(Time: $2\frac{1}{2}$ hours)

[Total Marks: 60]

N. B.: (1) **All** questions are **compulsory**.
(2) Make **suitable assumptions** wherever necessary and **state the assumptions** made.
(3) Answers to the **same question** must be **written together**.
(4) Numbers to the **right** indicate **marks**.
(5) Draw **neat labeled diagrams** wherever **necessary**.
(6) Use of **Non-programmable** calculator is **allowed**.

1. Attempt *any two* of the following: **12**

a. What is information security? What are the various elements of information security? Explain.
b. What information can be gathered by tracking email communication? Explain.
c. Write a short note on Banner Grabbing.
d. Explain the countermeasures for DNS enumeration and SMTP enumeration.

2. Attempt *any two* of the following: **12**

a. Explain the Vulnerability Management Life Cycle.
b. Explain the various ways to defend against privilege escalation.
c. Explain various components of malware program.
d. What are protocols vulnerable to sniffing? Explain.

3. Attempt *any two* of the following: **12**

a. What are the reasons for insider attacks? Explain.
b. Explain DDOS-attack penetration testing process.
c. Explain session hijacking using CRIME attack.
d. Explain the ways to defend against firewall evasion.

4. Attempt *any two* of the following: **12**

a. What are the various damages caused by attacker on a web server?
b. Explain authorization attack.
c. Explain blind SQL injection.
d. Explain Wi-Fi authentication modes.

5. Attempt *any two* of the following: **12**

a. Explain the ways to defend against SMS phishing attacks.
b. Explain the IoT architecture.
c. Explain Man-in-the-Cloud attack. State its countermeasures.
d. Explain various code-breaking techniques.
