



MALLA REDDY VISHWAVIDYAPEETH

SCHOOL OF DIGITAL HEALTH SCIENCES AND TECHNOLOGY

Program

Bachelor of Science (B.Sc.)

Digital Forensics and Cyber Security

2026-27

MALLA REDDY VISHWAVIDYAPEETH

SCHOOL OF DIGITAL HEALTH SCIENCES AND TECHNOLOGY

BACHELOR OF SCIENCE (B.Sc.) IN DIGITAL FORENSICS AND CYBER SECURITY

VISION

Vision of the School

1. To be a nationally recognized centre of excellence in Digital Health, Computing and Cyber Security education, research and innovation, producing globally competent professionals who protect digital systems and uphold the integrity of digital evidence.

Vision of the Programme (B.Sc. Digital Forensics and Cyber Security)

1. To develop industry-ready graduates capable of securing digital systems, investigating cyber incidents, and presenting legally sound digital evidence that safeguards individuals, organizations and critical infrastructure.

MISSION

Mission of the School

1. To impart a strong foundation in computing, networks and mathematics integrated with modern cyber-security and forensic technologies.
2. To nurture innovation, analytical thinking and entrepreneurial skills for developing effective cyber-security and forensic solutions.
3. To provide hands-on exposure to networks, cryptography, malware analysis, digital forensics and penetration testing through state-of-the-art laboratories and industry partnerships.
4. To instill professional ethics, legal awareness and regulatory compliance essential to responsible cyber-security and forensics practice.
5. To foster lifelong learning, research aptitude and community engagement for improving digital trust and safety across society.

Mission of the Programme

1. Build strong foundations in computing, networks, mathematics and programming relevant to cyber-security and forensics practice.
2. Develop competence in cryptography, network security, malware analysis, digital forensics, ethical hacking and incident response.
3. Provide practical exposure to SOC operations, penetration testing, cloud/mobile/IoT forensics and cyber-law compliance through dedicated laboratories and internships.
4. Cultivate research, critical-thinking, project-management and entrepreneurial skills through a capstone research project and start-up pathway course.

PROGRAMME EDUCATIONAL OBJECTIVES (PEOs)

Within a few years of graduation, graduates of the B.Sc. Digital Forensics and Cyber Security programme will:

1. Apply integrated computing, networking and forensic knowledge to secure systems, detect intrusions, and investigate digital crime in organizational and law-enforcement settings.
2. Pursue successful careers as digital forensics analysts, SOC analysts, penetration testers, incident responders, cyber-security compliance officers, or progress to higher studies (M.Tech./M.Sc./MBA/MS) and research.
3. Demonstrate professional, ethical and legal responsibility in handling sensitive data, digital evidence and security incidents.
4. Engage in lifelong learning, innovation and entrepreneurship to address emerging challenges in cyber security and digital forensics, including in under-served regions.

PROGRAMME OUTCOMES (POs)

On completion of the programme, graduates will be able to:

1. Demonstrate comprehensive understanding of digital forensics principles, methodologies, and tools used to collect, preserve, and analyze digital evidence for legal and investigative purposes.
2. Apply technical skills in network security, cryptography, ethical hacking, and intrusion detection to protect digital systems and infrastructure from cyber threats.
3. Design and implement effective incident response strategies, disaster recovery plans, and security auditing frameworks to mitigate and recover from cyber attacks.
4. Analyse and apply cyber laws, compliance standards, and ethical guidelines governing digital forensics investigations and cyber security operations.

5. Conduct independent research, evaluate emerging threats and technologies, and develop innovative solutions to advance the field of digital forensics and cyber security.

PROGRAMME SPECIFIC OUTCOMES (PSOs)

1. Perform end-to-end digital-forensic investigations across computer, mobile, cloud and IoT environments using industry-standard tools and legally sound procedures.
2. Design and operate network and system security controls, including firewalls, IDS/IPS, SIEM and SOC workflows, to defend organizational infrastructure.
3. Plan and execute authorized ethical-hacking and penetration-testing engagements, and report findings with actionable, prioritized remediation guidance.
4. Apply cyber-law, data-protection and governance frameworks to ensure legally compliant and ethically sound cyber-security and forensics practice.

MALLA REDDY VISHWAVIDYAPEETH
SCHOOL OF DIGITAL HEALTH SCIENCES AND TECHNOLOGY
BACHELOR OF SCIENCE (B.Sc.) IN DIGITAL FORENSICS AND CYBER SECURITY
COURSE STRUCTURE

I year I semester

S.NO	SUBJECT	L	T	P	C
1	Introduction to Digital Forensics and Cyber Security	4	-	-	4
2	Computer Fundamentals	2	-	-	2
3	Programming Fundamentals (C & Python)	2	-	2	4
4	Discrete Mathematics	2	-	-	2
5	English & Communication Skills	2	-	-	2
6	Practical's in Programming Fundamentals	-	-	2	2
7	Practical's in Basic Computer and Network Commands	-	-	4	4
	TOTAL	12	-	8	20

I year II semester

S.NO	SUBJECT	L	T	P	C
1	Network Security Fundamentals	2	-	-	2
2	Operating Systems	2	-	-	2
3	Introduction to Cryptography	2	-	-	2
4	Legal and Ethical Issues in Cyber Security	2	-	-	2
5	Linux and Shell Scripting	2	-	-	2
6	Essentials of Research Design and Technical Writing	2	-	-	2
7	Data Structures for Security Applications	2	-	-	2
8	Cyber Hygiene and Digital Citizenship	2	-	-	2
9	Practical's in Networking	-	-	2	1
10	Practical's in Linux/OS Administration	-	-	2	1
11	Practical's in Cryptography	-	-	4	2
	TOTAL	16	-	8	20

II year III semester

S.NO	SUBJECT	L	T	P	C
1	Digital Forensics Investigation	2	-	-	2
2	Ethical Hacking	2	-	-	2
3	Database Security	2	-	-	2
4	Web Application Security	2	-	-	2
5	Computer Networks and Protocol Security	2	-	-	2
6	Operating Systems Security and Hardening	2	-	-	2

S.NO	SUBJECT	L	T	P	C
7	Cyber Threat Intelligence	2	-	-	2
8	Scripting for Security Automation (Python)	2	-	-	2
9	Practical's in Digital Forensics Tools	-	-	4	2
10	Practical's in Ethical Hacking Labs	-	-	2	1
11	Practical's in Web Application Security	-	-	2	1
	TOTAL	16	-	8	20

II year IV semester

S.NO	SUBJECT	L	T	P	C
1	Malware Analysis and Reverse Engineering	2	-	-	2
2	Intrusion Detection and Prevention Systems	2	-	-	2
3	Cyber Security Management and Risk Assessment	2	-	-	2
4	Mobile and IoT Forensics	2	-	-	2
5	Memory and Network Forensics	2	-	-	2
6	Applied Cryptography and PKI	2	-	-	2
7	Security Operations Center (SOC) Fundamentals	2	-	-	2
8	Vulnerability Assessment Tools	2	-	-	2
9	Practical's in Malware Analysis	-	-	2	1
10	Practical's in IDS/IPS	-	-	2	1
11	Practical's in Mobile and Network Forensics	-	-	4	2
	TOTAL	16	-	8	20

III year V semester

S.NO	SUBJECT	L	T	P	C
1	Advanced Digital Forensics	3	-	-	3
2	Penetration Testing	3	-	-	3
3	Cloud Security	2	-	-	2
4	Block chain and Crypto currency Forensics	3	-	-	3
5	Bug Bounty and Responsible Disclosure Practices	2	-	-	2
6	Practical's in Penetration Testing	-	-	4	2
7	Practical's in Cloud Security	1	-	2	2
8	Internship	-	-	-	3
	TOTAL	14	-	6	20

III year VI semester

S.NO	SUBJECT	L	T	P	C
1	Incident Response and Disaster Recovery	3	-	-	3

S.NO	SUBJECT	L	T	P	C
2	Security Auditing and Compliance	2	-	-	2
3	Cyber Law and Compliance	2	-	-	2
4	Governance, Risk and Compliance (GRC) for Cyber Security	2	-	-	2
5	Security Information and Event Management (SIEM)	2	-	-	2
6	Wireless and IoT Security	3	-	-	3
7	Cyber Forensics for E-Commerce and Fintech	2	-	-	2
8	Ethics, Privacy and Data Protection Regulations	2	-	-	2
9	Entrepreneurship in Cyber Security	2	-	-	2
	TOTAL	20	-	-	20

