KUMARAGURU college of technology
character is life

Register Number:……

MCA DEGREE EXAMINATIONS: DEC 2015

(Regulation 2014)

Third Semester

MASTER OF COMPUTER APPLICATIONS

P14CAT302: Information Security

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

Answer all the Questions:-

PART A (10 x 1 = 10 Marks)

1. Assertion (A): The process of sending e-mail message with a modified field is a major problem for many users. [K_2]

   Reason (R): Because all people are using e-mail today.

   a) Both A and R are wrong
   b) Both A and R are correct
   c) A is correct and R is wrong
   d) A is wrong and R is correct

2. Distributed Denial of service is an example for _____. [K_1]

   a) Direct attack
   b) Indirect Attack
   b) Threat
   d) Vulnerability

3. _____ hacks the public telephone network to make free calls or disrupt services. [K_2]

   a) Sniffers
   b) Hackers
   c) Script Kiddies
   d) Phreaker

4. Match List I with List II and select the correct answer using the codes given below: [K_3]

List I	List II
A. Monitoring data over network	i. Brute force attack
B. Routing large number of e-mail	ii. Denial of Service
C. Making Large number of connections to the target	iii. Sniffers
D. Trying all possible combination	iv. Mail bombing

	A	B	C	D
a)	i	iii	iv	ii
b)	iii	iv	ii	i
c)	ii	iii	i	iv
d)	iv	iii	ii	i

5. Assertion (A): Policy is not important as standard. [K_2]

Reason (R):Standards are built on policy and carry the weight of policy.

a) Both A and R are wrong b) Both A and R are correct

c) A is correct and R is wrong d) A is wrong and R is correct

6. The informal standards are named as _____. [K_1]

a) De facto Standard b) Security Policy

c) De jure Standard d) Access Control Lists

7. The circuit gateway firewall operates on the _____ layer. [K_1]

a) network b) transport

c) session d) presentation

8. Assertion (A): Host based IDPS is better than Network based IDPS. [K_3]

Reason (R): It can access encrypted information travelling in the network and make decisions about the attack.

a) Both A and R are wrong b) Both A and R are correct

c) A is correct and R is wrong d) A is wrong and R is correct

9. _____determines the impact that a specific technology or an approach can have on the organization's information assets and what it may cost. [K_1]

a) Cost benefit analysis b) Project plan

c) Work breakdown structure d) Change management

10. Arrange in a sequence of executing the project plan. [K_3]

1) Supervising tasks 2) Wrapping up

3) Planning the project 4) Action steps

a) 1,2,3,4 b) 4,3,2,1

c) 3,1,4,2 d) 1,3,4,2

PART B (10 x 2 = 20 Marks)

11. Identify the layers of security. [K_2]
12. Analyze the primary responsibility of Chief Information Security Officer. [K_4]
13. Write a note on Cyberterrorism. [K_2]
14. Discover the general causes of unethical and illegal behavior. [K_4]
15. Choose the elements that should be included in EISP elements. [K_3]
16. Newsletter is the most cost effective method of disseminating security information. Justify. [K_5]
17. Identify and describe the firewall that enables an organization to make a security improvement without replacing existing firewalls. [K_3]
18. Define honey pots and judge its responsibilities. [K_5]

19. Discuss about Lewin Change model. [K_4]

20. Analyze about digital forensics. [K_4]

PART C (10 x 5 = 50 Marks)

21. Elaborate the components of Information System. [K_3]

22. Compare Security Systems Life Cycle with Systems Development Life Cycle in detail. [K_3]

23. Define attack and discuss about major types of attack used against controlled systems. [K_4]

24. Compile in detail about Risk Assessment. [K_4]

25. Examine the design of security architecture with an example. [K_3]

26. Determine the major steps in Contingency planning. [K_3]

27. Inspect the four common architectural implementations of a firewall. [K_5]

28. Discuss about the deployment and implementation strategies for an IDPS. [K_4]

29. Evaluate the technical aspects in implementing information security. [K_3]

30. Discover the need for project management of information systems security. [K_4]

PART D (2 x 10 = 20 Marks)

31. Elaborate the importance of scanning and analysis tools and discuss in detail about access control devices. [K_4]

32. ABC Software Company has a new application development project, with projected revenues of Rs.12,00,000. Using the Table - 1 calculate the ARO and ALE for each threat category that ABC Software Company faces for this project. [K_4]

Table - 1

Threat Category	Cost per Incident (SLE)	Frequency of Occurrence
Programmer mistakes	Rs.8,500	1 per week
Loss of intellectual property	Rs.70,000	1 per 6 months
Software piracy	Rs.500	1 every other week
Theft of information (hacker)	Rs.3,000	1 per quarter
Theft of information (employee)	Rs.5,000	1 per 6 months

Assume a year has passed and XYZ has improved security by applying a number of controls. Using the information from table 1 and table 2, calculate the post-control ARO, ALE, and CBA for each threat category listed in the table 2. For each threat category, determine if the proposed control is worth the cost:

Table - 2

Threat Category	Cost per Incident (SLE)	Frequency of Occurrence	Cost of Control	Type of Control
Programmer mistakes	Rs.6,500	1 every other week	Rs.40,000	Training
Loss of intellectual property	Rs.75,000	1 per year	Rs.20,000	Firewall/IDS
Software piracy	Rs.600	1 per month	Rs.15,000	Firewall/IDS
Theft of information (hacker)	Rs.2,000	1 per 6 months	Rs.15,000	Firewall/IDS
Theft of information (employee)	Rs.6,000	1 per year	Rs.12,000	Physical security

****