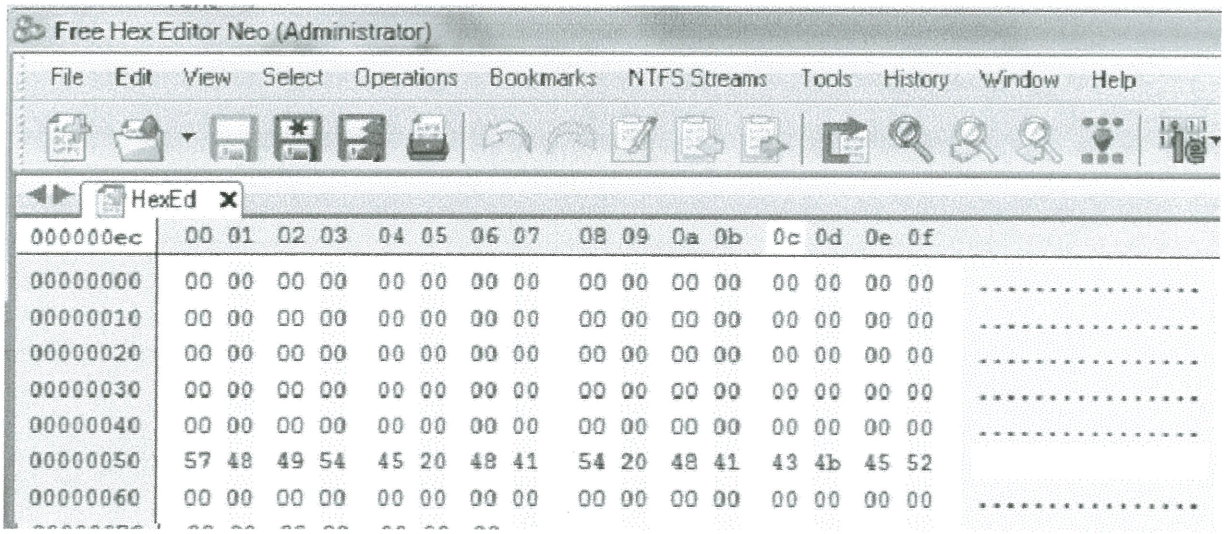
(A) white hat hacker
(B) black hat hacker
(C) gray hat hacker
(D) phreaker

Q16 A ______ is a hacker of a telecommunications system.

(A) white hat hacker
(B) black hat hacker
(C) gray hat hacker
(D) phreaker

Q17 If given Hex 41 as "A", Hex 42 as "B", what is the actual word in the following Hex Editor file depicted in **FIGURE Q17**?

(A) WHITE HAT HACKER
(B) BLACK HAT HACKER
(C) HACKER ARE COMING
(D) WHITE AND BLACKY



```
000000ec   00 01  02 03   04 05  06 07    08 09  0a 0b   0c 0d  0e 0f

00000000   00 00  00 00   00 00  00 00    00 00  00 00   00 00  00 00    ................
00000010   00 00  00 00   00 00  00 00    00 00  00 00   00 00  00 00    ................
00000020   00 00  00 00   00 00  00 00    00 00  00 00   00 00  00 00    ................
00000030   00 00  00 00   00 00  00 00    00 00  00 00   00 00  00 00    ................
00000040   00 00  00 00   00 00  00 00    00 00  00 00   00 00  00 00    ................
00000050   57 48  49 54   45 20  48 41    54 20  48 41   43 4b  45 52
00000060   00 00  00 00   00 00  00 00    00 00  00 00   00 00  00 00    ................
```

FIGURE Q17

Q18 What will happen to the file if we changed more than 70% of its content and open the file using Microsoft Word Version 7?

(A) File is viewable with some distortion
(B) File is corrupted and user is not able to view it content
(C) File can be view as the original file
(D) Half of the file is corrupted and only 20% file content viewable

Q19 Which of the following is **NOT** in the guidelines for password selection:

(A) Choose long password.
(B) Avoid using actual names or words.
(C) Do not change password regularly
(D) Use characters other than just A to Z.

Q20 One time passwords are very important for ___________ because an intercepted password is useless.

(A) authorization
(B) authentication
(C) verification
(D) identification

Q21 What is the equivalent HEXADECIMAL code for the following OCTAL number (773) Hex Editor?

(A) 507
(B) 705
(C) 711
(D) 557

Q22 Digital watermarking is an example of security mechanism for enforcing the concept of _______________.

(A) Confidentiality
(B) Integrity
(C) Availability
(D) Privacy

Q23 Steganography is a process of hiding a secret message in ____________.

(A) a computer
(B) a still image
(C) another ciphertext
(D) another secret message with a very strong password

Q24 If a database is to serve as a central repository of data, users must be able to trust the __________ of the data values.

(A) accuracy
(B) integrity
(C) logic
(D) validity

Q25 The integrity of database elements is their ___________________.

(A) correctness or validity
(B) correctness or accuracy
(C) correctness or consistency
(D) correctness or timely

(25 marks)

SECTION B

Q26 Write short notes on the following topics:

(a) **ONE (1)** similarity and **ONE (1)** difference between Steganography and Watermarking

(b) **FIVE (5)** Classifications of Electronic Commerce (EC)

(c) Database Security

(d) **THREE (3)** Offences under Malaysia Computer Crime Act 1997, Act 563.

(20 marks)

Q27 (a) Write a complete C programming code for implementing transposition cipher using MIRACLE as the keyword.

(15 marks)

(b) Decipher the following ciphertext "LSTOMIEYOEUTERLCRUR" using transposition cipher text if the key is "MARVELOUS".

(10 marks)

Q28 The following RSA algorithm parameters are used to encrypt message by sender and decrypt message by receiver respectively.

Given the following values:

- Choose p = 3 and q = 11
- Choose e such that 1 < e < φ(n) and e and n are co-prime. Let e = 7
- Compute a value for d such that (d * e) mod φ(n) = 1.
- One solution is d = 3 [(3 * 7) mod 20 = 1]
- The encryption of $m = 2$ is $c = 2^7 \bmod 33 = 29$
- The decryption of $c = 29$ is $m = 29^3 \bmod 33 = 2$

(a) What are the corresponding values of n and φ(n)?

(5 marks)

(b) What are the corresponding values of Public Key **(e, n)** and Private Key **(d, n)?**

(5 marks)

SECTION C

Q29 Consider the following scenario:

> You just had been appointed as a new security administrator for a new airport. Your team has been asked to prepare a **proposal** for implementing secure online system (e-FLY). With this new e-FLY, customers are able to make an online booking, reschedule flying time, make payment online and also view their booking status.

Propose a security design document consisting of physical and logical design, technologies, techniques and security mechanisms. Your proposal must address confidentiality, integrity and availability requirement associated with this system.

(20 marks)

- END OF QUESTION -