IV year VII semester

S.NO	SUBJECT	L	T	P	C
1	Cyber Security Research and Development	2	-	-	2
2	Cyber Security Project Management	3	-	-	3
3	Advanced Penetration Testing and Red Teaming	2	-	2	3
4	Threat Hunting and Advanced Persistent Threats	2	-	2	3
5	Cyber-Physical Systems and Critical Infrastructure Security	2	-	2	3
6	Social Media and OSINT Investigations	2	-	-	2
7	Artificial Intelligence for Cyber Security	2	-	-	2
8	Research Project Design (Proposal)	-	-	4	2
	TOTAL	15	-	10	20

IV year VIII semester

S.NO	SUBJECT	L	T	P	C
1	Research Project / Dissertation	-	-	20	10
2	Emerging Threats and Technologies in Cyber Security	4	-	-	4
3	Critical Thinking in Cyber Security	4	-	-	4
4	Cyber Security Start-up Pathway	2	-	-	2
	TOTAL	10	-	20	20

1.1 Under Graduate Programme

Sl. No.	Course	Duration	Eligibility for admission
1	B.Sc. in Digital Forensics and Cyber Security	4 years (8 semesters)	Candidate must have passed 10+2 (or equivalent) examination from a recognized Board with Physics, Chemistry, and Biology/Mathematics/Computer Science as principal subjects, along with English as a subject of study. Minimum aggregate of 60% marks (40% for SC/ST/OBC and other reserved categories as per applicable State/UGC norms) in the qualifying examination. Admission shall be based on merit in qualifying examination and/or any national/state-level entrance test as notified by the University from time to time, followed by counseling as per Malla Reddy Vishwavidyapeeth admission regulations.

1.2. Medium of Instruction:

English.

1.3. Duration of the Course

4 years (8 semesters).

1.4 Examination Regulations**1.4.1 Attendance:**

A minimum of 75% attendance in each course (theory and practical) is mandatory for eligibility to appear in the End-Semester Examination; condonation up to 65% may be granted by the Vice-Chancellor on genuine medical/other grounds as per University rules.

1.4.2 Internal Assessments:

Course Type	Component	Weightage	Description
Theory Courses	Continuous Internal Assessment (CIA)	30%	Two mid-term tests (best of 2 or average), assignments/quizzes, seminars, attendance.
Practical / Laboratory Courses	Continuous Internal Assessment	30%	Lab records, in-lab performance, viva-voce during the semester.

Exam pattern for internal assessment**Theory Courses (Internal Examination, 30 marks, 2 hours)**

Section	Instruction	No. of Questions	Total Marks
A	Very Short Questions	5 × 2 marks	10
B	Short Questions	2 × 5 marks	10
C	Essay Questions	1 × 10 marks	10

Practical Courses (Internal Examination, 30 marks, 2 hours)

Section	Instruction	Total Marks
A	Spotter- Lab practical evaluation	15
B	Viva voce	15
	Total	30

1.4.3 University Examinations (External):

Course Type	Component	Weightage	Description
Theory Courses	End-Semester University Examination (ESE)	70%	Written examination of 3 hours covering the entire syllabus (all units).
Practical / Laboratory Courses	End-Semester Practical Examination	70%	Conduct of experiment/task, output/demo, record and viva-voce by internal + external examiner.

Theory Courses (End-Semester Examination, 70 marks, 3 hours)

Section	Instruction	No. of Questions	Total Marks
A	Very Short Questions	10 × 2 marks	20
B	Short Questions	6 × 5 marks	30
C	Essay Questions	2 × 10 marks	20

Total End-Semester marks = 70 (scaled from the above, or awarded directly out of 70 as per University question-paper template); combined with 30 CIA marks to yield 100.

Practical Courses (End-Semester Examination, 0 marks)

Section	Instruction	Total Marks
A	Spotter- Lab practical evaluation	20
B	Major Practical	10
C	Internal Viva	15
D	External Viva	15
E	Record	10
	Total	70

A student must secure a minimum of 'P' grade (40% aggregate, with at least 40% in ESE) to pass a course. A student who fails in a course may reappear in the subsequent supplementary/arrear examination.

Promotion to the next semester is automatic; however, a student must clear all backlog courses up to Semester IV before being permitted to register for Semester VII, and must clear all UG-level backlogs before the award of degree.

Malpractice in examinations shall be dealt with as per the University's Unfair Means regulations, ranging from cancellation of the concerned examination to debarment.

The Research Project/Dissertation (Semester VIII) must be submitted with a plagiarism similarity index within University-prescribed limits (typically ≤10% excluding references) prior to viva-voce.

I year I semester

S.NO	SUBJECT	L	T	P	C
1	Introduction to Digital Forensics and Cyber Security	4	-	-	4
2	Computer Fundamentals	2	-	-	2
3	Programming Fundamentals (C & Python)	2	-	2	4
4	Discrete Mathematics	2	-	-	2
5	English & Communication Skills	2	-	-	2
6	Practical's in Programming Fundamentals	-	-	2	2
7	Practical's in Basic Computer and Network Commands	-	-	4	4
	TOTAL	12	-	8	20

SEMESTER-I

INTRODUCTION TO DIGITAL FORENSICS AND CYBER SECURITY L/T/P/C

4/-/-4

Learning Outcome:

On completion of this course, students will be able to:

1. Explain the fundamental concepts, history and scope of digital forensics and cyber security.
2. Describe the categories of cybercrime and the digital-evidence lifecycle.
3. Identify the professional roles, career pathways and ethical responsibilities of a digital-forensics/cyber-security practitioner.
4. Discuss the relevance of Indian and international cyber-security frameworks to the profession.

UNIT-I

FOUNDATIONS OF CYBER SECURITY

Confidentiality, integrity and availability (CIA triad); threat, vulnerability and risk; overview of the cyber-threat landscape.

UNIT-II

FOUNDATIONS OF DIGITAL FORENSICS

Definition and scope of digital forensics; branches (computer, network, mobile, cloud, IoT forensics); evidentiary value of digital data.

UNIT-III

CYBERCRIME LANDSCAPE

Categories of cybercrime (hacking, phishing, ransom ware, identity theft, financial fraud, cyber terrorism); case studies.

UNIT-IV

DIGITAL EVIDENCE LIFECYCLE

Identification, preservation, collection, examination, analysis and presentation of digital evidence; chain of custody.

UNIT-V

PROFESSION AND ETHICS

Career pathways in digital forensics/cyber security; professional codes of conduct; overview of Indian IT Act 2000 and global frameworks.

SUGGESTED REFERENCES

1. William Stallings & Lawrie Brown, *Computer Security: Principles and Practice*, latest edition.
2. Eoghan Casey, *Digital Evidence and Computer Crime*, latest edition.
3. Nelson, Phillips & Steuart, *Guide to Computer Forensics and Investigations*, latest edition.

COMPUTER FUNDAMENTALS

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Describe the architecture and functional units of a digital computer.
2. Explain number systems, Boolean logic and data representation.
3. Describe operating-system and file-system fundamentals relevant to forensic examination.
4. Explain the basics of computer networks and the internet.

UNIT-I

COMPUTER ORGANIZATION

CPU, memory hierarchy, I/O subsystems, bus architecture; von Neumann model.

UNIT-II

DATA REPRESENTATION

Number systems, Boolean algebra, character encoding, binary/hex representation of data relevant to forensic byte-level analysis.

UNIT-III

OPERATING SYSTEMS BASICS

Functions of an OS, process/file management, an overview of Windows, Linux and macOS file systems.

UNIT-IV

STORAGE AND FILE SYSTEMS

Disk architecture, partitions, FAT/NTFS/text file systems, file metadata.

UNIT-V

NETWORKS AND INTERNET BASICS

Network topologies, OSI/TCP-IP model overview, IP addressing, basics of internet services relevant to cyber security.

SUGGESTED REFERENCES

1. P. Norton, *Introduction to Computers*, latest edition.
2. Andrew S. Tanenbaum, *Structured Computer Organization*, latest edition.

PROGRAMMING FUNDAMENTALS (C & PYTHON)

L/T/P/C

2/-/2/4

Learning Outcome:

On completion of this course, students will be able to:

1. Design algorithms and flowcharts for computational problems.
2. Write, debug and execute programs in C.
3. Write, debug and execute programs in Python for security-automation tasks.
4. Apply data structures and file-handling concepts in program design.

UNIT-I

PROBLEM SOLVING AND ALGORITHMS

Algorithm design, flowcharts, pseudo code; structured programming concepts.

UNIT-II

C PROGRAMMING BASICS

Data types, control structures, functions, arrays, pointers and structures in C.

UNIT-III

PYTHON PROGRAMMING BASICS

Python syntax, control structures, functions, data types, modules relevant to scripting for security tasks.

UNIT-IV

DATA STRUCTURES OVERVIEW

Arrays, linked lists, stacks and queues; introductory complexity concepts.

