KUMARAGURU
college of technology
character is life

Register Number: …….

B.E/B.TECH DEGREE EXAMINATIONS: NOV/DEC2014

(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. Which of the following refers to the implementation of security in an organization?
   a) Threat agent b) Security posture
   c) Security object d) Security blueprint
2. Which of the following are the responsibilities of data custodians?
   Storage ii. Implementation iii. Information protection iv. Analysis
   a) i & ii b) iii & iv
   c) i & iii d) ii & iii
3. Which of the following act protects the confidentiality and security of health-care data?
   a) Communication Act b) Computer Security Act
   c) Kennedy-Kassebaum Act d) Federal Privacy Act
4. Which type of threat cannot replicate itself within a system, but can transmit its copies by means of e-mail?
   a) Malware b) Virus
   c) Worm d) Trojan horse
5. The process of searching trash and recycling is known as
   a) Clean desk policy b) Dumpster searching
   c) Disk searching d) Dumpster diving
6. Which of the following is not a component of risk management?
   a) Implement the controls b) Define the risks
   Establish an information security policy d) Set benchmarks

7. Which of the following is relevant to buffer against outside attacks?

a) Proxy server
b) Firewall subnet
c) Demilitarized zone
d) Cache server

8. When is DRP used?

a) Assess incident damage
b) Recovery from Disaster
c) Incident response planning
d) Data Recovery

9. Which organization offers the Certification Information System Security Professional (CISSP) certification?

a) Information Systems Audit and Control Association
b) International Information System Security Certification Consortium
c) International Standards Organization
d) SANS Institute

10. Which of the following is not a firewall analysis tool?

a) HPING
b) Firewalk
c) Scilab
d) Nmap

PART B (10 x 2 = 20 Marks)

11. What is the difference between vulnerability and exposure?
12. Define Security. What are the layers of Security?
13. Why do employees constitute one of the greatest threats of Information Security?
14. What is a policy? How is it different from a law?
15. What are the thumb rules applied in selecting the preferred risk mitigation strategy?
16. Differentiate between benchmark and baseline.
17. What is contingency planning? How is it different from route management planning?
18. List the inherent problems with ISO 17799.
19. What is a mantrap? When should it be used?
20. What are the advantages and disadvantages of honey pot approach?

PART C (5 x 14 = 70 Marks)

21. a) (i) Assume a security model is needed for the protection of information in your class. Using NSTISSC model, examine each of the cells and write brief statements for each cell. (8)

(ii) Illustrate the critical characteristics of information. How are they used in the study of computer security? (6)

(OR)

b) (i) Investigate about components of System Development Life Cycle (SDLC) with neat sketch. (8)

(ii) Summarize the problem areas found in software development. (6)

22.	a)	(i)	Bring out the ethical concepts in information security and the prevention to illegal and unethical behavior.	(8)
		(ii)	Identify the threats and possible vulnerabilities for each threat.	(6)
			(OR)	
	b)	(i)	List and discuss about the roles and focus of any four professional organizations in providing information security.	(8)
		(ii)	Summarize the various groups of threats faced by an organization	(6)
23.	a)	(i)	Sketch and illustrate the various components of risk identification process.	(8)
		(ii)	List and exhibit any three approaches to mitigate risk.	(6)
			(OR)	
	b)	(i)	Bring out in detail the three common methods of risk avoidance.	(8)
		(ii)	Why do components need more examination from an information security perspective than from a systems development perspective?	(6)
24.	a)	(i)	Can an organization that does not use the VISA cardholder protection system in conjunction with the processing of credit cards benefit from VISA's security framework? How?	(8)
		(ii)	Summarize any four significant points of the NIST SP 800-14 Security model.	(6)
			(OR)	
	b)	(i)	List and give an account of the various components used in designing the security architecture.	(8)
		(ii)	Briefly describe management, operational and technical controls, and explain when each would be applied as part of a security framework?	(6)
25.	a)	(i)	Illustrate the different types of Intrusion Detection System (IDS) with their advantages and disadvantages.	(8)
		(ii)	Summarize the cryptographic tools used for providing the security.	(6)
			(OR)	
	b)	(i)	Write short notes on scanning and analysis tool used during design.	(8)
		(ii)	Enumerate the credentials of the various information security certifications.	(6)

****