Code No. 11240 / S

FACULTY OF ENGINEERING

B.E. 4/4 (CSE/IT) I-Semester (Suppl.) Examination, May / June 2019

Subject : Information Security

Time : 3 Hours **Max. Marks: 75**

Note: Answer all questions from Part-A & any five questions from Part-B.

PART – A (25 Marks)

1	What are the critical characteristics of information?	3
2	Differentiate between virus & worms.	3
3	What are the general causes of unethical and illegal behaviour?	3
4	How transport mode is used in VPN?	2
5	What is vulnerability?	2
6	What is message digest?	2
7	Define data confidentiality.	3
8	What are requirements of digital signature?	3
9	What are the risk control strategies?	2
10	What is due care?	2

PART – B (50 Marks)

11 Differentiate between threat and attack. Explain different types of attacks. 10

12 Discuss the following aspects of continuity strategies: (4+3+3)
   a) Incident Response
   b) Disaster Recovery
   c) Business Continuity

13 What are the different firewall architectures? Explain 10

14 a) Write about RSA algorithm with an example. 5
   b) What are the 3 basic operations in cryptography? 5

15 What are the different protocals used for secure communication? 10

16 a) What is the difference between configuration management and change management? 5
   b) What are the primary objectives of internal monitoring domain? 5

17 Write a short note on: 10
   a) Security Education, Training and Awareness
   b) Biometric control
   c) Vernum Cipher

*****

Code No.2261/BL

FACULTY OF ENGINEERING

B. E. (CSE/IT) 4/4 – I - Semester (Backlog) Examination, October 2020

Subject: Information Security

Time: 2 hours **Max. Marks: 75**

PART – A

Note: Answer any seven questions. **(7x3 = 21 Marks)**

1. What are the three main goals of Information Security?
2. Differentiate between a threat and an Attack?
3. What is Data confidentiality?
4. What is Race condition?
5. What are the different Cipher Methods?
6. What is Benchmarking?
7. Explain codes of ethics?
8. Draw the 3-D NSTISSC Model of Security.
9. Write about digital forensics.
10. How does a packet filtering firewall work?

PART – B

Note: Answer any three questions. **(3x18 = 54 Marks)**

11. (a) Explain Security System Development Life-cycle with diagram.
    (b) Discuss the components of Information Security.
12. (a) Explain Law and Ethics of Information Security.
    (b) What are the different attacks to Information System?
13. Explain Firewall Architecture in detail.
14. (a) What is VPN? Briefly discuss two approaches using which a VPN can be implemented.
    (b) What is Honey pot? Explain its role.
15. What is IDPS? Explain different types of IPS in detail.
16. (a) What are the technical aspects of Information System? Implementation in detail.
    (b) Explain in detail Security Management Maintenance Model.
17. Write a short note on:
    (a) Digital Signature.
    (b) Cost Benefit Analysis (CBA).
    (c) Public Key Information (PKI).

******

Code No. 2778/CBCS/S

FACULTY OF ENGINEERING

B.E. VII- Semester (CSE)(CBCS)(Suppl.) Examination, October 2020

Subject: Information Security

Time: 2 hours

Max. Marks: 70

PART – A

Note: Answer any five questions. (5x2 = 10 Marks)

1. What is Security Blueprint?
2. Differentiate between a threat and an attack?
3. Draw 3-D NSTISSC Model of Security.
4. Specify the five elements of Business Impact Analysis?
5. What are the different Cipher Methods?
6. What is residual risk?
7. What is timing attack?
8. How is a Policy different from a Law?
9. Define Honeypots?
10. What is cost Benefit Analysis?

PART – B

Note: Answer any four questions. (4x15 = 60 Marks)

11. (a) Explain critical characteristics of Information?
    (b) What are the various threats of information Security?

12. What is Risk Management? Discuss the various components of risk Management?
13. (a) What is a VPN? Differentiate between tunnel mode and transport mode?
    (b) Explain different types of IDPS?

14. Explain in detail cipher Methods using Encryption?

15. (a) Explain Bull's Eye Model?
    (b) What are the non-technical aspects of Implementation?

16. (a) Explain DES Algorithm in detail?
    (b) Discuss the attacks on Crypto system?

17. Write short note on:
    (a) Public key Infrastructure.
    (b) Dos and DDos attack
    (c) Types of Law

****

Code No. 298/S

FACULTY OF ENGINEERING AND INFORMATICS

B.E. 4/4 (CSE/IT) I-Semester (Suppl) Examination, May/June 2018
Subject: Information Security

Time: 3 Hours **Max. Marks: 75**

Note: Answer All Questions From Part-A & Any five Questions From Part-B.

