MALLA REDDY VISHWAVIDYAPEETH

SCHOOL OF DIGITAL HEALTH SCIENCES AND TECHNOLOGY

Program

Master of Science (M.Sc.)

Digital Forensics and Cyber Security

2026–27

MALLA REDDY VISHWAVIDYAPEETH
SCHOOL OF DIGITAL HEALTH SCIENCES AND TECHNOLOGY
MASTER OF SCIENCE (M.Sc.) IN DIGITAL FORENSICS AND CYBER SECURITY

VISION

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.
2. To develop research-capable, industry- and academia-ready postgraduates who can independently lead advanced cyber-security defence, digital-forensic investigation and security research that safeguards individuals, organizations and critical infrastructure against sophisticated cyber threats.

MISSION

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 instil 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.
6. Deepen competence in advanced network security, cryptography, and research methodology relevant to advanced cyber-security and forensics practice.
7. Build advanced proficiency in penetration testing, intrusion detection, security auditing and compliance applied to complex, real-world organizational environments.
8. Develop mastery of advanced digital-forensic investigation, malware reverse engineering, cloud/mobile/IoT forensics, and AI-driven threat detection through specialization electives and dedicated practicals.
9. Cultivate independent research aptitude, critical thinking, and project-leadership competence through an intensive Thesis/Research Project in the final semester.

PROGRAM EDUCATIONAL OBJECTIVES (PEOs)

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

1. Lead the design, defence and forensic investigation of complex cyber-security incidents across organizational, governmental and critical-infrastructure environments.
2. Advance into senior/specialist careers such as Senior SOC Analyst/Lead, Digital Forensics Examiner/Expert Witness, Threat Intelligence Analyst, Red Team Lead, or Security Researcher, or pursue doctoral research (Ph.D.) in cyber security or digital forensics.
3. Demonstrate advanced professional, ethical and legal responsibility while conducting security research, investigations and disclosure of vulnerabilities.
4. Conduct independent, rigorous research and lead innovation in emerging cyber-security domains, including AI-driven security, cloud/IoT security and critical-infrastructure protection.

PROGRAM OUTCOMES (POs)

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

1. **Network Security & Cryptography:** Analyze and implement advanced network security protocols, cryptographic algorithms (symmetric/asymmetric), PKI, and wireless security to protect health and enterprise IT infrastructures.
2. **Digital Forensics Investigation:** Conduct end-to-end digital forensics investigations including disk, memory, network, mobile, and IoT forensics while maintaining chain of custody and legal admissibility.
3. **Malware Analysis & Reverse Engineering:** Perform static and dynamic malware analysis, reverse engineer binaries using IDA Pro/Ghidra, develop YARA rules, and analyze advanced threats (rootkits, ransomware, APTs).
4. **Penetration Testing, Incident Response & Compliance:** Plan and execute penetration tests (network, web, wireless), manage incident-response lifecycles, and implement security-auditing frameworks (ISO 27001, NIST CSF, PCI-DSS).
5. **Cyber Threat Intelligence & Project Management:** Collect and analyze OSINT, apply MITRE ATT&CK for threat hunting, manage security projects (SOC building, DR/BCP), and communicate technical risks to executive and legal audiences.
6. **Research, Innovation and Professional Responsibility:** Conduct independent, ethically sound research; evaluate emerging threats and technologies; and apply cyber-law, data-privacy and professional-ethics principles in investigation, disclosure and reporting.

PROGRAM SPECIFIC OUTCOMES (PSOs)

At the end of the programme, graduates of M.Sc. Digital Forensics and Cyber Security will specifically be able to:

1. Independently conduct advanced digital-forensic investigations (disk, memory, network, mobile, cloud and IoT) and produce legally admissible expert reports and testimony.
2. Design, deploy and lead security operations (SOC, SIEM, IDS/IPS) and incident-response/disaster-recovery programmes for complex organizational and critical infrastructure.
3. Plan and execute advanced offensive-security engagements (penetration testing, red teaming, threat hunting) and reverse-engineer/analyse sophisticated malware and APT campaigns.
4. Conduct independent, ethically sound research culminating in a thesis addressing an original problem in cyber security or digital forensics, in compliance with legal, regulatory and governance frameworks.

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

Semester I

S.NO	SUBJECT	L	T	P	C
1	Advanced Network Security and Cryptography	3	-	-	3
2	Advanced Digital Forensics Investigation Techniques	3	-	-	3
3	Malware Analysis and Reverse Engineering	3	-	-	3
4	Research Methodology in Cyber Security and Forensics	2	-	-	2
5	English & Communication Skills	2	-	-	2
6	Computer Foundation for Security Professionals	2	-	-	2
7	Practical: Advanced Network Security Configuration	-	-	4	2
8	Practical: Digital Forensics Tools	-	-	4	2
9	Introduction to GitHub & Version Control	1	-	-	1
	TOTAL	**16**	**-**	**8**	**20**

