Register Number:……………..

KUMARAGURU
college of technology
character is life

## B.TECH DEGREE EXAMINATIONS: MAY 2017

(Regulation 2014)

Sixth Semester

## INFORMATION TECHNOLOGY

U14ITTE62: Information Security

### COURSE OUTCOMES

**CO1:** Describe threats to information security and security SDLC.

**CO2:** Identify the security threats and attacks.

**CO3:** Analyze the mechanism to assess and control risk.

**CO4:** Describe the types of security policies and standards

**CO5:** Identify security issues related to personnel decisions, and qualifications of security personnel.

**Time: Three Hours** **Maximum Marks: 100**

**Answer all the Questions:-**

**PART A (10 x 1 = 10 Marks)**

1. Match the List I with List II CO2 [K$_3$]

| **List I** | **List II** |
|---|---|
| A. Mandatory Access Control | i. Uses identity of subject |
| B. Discretionary Access Control | ii. Lattice-based control |
| C. Role-based Access Control | iii. Rule-based |
| D. Non-discretionary control | iv. Uses a subject’s task |

| | A | B | C | D |
|---|---|---|---|---|
| a) | ii | i | iii | iv |
| b) | iii | iv | ii | i |
| c) | ii | iv | iii | i |
| d) | iii | i | iv | ii |

2. The risk that has not been completely avoided is known as _________. CO3 [K$_2$]

a) Threat b) Mitigation

c) Residual risk d) Extortion

3. Actions involved in risk analysis are, CO3 [$K_3$]

1.Determine which assets are most valuable

2. Assign value to asset

3. Determine the likelihood of each risk occurring

4. Focuses on analyzing intangible properties

a) 1,3 b) 1,4

c) 1,2 d) 2,3

4. Luring attackers from physical system is called ____________. CO2 [$K_2$]

a) Honey pot b) Distraction

c) Honey Net d) Fly Trapping

5. Assertion (A): Packet-filtering Routers has lack of auditing and strong authentication CO4 [$K_3$]

Reason (R): The complexity of the access control lists degrades network performance

a) Both A and R are Individually true and R is the correct explanation of A b) Both A and R are Individually true but R is not the correct explanation of A

c) A is true but R is false d) A is false but R is true

6. Match the List I with List II CO3 [$K_3$]

| **List I** | **List II** |
|---|---|
| A. Risk Avoidance | i. Buy insurance |
| B. Risk Mitigation | ii. Disable mail |
| C. Risk Acceptance | iii. Firewall |
| D. Risk Transference | iv. Small risk |

| | A | B | C | D |
|---|---|---|---|---|
| a) | ii | i | iii | iv |
| b) | iii | iv | ii | i |
| c) | ii | iii | iv | i |
| d) | iii | i | iv | ii |

7. The sequence of Information security phases are CO1 [$K_2$]

1. Analysis Phase
2. Physical Design Phase
3. Investigation phase
4. Logical Design Phase

a) 2-3-4-1 b) 1-3-2-4

c) 3-4-2-1 d) 3-1-4-2

8. Types of fabrication attack CO2 $[K_2]$

1. Tampering a resource
2. Impersonation
3. Masquerading
4. Confidentiality attack

a) 1,3 b) 1,4

c) 2,3 d) 2,4

9. Assertion (A): Hardware firewalls have faster processing possible for high-bandwidth environments. CO5 $[K_3]$

Reason (R): More expensive than software firewalls.

a) Both A and R are Individually true and R is the correct explanation of A b) Both A and R are Individually true but R is not the correct explanation of A

c) A is true but R is false d) A is false but R is true

10. The steps in vulnerability assessment are CO4 $[K_2]$

1.Scanning

2.Record Keeping

3.Planning and Target selection

4.Analysis

a) 1-4-3-2 b) 3-1-4-2

c) 1-3-4-2 d) 1-2-3-4

## PART B (10 x 2 = 20 Marks)
## (Answer not more than 40 words)

11. List three components of the C.I.A. triangle? Why is it incompetent? CO1 $[K_3]$

12. What is an asset? List its types. CO3 $[K_2]$

13. Compare exploit and vulnerability. CO3 $[K_2]$

14. State the reason for command injection problem. CO2 $[K_2]$

15. Differentiate discretionary and non discretionary access controls. CO4 $[K_2]$

16. State the methods for data interception. CO2 $[K_2]$

17. Outline an attack profile CO3 $[K_2]$

18. State the disadvantages of network IDPS. CO4 $[K_2]$

19. State the principle of Kerberos. CO5 $[K_2]$

20. How is a vulnerability list prepared? CO5 $[K_2]$

**Answer any FIVE Questions:-**
**PART C (5 x 14 = 70 Marks)**
**(Answer not more than 300 words)**

**Q.No. 21 is Compulsory**

21. Compare phases of SDLC and Sec SDLC models. CO1 $[K_3]$

22. Analyze the parameters that are necessary to calculate, estimate or derive values for information assets. CO1 $[K_2]$

23. Summarize the major types of attacks used in controlled systems and suggest means to avoid them. CO2 $[K_3]$

24. i) Outline steps for preparation of blueprint for security. (7) CO4 $[K_2]$
ii) Describe the security principles covered by NIST model. (7) CO4 $[K_2]$

25. Identify the threats and possible vulnerabilities for each threat. CO3 $[K_2]$

26. Describe the Plan-Do-Check-Act cycle as described by ISO 27000 series. CO4 $[K_3]$

27. Describe the various types of intrusion detection and prevention systems. State the advantages of each of them. CO5 $[K_3]$

************