MAY 2014 **P/ID 77820/PMG01**

Time : Three hours Maximum : 100 marks

PART A — (5 × 6 = 30 marks)

Answer any FIVE questions.

1. What is web security? Explain web security considerations.

2. What is AJAX? What technologies are being used in AJAX?

3. Define Honeypot. Explain the different types of honeypot.

4. Explain the concept of cryptography.

5. What is functional testing? Compare function testing with security testing.

6. What are the approaches for intrusion detection?

7. Explain the steps involved in threat modelling process.

8. Why we do need port scanning? Illustrate with example.

PART B — (5 × 10 = 50 marks)

Answer any FIVE questions.

9. Explain the different controls of ASP. NET AJAX. State the features of AJAX.

10. Briefly explain the different types of firewall and its configurations.

11. Define digital forensic. What are the challenges in digital forensics?

12. What are the causes of vulnerabilities arising out of improper use of cryptosystems?

13. What are the security policy guidelines? Explain.

14. Explain the OWASP testing framework.

15. How security policies and procedures for business use of web services are evolved?

16. A computer security expert has said that without integrity no system can provide confidentiality — Do you agree? Justify.

PART C — (1 × 20 = 20 marks)

Compulsory

17. A graduate student accidently releases a program that spreads from computer to computer system. Actually no files it delete but requires much time to implement the necessary defences. The student is convicted. Despite demand that he be sent to prison for the maximum time possible, the judge sentences him to pay a fine and perform community service.

What factors do you believe caused the judge to hand down the sentence he did?

What would you have done were you the judge?

What extra information would you have needed to make your decision?

———————