TT Pattern

3 Questions on each module (8,7,10)weightage)

Internal Options Possible

Chapter 1 Questions:

Genetic Algorithms

ANN

RNN

Fuzzy Logic

Rule Based

Sinkhole Attack

Byzantine Attack

Sybil Attack

Sensor Stimuli Attack

Sources of Security Threats

Attacks Against IOT Devices

Conventional vs AI approaches to coding

Supervised vs Unsupervised Learning

Classification of ML models based on Traditional Taxonomy

Classification of ML models based on Learning Approaches.

Chapter 2 Questions

History of Firewalls

Classification of Firewalls based on Delivery Method

Classification of Firewalls based on Operation Method

Short Note on Firewall Architectures

Process of Firewall Design

Components of Firewall Policy

Classification of Firewall Policies

Steps to create a firewall policy

Application of Fuzzy Logic in Firewall Design

Next generation Firewalls

Application of ML in Firewall Design

Short Note on Firewall Evaluation

Explain how firewalls could be made robust using AI-ML-DL Techniques

Chapter 3 Questions

Attack Methodology of an intrusion Process

Functions of an IDS

History of IDS Development

IDS vs IPS

Challenges in IDS Design

Goals of an IDS

Goals of an IPS

Firewall vs IPS

Host based IDS

Network IDS

WIDS

NIDS vs NBA

HIDS vs NIDS

AI in IDS

Chapter 4

Short Note on File Infector Virus and steps to prevent it

Short Note on Companion Virus and steps to prevent it

Short Note on Boot Sector Viruses and steps to prevent it

Short Note on Polymorphic and Metamorphic Viruses and steps to prevent it

Short Note on the Evolution of Viruses.

Classification of Viruses

Differentiate Virus,Worms and Trojans

Explain the common methods of malware propagation

Short Note on the importance of anti malware protection

Short Note on role of Threat intelligence in Anti Malware protection

Detailed Note on How the Stuxnet virus Propagated.

Detailed Note on How the Morris Worm Propagated.

Detailed Note on How the Jerusalem Virus Propagated.

Explain the principles of malware detection

Explain the common features of anti malware tools

Chapter 5

Ethical Hacking vs. Malicious Hacking

Common Hacking Techniques

Social Engineering Attacks

Phishing and Spear Phishing

Distributed Denial-ofService (DDoS) Attack

Short Note on Wireless Network Hacking

Short Note on Incident response and forensics

Short Note on Data Science Investigation of a Cyber Crime

Short Note on Predictive Modelling for Cyber Crime Detection

Short Note on the Challenges for a Cyber Crime Investigation

Chapter 6

Briefly explain what a Generative Adversarial Network (GAN) is used for.

Differentiate between traditional autoencoders and adversarial autoencoders in terms of their training objectives and capabilities for generating robust representations.

Explain why adversarial examples can cause machine learning models to make incorrect predictions, in a few sentences.

List two challenges associated with deploying adversarial defense mechanisms in real-world applications, using everyday language.

Explain the purpose of adversarial autoencoders

Differentiate between traditional machine learning and adversarial machine learning using a simple example.

Describe how a GAN might be used to create realistic images of fictional creatures

Explain one simple method that could be used to defend against adversarial attacks on a text-based spam detection system.

List two potential consequences of relying on machine learning models that are vulnerable to adversarial attacks.

Describe one real-world scenario where adversarial attacks could be used to manipulate financial data.

Describe one potential consequence of a self-driving car being vulnerable to adversarial attacks, using a simple scenario like navigating through traffic.