UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER I
SESSION 2017/2018

COURSE NAME	:	CORPORATE SECURITY ENGINEERING
COURSE CODE	:	BIS 33103
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	DECEMBER 2017 / JANUARY 2018
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER **ALL** QUESTIONS IN THIS QUESTION BOOKLET

THIS QUESTION PAPER CONSISTS OF **TEN (10)** PAGES

SECTION A
Choose the BEST answer for each of the following questions.

Q1 What security principle helps prevent users from accessing memory spaces assigned to applications being run by other users?

A. Separation of privilege.
B. Layering.
C. Process isolation.
D. Least privilege.

Q2 Which Bell LaPadula property keeps lower level subjects from accessing objects with a higher security level?

A. * (star) Security Property.
B. No write up property.
C. No read up property.
D. No read down property.

Q3 What is a covert channel?

A. A method that is used to pass information and that is not normally used for communication.
B. Any communication used to transmit secret or top secret data.
C. A trusted path between the TCB and the rest of the system.
D. Any channel that crosses the security perimeter.

Q4 Which of the following is a principle of the Confidentiality, Integrity, Availability (CIA) Triad that means authorized subjects are granted timely and uninterrupted access to objects?

A. Identification.
B. Availability.
C. Encryption.
D. Layering.

Q5 Which of the following is **NOT** considered a violation of confidentiality?

A. Stealing passwords.
B. Eavesdropping.
C. Hardware destruction.
D. Social engineering.

Q6 Which of the following describes the freedom from being observed, monitored, or examined without consent or knowledge?

A. Integrity.
B. Privacy.
C. Authentication.
D. Accountability.

Q7 What ensures that the subject of an activity or event cannot deny that the event occurred?

A. CIA Triad.
B. Abstraction.
C. Nonrepudiation.
D. Hash totals.

Q8 Which of the following is typically **NOT** a characteristic considered when classifying data?

A. Value.
B. Size of object.
C. Useful lifetime.
D. National security implications.

Q9 What is the **MOST** common method of distribution for viruses?

A. Unapproved software
B. E-mail
C. Websites
D. Commercial software

Q10 How to prevent virus infections in case of technical control cannot be used?

A. Security baselines.
B. Awareness training.
C. Traffic filtering.
D. Network design.

Q11 Who does not need to be informed when records about their activities on a network are being recorded and retained?

A. Administrators.
B. Normal users.
C. Temporary guest visitors.
D. No one.

Q12 What is the **BEST** form of antivirus protection?

A. Multiple solutions on each system.
B. A single solution throughout the organization.
C. Concentric circles of different solutions.
D. One-hundred-percent content filtering at all border gateways.

Q13 Which of the following is **NOT** a security-focused design element of a facility or site?

A. Separation of work and visitor areas.
B. Restricted access to areas with higher value or importance.
C. Confidential assets located in the heart or center of a facility.
D. Equal access to all locations within a facility.

Q14 Which of the following is a double set of doors that is often protected by a guard and is used to contain a subject until their identity and authentication is verified?

A. Gate.
B. Turnstile.
C. Mantrap.
D. Proximity detector.

Q15 What is the **MOST** important goal of all security solutions?

A. Prevention of disclosure.
B. Maintaining integrity.
C. Human safety.
D. Sustaining availability.

(30 marks)

SECTION B

Q16 Describe **FOUR (4)** causes of information loss.

(4 marks)

Q17 Recommend **THREE (3)** important factors to consider an offsite storage facility site for University Tun Hussein Onn Malaysia (UTHM).

(6 marks)

Q18 UTHM Holding is to provide Virtual Private Network (VPN) access to its mobile team servicing its clients. The team will access the headquarters corporate resources via several remote workstations. Propose **THREE (3)** countermeasures to reduce security risks at the remote workstations.

(9 marks)

Q19 UTHM used metal keys to unlock doors to some of its server room.

(a) Why metal keys are discouraged for use as a primary access controls?

(4 marks)

(b) Suggest **TWO (2)** situations in which metal keys are suitable for use as a secondary access control.

(4 marks)

(c) A strict procedure is necessary to manage the distribution of these metal keys. Recommend **TWO (2)** procedures to help UTHM achieved this goal.

(4 marks)

Q20 Describe **FIVE (5)** duties of a security guards at UTHM gates.

(5 marks)

Q21 A critical power station at UTHM is to be fenced to control intrusion. Recommend **TWO (2)** possible heights and describe its effectiveness.

(6 marks)

Q22 Ten staffs are working in a UTHM main server room. A result of an inspection found out that the relative humidity level in the room is at 21%. As a security specialist, assess whether this level is suitable for human and equipment. State your recommendation and reasoning.

(8 marks)

-END OF QUESTION-