الاختبار ☑النهائي ☐ البديل

الإجابة على نفس الورقة

الدبلوم: أمن سيبراني	المستوى: الثالث
اسم المقرر: مبادئ التصميم في الامن السيبراني	الشعبة:
رمز المقرر: 0103 سبر	زمن الاختبار:

الاسم:.....
الرقم الجامعي: .....
الشعبة:.....
اليوم:.....
التاريخ :.....

رقم السؤال	الدرجة		توقيع المصحح	توقيع المدقق
	رقماً	كتابة		
الأول				
الثاني				
الثالث				
الرابع				
المجموع				
درجة الأعمال الفصلية				
المجموع الكلي				

Q1: Choose the correct answer: 10 points

#	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Answer	D	D	A	A	A	B	D	C	C	D	A	C	B	A	C	B	B	B	D	B

1) In modular design, the goal is to have each component meet conditions that are:
   A) Simple.
   B) Small.
   C) Single purpose.
   D) A, B, and C.

2) What principle is focused on conflict of interest where a certain user should not be accessing confidential information belonging to two separate interested and/or participating stakeholders:
   A) Biba Model or Biba Integrity Model.
   B) The Harrison–Ruzzo–Ullman model.
   C) The Clark-Wilson Model.
   D) The Chinese Wall models.

3) The elements of Clark-Wilson model are:
   A) Users, TPs, CDIs, IVPs and UDIs.
   B) CIA-T.
   C) HRU, Chinese wall, Biba
   D) Access, Manage, and Audit.

4) The common factor between SoD and Least Privilege is?
   A) Easy to trace.
   B) Easy to attack.
   C) They should be public.
   D) There is no privileges.

5) What is Least Privilege Principle in Cybersecurity?
   A) It is the principle that system users and applications should only have the necessary privileges to complete their required tasks.
   B) It involves dividing critical tasks to minimize the risk of a single individual subverting a system or critical process without detection.
   C) A, B
   D) It means secure software development.

6) The goal of modular design in a system is to:
   A) Have better maintenance of the system
   B) Minimize the complexity of the system
   C) Improve performance of the system
   D) All of the above

7) Cohesion is:
   A) The degree to which the user or a component depends on the trustworthiness of another component.
   B) The degree to which the security behavior of the component is demonstrably compliant with its stated functionality.
   C) The degree with which a component depends on other components in the system.
   D) The degree to which the elements of the module are functionally related, and every aspect of the component is tied to the component's single purpose.

8) To protect against errors and risks, as well as reduce surprises, the organization must provide:
   A) Risk management.
   B) Product Management.
   C) Management support.
   D) Technical support.

9) Providing a user with a enough rights on their PC is an example of ….. .
   A) Separation of duties principle
   B) Defense in depth principle
   C) Least privilege principle
   D) Modular design principle

10) It could be considered an add-on to the BLP model:
   A) Biba model
   B) Clark Wilson model
   C) Chinese wall model
   D) HRU model

11) "Unauthorized insiders trying to access servers and data" It is one of ways to:
   A) Detect security incidents.
   B) Modular design.
   C) Simplification.
   D) Minimization.

12) An example of data security of Multi-Layers of security defense is:
   A) Firewall
   B) IDS
   C) Encryption
   D) VPN

13) Multi-layered security related to the defense in depth, which is based on a slightly different idea where:
   A) Multi-layer is easier than defense in depth.
   B) Strategies and resources are used to slow or delay or hinder a threat.
   C) Defense in depth is more comprehensive han multi-layer.
   D) There is no different between them.

14) Which one of the following principles is one of Zero Trust seeks key principles based on the NIST guidelines:
   A) Continuous verification
   B) Polices
   C) Simplicity.
   D) Safety.

15) To identify threats or risks to assets ask we need to answer:
   A) Who or what could cause it harm?
   B) How could this occur?
   C) A,B
   D) What is the threats?

16) Biba model rules:
   A) Allowed – "READ DOWN" \ "WRITE UP"
   B) Allowed – "READ UP" \ "WRITE DOWN"
   C) Disallowed all the rules.
   D) Allowed all the rules.

