Q.20 Explain the step in Risk and Threat Analysis . (CO1)

Q.21 Discuss the examples of Identification and Authentication Systems. (CO3)

Q.22 Explain the Purpose and Benefits of a DMZ in Network & Information Security. (CO4)

SECTION-D

Note: Long answer type questions. Attempt any two questions out of three questions. (2x8=16)

Q.23 Discuss different types of Trojan horses .Explain the various primary methods used by attackers. (CO1)

Q.24 Discuss Substitution Techniques in Cryptography . Explain its types. (CO2)

Q.25 Discuss the importance and challenges of Cyber Law in the digital world. (CO4)

No. of Printed Pages : 4 223864B

Roll No. .....

6 th Sem. / Artificial Intelligence & Machine Learning

Subject : Network and Information Security

Time : 3 Hrs. M.M. : 60

SECTION-A

Note: Multiple choice questions. All questions are compulsory (6x1=6)

Q.1 Which is the primary function of a firewall in computer security ? (Co2)

a) Encrypting data
b) Blocking unauthorized access to a network
c) Monitoring network traffic
d) Managing passwords

Q.2 What is the purpose of the encryption process in information security ? (CO1)

a) To compress data
b) To create a backup of data
c) To convert data into a readable format
d) To convert data into an unreadable format to prevent unauthorized assess

Q.3 What is the primary purpose of SSL/TLS protocol ? (CO2)

a) To compress data
b) To secure communication over a network
c) To store data securely
d) To manage user authentication

Q.4 Which of the following describes the concept of non-repudiation in cryptography ? (CO3)

a) To encrypt messages
b) To verify the integrity of a message
c) To prove that a transaction or communication cannot be denied by the sender
d) To generate a unique key for each session

Q.5 What is the full form of SMTP ? (CO3)

a) Simple Mail Transport Protocol
b) Simple Mail Transfer Protocol
c) Single Mail Transfer Process
d) Single Mail Transfer Process

Q.6 What does the term "phishing" refer to ? (CO1)

a) A technique used to hack passwords
b) Sending fraudulent emails to obtain sensitive information
c) A method of encryption
d) An attack that involves physically stealing computer

SECTION-B

Note: Objective/ Completion type questions. All questions are compulsory. (6x1=6)

Q.7 Define virus. (CO1)

Q.8 What os Non Repudiation ? (CO2)

Q.9 Define cyber defamation (CO3).

Q.10 Define Authorization . (CO2)

Q.11 What is the primary objective of ISO 27001?(CO3)

Q.12 What is retina scanning ? (CO2)

SECTION-C

Note: Short answer type questions. Attempt any eight questions out of ten questions. (8x4=32)

Q.13 Explain the needs of Computer Security. (CO3)

Q.14 Discuss the role of audit logs in access control systems. (CO4)

Q.15 Discuss the concept of public key infrastructure (PKI) (CO2)

Q.16 Explain the difference between NIDS and HIDS. (CO2)

Q.17 Define the cryptanalysis and cryptology. Describe the key concepts. (CO2)

Q.18 Explain the differences between Transport mode and Tunnel mode in IPSec. (CO3)

Q.19 Explain the differences Between ISO/IEC 20000 and ITIL. (CO4)