KUMARAGURU
college of technology
character is life

Register Number: ………………..

B.E/B.TECH DEGREE EXAMINATIONS: APRIL 2015

(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. Identify critical characteristic of Information preventing disclosure or exposure to unauthorized individuals or systems.

a) Availability b) Accuracy
c) Authenticity d) Confidentiality

2. Recognize which one of the following is not a component of Information System

a) People b) Data
c) Manual d) Procedures

3. Name the type of attack that includes the execution of viruses, worms, Trojan horses and active Web scripts with the intent to destroy or steal information

a) Malicious code b) Spaghetti code
c) Source code d) Executable code

4. Label the appropriate category of unethical and illegal behavior

a) Quarrelling b) Shouting
c) Talking d) Ignorance

5. Give a term related to Information security management

a) Identifying and Clarifying risk b) Clarifying risk
c) Identifying risk d) Mitigating risk

6. Identify the likelihood of vulnerabilities as specified by National Institute of Standards and Technology

a) 0 for low and 1.0 for high b) 0.1 for low and 1.0 for high
c) 0 for low and 1.5 for high d) 0.1 for low and 1.5 for high

7. Match the expansion for SYSSP

a) Systems Specific Policy b) Systems Specified Policy

c) Software Specific Policy d) Software Specified Policy

8. State the term relevant to immediate determination of incident damage assessment

a) Denial of Service b) Masquerade

c) Vulnerability d) Scope of the breach of confidentiality

9. Give the name of the device that works under the Windows NT Executive and is also the kernel of Windows NT

a) Firewall b) Kernel proxy

c) Proxy Server d) Database Server

10. Name the successor to 3DES

a) 4DES b) DMZ

c) AES d) DES

PART B (10 x 2 = 20 Marks)

11. State the significance of NSTISSC Security Model.
12. Outline the concept of risk management in SDLC.
13. Identify the important functions of information security offered for an organization.
14. Outline the essential concepts of Distributed Denial-Of-Service (DDoS)
15. Outline the need for personnel security clearance.
16. Outline single loss expectancy of a risk.
17. State the use usage of ACL.
18. Define Crisis management and list its significance.
19. State the usage of DMZ.
20. List the services of Kerberos.

PART C (5 x 14 = 70 Marks)

21. a) (i) Illustrate Computer as a subject and object of attack. (4)

(ii) Infer how security and access can be balanced. (10)

(OR)

b) (i) Illustrate the SDLC phases. (4)

(ii) Examine the SDLC Methodology. (10)

22. a) (i) Categorize the six categories of known attack vectors with the relevant description. (10)

(ii) Write the significant points about U.S. Copyright Law. (4)

(OR)

b) (i) Categorize the five groups of real and present threats with the relevant description. (10)

(ii) Write the significant points about Digital Millennium Copyright Act (DMCA). (4)

23. a) Describe the various risk identification technique.

(OR)

b) Examine how risk can be assessed in an organization.

24. a) Examine the various Security Policies.

(OR)

b) Write about Fire walls and its significance.

25. a) Examine the various types of access controls.

(OR)

b) Describe the Intrusion Detection Systems (IDS).

****