Register Number: ……..

B.E / B.TECH DEGREE EXAMINATIONS: APRIL 2014

(Regulation 2009)

Eighth Semester

ITY122: INFORMATION SECURITY

(Common to CSE/IT)

Time: Three Hours **Maximum Marks: 100**

Answer all the Questions:-

PART A (10 x 1 = 10 Marks)

1. The _____ of information is the quality or state of having ownership or control of some object or item
   a) Integrity b) Utility
   c) Possession d) Accuracy
2. When a system is compromised and used to attack other systems is known as
   a) Indirect Attacks b) Direct Attacks
   c) Virus d) Hoaxes
3. A malicious program that replicates itself constantly without requiring another program o provide a safe environment for replication is known as
   a) Virus b) Worm
   c) Trojan Horses d) Polymorphic threat
4. Which law regulates the structure and administration of government agencies and their relationships with citizens, employees and other governments providing careful checks and balances?
   a) Civil Law b) Tort Law
   c) Private Law d) Public Law
5. Which control approach that attempts to shift the risk to other assets, other processes, or other organization?
   a) Transference b) Mitigation
   c) Risk Assessment d) Avoidance
6. The Cost Benefit Analysis (CBA) is calculated as
   a) ALE(post) – ALE(prior) - ACS b) ALE(post) + ALE(prior) - ACS
   c) ALE(prior) – ALE(post) - ACS d) ACS - ALE(post) – ALE(prior)
7. Name the table that specifies which subjects and objects a user or group can access
   a) State Table b) Capability Table

   c) Flow Table d) Symbol Table
8. The process of collecting, analyzing, and preserving computer related evidence is termed as
   a) Alert Roster b) Contingency Plan
   c) Gateway Router d) Computer Forensics
9. A collection of brute-force methods that attempt to deduce statistical relationships between the structure of the unknown key and the cipher text is
   a) Man-in-the-Middle Attack b) Dictionary Attack
   c) Correlation Attacks d) Selected Plain Text
10. Name the process of attracting attention to a system by placing tantalizing bits of information in key locations
    a) Entrapment b) Packet Sniffer
    c) Foot Printing d) Enticement

PART B (10 x 2 = 20 Marks)

11. Why is methodology important in implementing the information security?
12. Sketch the NSTISSC security model.
13. What is a buffer overflow, and how is it used against Web Server?
14. What are the general categories of unethical and illegal behavior?
15. What is Risk Management?
16. Define Residual Risk.
17. How contingency planning is different from routine management planning?
18. List out the major activities of crisis management.
19. How E-Mail systems are secured?
20. List the major sources of physical loss.

PART C (5 x 14 = 70 Marks)

21. a) (i) Briefly explain the components of an information system and their security. (7)
    (ii) Explain in detail the two different approaches to information security implementation. (7)

    (OR)

    b) Compare and Contrast the various phases of SDLC and SecSDLC.

22. a) (i) Explain the four important functions of information security in an organization. (7)
    (ii) Discuss briefly about the different software attacks which are faced by an organization. (7)

(OR)

b) (i) Briefly discuss the different U.S. laws developed and implemented for information security? (9)

(ii) List and enumerate the ten commandments of computer Ethics. (5)

23. a) Explain in detail the various Risk Control Strategies to be followed in an organization to control the vulnerabilities.

(OR)

b) (i) Discuss the various feasibility studies in measuring how ready an organization is in implementing the information security controls. (7)

(ii) Explain in detail the different factors to be considered in risk-rating estimate. (7)

24. a) State the purpose of ISO / IEC 17799 standard and also explain the ten major process steps of ISO / IEC 17799 standard.

(OR)

b) (i) Explain the various architectures used in designing the security. (7)

(ii) Briefly discuss the four phases of Incident Response Planning (IRP). (7)

25. a) (i) Explain the different types of architectural implementations of firewalls with neat sketch. (7)

(ii) Discuss the various functions of Chief Information Security Officer(CISO). (7)

(OR)

b) Explain in detail why NIST is compelling to acquire and use an Intrusion Detection Systems (IDSs) and also discuss its types and detection methods?

****