P.G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Examination

June, 2019

01494

MSEI-025 : APPLICATION AND BUSINESS SECURITY DEVELOPMENTS

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 any **two** questions out of three short answer type questions.*

*Section D – Answer any **two** questions out of three long answer type questions.*

SECTION A

*Answer **all** the objective type questions.*

1.   What does XML stand for ?   *1*

     (a)   X-Markup Language

     (b)   Example Markup Language

     (c)   Extra Modern Link

     (d)   Extensible Markup Language

2. TLS stands for _____ . *1*

(a) Transport Layer Superior

(b) Transport Layer Security

(c) Transport Layer Supervisor

(d) Transport Layer Secure

3. SSL stands for _____ . *1*

(a) Secure Sockets Layer

(b) Secure Supervisor Layer

(c) Secure Superior Layer

(d) None of the above

4. HTTPS stands for Hypertext Transfer Protocol Secure. *1*

(a) True

(b) False

5. Which of the following is the best way to set up SSH for communicating between systems without needing passwords ? *1*

(a) Use SSH-keygen for generating public-private keys.

(b) Disable passwords on specific accounts that will use SSH.

(c) Both a and b

(d) None of the above

6. Integrated windows authentication make use of
_____ .   *1*

- (a) Digest
- (b) SSL/TLS
- (c) Client Certificate
- (d) Kerberos

7. In Windows, what is the tool which creates a public-private key pair ?   *1*

- (a) makecert.exe
- (b) generatecert.exe
- (c) strong.exe
- (d) sn.exe

8. Confidentiality with asymmetric-key cryptosystem has its own _____ .   *1*

- (a) Entities
- (b) Data
- (c) Problems
- (d) Translator

9. Message authentication is a service beyond
_____ .   *1*

- (a) Message Confidentiality
- (b) Message Integrity
- (c) Message Splashing
- (d) Message Sending

10. A hash function guarantees integrity of a message. It guarantees that message has not been _____ . *1*

(a) Replaced

(b) Overviewed

(c) Changed

(d) Violated

SECTION B

*Answer **all** the very short answer type questions.*

11. What is the difference between access control and authorization ? *2*

12. Describe data decryption technique. *2*

13. How can SQL Injection attacks be prevented ? *2*

14. What is the difference between http and https ? *2*

15. What are two forms of error handling ? *2*

SECTION C

*Answer any **two** questions out of the three short answer type questions.*

16. Explain the working of SMTP and SSL. *5*

17. What are the rules defined for "rule based access 2 control mechanisms" ? *5*

18. What are interface design elements ? Explain with example. *5*

SECTION D

*Answer any **two** questions out of three long answer type questions.*

19. Explain the working of firewall with diagram.   *10*

20. Write short notes on the following :   *5×2=10*

    (a)   Cookie Injection

    (b)   Application Security Assessment

    (c)   Network Security

    (d)   Logging

    (e)   Error Suppression

21. Explain the working of PGP with diagram.   *10*

———