UNIT-V

FILE HANDLING AND BASIC I/O

File read/write operations in C and Python; use of Python scripts for log/file parsing tasks.

SUGGESTED REFERENCES

1. E. Balagurusamy, *Programming in ANSI C*, latest edition.
2. Allen B. Downey, *Think Python*, latest edition.

DISCRETE MATHEMATICS

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Apply set theory, relations and functions to computing problems.
2. Apply propositional and predicate logic to reasoning tasks.
3. Apply graph theory concepts relevant to network-topology analysis.
4. Apply combinatorics and number theory concepts relevant to cryptography.

UNIT-I

SETS, RELATIONS AND FUNCTIONS

Set operations, relations, equivalence classes, functions and their properties.

UNIT-II

MATHEMATICAL LOGIC

Propositional logic, predicate logic, logical equivalences and inference rules.

UNIT-III

GRAPH THEORY

Graphs, trees, connectivity, shortest paths -- relevance to network topology and routing analysis.

UNIT-IV

COMBINATORICS

Permutations, combinations, the pigeonhole principle relevant to password/key-space analysis.

UNIT-V

NUMBER THEORY

Modular arithmetic, prime numbers, the Euclidean algorithm -- foundations for cryptographic algorithms.

SUGGESTED REFERENCES

1. Kenneth H. Rosen, *Discrete Mathematics and Its Applications*, latest edition.

ENGLISH & COMMUNICATION SKILLS

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Demonstrate effective written communication for technical and investigative reports.
2. Demonstrate effective oral presentation and interview skills.
3. Apply grammar and vocabulary appropriate to professional/technical writing.
4. Draft basic forensic/incident-report documentation.

UNIT-I

GRAMMAR AND VOCABULARY

Core grammar, sentence construction, and technical vocabulary building.

UNIT-II

TECHNICAL WRITING

Report writing, email etiquette, documentation standards relevant to forensic and incident reports.

UNIT-III

ORAL COMMUNICATION

Presentation skills, group discussions, interview preparation.

UNIT-IV

READING AND COMPREHENSION

Critical reading of technical and case-study material.

UNIT-V

PROFESSIONAL COMMUNICATION IN CYBER SECURITY

Communicating findings to technical and non-technical/legal stakeholders.

SUGGESTED REFERENCES

1. Wren & Martin, *High School English Grammar and Composition*, latest edition.

PRACTICAL'S IN PROGRAMMING FUNDAMENTALS

L/T/P/C

-/-/2/2

Learning Outcome:

On completion of this course, students will be able to:

1. Implement and debug C and Python programs.
2. Apply basic data structures in solving simple programming exercises.

UNIT-I

LAB EXERCISES

C programming exercises: control structures, functions, arrays, pointers.

UNIT-II

LAB EXERCISES

Python scripting exercises: file parsing, simple automation scripts, basic data-structure implementation.

SUGGESTED REFERENCES

1. Course lab manual prescribed by the Board of Studies.

PRACTICAL'S IN BASIC COMPUTER AND NETWORK COMMANDS L/T/P/C

-/-/4/4

Learning Outcome:

On completion of this course, students will be able to:

1. Operate command-line utilities on Windows and Linux.
2. Use basic network diagnostic commands and utilities.

UNIT-I

LAB EXERCISES

Windows/Linux command-line basics, file/directory operations, permissions.

UNIT-II

LAB EXERCISES

Network commands: ping; trace route, ipconfig/ipconfig, netstat, and nslookup.

SUGGESTED REFERENCES

1. Course lab manual prescribed by the Board of Studies.

I year II semester

S.NO	SUBJECT	L	T	P	C
1	Network Security Fundamentals	2	-	-	2
2	Operating Systems	2	-	-	2
3	Introduction to Cryptography	2	-	-	2
4	Legal and Ethical Issues in Cyber Security	2	-	-	2
5	Linux and Shell Scripting	2	-	-	2
6	Essentials of Research Design and Technical Writing	2	-	-	2
7	Data Structures for Security Applications	2	-	-	2
8	Cyber Hygiene and Digital Citizenship	2	-	-	2
9	Practical's in Networking	-	-	2	1
10	Practical's in Linux/OS Administration	-	-	2	1
11	Practical's in Cryptography	-	-	4	2
	TOTAL	16	-	8	20

SEMESTER-II

NETWORK SECURITY FUNDAMENTALS

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Explain networking protocols and their security implications.
2. Describe common network attacks and corresponding defence mechanisms.
3. Configure basic firewall and access-control mechanisms.
4. Analyze network traffic for security anomalies.

UNIT-I

NETWORKING FOUNDATIONS

OSI/TCP-IP model, routing and switching basics, common protocols (HTTP, DNS, DHCP, FTP).

UNIT-II

NETWORK THREATS

Sniffing, spoofing, man-in-the-middle, denial-of-service and distributed denial-of-service attacks.

UNIT-III

PERIMETER DEFENSES

Firewalls, VPNs, proxies, network segmentation and access-control lists.

UNIT-IV

NETWORK MONITORING

Packet capture and analysis, intrusion-detection basics, log-based anomaly detection.

UNIT-V

WIRELESS NETWORK SECURITY

Wi-Fi security protocols (WEP/WPA/WPA2/WPA3), wireless attack vectors and mitigations.

SUGGESTED REFERENCES

1. William Stallings, *Network Security Essentials*, latest edition.
2. Behrouz Forouzan, *Data Communications and Networking*, latest edition.

OPERATING SYSTEMS

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Explain process, memory and file-system management in modern operating systems.
2. Describe OS security models and access-control mechanisms.
3. Compare Windows, Linux and macOS architectures from a security standpoint.
4. Apply OS-hardening principles.

UNIT-I

PROCESS MANAGEMENT

Processes, threads, scheduling, inter-process communication.

UNIT-II

MEMORY MANAGEMENT

Paging, segmentation, virtual memory concepts relevant to exploitation/defence.

UNIT-III

FILE SYSTEMS

File-system structures, permissions and access-control models.

UNIT-IV

OS SECURITY MODELS

Discretionary/mandatory access control, user privilege models, authentication mechanisms.

UNIT-V

OS HARDENING

Patch management, service minimization, secure configuration baselines for Windows/Linux.

SUGGESTED REFERENCES

1. Silberschatz, Galvin & Gagne, *Operating System Concepts*, latest edition.

INTRODUCTION TO CRYPTOGRAPHY

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Explain the principles of classical and modern cryptography.
2. Differentiate symmetric and asymmetric encryption schemes.
3. Explain hashing, digital signatures and key-management concepts.
4. Apply cryptographic principles to secure-communication scenarios.

UNIT-I

FOUNDATIONS OF CRYPTOGRAPHY

Classical ciphers, cryptographic goals, cryptanalysis basics.

UNIT-II

SYMMETRIC-KEY CRYPTOGRAPHY

DES, AES, block/stream cipher modes of operation.

UNIT-III

ASYMMETRIC-KEY CRYPTOGRAPHY

RSA, Diffie-Hellman key exchange, elliptic-curve cryptography basics.

UNIT-IV

HASHING AND DIGITAL SIGNATURES

Hash functions (MD5, SHA family), message-authentication codes, digital-signature schemes.

UNIT-V

KEY MANAGEMENT AND PKI BASICS

Key generation/distribution/storage, an introduction to public-key infrastructure and certificates.

SUGGESTED REFERENCES

1. William Stallings, *Cryptography and Network Security*, latest edition.

LEGAL AND ETHICAL ISSUES IN CYBER SECURITY

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Describe the Indian IT Act 2000 and its amendments.
2. Explain global cyber-law frameworks and data-protection regulations.
3. Discuss professional ethics in cyber security and digital forensics.
4. Analyze case studies involving cyber-law violations.

UNIT-I

INDIAN CYBER LAW

The Information Technology Act, 2000 and amendments; offences and penalties.

UNIT-II

GLOBAL FRAMEWORKS

GDPR, DPDP Act, and an overview of international cyber-law cooperation.

UNIT-III

INTELLECTUAL PROPERTY AND CYBERCRIME

IP protection in the digital domain, software piracy, and related offences.

UNIT-IV

PROFESSIONAL ETHICS

Codes of conduct for forensic examiners and security professionals; conflicts of interest.

UNIT-V

CASE STUDIES

Analysis of landmark cyber-law cases and their implications for practice.

SUGGESTED REFERENCES

1. Pavan Duggal, *Cyber Law*, latest edition.

LINUX AND SHELL SCRIPTING

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Navigate and administer Linux systems from the command line.
2. Write shell scripts to automate security and administrative tasks.
3. Apply file-permission and user-management concepts in Linux.

