ADVANCED CERTIFICATE IN INFORMATION SECURITY (ACISE)

Term-End Examination

December, 2013

OSEI-042 : SECURING INTERNET ACCESS

Time : 2 hours   Maximum Marks : 50

Note :   *Section A : Answer **all** the objective type questions.*

   *Section B : Answer **all** the very short answer type questions.*

   *Section C : Answer **two** out of **three** short answer type questions.*

   Section D : Answer 2 out of 3 long answer type questions.

SECTION - A
(Attempt **all** the questions)

1.   _____ is the predecessor of TLS protocol.   **1**

2.   _____ is a crime in which a criminal obtains   **1**
     key personal information about a person.

3.   Skimmimg is theft of _____ information.   **1**

4.   _____ is a directory service where companies   **1**
     can register & search for web services.

5. The three parameters essential for digital evidence is _____, Authenticity and Reliability. 1

6. Risk management relies on four basic strategies namely Avoidance, Transference, _____ and Acceptance. 1

7. The formula for calculating single loss expectancy or SLE is :
SLE =_____ 1

8. _____ is the sending of a picture or a message from one user to an unsuspecting user through Bluetooth wireless technology. 1

9. The name of team responsible for handling digital incidences is _____ 1

10. _____ is a way of attempting to acquire sensitive info such as username, passwords etc by masquerading as trustworthy entity in electronic communication. 1

SECTION-B
Very short answer type questions
(Attempt **all** the questions)

11. What are the steps to delete browsing history of a browser ? 2

12. Write a short note on DES. 2

13. What are various cyber crimes that can happen against organisations ? 2

14 Explain cookie manipulation and cross-site scripting. 2

15. What is the role of OTP in online services ? 2

SECTION-C

(Attempt **2** out of **3** short answer type questions)

16. How are cookies used by websites ? What are the security risks associated with them ? **5**

17. Describe any two encryption algorithms. **5**

18. Explain two types of digital water marking. **5**

SECTION-D

(Attempt **2** out of **3** long answer type questions)

19. Discuss the threats associated with online transactions. Suggest guidelines to avoid them. **10**

20. Write a detailed note on cyber forensics. **10**

21. How CSIRT members play their roles in handling ? Explain various models for incident response used by CSIRT. **10**

––––––––