Semester II

S.NO	SUBJECT	L	T	P	C
1	Penetration Testing and Vulnerability Assessment	3	-	-	3
2	Intrusion Detection and Prevention Systems	3	-	-	3
3	Security Auditing and Compliance	3	-	-	3
4	Network Forensics and Traffic Analysis	2	-	-	2
5	Cyber Security Regulations and Ethics	2	-	-	2
6	Open Source Intelligence (OSINT) and Threat Hunting	2	-	-	2
7	Practical: Penetration Testing Techniques	-	-	4	2
8	Practical: Security Auditing Techniques	-	-	4	2
9	Soft Skills and Professional Development	1	-	-	1
	TOTAL	**16**	**-**	**8**	**20**

MALLA REDDY VISHWAVIDYAPEETH

SCHOOL OF DIGITAL HEALTH SCIENCES AND TECHNOLOGY

MASTER OF SCIENCE (M.Sc.) IN DIGITAL FORENSICS AND CYBER SECURITY

COURSE STRUCTURE

Semester III

S.NO	SUBJECT	L	T	P	C
1	Cyber Security Incident Response and Disaster Recovery	3	-	-	3
2	Cloud Security and Virtualization Security	3	-	-	3
3	Cyber Law and Ethical Hacking	3	-	-	3
4	Mobile and IoT Forensics	2	-	-	2
5	AI and Machine Learning in Cyber Security	2	-	-	2
6	Practical: Incident Response Implementation	-	-	6	3
7	Practical: Cloud Security Implementation	-	-	6	3
8	Seminar: Emerging Threats and Case Studies	1	-	-	1
	TOTAL	**14**	**-**	**12**	**20**

Semester IV

S.NO	SUBJECT	L	T	P	C
1	Advanced Malware Analysis and Reverse Engineering	3	-	-	3
2	Cyber Threat Intelligence and Hunting	3	-	-	3
3	Digital Forensics and Cyber Security Project Management	2	-	-	2
4	Thesis / Research Project	-	-	1	2
	TOTAL	**8**	**-**	**-**	**20**

1.1 Post Graduate Programme

Sl. No.	Course	Duration	Eligibility for admission
1	M.Sc. Digital Forensics and Cyber Security	2 years (4 semesters)	1. Candidate must hold a Bachelor's degree (3- or 4-year, NEP 2020 compliant) in Digital Forensics and Cyber Security, Computer Science/IT, Information Security, Electronics/Computer Engineering, or any other discipline recognised as equivalent by the University, from a recognised university. 2. Minimum aggregate of 50% marks (45% for SC/ST/OBC and other reserved categories as per applicable State/UGC norms) in the qualifying Bachelor's degree. 3. Admission shall be based on merit in the qualifying examination and/or any national/state-level postgraduate entrance test (e.g., CUET-PG or University-conducted entrance test) as notified by the University from time to time, followed by counselling as per Malla Reddy Vishwavidyapeeth admission regulations. 4. Candidates from non-computing backgrounds may be required to complete a bridge module (in coordination with the School) in computer foundations and networking fundamentals during Semester I.

1.2. Medium of Instruction:

English.

1.3. Duration of the Course

2 years (4 semesters).

1.4 Examination Regulations

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.

MALLA REDDY VISHWAVIDYAPEETH

SCHOOL OF DIGITAL HEALTH SCIENCES AND TECHNOLOGY

MASTER OF SCIENCE (M.Sc.) IN DIGITAL FORENSICS AND CYBER SECURITY

Semester I

S.NO	SUBJECT	L	T	P	C
1	Advanced Network Security and Cryptography	3	-	-	3
2	Advanced Digital Forensics Investigation Techniques	3	-	-	3
3	Malware Analysis and Reverse Engineering	3	-	-	3
4	Research Methodology in Cyber Security and Forensics	2	-	-	2
5	English & Communication Skills	2	-	-	2
6	Computer Foundation for Security Professionals	2	-	-	2
7	Practical: Advanced Network Security Configuration	-	-	4	2
8	Practical: Digital Forensics Tools	-	-	4	2
9	Introduction to GitHub & Version Control	1	-	-	1
	TOTAL	**16**	**-**	**8**	**20**

SEMESTER-I

ADVANCED NETWORK SECURITY AND CRYPTOGRAPHY

L/T/P/C
3/-/-/3

Learning Outcome:

1. Analyse advanced network-security threats and design defence-in-depth architectures for enterprise infrastructures.
2. Apply symmetric and asymmetric cryptographic algorithms and hashing schemes to secure data and communications.
3. Design and evaluate PKI deployments, X.509 certificate management and SSL/TLS hardening strategies.
4. Configure secure network protocols (IPSec, VPN, 802.1X) and assess wireless and emerging-technology security risks.

