Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER I
SESSION 2019/2020

COURSE NAME	:	COMPUTER SECURITY
COURSE CODE	:	BEC 41903
PROGRAMME	:	BEJ
EXAMINATION DATE	:	DECEMBER 2019 / JANUARY 2020
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER **ALL** QUESTIONS

THIS QUESTION PAPER CONSISTS OF **EIGHT (8)** PAGES

PART A: Objective Questions. (20 marks)

Q1 Malicious code can do much harm except _____.

(A) writing a message on a computer screen
(B) stopping a running program
(C) erasing a stored files
(D) the program will be running fast

Q2 Which of the statement is FALSE?

(A) Virus: Attach itself to program and propagates copies of itself to other programs.
(B) Trapdoor: Propagates copies of itself through a network.
(C) Trojan horse: Contains unexpected, additional functionality.
(D) Time bomb: Triggers action when specified time occurs.

Q3 Viruses are attached by these ways except _____.

(A) appended viruses
(B) viruses that surround a program
(C) reborn itself
(D) integrated viruses and replacement

Q4 The virus writer may find these qualities appealing in a virus,

(A) It is hard to detect.
(B) It is not easily destroyed or deactivated.
(C) It spreads infection widely.
(D) It is machine non-independent and OS non-independent.

Q5 Control against program threats. There are many ways a program can fail and many ways to turn the underlying faults into security failures. In these matters, we will look at three types of controls except _____.

(A) timing
(B) developmental
(C) operating system
(D) administrative

Q6 Which computing system requires protection?

(A) Memory
(B) Network
(C) Sharable data
(D) All of the above

Q7 Which is not an authentication mechanism used to confirm a user's identity?

(A) Password
(B) A secret hanshake
(C) Fingerprint
(D) None of the above

Q8 Which of the following is not a common file permission?

(A) Write
(B) Execute
(C) Stop
(D) Read

Q9 Which of the following is the least secured method of authentication?

(A) Key card
(B) Fingerprint
(C) Retina pattern
(D) Password

Q10 Data integrity means _____.

(A) providing first access to stored data
(B) ensuring correctness and consistency of data
(C) providing data sharing
(D) None of the above

Q11 Prevention of access to the database by unauthorized users is referred to as _____.

(A) integrity
(B) productivity
(C) security
(D) reliability

Q12 Which of the following is not monitor by database security solution?

(A) Database changes
(B) Sensitive data access
(C) Database complexity
(D) Security events

Q13 What does it mean for a user to access a database through a multi-tier infrastructure?

(A) The user accesses the database through web or application servers
(B) The user opens connections to multiple databases simultaneously
(C) Each user connection to the database is layered to improve performance
(D) Multiple levels of access to the database are available to the user

Q14 Inference consists of several type of attack. Which is not one of it?

(A) Direct
(B) Indirect
(C) Undirect
(D) All of the above

Q15 Data always be considered in only two categories, which are _____.

(A) Public and Private
(B) Open and Close
(C) Encrypt and Decrypt
(D) Sensitive and Non-sensitive

Q16 Which of the following make a network vulnerable to interception?

i. Anonymity
ii. Sharing
iii. Complexity of system
iv. Operation system

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

Q17 Attackers use Trojan horse to hack the victim machine. Which are the type of security attack involve?

(A) Distributed denial-of-service (DDoS)
(B) Denial-of-service (DoS)
(C) Man-in-the-middle (MitM)
(D) Eavesdropping attack

Q18 Which of the following is an example of passive reconnaissance?

(A) Telephonic calls to target victim.
(B) Attacker as a fake person for Help Desk support.
(C) Talk to the target user in person.
(D) Search about target records in online people database.

Q19 _____ is the information gathering phase in ethical hacking from the target user.

(A) Reconnaissance
(B) Scanning
(C) Gaining access
(D) Maintaining access

Q20 Legal devices to protect the rights of developers and owners of programs and data are as follow except _____.

