Total No. of Questions: 6 *Total No. of Printed Pages:3*

Enrollment No.....

Faculty of Engineering

End Sem (Even) Examination May-2022

CB3CO13 Information Security

Programme: B.Tech. Branch/Specialization: CSBS

Duration: 3 Hrs. **Maximum Marks: 60**

Note: All questions are compulsory. Internal choices, if any, are indicated. Answers of Q.1 (MCQs) should be written in full instead of only a, b, c or d.

Q.1 i. The Lack of access control policy is a _____. **1**

(a) Bug (b) Threat

(c) Vulnerability (d) Attack

ii. Possible threat to any information cannot be _____. **1**

(a) Reduced (b) Transferred

(c) Protected (d) Ignored

iii. Information security policies are usually the result of risk assessments, in which vulnerabilities are identified and safeguards are chosen. **1**

The above statement is:

(a) Correct (b) Incorrect

(c) Partially correct (d) Can't say anything.

iv. Which of the following refers to stealing one's idea or invention of others and use it for their own benefits? **1**

(a) Piracy

(b) Plagiarism

(c) Intellectual property rights

(d) All of these

v. Which one of the following principles of cyber security refers that the security mechanism must be as small and simple as possible? **1**

(a) Open-Design (b) Economy of the Mechanism

(c) Least privilege (d) Fail-safe Defaults

vi. Which of the following is just opposite to the Open Design principle? **1**
(a) Security through obscurity
(b) Least common mechanism
(c) Least privileges
(d) Work factor

vii. In the computer networks, the encryption techniques are primarily used for improving the _____. **1**
(a) Security (b) Performance
(c) Reliability (d) Longevity

viii. _____ typically creates a secure, encrypted virtual "tunnel" over the open internet. **1**
(a) Trojan (b) Worm (c) Virus (d) None of these

ix. Which one of the following is considered as the most secure Linux operating system that also provides anonymity and the incognito option for securing the user's information? **1**
(a) Ubuntu (b) Tails (c) Fedora (d) All of these

x. Suppose an employee demands the root access to a UNIX system, where you are the administrator; that right or access should not be given to the employee unless that employee has work that requires certain rights, privileges. It can be considered as a perfect example of which principle of cyber security? **1**
(a) Least privileges (b) Open Design
(c) Separation of Privileges (d) Both (a) and (c)

Q.2 i. Define Confidentiality and Integrity in Information security. **4**
ii. What is the difference between attack and vulnerability? List and define any four attacks. **6**
OR iii. What are different phases of Security Systems Development Life Cycle. Explain them in brief. **6**

Q.3 i. What is a security policy? What is its importance? **4**
ii. Describe three major types of security policies. **6**

OR iii. Brief about the elements of an Issue-Specific Security Policy Statement. **6**

Q.4 i. What is information Security Blueprint? **4**
ii. List and explain the different types of access control. **6**
OR iii. How evaluation takes place to build a system with assurance? **6**

Q.5 i. What are security Audits? How are they performed? **4**
ii. What is digital forensics? Write steps to be performed during digital investigation. **6**
OR iii. What is intrusion detection system? Explain its categories and operating models in detail. **6**

Q.6 Attempt any two:
i. Explain the security architecture design process with neat sketch. **5**
ii. What are the possible threats/attacks database? Define any five of them. **5**
iii. What are the different security features available in UNIX/LINUX based operating system? Describe any five. **5**

******

Marking Scheme
CB3CO13 Information Security

Q.1	i.	The Lack of access control policy is a _____. (c) Vulnerability	**1**
	ii.	Possible threat to any information cannot be _____. (d) Ignored	**1**
	iii.	Information security policies are usually the result of risk assessments, in which vulnerabilities are identified and safeguards are chosen. The above statement is: (a) Correct	**1**
	iv.	Which of the following refers to stealing one's idea or invention of others and use it for their own benefits? (a) Piracy	**1**
	v.	Which one of the following principles of cyber security refers that the security mechanism must be as small and simple as possible? (b) Economy of the Mechanism	**1**
	vi.	Which of the following is just opposite to the Open Design principle? (a) Security through obscurity	**1**
	vii.	In the computer networks, the encryption techniques are primarily used for improving the _____. (a) Security	**1**
	viii.	_____ typically creates a secure, encrypted virtual "tunnel" over the open internet. (d) None of these	**1**
	ix.	Which one of the following is considered as the most secure Linux operating system that also provides anonymity and the incognito option for securing the user's information? (b) Tails	**1**
	x.	Suppose an employee demands the root access to a UNIX system, where you are the administrator; that right or access should not be given to the employee unless that employee has work that requires certain rights, privileges. It can be considered as a perfect example of which principle of cyber security? (a) Least privileges	**1**

Q.2	i.	Confidentiality in Information security		2 marks	**4**
		Integrity in Information security		2 marks	
	ii.	Difference between attack and vulnerability		2 marks	**6**
		Definition of any four attacks	(1 mark * 4)	4 marks	
OR	iii.	Different six phases	(1 mark * 6)	6 marks	**6**
Q.3	i.	Definition of security policy		2 marks	**4**
		Its importance		2 marks	
	ii.	Any three major types	(2 marks *3)	6 marks	**6**
OR	iii.	Any six elements	(1 mark * 6)	6 marks	**6**
Q.4	i.	Information Security Blueprint		4 marks	**4**
	ii.	List of access control		2 marks	**6**
		Explanation of access control		4 marks	
OR	iii.	Evaluation process			**6**
		As per explanation		6 marks	
Q.5	i.	Security Audits		2 marks	**4**
		How are they performed		2 marks	
	ii.	Digital forensics		2 marks	**6**
		Steps to be performed		4 marks	
OR	iii.	Intrusion detection system		2 marks	**6**
		Its categories and operating models		4 marks	
Q.6		Attempt any two:			
	i.	Explanation		3 marks	**5**
		Diagram		2 marks	
	ii.	List of possible threats/attacks		1 mark	**5**
		Any four definitions	(1 mark * 4)	4 marks	
	iii.	Any five features	(1 mark * 5)	5 marks	**5**

******