الاختبار ☐النهائي ☑ البديل

الإجابة على نفس الورقة

الدبلوم : امن 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	A	B	A	A	B	D	C	C	D	A	C	C	B	D	C	A	A	A	B	C

1) In modular design which one of the following is one of conditions to meet in the component:
   A) Simple.
   B) Large.
   C) Multi-purpose.
   D) A,B, and C.

2) What is the model that addresses these issues by defining an authorization system to allocate access rights and verifying compliance with any given policy preventing non-authorized access:
   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:
   A) Users, TPs ,CDIs, IVPs and UDIs.
   B) CIA-T.
   C) HRU, Chinese wall, Biba
   D) Access, Manage, and Audit.

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

5) What is Separation of duties?
   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) What is the Cybersecurity definition?
   A) It means data is at hand in a timely manner.
   B) It means secure software development.
   C) It is the guiding principle for how a system is built and is applicable on all levels, from code to architecture.
   D) It is protecting computer systems from unauthorized access or being otherwise damaged or made inaccessible.

7) Coupling 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) What is the meaning of Minimization?
   A) Simplifying the task of managing security.
   B) Complex the task.
   C) The state of being complicated.
   D) Minimize the size, quantity, and complexity.

10) What is the model that is revers of BLP model:
   A) Biba model.
   B) Clark Wilson model
   C) Chinese wall model
   D) HRU model

11) "Evaluate What You Need From Multipurpose Security Suites" It is one of ways to:
   A) Detect security incidents.
   B) Modular design.
   C) Simplification.
   D) Minimization.

12) The goal of "Analyze Risks" is:
   A) More security.
   B) Less attacks.
   C) To order resulting risks to treat them.
   D) To protect systems.

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 secure than multi-layer.
   D) There is no different between them.

14) What is the best answer of the following principles of Zero Trust seeks key principles based on the NIST guidelines:
   A) Continuous verification
   B) Limit the "blast radius"
   C) Automate context collection and response.
   D) A,B, and C.

15) To identify assets we need to collect information of:
   A) "Anything which needs to be protected."
   B) Tangible or intangible
   C) A,B
   D) What is the assets?

16) BLP 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 incident response is:
   A) enacted to reduce recovery times and costs associated with the compromise of systems.
   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 achieve cybersaftey.

18) "Choke point" is:
   A) It is a centralized piece of code through which control must pass
   B) All unnecessary services off by default.
   C) Remove unnecessary interfaces and functionality.
   D) Remove or disable code known to create vulnerabilities.

19) Threats may be:
   A) The goal of security
   B) Natural disasters or Man-made and either accidental or deliberate
   C) A,B.
   D) Cybersaftey.

20) ---------- "are security measures consisting of policies or procedures directed at an organization's employees, e.g., instructing users to label sensitive information as "confidential" which is the best answer:
   A) Technical controls.
   B) Physical controls.
   C) Administrative controls.
   D) Accounts controls.

Q2: Put (T) for correct sentences and (F) for wrong sentences: 10 points

#	Question	Answer
1	In Separation of Duties, it should no one can oversee an entire critical task from beginning to end	T
2	Security classification control the manner by which a subject may access an object	F
3	Optimize is one of zero trust stages	T
4	A multi-layered security strategy is efficient and effective method of detecting and eliminating threats at multiple levels.	T
5	One of the Design approach disadvantages is that non-security experts can naturally write a secure code	F
6	Low cohesion between modules is better than high or tight cohesion	F
7	A well-designed modular system minimizes the dependencies between modules	T
8	The worst enemy of security is complexity	T
9	In multi-layered security the layers make defenses weaker and provide a weak foundation for cyber security program	F
10	Encapsulation and information hiding are good security practices because they lead to modules that can be understood, analyzed, and trusted.	T
11	Security 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"	T
12	Identify assets in the organization is including tangible and intangible assets.	T
13	Zero Trust assumes that there is traditional network edge	F
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 disadvantages	T
15	The principle of least privilege can support the separation of duties	T
16	Creational, Structural, and Behavioral are the types of Zero trust	T
17	Biba model and BLP model have reverse implementation and rules.	T
18	The complexity allows system designers and programmers to identify unwanted access paths.	F
19	In the modular design a module's interface shouldn't be easy to use, easy to understand and easy to ensure correctness.	F
20	It's better to view security as a feature to be met than to view it as a concern to implement.	F

Q3: Answer the following: 10 points.

1) What is the meaning of Access Control?

Access control is a data security process that enables organizations to manage who is authorized to access corporate data and resources. Secure access control uses policies that verify users are who they claim to be and ensures appropriate control access levels are granted to users.

2) What are the different ways to detect incident response?

1. Unusual behavior from privileged user accounts.
2. Unauthorized insiders trying to access servers and data.
3. Anomalies in outbound network traffic.
4. Traffic sent to or from unknown locations.
5. Changes in configuration.
6. Hidden files.
7. Unexpected changes.
8. Abnormal browsing behavior.
9. Suspicious registry entries.

3) Advantages of design patterns:

1. Reusability in countless projects to solve problems with a common pattern
2. Spend less time figuring out how to solve a particular issue
3. Spend a safe time on implementing the solution and improve the quality of the software product
4. Provides more value for the money

4) What are Steps of Implementing Zero Trust?

1. Define the Attack Surface.
2. Implement Controls Around Network Traffic.
3. Architect a Zero Trust network.
4. Create a Zero Trust Policy.
5. Monitor Your Network.

5) Define Confidentiality

Most often associated with talking about security, is about keeping things secret that shouldn't be made known to the public. Your healthcare record is one of the best examples of confidential information.

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.	3	Disadvantages of design patterns.
2	Better system stability, minimize attacks, ..etc.	1	Vulnerability
3	Using design patterns requires extensive knowledge.	4	Security concerns
4	Confidentiality, integrity, availability, etc.	2	Benefits of implement least privilege
5	Define the Attack Surface, Implement Controls Around Network Traffic, etc.	9	Endpoint security
6	Primary Security Goal: Integrity	7	Hardening system
7	All unnecessary services off by default.	6	Biba model
8	the difference between security and functional safety can be summed up in word	10	Disadvantages of complexity in security
9	Layers of Defense in Cybersecurity	8	Intent
10	It makes vulnerabilities harder to fix once we find them	5	Steps of zero trust.