(A) patents
(B) copyrights
(C) Trade Secrets
(D) Malicious Access

PART B: Subjective Questions. (80 marks)

Q21 (a) Alice and Bob write encrypted messages to each other using a combination of Caesar and Rail Fence cipher. Specifically, each message is first encrypted using Caesar cipher with the key value K, and then such obtained ciphertext is further encrypted using Rail Fence cipher with M rails.

You have managed to seize one of their messages, as shown below. The only clue that you know about this message is that it contains **exactly one 3-letter word 'the'**. The other words are either longer or shorter than 'the'.

zlfxwhbhzo_rth_k_qp_oquhh

Your task is to decrypt the given message, and in doing so to determine the value of K and M that Alice and Bob are used.

(12 marks)

(b) Illustrates the diagram to show asymmetric encryption process between Alice and Bob for following purposes:

(i) Message confidentiality

(ii) Message authentication

Use components from **Figure Q21** to complete your answer.

(8 marks)

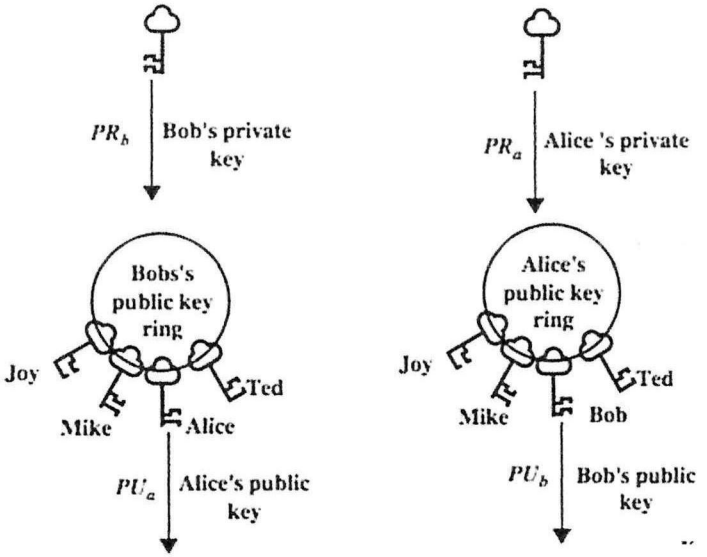

Figure Q21

Q22 (a) Passwords are still the most common method of user authentication. State FOUR (4) problems of using passwords.

(4 marks)

(b) Explain FOUR (4) basic steps needed to secure the operating system?

(4 marks)

(c) They are many attackers that we cannot know. First consider the motives of attackers. Focusing on motive may give some idea of who might attack a networked host or user. Discover THREE (3) important motives.

(6 marks)

(d) You are the IT manager of a company that provides laptop PCs to its sales employees. You are concerned about the security implications. This is because the sales staff can store sensitive data on their laptop PCs and then use them for email.

Identify TWO (2) risks to data on a laptop PC and briefly discuss how each risk can compromise the confidentiality, integrity or availability of the data.

(6 marks)

Q23 Maintaining data integrity and security are important for several reasons.

(a) What is the meaning of data standards?

(2 marks)

(b) Suppression and Concealing are two controls applied to data items. Briefly explain what these two methods are?

(4 marks)

(c) Discuss FOUR (4) requirements for database security.

(4 marks)

(d) Classify FIVE (5) database security threats and countermeasures.

(10 marks)

Q24 (a) IPsec is a suite of protocols for securing networks. Briefly outline how it provides confidentiality, integrity and authentication.

(3 marks)

(b) Draw a diagram to show where IPSec fits in the TCP/IP model.

(2 marks)

(c) Give TWO (2) examples of buffer flows as nonmalicious program error.

(4 marks)

(d) Alice and Bob are having another debate about computer and network security. Alice says that it is the job of security professionals to find all vulnerabilities and every threat and make sure the system is always 100% secure. Do you agree with Alice? You should explain your answer with FIVE (5) reasons.

(11 marks)

-END OF QUESTIONS -