Seat No.: ________ Enrolment No.______________

GUJARAT TECHNOLOGICAL UNIVERSITY

MCA – SEMESTER – III • EXAMINATION – SUMMER 2018

Subject Code: 3630012 **Date: 29-May-2018**

Subject Name: Information Security

Time: 02.30 pm to 5.00 pm **Total Marks: 70**

INSTRUCTIONS

(i) Attempt all the questions
(ii) Numbers indicated to the right are the full marks
(iii) Draw diagrams where necessary.
(iv) Figures on the right indicate Marks

Q:1 (a) Answer the following **06**

1 Vulnerability
2 Threat
3 Confidentiality
4 Unexpected Behaviour
5 Reconnaissance
6 Incomplete Mediation

Q:1 (b) Answer the following **08**

1 What is Interception? Give one example
2 Give two examples of vulnerabilities in automobile for which company
3 List different Hacker categories
4 Stream Cipher

Q.2 Answer the following

(a) On a typical Multi-user computing system (e.g., shared Unix/Linux at a company), who can modify the OS code of Payroll, a program developed and run by single user. According to you, who should be permitted to modify the code? **07**

(b) Discuss different types of faults. How would you fix them? **07**

OR

(b) What is Buffer Overflow? How can you overflow the program stack? Discuss with an example.. **07**

Q.3 Answer the following

(a) Discuss major Buffer overflow problems in Internet Information Services (IIS), the default Windows Web Server. **07**

(b) What is incomplete Mediation? What are the ways to resolve them? **07**

OR

Q.3 Answer the following

(a) Explain Clark-Wilson Commercial Security Policy **07**

(b) What is separation of Duty? Describe the Multilevel Security Policy. **07**

Q.4 Answer the following

(a) How SQL can be used to attack systems? Explain importance of special characters in SQL that can be used for attacks. **07**

(b) Discuss different ways by which vulnerabilities are introduced in the Networks. **07**

OR

Q.4 (a) (1) What is a Business Continuity Plan? Explain in detail with important characteristics. **04**

(2) How do you respond to a security incident? Discuss Incident response plan. **03**

(b) Discuss in detail Graham-Denning form Security model. **07**

Q.5 **Answer the following**

(a) (1) Discuss different ways by which vulnerabilities are introduced in the Networks. **04**

(2) Differentiate Active and Passive Attacks. How does an insider attack affects the network? **03**

(b) Discuss different countermeasures to Block, Prevent, and/or Defend the Network against Port Scanning. **07**

OR

Q.5 **Answer the following**

(a) (1) What is NSLookup? Explain the Command with options **04**

(2) If you live in country A and receive a certificate signed by a government certificate authority in country B, what conditions would cause you to trust that signature as authentic? **03**

(b) Discuss Confidentiality, Integrity and Availability for assets like Hardware, Software, Data, People and Supplies with a Matrix. **07**