Seat No: _____ **Enrollment No: _____**

PARUL UNIVERSITY

FACULTY OF IT & COMPUTER SCIENCE

MCA Winter 2019 – 20 Examination

Semester: 04 **Date: 12/12/2019**
Subject Code: 05201284 **Time: 2:00 pm to 4:30 pm**
Subject Name: Information Security and Cyber Forensics **Total Marks: 60**

Instructions:
1. All questions are compulsory.
2. Figures to the right indicate full marks.
3. Make suitable assumptions wherever necessary.
4. Start new question on new page.

Q.1 Answer the followings.

A. Answer / Define the following in short. **(05)**

1. What is Passive eavesdropping?
2. What are the benefits of OS Patching Service?
3. Define vulnerability.
4. What is Trust model?
5. Define Threat model.

B. Fill in the blanks / Mark True or False. (Each of 01 marks) **(10)**

1. 802.11 is the most widely used standard among _____ standards.
2. _____ is useful to counter eavesdropping, or to obstruct jamming of local area network.
3. _____ reduces the exposure to attack.
4. A _____ attempts to learn or make use of information from the system but does not affect system resources.
5. The _____ acts as an intermediary between application programs and the computer hardware.
6. Foreign Espionage is also known as sniffing or eavesdropping. (True / False)
7. An IDS also can log various types of traffic on the network for analysis later. (True / False)
8. Photos of physical (electronic) evidence establish the chain of custody and make it less authentic. (True / False)
9. Anti-computer forensics is a set of techniques used as countermeasures to digital forensic analysis. (True / False)
10. Forensic examiners have to conduct well-defined procedures when dealing with digital handheld devices. (True / False)

Q.2 Answer the followings. (3 Marks Questions.) (Any Five) **(15)**

1. Brief IDS and VPN.
2. Justify Buffer overflow is less dangerous than stack overflow with example.
3. What are the legal challenges in forensics?
4. Explain Data management in information security.
5. Explain Operating systems security.
6. List and define Methods of protection.

Q.3 Answer the following. (5 Marks Questions) (Any three) **(15)**

1. List and define Wireless security protocols.
2. What are the technical challenges in forensics? List and define.
3. Explain Network forensics with its examination steps.
4. What traffic protocols and network layers are analyzed in network forensics? Give short description for each.

Q.4 Answer the following in detail.

A. Elaborate Chain of custody in detail. **(05)**

B. (1) Recognize two case studies on virus attacks. **(05)**

B. (2) Elaborate Fence and Base-Bound registers with neat diagram. **(05)**

OR

B. (1) List and elaborate basic security principles for information systems development. **(05)**

B. (2) List out and elaborate WLAN standards. **(05)**