Part – A (25 Marks)

1. What are the various characteristics of information? 3
2. Differentiate between DoS and DDoS 2
3. Define : Residual Risk 2
4. Write short notes on Policy Vs law 3
5. What is information security Blueprint? 2
6. Write about VPNs. 3
7. Define cryptography and Cryptanalysis 2
8. Differentiate symmetric and Asymmetric Encryption. 3
9. Write about internal control strategies 3
10. What is Bull's eye model? 2

PART –B (5x10 = 50 Marks)

11. What is a threat? Explain the different types of threats in detail? 10
12. Explain the various Risk control Strategies in detail? 10
13. Briefly explain the categorization of firewalls 10
14. What is IDPS? Explain the various types of IDPS and its detection methods in detail?10
15. Explain the various steps involved ion information security project management? 10
16. a) Outline any five attacks 5
    b) Discuss about the Risk Assessment 5
17. Write short notes on the following:
    a) Digital signatures 4
    b) Triple DES 3
    c) Digital Forensics 3

****

Code No. 298

FACULTY OF ENGINEERING & INFORMATICS

B.E. 4/4 (CSE/IT) I - Semester (Main & Backlog) Examination, December 2017

Subject : Information Security

Time : 3 Hours **Max. Marks: 75**

Note: Answer all questions from Part-A and answer any five questions from Part-B.

PART – A (25 Marks)

1 Explain the Mc Cumber cube and illustrate its role in Information security. (2)
2 What is the difference between DoS and DDoS attack? Which one of them is more dangerous? (3)
3 What is a policy and how does it differ from Law? (2)
4 Specify reasons why risk appetite varies from organization to organization. (3)
5 Highlight the relationship between policy, standards and practices / procedures / Guidelines. (2)
6 List the three concerns to be addressed while selecting a firewall for an organization. (3)
7 Give advantages and disadvantages of padded cell. (3)
8 Discuss the commonly used attacks on crypto systems. (2)
9 Short list the various roles for staffing the information security functions. (3)
10 When an employee leaves the organization, discuss the activities to be performed under employment polices and matches. (2)

PART – B (50 Marks)

11 (a) Explain the various components of Information systems. (5)
(b) Illustrate few commonly encountered software development security problems. (5)

12 Describe the various stages of risk management and explain the stages of it with neat diagrams. (10)

13 (a) Define and elaborate the process of contingency planning. (5)
(b) Briefly describe the different ways for protecting remote connections. (5)

14 Discuss the protocols used for secure connections. (10)

15 Elaborate the major subject areas recommended for security maintenance. (10)

16 Statistical analysis, wouldn't be alone sufficient for performing risk analysis. Identify the qualitative risk control practices to be adopted by organization. (10)

17 Write short notes on the following: (10)
(a) Security Blueprint
(b) Scanning and Analysis Tools
(c) Non-technical aspects of security

*****

Code No. 3270/S

FACULTY OF ENGINEERING & INFORMATICS

B.E. 4/4 (CSE/IT) I - Semester (Suppl.) Examination, May / June 2017

Subject : Information Security

Time : 3 Hours **Max. Marks: 75**

Note: Answer all questions from Part-A and answer any five questionsfrom Part-B.

PART – A (25 Marks)

1 Define security and specify the different keys of security implemented by any organization. (2)

2 What is the most common form of violation of Intellectual property right? How does an organization protect from it? (3)

3 Which Law amended the computer fraud and abuse act of 1986, and what did it change? (2)

4 What is cost Benefit analysis? Given an example. (3)

5 Specify the five elements of a business impact analysis. (3)

6 Differentiate between static and dynamic packet filtering. (2)

7 In an IDPS, how does true attack stimulus and false attack stimulus differ? (2)

8 Define PKI and specify its role in cryptography. (3)

9 Illustrate Bulls eye model used in implementing information security. (3)

10 List the steps involved in configuration management. (2)

PART – B (50 Marks)

11 List the various stages of secure systems development lifecycle and compare the unique steps of it from a software development lifecycle. (10)

12 (a) List and explain the relevant US laws for preserving privacy of customer information. (4)

(b) If the information asset B has a value score of 100 and has two vulnerabilities, calculate the risk for the two cases. (6)

(i) Given, vulnerability X has a likelihood of 0.7 with a current control that addresses 40% of its risk. Assumptions and data are 70% accurate.

(ii) Given, vulnerability Y has a likelihood of 0.3 with no current control. Assumption and data one 50% accurate.