UNIT-I

LINUX FUNDAMENTALS

File system hierarchy, package management, process management.

UNIT-II

SHELL SCRIPTING BASICS

Bash scripting constructs, variables, loops, conditionals.

UNIT-III

AUTOMATION SCRIPTS

Writing scripts for log parsing, system monitoring and basic security checks.

UNIT-IV

USER AND PERMISSION MANAGEMENT

Users, groups, file permissions, sudo and access control.

SUGGESTED REFERENCES

1. William Shotts, *The Linux Command Line*, latest edition.

ESSENTIALS OF RESEARCH DESIGN AND TECHNICAL WRITING L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Explain the basics of research design and methodology.
2. Conduct literature reviews using academic databases.
3. Draft technical/research documents following professional standards.

UNIT-I

RESEARCH DESIGN BASICS

Research questions, hypotheses, qualitative/quantitative methods.

UNIT-II

LITERATURE REVIEW

Searching academic databases, citation management, avoiding plagiarism.

UNIT-III

TECHNICAL REPORT WRITING

Structure of technical/security reports, referencing standards.

UNIT-IV

RESEARCH ETHICS

Research integrity, ethical clearance basics relevant to security research involving data/systems.

SUGGESTED REFERENCES

1. Ranjit Kumar, *Research Methodology*, latest edition.

DATA STRUCTURES FOR SECURITY APPLICATIONS

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Implement common data structures relevant to security-tool development.
2. Analyze time/space complexity of algorithms used in security applications.
3. Apply hashing structures in the context of password/data-integrity checks.

UNIT-I

LINEAR DATA STRUCTURES

Arrays, stacks, queues, linked lists and their applications in log/packet processing.

UNIT-II

TREES AND HASH TABLES

Binary trees, hash tables and their role in indexing and integrity verification.

UNIT-III

SEARCHING AND SORTING

Search/sort algorithms relevant to large-scale log and evidence analysis.

UNIT-IV

GRAPHS IN SECURITY

Graph representations for network-topology and attack-path analysis.

SUGGESTED REFERENCES

1. Horowitz, Sahni & Anderson-Freed, *Fundamentals of Data Structures*, latest edition.

CYBER HYGIENE AND DIGITAL CITIZENSHIP

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Apply personal cyber-hygiene practices.
2. Identify social-engineering and online-fraud techniques.
3. Explain responsible and safe digital citizenship.

UNIT-I

PERSONAL CYBER HYGIENE

Password practices, multi-factor authentication, safe browsing.

UNIT-II

SOCIAL ENGINEERING AWARENESS

Phishing, vishing, smashing and pretesting techniques and defenses.

UNIT-III

DIGITAL CITIZENSHIP

Online privacy, digital footprints, safe social-media practices.

SUGGESTED REFERENCES

1. NCERT/industry cyber-hygiene handbooks as prescribed by the Board of Studies.

PRACTICAL'S IN NETWORKING

L/T/P/C

-/-/2/1

Learning Outcome:

On completion of this course, students will be able to:

1. Configure basic network devices and topologies.
2. Capture and analyze network traffic using standard tools.

UNIT-I

LAB EXERCISES

Configuring switches/routers in a simulated environment; sub netting exercises.

UNIT-II

LAB EXERCISES

Packet capture and analysis using Wireshark.

SUGGESTED REFERENCES

1. Course lab manual prescribed by the Board of Studies.

PRACTICAL'S IN LINUX/OS ADMINISTRATION

L/T/P/C

-/-/2/1

Learning Outcome:

On completion of this course, students will be able to:

1. Perform Linux system-administration tasks.
2. Write and test basic shell-automation scripts.

UNIT-I

LAB EXERCISES

Linux installation, user/permission management, package handling.

UNIT-II

LAB EXERCISES

Shell-scripting exercises for automation of routine security checks.

SUGGESTED REFERENCES

1. Course lab manual prescribed by the Board of Studies.

PRACTICAL'S IN CRYPTOGRAPHY

L/T/P/C

-/-/4/2

Learning Outcome:

On completion of this course, students will be able to:

1. Implement classical and modern encryption algorithms.
2. Use standard cryptographic libraries/tools for secure communication tasks.

UNIT-I

LAB EXERCISES

Implementing classical ciphers and symmetric encryption (AES) in Python/C.

UNIT-II

LAB EXERCISES

Implementing/using asymmetric encryption, hashing and digital signatures with standard libraries (OpenSSL/PyCryptodome).

SUGGESTED REFERENCES

1. Course lab manual prescribed by the Board of Studies.

II year III semester

S.NO	SUBJECT	L	T	P	C
1	Digital Forensics Investigation	2	-	-	2
2	Ethical Hacking	2	-	-	2
3	Database Security	2	-	-	2
4	Web Application Security	2	-	-	2
5	Computer Networks and Protocol Security	2	-	-	2
6	Operating Systems Security and Hardening	2	-	-	2
7	Cyber Threat Intelligence	2	-	-	2
8	Scripting for Security Automation (Python)	2	-	-	2
9	Practical's in Digital Forensics Tools	-	-	4	2
10	Practical's in Ethical Hacking Labs	-	-	2	1
11	Practical's in Web Application Security	-	-	2	1
	TOTAL	16	-	8	20

SEMESTER-III

DIGITAL FORENSICS INVESTIGATION

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Apply the digital-forensics investigation process to a simulated case.
2. Perform disk-imaging and evidence-preservation procedures.
3. Analyze file systems for evidentiary artifacts.
4. Prepare a forensically sound investigation report.

UNIT-I

FORENSIC INVESTIGATION PROCESS

Investigation models, first-responder procedures, legal considerations at the scene.

UNIT-II

EVIDENCE ACQUISITION

Disk imaging, write-blocking, hashing for integrity verification.

UNIT-III

FILE-SYSTEM FORENSICS

Analysis of FAT/NTFS/text file systems, recovering deleted data, metadata analysis.

UNIT-IV

FORENSIC TOOLS

Overview and use of standard forensic suites (e.g., Autopsy, FTK, EnCase-class tools).

UNIT-V

REPORTING AND TESTIMONY

Documentation standards, chain of custody, preparing findings for legal proceedings.

SUGGESTED REFERENCES

1. Nelson, Phillips & Steuart, *Guide to Computer Forensics and Investigations*, latest edition.
2. Eoghan Casey, *Digital Evidence and Computer Crime*, latest edition.

ETHICAL HACKING

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Explain the phases and methodology of ethical hacking.
2. Perform reconnaissance and vulnerability scanning in a lab environment.
3. Demonstrate exploitation techniques for identified vulnerabilities in a controlled setting.
4. Document findings following responsible-disclosure principles.

UNIT-I

ETHICAL HACKING METHODOLOGY

Reconnaissance, scanning, gaining access, maintaining access, covering tracks -- within legal/ethical boundaries.

UNIT-II

RECONNAISSANCE AND SCANNING

Foot printing techniques, port/vulnerability scanning tools.

UNIT-III

SYSTEM AND NETWORK EXPLOITATION

Exploiting common vulnerabilities in a controlled lab (password attacks, privilege escalation).

UNIT-IV

WEB AND APPLICATION EXPLOITATION

Exploiting common web-application vulnerabilities in a sandboxed environment.

UNIT-V

REPORTING AND RESPONSIBLE DISCLOSURE

Penetration-test reporting standards, responsible-disclosure and bug-bounty ethics.

SUGGESTED REFERENCES

1. EC-Council CEH courseware, latest edition.
2. Georgia Weidman, *Penetration Testing*, latest edition.

DATABASE SECURITY

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Explain database architectures and access-control models.
2. Identify common database vulnerabilities including SQL injection.
3. Apply database-hardening and auditing techniques.

UNIT-I

DATABASE FUNDAMENTALS

Relational database concepts, SQL basics relevant to security analysis.

UNIT-II

ACCESS CONTROL MODELS

Database user privileges, roles, discretionary/mandatory access control.

UNIT-III

DATABASE THREATS

SQL injection, privilege abuse, data-exfiltration techniques.

UNIT-IV

DATABASE HARDENING AND AUDITING

Encryption at rest, database auditing, backup and recovery security.

SUGGESTED REFERENCES

1. Ron Ben Natan, *Implementing Database Security and Auditing*, latest edition.

WEB APPLICATION SECURITY

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Explain the architecture of web applications and associated attack surfaces.
2. Identify vulnerabilities per the OWASP Top-10 classification.
3. Apply secure-coding and mitigation techniques for common web vulnerabilities.

UNIT-I

WEB APPLICATION ARCHITECTURE

Client-server model, HTTP/HTTPS, sessions and cookies.

UNIT-II

OWASP TOP-10 VULNERABILITIES

Injection, broken authentication, XSS, insecure deserialization and related classes.

