

(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 calculators is allowed.

Q1. Attempt the two of the following.

12 Marks

1. Explain the basic concepts of fault tolerance in detail.
2. Write short note on Failure behaviour of the network.
3. Define: i) Data confidentiality ii) Data Integrity iii) Availability.
4. Explain 3G security Architecture in detail.

Q2. Attempt the two of the following.

12 marks

1. Write short note on i) Vulnerability ii) Risk Assessment iii) Remediation
2. How to build a disaster recovery team?
3. Describe: i) Cold site ii) Hot site iii) Disaster Recovery as a service
4. How to develop a security policies? Explain the steps in detail.

Q3. Attempt the two of the following.

12 marks

1. Define: i) Vulnerability assessment ii) Penetration testing
2. Write short note on i) Privilege Escalation ii) Maintaining access iii) Covering tracks
3. Describe Exploits, Payloads and Encoders.
4. With an example explain the basic commands of msfconsole.

Q4. Attempt the two of the following.

12marks

1. How to perform HTTP and SMTP port scan using auxiliary modules in metasploit?
2. Write short notes on i) Password sniffing ii) Shodan
3. Explain msfvenom utility in detail.
4. Explain in detail how to create infectious media drive and Browser Autopwn.

Q5. Attempt the two of the following.

12 marks

1. Explain Decision making operators and Loops in Ruby with a suitable example.
2. Describe the following meterpreter commands with an example i) sysinfo ii) Kill iii) getwd iv) Del v) cat vi) upload and download
3. How to perform penetration testing on unknown network.
4. Write short note on Working with RailGun.
