(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. Explain how web application security can be improved by protecting against Distributed Denial-of-Service and Application Layer attacks.
b. Discuss IoT security challenges that threaten the financial safety of both individuals and organizations.
c. What is Fault tolerance? Explain the different levels of fault tolerance in Cloud computing.
d. Explain 3G Security Architecture in detail.

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

a. What Is Vulnerability Assessment? Explain how Vulnerability Assessment tools are helping the organizations in assessment process.
b. Explain the steps involved in Risk Management process.
c. What is Disaster Recovery? Discuss the Disaster Recovery methods used by the organizations.
d. Discuss in detail the elements to be considered for effective disaster recovery plan.

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

a. Discuss the components of Metasploit.
b. Explain the Phases of penetration testing life cycle.
c. Explain the variables of Metasploit.
d. Explain the needs and importance of penetration testing framework in detail.

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

a. Discuss NMAP and Nessus scanning approach in detail.
b. What is Client-side attack? Explain in detail the need of client-side attacks.
c. What is Shellcode? Explain reverse shell and blind shell in detail.
d. Explain Meterpreter in brief.

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

a. What is Metasploit? Explain some basic commands of Metasploit.
b. Explain the architecture of the Metasploit framework.
c. Discuss the basics of Ruby programming language in detail.
d. Explain the Exploiting SEH-based buffer overflows with Metasploit.

C66BA4E19AE80952A80AE3C88D198580