UNIT-III

SECURE CODING PRACTICES

Input validation, output encoding, secure session management.

UNIT-IV

WEB APPLICATION TESTING TOOLS

Overview of tools used for web-vulnerability assessment in a lab environment.

SUGGESTED REFERENCES

1. OWASP Foundation, *OWASP Testing Guide*, latest edition.

COMPUTER NETWORKS AND PROTOCOL SECURITY

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Analyze protocol-level vulnerabilities across the TCP/IP stack.
2. Apply secure network-design principles.
3. Evaluate VPN and secure-tunneling technologies.

UNIT-I

PROTOCOL STACK VULNERABILITIES

Layer-wise vulnerabilities in the TCP/IP model.

UNIT-II

ROUTING SECURITY

Routing-protocol security considerations, route hijacking.

UNIT-III

SECURE NETWORK DESIGN

Network segmentation, DMZ design, zero-trust principles.

UNIT-IV

VPN AND TUNNELING TECHNOLOGIES

IPSec, SSL/TLS VPNs and secure-tunneling protocols.

SUGGESTED REFERENCES

1. William Stallings, *Network Security Essentials*, latest edition.

OPERATING SYSTEMS SECURITY AND HARDENING

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Apply OS-hardening baselines for Windows and Linux.
2. Configure logging and auditing mechanisms at the OS level.
3. Evaluate patch-management strategies.

UNIT-I

HARDENING BASELINES

CIS-benchmark style hardening for Windows/Linux.

UNIT-II

LOGGING AND AUDITING

Event logs, syslog, audit frameworks for OS-level monitoring.

UNIT-III

PATCH AND CONFIGURATION MANAGEMENT

Patch-management lifecycle, configuration-management tools.

SUGGESTED REFERENCES

1. CIS Benchmarks documentation, latest edition, as prescribed by the Board of Studies.

CYBER THREAT INTELLIGENCE

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Explain the cyber-threat-intelligence lifecycle.
2. Analyze threat actor tactics, techniques and procedures using standard frameworks.
3. Apply open-source intelligence techniques to threat analysis.

UNIT-I

THREAT INTELLIGENCE LIFECYCLE

Collection, processing, analysis and dissemination of threat intelligence.

UNIT-II

THREAT FRAMEWORKS

MITRE ATT&CK and related frameworks for classifying adversary behavior.

UNIT-III

OSINT FOR THREAT ANALYSIS

Open-source intelligence-gathering techniques and tools.

SUGGESTED REFERENCES

1. MITRE ATT&CK framework documentation.

SCRIPTING FOR SECURITY AUTOMATION (PYTHON)

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Write Python scripts for automating routine security tasks.
2. Use Python libraries for network and log analysis.

UNIT-I

PYTHON FOR SECURITY

Python libraries relevant to security automation (socket, requests, regex).

UNIT-II

AUTOMATION SCRIPTS

Automating log parsing, basic network scanning and report generation.

SUGGESTED REFERENCES

1. TJ O'Connor, *Violent Python*, latest edition.

PRACTICAL'S IN DIGITAL FORENSICS TOOLS

L/T/P/C

-/-/4/2

Learning Outcome:

On completion of this course, students will be able to:

1. Use standard digital-forensics tools to acquire and analyze evidence.
2. Prepare a forensic case report from a simulated dataset.

UNIT-I

LAB EXERCISES

Disk imaging and hashing using forensic tools.

UNIT-II

LAB EXERCISES

Artifact analysis and report generation from a simulated forensic image.

SUGGESTED REFERENCES

1. Course lab manual prescribed by the Board of Studies.

PRACTICAL'S IN ETHICAL HACKING LABS

L/T/P/C

-/-/2/1

Learning Outcome:

On completion of this course, students will be able to:

1. Conduct reconnaissance and vulnerability scans in an isolated lab.
2. Document findings following a standard penetration-testing report format.

UNIT-I

LAB EXERCISES

Scanning and enumeration exercises in a sandboxed lab environment.

SUGGESTED REFERENCES

1. Course lab manual prescribed by the Board of Studies.

PRACTICAL'S IN WEB APPLICATION SECURITY

L/T/P/C

-/-/2/1

Learning Outcome:

On completion of this course, students will be able to:

1. Identify OWASP Top-10 vulnerabilities in a deliberately vulnerable web application.
2. Apply basic mitigation techniques.

UNIT-I

LAB EXERCISES

Testing a deliberately vulnerable web application in an isolated lab environment.

SUGGESTED REFERENCES

1. Course lab manual prescribed by the Board of Studies.

II year IV semester

S.NO	SUBJECT	L	T	P	C
1	Malware Analysis and Reverse Engineering	2	-	-	2
2	Intrusion Detection and Prevention Systems	2	-	-	2
3	Cyber Security Management and Risk Assessment	2	-	-	2
4	Mobile and IoT Forensics	2	-	-	2
5	Memory and Network Forensics	2	-	-	2
6	Applied Cryptography and PKI	2	-	-	2
7	Security Operations Center (SOC) Fundamentals	2	-	-	2
8	Vulnerability Assessment Tools	2	-	-	2
9	Practical's in Malware Analysis	-	-	2	1
10	Practical's in IDS/IPS	-	-	2	1
11	Practical's in Mobile and Network Forensics	-	-	4	2
	TOTAL	16	-	8	20

SEMESTER-IV

MALWARE ANALYSIS AND REVERSE ENGINEERING

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Classify malware types and their propagation mechanisms.
2. Perform static and dynamic malware analysis in a sandboxed environment.
3. Apply basic reverse-engineering techniques to analyze malicious binaries.

UNIT-I

MALWARE FUNDAMENTALS

Viruses, worms, trojans, ransom ware and their behavioral characteristics.

UNIT-II

STATIC ANALYSIS

File-format analysis, string/signature analysis, disassembly basics.

UNIT-III

DYNAMIC ANALYSIS

Sandboxed execution, behavioral monitoring, network-traffic analysis of malware.

UNIT-IV

REVERSE ENGINEERING BASICS

Introduction to disassemblers/debuggers for malware analysis.

SUGGESTED REFERENCES

1. Michael Sikorski & Andrew Honig, *Practical Malware Analysis*, latest edition.

INTRUSION DETECTION AND PREVENTION SYSTEMS

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Explain signature-based and anomaly-based intrusion-detection approaches.
2. Configure and tune IDS/IPS systems in a lab environment.
3. Analyze IDS alerts to distinguish true and false positives.

UNIT-I

IDS/IPS FUNDAMENTALS

Detection approaches, deployment models (host-based/network-based).

UNIT-II

SIGNATURE-BASED DETECTION

Rule writing and signature-based detection engines.

UNIT-III

ANOMALY-BASED DETECTION

Statistical and behavioral anomaly-detection approaches.

UNIT-IV

IDS/IPS DEPLOYMENT AND TUNING

Deployment architectures, alert tuning and false-positive management.

SUGGESTED REFERENCES

1. Rebecca Bace, *Intrusion Detection*, latest edition.

CYBER SECURITY MANAGEMENT AND RISK ASSESSMENT

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Apply risk-assessment methodologies to organizational cyber-security planning.
2. Explain security-policy development and governance frameworks.
3. Evaluate business-continuity and disaster-recovery planning approaches.

UNIT-I

RISK MANAGEMENT FUNDAMENTALS

Risk identification, assessment and treatment methodologies.

UNIT-II

SECURITY POLICY AND GOVERNANCE

Policy development, security frameworks (ISO 27001-class standards).

UNIT-III

BUSINESS CONTINUITY PLANNING

Continuity and disaster-recovery planning principles for cyber incidents.

SUGGESTED REFERENCES

1. ISO/IEC 27001 standard documentation, latest edition.

MOBILE AND IOT FORENSICS

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Explain mobile-device and IoT architectures relevant to forensic acquisition.
2. Perform logical and physical acquisition of mobile-device data in a lab setting.
3. Analyze artifacts from IoT devices for evidentiary value.

UNIT-I

MOBILE DEVICE FORENSICS

Android/iOS architecture, acquisition methods, app-data analysis.

UNIT-II

IOT FORENSICS FUNDAMENTALS

IoT architecture, data sources and acquisition challenges.

UNIT-III

CLOUD-SYNCHED DATA ANALYSIS

Analyzing cloud-synchronized mobile/IoT data for forensic evidence.

SUGGESTED REFERENCES

1. Andrew Hoog, *Android Forensics*, latest edition.

MEMORY AND NETWORK FORENSICS

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Perform memory acquisition and analysis in a forensic lab environment.
2. Analyze network-traffic captures for evidence of compromise.
3. Correlate memory and network artifacts in an incident-investigation scenario.

