Reg. No. : | | | | | | | | | | | | |

Question Paper Code : 41180

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2013.

Eighth Semester

Computer Science and Engineering

080230068 – INFORMATION SECURITY

(Regulation 2008)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — ($10 \times 2 = 20$ marks)

1. Differentiate how an exploit differ from vulnerability.

2. List any four measures to be taken for protecting confidentiality of information.

3. What are the differences between a skilled hacker and an unskilled hacker?

4. Give any three commandments of computer ethics.

5. Differentiate between mandatory access controls and lattice based access controls.

6. List any four risk control strategies that could be employed for securing information.

7. Where can a security administrator go to find information on established security frameworks?

8. State the objectives of the VISA security model.

9. What are the applications of a passive vulnerability scanner?

10. What is the average key size of a "strong encryption" system in use today?

PART B — (5 × 16 = 80 marks)

11. (a) (i) Enumerate in detail about the NSTISSC security with a neat block diagram.

(ii) Compare and contrast SecSDLC with SDLC with its merits and demerits.

Or

(b) (i) Discuss in detail about the steps that aids in balancing information security and access control.

(ii) Write a short note on the approaches for information security implementation.

12. (a) (i) Discuss in detail about the Man-in-the-Middle attack.

(ii) Why is information security a management problem? What can management do that technology cannot?

Or

(b) (i) How does technological obsolescence constitute a threat to information security?

(ii) Write a short note on the professional organizations of interest to information security professionals.

13. (a) (i) What is risk transference? Describe how outsourcing can be used for risk transference.

(ii) Explain in detail about the risk control cycle and various categories of controls.

Or

(b) (i) Explain in detail about the cost benefit analysis.

(ii) Enumerate in detail about the steps in risk identification and its assessment deliverables.

14. (a) Discuss in detail about the ISO 17799/BS 7799 security model with a neat block diagram.

Or

(b) Elaborate on the VISA International security model with their pros and cons.

15. (a) List and describe the typical relationships that organizations have with non employees. What are the special security precautions that an organization must consider for workers involved in these associations, and why are they significant?

Or

(b) Discuss the principles of intrusion detection systems.
