TED (15) – 5136

Reg. No.....

(REVISION — 2015)

Signature .....

DIPLOMA EXAMINATION IN ENGINEERING/TECHNOLOGY/ MANAGEMENT/COMMERCIAL PRACTICE — OCTOBER, 2018

INFORMATION SECURITY

[*Time* : 3 hours

(Maximum marks : 100)

PART — A

(Maximum marks : 10)

Marks

I Answer *all* questions in one or two sentences. Each question carries 2 marks.

1. State two related concepts of Confidentiality.
2. List the requirements for a message to be authentic.
3. Mention any four physical characteristics used for biometric authentication.
4. Differentiate between masquerader and misfeasor.
5. Define Denial of Service. (5×2 = 10)

PART — B

(Maximum marks : 30)

II Answer any *five* of the following questions. Each question carries 6 marks.

1. Explain security concepts and their relationship with a neat block diagram.
2. Mention the use of random numbers in information security applications.
3. With a neat sketch, briefly describe the operation of a biometric authentication system.
4. Explain various access control policies.
5. Explain the architecture of SNORT IDS.
6. Describe the classic DoS attack.
7. Discuss about the four general techniques used by firewalls. (5×6 = 30)

PART — C

Marks

(Maximum marks : 60)

(Answer *one* full question from each unit. Each full question carries 15 marks.)

UNIT — I

III (a) Briefly explain the security mechanisms in OSI security architecture. 8

(b) Discuss various security threats to computer system resources. 7

OR

IV (a) Explain the different ways of using hash functions for message authentication. 9

(b) Describe the ingredients and requirements of symmetric encryption. 6

UNIT — II

V (a) Describe in detail the use of smart tokens for user authentication. 8

(b) Explain various security issues to user authentication. 7

OR

VI (a) Explain various password vulnerabilities and their counter measures. 8

(b) Discuss access control principle and its relation to other security functions. 7

UNIT — III

VII (a) Explain in detail about NIDS sensors and their deployment. 9

(b) Discuss the need and efforts for a standard Intrusion Detection Exchange Format. 6

OR

VIII (a) Explain worm technologies. 8

(b) Explain the functionality of the malware BOT. 7

UNIT — IV

IX (a) Describe the DoS attack which uses the broadcast address of a network. 8

(b) Explain various forms of flooding attacks. 7

OR

X (a) Explain in detail about stateful inspection firewall. 7

(b) Discuss about firewall locations and configurations in a network. 8

———————