UNIT-I

MEMORY FORENSICS FUNDAMENTALS

Volatile-memory structures, acquisition tools and techniques.

UNIT-II

MEMORY ANALYSIS

Process, network-connection and malware-artifact analysis from memory dumps.

UNIT-III

NETWORK FORENSICS

Full packet capture analysis, protocol reconstruction and traffic-pattern analysis.

UNIT-IV

CORRELATED INCIDENT ANALYSIS

Combining memory and network artifacts to reconstruct an incident timeline.

SUGGESTED REFERENCES

1. Michael Hale Ligh et al., *The Art of Memory Forensics*, latest edition.

APPLIED CRYPTOGRAPHY AND PKI

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Apply public-key infrastructure concepts to secure communication systems.
2. Evaluate certificate-based authentication mechanisms.
3. Analyze common cryptographic implementation flaws.

UNIT-I

PKI ARCHITECTURE

Certificate authorities, digital certificates, certificate lifecycle management.

UNIT-II

APPLIED PROTOCOLS

TLS/SSL handshake, certificate-based authentication.

UNIT-III

CRYPTOGRAPHIC IMPLEMENTATION ISSUES

Common implementation flaws and mitigation approaches.

SUGGESTED REFERENCES

1. William Stallings, *Cryptography and Network Security*, latest edition.

SECURITY OPERATIONS CENTER (SOC) FUNDAMENTALS

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Explain the structure, roles and workflows of a Security Operations Center.
2. Analyze security alerts using standard SOC tools and dashboards.
3. Apply escalation and incident-triage procedures.

UNIT-I

SOC STRUCTURE AND ROLES

Tiered analyst roles, SOC workflows and shift operations.

UNIT-II

MONITORING TOOLS

SIEM dashboards, alert triage, ticketing workflows.

UNIT-III

ESCALATION AND TRIAGE

Incident triage, prioritization and escalation procedures.

SUGGESTED REFERENCES

1. Industry SOC playbooks/standards as prescribed by the Board of Studies.

VULNERABILITY ASSESSMENT TOOLS

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Use standard vulnerability-assessment tools to scan lab systems.
2. Interpret vulnerability-scan reports and prioritize remediation.

UNIT-I

VULNERABILITY SCANNING FUNDAMENTALS

Scan types, credentialed vs. non-credentialed scanning.

UNIT-II

TOOL-BASED ASSESSMENT

Hands-on use of standard vulnerability-scanning tools and report interpretation.

SUGGESTED REFERENCES

1. Course lab manual and vendor documentation prescribed by the Board of Studies.

PRACTICAL'S IN MALWARE ANALYSIS

L/T/P/C

-/-/2/1

Learning Outcome:

On completion of this course, students will be able to:

1. Perform static and dynamic analysis of sample malware in an isolated sandbox.

UNIT-I

LAB EXERCISES

Static/dynamic analysis exercises using an isolated malware-analysis sandbox.

SUGGESTED REFERENCES

1. Course lab manual prescribed by the Board of Studies.

PRACTICAL'S IN IDS/IPS

L/T/P/C

-/-/2/1

Learning Outcome:

On completion of this course, students will be able to:

1. Configure and tune an IDS/IPS in a simulated network.

UNIT-I

LAB EXERCISES

Deploying and tuning an open-source IDS/IPS in a lab network.

SUGGESTED REFERENCES

1. Course lab manual prescribed by the Board of Studies.

PRACTICAL'S IN MOBILE AND NETWORK FORENSICS

L/T/P/C

-/-/4/2

Learning Outcome:

On completion of this course, students will be able to:

1. Perform mobile-device data acquisition and network-traffic analysis on simulated case data.

UNIT-I

LAB EXERCISES

Mobile-device acquisition exercises using forensic tools.

UNIT-II

LAB EXERCISES

Network-traffic capture and forensic analysis exercises.

SUGGESTED REFERENCES

1. Course lab manual prescribed by the Board of Studies.

III year V semester

S.NO	SUBJECT	L	T	P	C
1	Advanced Digital Forensics	3	-	-	3
2	Penetration Testing	3	-	-	3
3	Cloud Security	2	-	-	2
4	Block chain and Crypto currency Forensics	3	-	-	3
5	Bug Bounty and Responsible Disclosure Practices	2	-	-	2
6	Practical's in Penetration Testing	-	-	4	2
7	Practical's in Cloud Security	1	-	2	2
8	Internship	-	-	-	3
	TOTAL	14	-	6	20

SEMESTER-V

ADVANCED DIGITAL FORENSICS

L/T/P/C

3/-/-3

Learning Outcome:

On completion of this course, students will be able to:

1. Apply advanced forensic techniques to complex multi-source investigations.
2. Analyze anti-forensic techniques and corresponding countermeasures.
3. Prepare an expert forensic report for a complex simulated case.

UNIT-I

ADVANCED INVESTIGATION TECHNIQUES

Timeline analysis, multi-source evidence correlation.

UNIT-II

ANTI-FORENSICS

Data-hiding, encryption and anti-forensic techniques and their detection.

UNIT-III

CLOUD AND VIRTUALIZATION FORENSICS

Forensic acquisition considerations for cloud and virtualized environments.

UNIT-IV

EXPERT REPORTING

Preparing comprehensive expert-witness-quality forensic reports.

SUGGESTED REFERENCES

1. Eoghan Casey, *Handbook of Digital Forensics and Investigation*, latest edition.

PENETRATION TESTING

L/T/P/C

3/-/-3

Learning Outcome:

On completion of this course, students will be able to:

1. Plan and scope a penetration-testing engagement.
2. Execute a structured penetration test in a lab environment following standard methodologies.
3. Prepare a professional penetration-testing report with remediation guidance.

UNIT-I

PENETRATION TESTING METHODOLOGIES

Standard frameworks (PTES-class methodologies), engagement scoping and rules of engagement.

UNIT-II

NETWORK PENETRATION TESTING

Internal/external network penetration-testing techniques in a lab.

UNIT-III

APPLICATION PENETRATION TESTING

Web/application-layer penetration-testing techniques in a lab.

UNIT-IV

REPORTING AND REMEDIATION

Structuring findings, risk ratings and remediation recommendations.

SUGGESTED REFERENCES

1. Georgia Weidman, *Penetration Testing*, latest edition.
2. PTES documentation.

CLOUD SECURITY

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Explain cloud service and deployment models and their security implications.
2. Apply the shared-responsibility model to cloud-security planning.
3. Evaluate cloud-native security controls and configuration risks.

UNIT-I

CLOUD FUNDAMENTALS

IaaS/PaaS/SaaS models, deployment models, shared-responsibility model.

UNIT-II

CLOUD SECURITY CONTROLS

Identity and access management, encryption, network security in the cloud.

UNIT-III

CLOUD MISCONFIGURATION AND THREATS

Common cloud misconfigurations and associated threat scenarios.

SUGGESTED REFERENCES

1. NIST cloud-security guidance documents, latest edition.

BLOCK CHAIN AND CRYPTO CURRENCY FORENSICS

L/T/P/C

3/-/-3

Learning Outcome:

On completion of this course, students will be able to:

1. Explain block chain architecture and crypto currency transaction models.
2. Apply block chain-forensic techniques to trace crypto currency transactions.
3. Discuss regulatory considerations in crypto currency-related investigations.

UNIT-I

BLOCK CHAIN FUNDAMENTALS

Distributed-ledger architecture, consensus mechanisms, smart contracts overview.

UNIT-II

CRYPTO CURRENCY TRANSACTIONS

Wallet structures, transaction models, addresses analysis.

UNIT-III

BLOCK CHAIN FORENSIC ANALYSIS

Transaction-tracing techniques and tools for crypto currency investigations.

UNIT-IV

REGULATORY LANDSCAPE

Overview of regulatory approaches to crypto currency-related crime.

SUGGESTED REFERENCES

1. Andreas Antonopoulos, *Mastering Bitcoin*, latest edition.

BUG BOUNTY AND RESPONSIBLE DISCLOSURE PRACTICES

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Explain the bug-bounty ecosystem and responsible-disclosure principles.
2. Prepare a professional vulnerability-disclosure report.

UNIT-I

BUG BOUNTY ECOSYSTEM

Bug-bounty platforms, scope definitions, reward structures.

UNIT-II

RESPONSIBLE DISCLOSURE

Coordinated vulnerability disclosure principles and reporting templates.

SUGGESTED REFERENCES

1. Industry responsible-disclosure guidelines as prescribed by the Board of Studies.

PRACTICAL'S IN PENETRATION TESTING

L/T/P/C

-/-/4/2

Learning Outcome:

On completion of this course, students will be able to:

1. Conduct an end-to-end penetration test on a lab environment and produce a professional report.

UNIT-I

LAB EXERCISES

Structured penetration-testing exercise on an isolated lab network/application.