17) The main aim of incident response:
   A) It is to increase security cost.
   B) It is to contain the threat, reducing the cost and recovery time associated with handling a breach or cybercriminal attack.
   C) It is used to apply security requirements.
   D) It is used to reduce cyber resilience.

18) **"Hardening"** a system means:
   A) It is a centralized piece of code through which control must pass
   B) All unnecessary services off by default.
   C) Add extra functionalities and services
   D) Remove or disable code known to create vulnerabilities.

19) Threats in cybersecurity includes:
   A) Physical breach to data
   B) Natural disasters
   C) XSS Vulnerabilities
   D) All of the above

20) Security measures that prevent physical access to IT systems, such as security guards or locked doors, are:
   A) Technical controls.
   B) Physical controls.
   C) Administrative controls.
   D) Accounts controls.

Q2: Put (T) for correct sentences and (F) for wrong sentences: <u>10 points</u>

#	Question	Answer
1	In Separation of Duties it should only one person should oversee an entire critical task from beginning to end	F
2	Security classes control the manner by which a subject may access an object	T
3	Optimize is one of zero trust steps	F
4	A multi-layered security strategy is slow method of detecting and eliminating threats at multiple levels.	F
5	One of the Design approach advantages is that non-security experts can naturally write a secure code	T
6	Email security and antivirus can help mitigate the risks posed by malware	T
7	The goal of modular design is to manage complexity by minimizing the complexity of each module	T
8	The worst enemy of security is simplicity	F
9	In multi-layered security the layers strengthen defenses and provide a solid foundation for cyber security program	T
10	Encapsulation and information hiding are not good security practices because they lead to modules that can't be understood, analyzed, and trusted.	F
11	Safety is "The state of being away from hazards caused by deliberate intention of human to cause harm. The source of hazard is posed by human deliberately"	F
12	Identify assets in the organization is including only tangible assets.	F
13	Zero Trust assumes that there is no traditional network edge	T
14	"Having design patterns available can also lead to people believing that apparently all problems can be solved using existing design patterns" is one of design patterns advantages	F
15	The principle of least privilege can't support the separation of duties	F
16	Creational, Structural, and Behavioral are the types of design patterns	T
17	Biba model and BLP model have the same implementation and rules.	F
18	The simplicity allows system designers and programmers to identify unwanted access paths.	T
19	In the modular design a module's interface should be easy to use, easy to understand and easy to ensure correctness.	T
20	It's better to view security as a concern to be met than to view it as a set of features to implement.	T

Q3: Answer the following: 10 points.

1) What are the components of Access Control?
   1. Authentication
   2. Authorization
   3. Access
   4. Manage
   5. Audit

2) What are the phases of incident response?
   1. The preparation phase
   2. The detection and analysis phase
   3. The containment, eradication, and recovery phase
   4. The post-event activity phase.

3) Benefits Of Implementing Modular design:
   1. Maintenance
   2. Understandability
   3. Reuse
   4. Correctness
   5. Testing
   6. Scalability

4) What are Stages of Implementing Zero Trust?
   1. Visualize
   2. Mitigate
   3. Optimize

5) Define IT Security Management
   It is a process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity and reliability.

Q4: Match the correct answer from column A to column B: 10 points

#	A	The answer	B
1	It is a weakness in an asset or group of assets which can be exploited by a threat.	7	Choke point
2	Better system stability, minimize attacks, ..etc.	6	BLP model
3	Using design patterns requires extensive knowledge.	10	Disadvantages of complexity in security
4	Confidentiality, integrity, availability, etc.	8	Intent
5	Define the Attack Surface, Implement Controls Around Network Traffic, etc.	5	Steps of zero trust.
6	Primary Security Goal: Confidentiality	3	Disadvantages of design patterns.
7	It is a centralized piece of code through which control must pass	1	Vulnerability
8	the difference between security and functional safety can be summed up in word	4	Security concerns
9	Layers of Defense in Cybersecurity	2	Benefits of implement least privilege
10	It makes vulnerabilities harder to fix once we find them	9	Endpoint security