Unit I

Syllabus :

Cyber-attacks, Vulnerabilities, Defence Strategies and Techniques, Authentication Methods and Protocols, Defence in Depth Strategies. Access Control Policies: DAC, MAC, Multi-level Security Models: Biba Model, Bell La Padula Model, Single Sign on, Federated Identity Management.

Unit II

Syllabus :

Malicious and Non-Malicious programming errors, Targeted Malicious codes: Salami Attack, Linearization Attack, Covert Channel, Control against Program threats.

Operating System Security: Memory and Address protection, File Protection Mechanism, User Authentication.

Linux and Windows: Vulnerabilities, File System Security.

Unit III

Syllabus :

OWASP, Web Security Considerations, User Authentication and Session Management, Cookies, SSL, HTTPS, SSH, Privacy on Web, Web Browser Attacks, Account Harvesting, Web Bugs, Click jacking, Cross-Site Request Forgery, Session Hijacking and Management, Phishing and Pharming Techniques, Web Service Security, OAuth 2.0

Unit V

Syllabus :

Cybercrime and its types, Intellectual property, Privacy, Ethical issues.

Protecting Programs and Data, Information and the Law, Rights of Employees and Employers, Redress for Software Failures, Computer Crime, Ethical Issues in Computer Security, Case studies of ethics.

Unit VI

Syllabus :

Introduction to Digital Forensics, Acquiring Volatile Data from Windows and Unix systems, Forensic Duplication Techniques, Analysis of forensic images using open source tools like Autopsy and SIFT, Investigating logs from Unix and windows systems, Investigating Windows Registry.

❑❑❑