13 (a) List and describe six continuity strategies adopted when planning for Business continuity. (5)

(b) IPsec is achieved in 2 modes, which is dominant protocol used in VPN. Describe. (5)

14 (a) List and explain the types of intrusion detection and prevention systems. (6)

(b) Demonstrate asymmetric encryption using RSA algorithm taking an example. (4)

15 Describe the process employed for performing Digital forensics. (10)

16 (a) Explain risk analysis by elaborating the relation between threats, attack and vulnerabilities. (5)

(b) Elaborate EISP, ISSP and SYSSP documents and their key components. (5)

17 Write short notes on the following: (10)

(a) Security Education, Training and Awareness (b) Cipher methods

(c) Employee policies and practices

*****

Code No. 3270

FACULTY OF ENGINEERING

B.E. 4/4 (CSE / I.T.) I - Semester (Main) Examination, December 2016

Subject : Information Security

Time : 3 hours **Max. Marks : 75**

Note: Answer all questions from Part-A. Answer any FIVE questions from Part-B.

PART – A (25 Marks)

1	What is the difference between vulnerability and exposure?	2
2	What is Race conditions?	2
3	Describe risk transference.	2
4	What is cost benefit analysis?	2
5	What are the three common methods of risk avoidance?	3
6	What is security blue print?	3
7	List and describe three major steps in executing the project plan.	3
8	What are the two basic functions used in encryption algorithm?	2
9	What are the different Cipher methods?	3
10	What are the requirements of digital signature?	3

PART – B (50 Marks)

11	Difference between threat and attack. Explain different types of attacks.	10
12 a)	What is Risk identification? Explain different components of risk identification.	5
b)	Explain risk handling decesion points.	5
13 a)	Write briefly about scanning and analysis tools.	5
b)	Discuss in detail different firewall architectures.	5
14	What is IDPS? Explain different types of IDPS in detail.	10
15 a)	Explain Bull's-Eye model.	5
b)	Explain about maintenance model.	5
16 a)	What is VPN? Briefly discuss the two approaches using which a VPN can be implemented?	5
b)	What Is Honey pot? Explain its role.	5
17	Discuss short notes on :	10
	a) Defense in depth	
	b) Disaster recovery	
	c) NSTISSC security model	

******

Code No. 5271

FACULTY OF INFORMATICS

B.E. 4/4 (CSE /IT) I - Semester (Main) Examination, December 2015

Subject : Information Security

Time : 3 hours **Max. Marks : 75**

Note: Answer all questions from Part-A. Answer any FIVE questions from Part-B.

PART – A (25 Marks)

1	What are the components of an Information system?	3
2	How to balance information security and its accessibility?	2
3	What are the different types of laws?	2
4	Differentiate between IRP, DRP and BCP.	3
5	Define : Firewall and DMZ	2
6	Write brief note on proxy server.	3
7	Differentiate between digital certificates and digital signatures.	2
8	What is public key encryption?	3
9	Differentiate between certification and accreditation.	2
10	List out the various employment policies and practices.	3

PART – B (5 10 = 50 Marks)

11	Explain the various stages involved in sec SDLC in detail.	10
12	Explain the process of Risk identification in detail.	10
13 a)	Explain the various firewall architectures.	6
b)	Write about securing authentication with Kerberos.	4
14 a)	Write about symmetric encryption.	3
b)	Explain RSA algorithm with an example.	7
15	Explain the security maintenance model.	10
16 a)	Discuss about how to select a risk control strategy in detail.	6
b)	Write about RADIUS and TACACS.	4
17	Write short notes on the following :	
a)	ACLS	3
b)	DES	4
c)	IDPS	3

******

Code No. 9230 / S

FACULTY OF ENGINEERING

B.E. 4/4 (CSE) I – Semester (Suppl.) Examination, June / July 2015

Subject: Information Security

Time: 3 Hours **Max.Marks: 75**

Note: Answer all questions from Part A. Answer any five questions from Part B.

PART – A (25 Marks)

1	What are the critical characteristics of information?	2
2	Differentiate DOS and DDOS.	3
3	What is digital forensics?	2
4	Define security policy, standards and practices.	3
5	Draw the spheres of security.	3
6	How are proxy servers used in information security?	2
7	What are the different firewall processing modes?	3
8	What is residual risk?	2
9	Differentiate between law and ethics.	2
10	What are the different protocols for secure electronic transacting?	3

PART – B (50 Marks)

11	a) Give the security SDLC.	4
	b) What are the different threats that pose damages to information systems?	6
12	Discuss different risk control strategies.	10
13	Discuss different firewall architectures.	10
14	Explain information security project management.	10
15	a) Explain different techniques protecting remote connections?	5
	b) Explain Kerberos.	5
16	Explain different types of IDPSs.	10
17	Write short notes on:	
	a) Vernum cipher	3
	b) Honey pot	4
	c) Viruses and worms	3

****