TED (15)5136
(Revision- 2015)

A21-09184

Reg. No…….....
Signature. .....

DIPLOMA EXAMINATION IN ENGINEERING/TECHNOLOGY/MANAGEMENT/
COMMERCIAL PRACTICE – APRIL -2021.

INFORMATION SECURITY

(Maximum Marks: 75) [Time: 2.15 hours]

PART–A

Marks

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

1. List any four objectives of computer security.
2. State the purpose of using salt value in hashed password scheme.
3. Define Discretionary Access Control (DAC).
4. List any two parasitic type malware.
5. Define Denial of Service. (3x2=6)

PART - B

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

1. Explain the relationships between various security concepts using a block diagram.
2. Illustrate the use of public key certificate with a block diagram.
3. Explain and compare various features used for biometric authentication.
4. Explain the architecture of SNORT.
5. Describe the procedure followed by BOTs to construct attack network.
6. List the capabilities and limitations of firewall.
7. Explain source address spoofing attack. [4x6 =24]

PART - C

(Answer **any of the three units** from the following. Each full question carries 15 marks)

UNIT I

III (a) Explain various message authentication methods using hash function. (9)

(b) Discuss about various threats to assets. (6)

OR

IV (a) State the need for a security architecture for open systems. Discuss briefly about various security mechanisms defined in the Security Architecture for Open Systems. (9)

(b) Explain public key encryption mechanism to achieve confidentiality. (6)

UNIT- II

V (a) Explain in detail about UNIX file access control. (9)

(b) Describe various means of authentication. (6)

OR

VI (a) Describe the concept of remote user authentication methods used with static and dynamic biometric systems. (8)

(b) Explain briefly about the requirements for access control. (7)

UNIT- III

VII (a) State the need for an Intrusion Detection Exchange Format. Specify the key elements of the model for an intrusion detection message exchange. (8)

(b) Explain various worm technologies. (7)

OR

VIII (a) Explain briefly about the general approaches used for intrusion detection. (9)

(b) Discuss the functions of rootkits. (6)

UNIT – IV

IX (a) With the help of a block diagram, explain distributed denial of service attack. (8)

(b) Write a short note on Bastian Host. (7)

OR

X (a) Explain packet filter and stateful inspection firewalls. (8)

(b) Compare and contrast reflection and amplification attacks. (7)

****