Roll No: ----------

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, December 2017

Program: B.Tech (CSE+SCF) **Semester – III**
Subject (Course): Information Security Fundamentals **Max. Marks : 100**
Course Code : CSIB213 **Duration : 3 Hrs**
No. of page/s: 02

Section A

1. i) Your company is covered under a liability insurance policy, which provides various liability coverage for information security risks, including any physical damage of assets, hacking attacks, etc. Which of the following risk management techniques is your company using? [2]
   A. Risk acceptance B. Risk transfer C. Risk avoidance D. Risk mitigation.

   ii) Out of the options given, which one is the STRONGEST password [2]-
   A. @#$)*&^% B. akHGksmLN C. UcSc4Evr! D. Password1

   iii) Which of the following is a practice of OS hardening- [2]
   A. antivirus B. firewall C. patching and updating D. data leakage prevention

   iv) What is used to protect network from outside internet access? [2]
   a) A trusted antivirus b) 24 hours scanning for virus
   c) Firewall to separate trusted and untrusted network
   d) Deny users access to websites which can potentially cause security leak

2. A friend sends an electronic Hallmark greeting card (e-card) to your work email. You need to click on the attachment to see the card. What should you do? [2]

3. Differentiate between NIDS and HIDS. [2]

4. Explain the following terms- [4*2]
   a) Cross Site Request Forgery b) LDAP c) SQL Injection d) Phishing

Section B

5. What is Information Security? How it is achieved by CIA? Write down the steps for drafting an Information Security Strategy Plan for www.amazon.com [2+3+5]

6. Explain the process of OPSEC? What are the benefits of implementing OPSEC? Mention any 5 applications of OPSEC in personal life? [2+3+5]

7. A) The cause of physical security issue can be either natural or man-made. Comment on the statement and explain the various technical controls in physical security. [4]

   B) Write down various Cryptographic techniques. [6]

8. Define the scope and benefits of implementing Network Security. Explain the various mitigation and deterrent techniques in Network Security. [5+5]

Section C

9. A) Explain the process of Information Security Audit. Write down various security audit standards. [10]

   B) What are various GRC Pillars? Explain the benefits of GRC and any 2 tools for GRC. [10]

10. A) Differentiate between Web Application Security and Mobile Application Security? Explain about various vulnerabilities and risks involved in both. [10+10]

    OR

    B) What is Application Security? Explain various tools and techniques used for Application Security. What are the various vulnerabilities in Database [4+10+6]

Roll No: ----------

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, December 2017

Program: B.Tech (CSE+SCF) **Semester – III**
Subject (Course): Information Security Fundamentals **Max. Marks : 100**
Course Code : CSIB213 **Duration : 3 Hrs**
No. of page/s: 02

Section A

1. i) Which of the following is a regulatory standard for Healthcare? [2]
   A. SOX B. GLBA C. HIPAA D. None of the above.

   ii) In a certain method, a system is accessed from an attacker's point of view, what is that method known as? [2]
   A. Flood Gating B. Loop Recon
   C. Penetration Testing D. Vulnerability Scanning

   iii) Which of the following is a practice of OS hardening- [2]
   A. antivirus B. firewall
   C. patching and updating D. data leakage prevention

   iv) Which component of physical security is meant for outer layer access control? [2]
   a) Mantraps b) Locked Doors
   c) Security zones d) Perimeter Security

2. A friend sends an electronic Hallmark greeting card (e-card) to your work email. You need to click on the attachment to see the card. What should you do? [2]

3. Differentiate between NIDS and HIDS. [2]

4. Explain the following terms- [4*2]
   b) Denial of Service b) LDAP c) SQL Injection d) Social Engineering

Section B

5. Define the scope and benefits of implementing Network Security. Explain the various mitigation and deterrent techniques in Network Security. [5+5]

6. The cause of physical security issue can be either natural or man-made. Comment on the statement and explain the various technical and logging controls in physical security. [6]

7. A) What is Log Management? Explain the various sources used for logs generation. [7]

   B) Explain the process of Information Security Audit. Write down various security audit standards. [7]

8. What is Information Security? How it is achieved by CIA? Write down the steps for drafting an Information Security Strategy Plan for www.amazon.com [2+3+5]

Section C

9. A) Explain the process of OPSEC? What are the benefits of implementing OPSEC? Mention any 5 applications of OPSEC in personal life? [2+3+5]

   B) Differentiate between Symmetric and Asymmetric Cryptography? Write down various Cryptographic techniques. [10]

10. A) Differentiate between Web Application Security and Mobile Application Security? Explain about various vulnerabilities and risks involved in both. [10+10]

    OR

    C) What is Application Security? Explain various tools and techniques used for Application Security. What are the various vulnerabilities in Database [4+10+6]