SUGGESTED REFERENCES

1. Course lab manual prescribed by the Board of Studies.

PRACTICAL'S IN CLOUD SECURITY

L/T/P/C

-/-/2/2

Learning Outcome:

On completion of this course, students will be able to:

1. Configure and assess security controls on a cloud-lab environment.

UNIT-I

LAB EXERCISES

Configuring IAM, storage and network security controls on a cloud sandbox account.

SUGGESTED REFERENCES

1. Course lab manual prescribed by the Board of Studies.

INTERNSHIP

L/T/P/C

-/-/-3

Learning Outcome:

On completion of this course, students will be able to:

1. Apply classroom knowledge to real/simulated organizational cyber-security or forensics tasks.
2. Reflect on professional practice and workplace expectations through a structured internship report.

UNIT-I

INTERNSHIP PLACEMENT

Structured placement with an industry, government, or campus-based security/forensics unit under faculty and industry mentorship.

SUGGESTED REFERENCES

1. Internship guidelines as prescribed by the Board of Studies.

III year VI semester

S.NO	SUBJECT	L	T	P	C
1	Incident Response and Disaster Recovery	3	-	-	3
2	Security Auditing and Compliance	2	-	-	2
3	Cyber Law and Compliance	2	-	-	2
4	Governance, Risk and Compliance (GRC) for Cyber Security	2	-	-	2
5	Security Information and Event Management (SIEM)	2	-	-	2
6	Wireless and IoT Security	3	-	-	3
7	Cyber Forensics for E-Commerce and Fintech	2	-	-	2
8	Ethics, Privacy and Data Protection Regulations	2	-	-	2
9	Entrepreneurship in Cyber Security	2	-	-	2
	TOTAL	20	-	-	20

SEMESTER-VI

INCIDENT RESPONSE AND DISASTER RECOVERY

L/T/P/C

3/-/-3

Learning Outcome:

On completion of this course, students will be able to:

1. Apply a structured incident-response lifecycle to a simulated cyber incident.
2. Develop a disaster-recovery and business-continuity plan.
3. Coordinate a tabletop incident-response exercise.

UNIT-I

INCIDENT RESPONSE LIFECYCLE

Preparation, detection, containment, eradication, recovery and lessons-learned phases.

UNIT-II

INCIDENT HANDLING TECHNIQUES

Triage, evidence preservation during response, communication protocols.

UNIT-III

DISASTER RECOVERY PLANNING

Recovery-point/recovery-time objectives, backup strategies, DR-site models.

UNIT-IV

TABLETOP EXERCISES

Designing and conducting simulated incident-response exercises.

SUGGESTED REFERENCES

1. NIST SP 800-61, *Computer Security Incident Handling Guide*, latest edition.

SECURITY AUDITING AND COMPLIANCE

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Plan and conduct a security audit against a recognized standard.
2. Prepare compliance documentation for common regulatory frameworks.

UNIT-I

SECURITY AUDIT FUNDAMENTALS

Audit planning, scoping, evidence gathering.

UNIT-II

COMPLIANCE FRAMEWORKS

ISO 27001, SOC 2 and other prevalent compliance frameworks.

UNIT-III

AUDIT REPORTING

Findings documentation, corrective-action planning.

SUGGESTED REFERENCES

1. ISO/IEC 27001 and related audit standards, latest edition.

CYBER LAW AND COMPLIANCE

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Analyze cyber-law provisions applicable to digital-forensics evidence admissibility.
2. Explain sector-specific compliance obligations (financial, healthcare, critical infrastructure).

UNIT-I

EVIDENCE ADMISSIBILITY

Legal standards for admissibility of digital evidence in Indian courts.

UNIT-II

SECTOR-SPECIFIC COMPLIANCE

Compliance obligations for financial, healthcare and critical-infrastructure sectors.

UNIT-III

INTERNATIONAL COOPERATION

Cross-border cybercrime cooperation frameworks and mutual legal assistance.

SUGGESTED REFERENCES

1. Pavan Duggal, *Cyber Law*, latest edition.

GOVERNANCE, RISK AND COMPLIANCE (GRC) FOR CYBER SECURITY

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Explain the components of a GRC programme.
2. Apply GRC tools/frameworks to organizational risk-management planning.

UNIT-I

GRC FUNDAMENTALS

Governance structures, risk-management processes, compliance obligations.

UNIT-II

GRC FRAMEWORKS AND TOOLS

Overview of common GRC frameworks and supporting tools.

SUGGESTED REFERENCES

1. ISACA GRC guidance documents, latest edition.

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) L/T/P/C
2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Configure log sources and correlation rules within a SIEM platform.
2. Analyze SIEM-generated alerts to identify security incidents.

UNIT-I

SIEM ARCHITECTURE

Log collection, normalization, correlation-engine concepts.

UNIT-II

SIEM USE CASES

Building and tuning correlation rules and dashboards for common attack scenarios.

SUGGESTED REFERENCES

1. Vendor-neutral SIEM documentation prescribed by the Board of Studies.

WIRELESS AND IOT SECURITY

L/T/P/C

3/-/-/3

Learning Outcome:

On completion of this course, students will be able to:

1. Analyze security weaknesses in wireless and IoT protocols.
2. Apply mitigation techniques for common wireless/IoT attack scenarios.

UNIT-I

WIRELESS SECURITY

Wi-Fi/Bluetooth protocol vulnerabilities and mitigation.

UNIT-II

IOT SECURITY

IoT architecture-level vulnerabilities, device-hardening approaches.

SUGGESTED REFERENCES

1. Industry IoT-security guidance documents, latest edition.

CYBER FORENSICS FOR E-COMMERCE AND FINTECH

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Explain fraud patterns specific to e-commerce and fintech platforms.
2. Apply forensic techniques to financial-fraud investigation scenarios.

UNIT-I

E-COMMERCE/FINTECH FRAUD PATTERNS

Payment fraud, account takeover, transaction-fraud patterns.

UNIT-II

FINANCIAL FORENSIC TECHNIQUES

Forensic accounting basics and digital-evidence techniques for financial fraud.

SUGGESTED REFERENCES

1. RBI/industry fraud-risk-management guidance documents.

ETHICS, PRIVACY AND DATA PROTECTION REGULATIONS

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Explain global data-protection regulatory landscapes (GDPR, DPDP Act).
2. Apply privacy-by-design principles to system/process design.

UNIT-I

DATA PROTECTION REGULATIONS

GDPR, India's DPDP Act and comparative regulatory approaches.

UNIT-II

PRIVACY ENGINEERING

Privacy-by-design and privacy-impact-assessment methodologies.

SUGGESTED REFERENCES

1. DPDP Act 2023 and GDPR official texts.

ENTREPRENEURSHIP IN CYBER SECURITY

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Explain the start-up ecosystem for cyber-security products and services.
2. Develop a basic business plan for a cyber-security venture idea.

UNIT-I

CYBER SECURITY START-UP LANDSCAPE

Product/service categories, market opportunities in security start-ups.

UNIT-II

BUSINESS PLANNING BASICS

Business-model canvas application to a cyber-security venture idea.

SUGGESTED REFERENCES

1. Standard entrepreneurship textbooks prescribed by the Board of Studies.

IV year VII semester

S.NO	SUBJECT	L	T	P	C
1	Cyber Security Research and Development	2	-	-	2
2	Cyber Security Project Management	3	-	-	3
3	Advanced Penetration Testing and Red Teaming	2	-	2	3
4	Threat Hunting and Advanced Persistent Threats	2	-	2	3
5	Cyber-Physical Systems and Critical Infrastructure Security	2	-	2	3
6	Social Media and OSINT Investigations	2	-	-	2
7	Artificial Intelligence for Cyber Security	2	-	-	2
8	Research Project Design (Proposal)	-	-	4	2
	TOTAL	15	-	10	20

SEMESTER-VII

CYBER SECURITY RESEARCH AND DEVELOPMENT

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Formulate a research problem in an emerging cyber-security/forensics area.
2. Apply research methodologies to evaluate proposed security solutions.
3. Present research findings in a structured technical format.

UNIT-I

RESEARCH PROBLEM FORMULATION

Identifying research gaps in cyber security/digital forensics.

UNIT-II

APPLIED RESEARCH METHODS

Experimental design, evaluation metrics for security solutions.

UNIT-III

EMERGING RESEARCH AREAS

Overview of current research directions (AI-driven security, quantum-safe cryptography, etc.).

UNIT-IV

TECHNICAL PRESENTATION

Structuring and presenting a research paper/poster.

