S No 3623

CODE : .....

LNMIIT
The LNM Institute of Information Technology

LNMIIT/B. Tech./CSE/PC/2018-19/ODD/CSE-6072/ET

The LNM Institute of Information Technology

Computer Science & Engineering

CSE-6072-Computer Security

Exam Type: End Term

Max. Marks: 50

Date:03/11/2018

Time : 3 Hours

Instruction:

- **All questions are compulsory. No queries will be entertained during exams.**
- **Answer each descriptive question precisely within 1 page, none of them requires more than 1 page.**

PART A: MCQs (Make sure that MCQs are attempted on the first page of the answer-sheet)

MCQ1. Which of the following describes the first step in establishing an encrypted session using a Symmetric Key Encryption?

A. Key clustering B. Key compression C. Key signing D. Key exchange

MCQ2. Copyright provides what form of protection:

A. Protects an author's right to distribute his/her works
B. Protects information that provides a competitive advantage
C. Protects the right of an author to prevent unauthorized use of his/her works.
D. Protect the right of an author to prevent viewing of his/her works.

MCQ3. In a typical information security program, what is the primary responsibility of information (data) owner?

A. Ensure the validity and accuracy of data. B. Determine the information sensitivity or classification level.
C. Monitor and audit system users. D. Ensure availability of data

MCQ4. When an employee transfers within an organization …

A. The employee must undergo a new security review B. The old system IDs must be disabled.
C. All access permission should be reviewed. D. The employee must turn in all access devices.

MCQ5. A system security engineer is evaluation methods to store user passwords in an information system, so what may be the best method to store user passwords and meeting the confidentiality security objective?

A. Password-protected file B. File restricted to one individual
C. One-way encrypted file D. Two-way encrypted file

MCQ6. What is the inverse of confidentiality, integrity, and availability (C.I.A.) triad in risk management?

A. misuse, exposure, destruction B. authorization, non-repudiation, integrity
C. disclosure, alteration, destruction D. confidentiality, integrity, availability

MCQ7. As an information systems security manager (ISSM), how would you explain the purpose for a system security policy?

A. A definition of the particular settings that have been determined to provide optimum security
B. A brief, high-level statement defining what is and is not permitted during the operation of the system
C. A definition of those items that must be excluded on the system
D. A listing of tools and applications that will be used to protect the system

MCQ8. Under what circumstance might a certification authority (CA) revoke a certificate?

A. The certificate owner has not utilized the certificate for an extended period
B. A brief, high-level statement defining what is and is not permitted during the operation of the system
C. A definition of those items that must be excluded on the system
D. A listing of tools and applications that will be used to protect the system

MCQ9. What is the trusted registry that guarantees the authenticity of client and server public keys?

A. Public key notary.
B. Certification authority.
C. Key distribution centre.
D. Key revocation certificate.

MCQ10. Which of the following mechanism is used to achieve non-repudiation of a message delivery?

A. Sender encrypts the message with the recipient's public key and signs it with their own private key.
B. Sender computes a digest of the message and sends it to a Trusted Third Party (TTP) who signs it and stores it for later reference.
C. Sender sends the message to a TTP who signs it together with a time stamp and sends it on to the recipient.
D. Sender gets a digitally signed acknowledgment from the recipient containing a copy or digest of the message.

PART B Descriptive Questions

Q1: (A) What is cross-site scripting attack (2 Marks)? (B) Discuss with an example how the cross-site scripting (XSS) attacks can be launched (2 Marks). (C) What is the simplest way to secure our web application from XSS Attacks (1 Mark)? 5 (2+2+1) Marks

Q2: Discuss in details the man-in-the-browser attack with the help of an example attack. 5 Marks

Q3: Consider a scenario that a government organization is suffering a lot from the port scanning attacks. They are planning to purchase a Firewall to stop the port scanning attack. (A) We studied various types of Firewalls, which of the Firewall is most suitable and cost effective firewall to handle this situation (2 Marks)? (B) Justify your answer to **Part (A)** of this question (3 Marks). 5 (2+3) Marks

Q4: (A) What do you mean by SQL Injection (1 Mark)? (B) How it is performed (2 Marks)? (C) Give an example query fragment to achieve SQL injection (2 Marks). 5 (1+2+2) Marks

Q5: List the top 10 secure coding practices. 5 Marks

Q6: Consider a situation that after 10 years The LNMIIT grows well and starts two more campuses. We need to have the network connectivity among all three campuses in such a way, as if they are a single private network. (A) What is the technical name of this network composed of three separate networks (1 Mark)? (B) On the basis of our study which cost effective security product you will recommend to use for desired connectivity among all three campuses (1 Mark)? (C) Justify your answer to **Part (B)** of this question (3 Marks). 5 (1+1+3) Marks

Q7: Briefly discuss the eight dimensions of privacy. 5 Marks

Q8: (A) Explain how ethics and laws are different (3 Marks). (B) Briefly discuss the two types of ethical principles (2 Marks). 5 (3+2) Marks