

A1B
20/1/16 AN

Reg. No. :

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Question Paper Code : 21749

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2015.

Eighth Semester

Computer Science and Engineering

IT 2042/IT 706/10144 CSE 58/10177 ITE 33 — INFORMATION SECURITY

(Common to Seventh Semester Information Technology)

(Regulations 2008/2010)

Time : Three hours

Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. What is e-mail spoofing?
2. Components of information system required for an organization.
3. Why is information security a management problem?
4. What is meant by active attack and passive attack?
5. What do you mean by risk management?
6. What are the thumb rules applied in selecting the preferred risk mitigation strategy?
7. What is the difference between an ACL and a configuration rule?
8. What is contingency planning?
9. What is the problem Faced by signature-based IDS?
10. Define footprinting.

PART B — (5 × 16 = 80 marks)

11. (a) (i) What is information security? Describe the critical characteristics of information. (8)
- (ii) Briefly explain the components of an information system. How will you balance the security and access? (8)

Or

- (b) (i) Explain the NSTISSC security model and the bottom-up approach to security implementation. (8)
 - (ii) Explain the various phases of security system development life cycle. (8)
12. (a) (i) Consider a statement: an individual threat agent, like a hacker can be represented in more than one threat category. If a hacker hacks into a network, copies a few files, defaces the web page, and steals credit card numbers, how many different threat categories does this attack cover? (8)
- (ii) With a neat diagram, explain IP spoofing. (8)

Or

- (b) Discuss about various codes of ethics, certifications, and professional organizations.
13. (a) Briefly discuss the risk assessment and the documenting its results. (16)

Or

- (b) Explain the various risk control strategies that help an organization. (16)
14. (a) (i) Brief about the elements of an Issue-Specific Security Policy Statement. (8)
- (ii) Brief about any four significant points of the NIST SP 800-14 security model. (8)

Or

- (b) Explain the security architecture design process with neat sketch.
15. (a) Explain the various types of intrusion detection systems.

Or

- (b) (i) Discuss the roles and responsibilities of information security staff. (8)
- (ii) Discuss the generations of firewall in detail. (8)