SUGGESTED REFERENCES

1. Recent peer-reviewed publications curated by the Board of Studies.

CYBER SECURITY PROJECT MANAGEMENT

L/T/P/C

3/-/-3

Learning Outcome:

On completion of this course, students will be able to:

1. Apply project-management methodologies to cyber-security project planning.
2. Develop a project plan including scope, schedule, and risk and resource management for a security initiative.

UNIT-I

PROJECT MANAGEMENT FUNDAMENTALS

Project life cycle, scope/schedule/cost management.

UNIT-II

SECURITY PROJECT PLANNING

Applying PM methodologies to security-tool rollout/audit/response projects.

UNIT-III

RISK AND RESOURCE MANAGEMENT

Risk registers, resource allocation, stakeholder communication for security projects.

SUGGESTED REFERENCES

1. PMI, *A Guide to the Project Management Body of Knowledge (PMBOK)*, latest edition.

ADVANCED PENETRATION TESTING AND RED TEAMING

L/T/P/C

2/-/2/3

Learning Outcome:

On completion of this course, students will be able to:

1. Plan and execute a red-team engagement in a controlled environment.
2. Apply advanced evasion and lateral-movement techniques within an authorized lab scope.
3. Report red-team findings with strategic remediation recommendations.

UNIT-I

RED TEAM OPERATIONS

Red-team vs. penetration-test scoping, adversary emulation concepts.

UNIT-II

ADVANCED EXPLOITATION TECHNIQUES

Lateral movement, privilege escalation and persistence in an authorized lab.

UNIT-III

EVASION TECHNIQUES

Detection-evasion concepts and defensive countermeasures.

UNIT-IV

REPORTING AND DEBRIEF

Strategic reporting and stakeholder debrief for red-team engagements.

SUGGESTED REFERENCES

1. Red Team Field Manual and related practitioner references.

THREAT HUNTING AND ADVANCED PERSISTENT THREATS

L/T/P/C

2/-/2/3

Learning Outcome:

On completion of this course, students will be able to:

1. Explain the characteristics and lifecycle of advanced persistent threats.
2. Apply proactive threat-hunting techniques using security telemetry.
3. Analyze APT case studies to identify indicators of compromise.

UNIT-I

APT CHARACTERISTICS

APT lifecycle, notable APT campaign case studies.

UNIT-II

THREAT HUNTING METHODOLOGY

Hypothesis-driven hunting, use of telemetry and threat-Intel feeds.

UNIT-III

INDICATORS OF COMPROMISE

Identifying and validating IoCs across endpoint/network telemetry.

UNIT-IV

HANDS-ON HUNTING EXERCISE

Structured threat-hunting exercise on simulated telemetry data.

SUGGESTED REFERENCES

1. MITRE ATT&CK framework and associated threat-hunting playbooks.

CYBER-PHYSICAL SYSTEMS AND CRITICAL INFRASTRUCTURE SECURITY

L/T/P/C

2/-/2/3

Learning Outcome:

On completion of this course, students will be able to:

1. Explain the architecture of industrial control systems and SCADA environments.
2. Analyze security risks specific to critical-infrastructure systems.
3. Apply defence-in-depth principles to cyber-physical system security.

UNIT-I

ICS/SCADA ARCHITECTURE

Industrial control system components, protocols (Modbus, DNP3).

UNIT-II

CRITICAL INFRASTRUCTURE THREATS

Notable incidents and threat models specific to critical infrastructure.

UNIT-III

DEFENCE STRATEGIES

Defence-in-depth, network segmentation for OT/IT convergence.

UNIT-IV

LAB EXERCISE

Simulated ICS-security assessment exercise.

SUGGESTED REFERENCES

1. Eric Knapp, *Industrial Network Security*, latest edition.

SOCIAL MEDIA AND OSINT INVESTIGATIONS

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Apply OSINT techniques to social-media-based investigations.
2. Discuss ethical and legal boundaries of OSINT collection.

UNIT-I

OSINT TECHNIQUES

Social-media reconnaissance, metadata analysis, OSINT tools.

UNIT-II

LEGAL AND ETHICAL BOUNDARIES

Privacy considerations and legal limits in OSINT-based investigations.

SUGGESTED REFERENCES

1. Michael Bazzell, *Open Source Intelligence Techniques*, latest edition.

ARTIFICIAL INTELLIGENCE FOR CYBER SECURITY

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Explain applications of AI/ML in threat detection and security automation.
2. Evaluate the strengths and limitations of AI-driven security tools.
3. Discuss adversarial-AI risks relevant to security systems.

UNIT-I

AI/ML IN SECURITY

Applications in malware classification, anomaly detection, phishing detection.

UNIT-II

SECURITY AUTOMATION WITH AI

SOAR concepts and AI-assisted triage/response.

UNIT-III

ADVERSARIAL AI

Adversarial-example risks and AI-model security considerations.

SUGGESTED REFERENCES

1. Recent survey papers on AI in cyber security curated by the Board of Studies.

RESEARCH PROJECT DESIGN (PROPOSAL)

L/T/P/C

-/-/4/2

Learning Outcome:

On completion of this course, students will be able to:

1. Formulate a research/dissertation proposal in a chosen cyber-security/forensics area.
2. Prepare a literature review and methodology for the proposed project.

UNIT-I

PROPOSAL DEVELOPMENT

Problem statement, objectives, scope and expected outcomes.

UNIT-II

LITERATURE REVIEW AND METHODOLOGY

Structured literature survey and proposed research methodology.

SUGGESTED REFERENCES

1. Guidelines issued by the Research and Innovation Committee.

IV year VIII semester

S.NO	SUBJECT	L	T	P	C
1	Research Project / Dissertation	-	-	20	10
2	Emerging Threats and Technologies in Cyber Security	4	-	-	4
3	Critical Thinking in Cyber Security	4	-	-	4
4	Cyber Security Start-up Pathway	2	-	-	2
	TOTAL	10	-	20	20

SEMESTER-VIII

RESEARCH PROJECT / DISSERTATION

L/T/P/C
-/-/20/10

Learning Outcome:

On completion of this course, students will be able to:

1. Execute the approved research project/dissertation under faculty guidance.
2. Analyze and interpret results relevant to the chosen cyber-security/forensics problem.
3. Prepare and defend a written dissertation before an evaluation committee.

UNIT-I

PROJECT EXECUTION

Implementation of the approved methodology under continuous guide assessment.

UNIT-II

ANALYSIS AND DOCUMENTATION

Data/result analysis, dissertation writing per University format.

UNIT-III

VIVA-VOCE DEFENCE

Defence of the dissertation before a committee including an external expert.

SUGGESTED REFERENCES

1. Dissertation guidelines issued by the Research and Innovation Committee.

EMERGING THREATS AND TECHNOLOGIES IN CYBER SECURITY L/T/P/C

4/-/-/4

Learning Outcome:

On completion of this course, students will be able to:

1. Analyze emerging threat trends relevant to next-generation technologies.
2. Evaluate the security implications of emerging technologies (5G, quantum computing, AI).

UNIT-I

EMERGING THREAT LANDSCAPE

Trends in ransom ware-as-a-service, supply-chain attacks, and deep fake-enabled fraud.

UNIT-II

EMERGING TECHNOLOGY SECURITY

Security implications of 5G, quantum computing and pervasive AI adoption.

SUGGESTED REFERENCES

1. Recent industry threat-landscape reports curated by the Board of Studies.

CRITICAL THINKING IN CYBER SECURITY

L/T/P/C

4/-/-4

Learning Outcome:

On completion of this course, students will be able to:

1. Apply structured critical-thinking frameworks to security decision-making scenarios.
2. Evaluate case studies to identify reasoning fallacies in incident/risk analysis.

UNIT-I

CRITICAL THINKING FRAMEWORKS

Structured-analytic techniques applied to security-decision scenarios.

UNIT-II

APPLIED CASE ANALYSIS

Case-study analysis of security decisions and reasoning pitfalls.

SUGGESTED REFERENCES

1. Richards J. Heuer Jr., *Psychology of Intelligence Analysis*, latest edition.

CYBER SECURITY START-UP PATHWAY

L/T/P/C

2/-/-/2

Learning Outcome:

On completion of this course, students will be able to:

1. Develop a business-model canvas for a cyber-security product/venture.
2. Prepare and deliver a start-up pitch for a cyber-security concept.

UNIT-I

BUSINESS MODEL DESIGN

Business-model canvas for a cyber-security venture.

UNIT-II

PITCHING AND GO-TO-MARKET

Preparing a pitch deck and outlining a go-to-market/regulatory pathway.

SUGGESTED REFERENCES

1. Standard lean-start-up references prescribed by the Board of Studies.