

(3Hours)

[Total Marks: 75]

- 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 labelled diagrams wherever necessary.
(6) Use of Non-programmable calculators is allowed.

Q1. Attempt any three of the following.

15 Marks

- What are Different levels of fault tolerance in Cloud computing?
- Describe the best practices to mitigate vulnerabilities?
- What are Security Issues in Cellular Networks?
- Explain Security Vulnerabilities in Wireless Sensor Networks?
- Write short note on risk management?

Q2. Attempt the three of the following.

15 Marks

- Explain 5 top elements of effective disaster recovery plan?
- What are the types of Disaster Recovery?
- How to build a disaster recovery team?
- Describe insider threat?
- Briefly explain Security Policies and plans development?

Q3. Attempt any three of the following.

15 marks

- What are the phases of penetration testing?
- What is Nessus and write the steps of installation?
- Differentiate between vulnerability assessment & penetration testing.
- Explain Kali Linux & virtual machine.
- Explain Metasploit framework?

Q4. Attempt any three of the following.

15 marks

- Write a note on TCP and UDP.
- Explain client-side attacks with Metasploit.
- Describe Auto exploitation with db autopwn.
- Write a note on NMAP scanning approach.
- Explain Post exploitation.

Q5. Attempt any three of the following.

15 marks

- What is system command of meterpreter?
- Describe working with variable and data types in ruby.
- Explain skeleton of Metasploit module.
- Explain the process for exploiting stack based buffer overflow.
- Explain decision making operators in ruby language.