UNIT-I

FUNDAMENTALS OF NETWORK SECURITY

1. OSI / TCP-IP security considerations
2. Security threats: reconnaissance, spoofing, DoS/DDoS, MITM
3. Defence-in-depth and layered security architecture

UNIT-II

CRYPTOGRAPHIC ALGORITHMS AND PROTOCOLS

1. Symmetric encryption: AES, DES, 3DES
2. Asymmetric encryption: RSA, ECC, Diffie-Hellman key exchange
3. Hashing: SHA-2, SHA-3, HMAC and digital signatures

UNIT-III

PUBLIC KEY INFRASTRUCTURE (PKI) AND CERTIFICATE MANAGEMENT

1. X.509 certificates, CA hierarchy, certificate revocation (CRL, OCSP)
2. SSL/TLS – handshake, versions, vulnerabilities and hardening
3. PKI deployment scenarios and best practices

UNIT-IV

NETWORK SECURITY PROTOCOLS AND SECURE COMMUNICATIONS

1. IPSec (AH, ESP, IKE), VPN technologies (SSL-VPN, L2TP)
2. Secure network design: DMZ, firewall rule sets, ACLs
3. 802.1X, RADIUS, TACACS+ for network access control

UNIT-V

WIRELESS SECURITY AND EMERGING THREATS

1. WPA2/WPA3, rogue AP detection, wireless intrusion prevention
2. Bluetooth, ZigBee, 5G security considerations
3. Post-quantum cryptography and future trends

REFERENCE BOOKS

1. Stallings, W. (2022). Cryptography and Network Security: Principles and Practice (8th ed.). Pearson.
2. Forouzan, B. A. (2021). Data Communications and Networking (5th ed.). McGraw-Hill.
3. Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography Engineering. Wiley.
4. Ciampa, M. (2021). CompTIA Security+ Guide to Network Security Fundamentals (7th ed.). Cengage.
5. Bernstein, D. J., & Lange, T. (2017). Post-Quantum Cryptography. Springer.

ADVANCED DIGITAL FORENSICS INVESTIGATION TECHNIQUES

L/T/P/C
3/-/-/3

Learning Outcome:

1. Apply digital-forensics principles and legal frameworks to maintain chain of custody and evidence admissibility.
2. Perform disk and file-system forensic analysis, including deleted-file recovery and disk imaging.
3. Conduct memory forensics using volatile-memory acquisition and analysis frameworks.
4. Conduct network forensics and log analysis, and prepare forensic investigation reports for court testimony.

UNIT-I

DIGITAL FORENSICS FUNDAMENTALS AND LEGAL FRAMEWORK

1. Principles of digital forensics: identification, preservation, analysis, presentation
2. Chain of custody, evidence admissibility, and legal standards (IT Act 2000, IPC)
3. Forensics lab setup and write-blocking techniques

UNIT-II

DISK AND FILE SYSTEM FORENSICS

1. FAT, NTFS, ext4, APFS file system internals
2. Deleted file recovery, slack space and unallocated cluster analysis
3. Disk imaging: dd, FTK Imager, Autopsy, EnCase

UNIT-III

MEMORY FORENSICS

1. Volatile memory acquisition (WinPMem, LiME)
2. Process analysis, network connections, registry hives in memory
3. Volatility framework: plugins, analysis workflows

UNIT-IV

NETWORK FORENSICS AND LOG ANALYSIS

1. Packet capture and analysis: Wireshark, tcpdump
2. SIEM log correlation: Splunk, ELK Stack
3. Reconstruction of network attacks from PCAP data

UNIT-V

REPORT WRITING AND COURT TESTIMONY

1. Structuring a forensic investigation report
2. Expert witness testimony: cross-examination preparation
3. Presenting technical evidence to non-technical audiences

REFERENCE BOOKS

1. Carrier, B. (2005). File System Forensic Analysis. Addison-Wesley.
2. Ligh, M. H., et al. (2014). The Art of Memory Forensics. Wiley.

3. Casey, E. (2011). Digital Evidence and Computer Crime (3rd ed.). Academic Press.
4. Sammons, J. (2012). The Basics of Digital Forensics. Syngress.
5. Carvey, H. (2018). Windows Forensic Analysis Toolkit (4th ed.). Syngress.

MALWARE ANALYSIS AND REVERSE ENGINEERING

L/T/P/C
3/-/-/3

Learning Outcome:

1. Explain the classification, behaviour and lifecycle of malware families.
2. Perform static and dynamic malware analysis using disassemblers, debuggers and sandboxed environments.
3. Reverse-engineer malicious binaries and develop detection signatures (YARA rules).
4. Analyse advanced threats such as rootkits, ransomware and APT toolsets.

UNIT-I

INTRODUCTION TO MALWARE AND THREAT LANDSCAPE

1. Malware types: viruses, worms, Trojans, ransomware, rootkits, APTs
2. Malware lifecycle: delivery, execution, persistence, exfiltration
3. Threat intelligence frameworks: MITRE ATT&CK, Cyber Kill Chain

UNIT-II

STATIC MALWARE ANALYSIS

1. File format analysis: PE, ELF headers, packing and obfuscation detection
2. String extraction, import/export table analysis, YARA rule creation
3. Tools: PEiD, pestudio, CFF Explorer, Ghidra (static mode)

UNIT-III

DYNAMIC MALWARE ANALYSIS

1. Safe lab setup: isolated VMs, INetSim, FakeNet-NG
2. Behavioural monitoring: Process Monitor, Regshot, Wireshark
3. Sandboxes: Cuckoo, ANY.RUN – automated analysis and report interpretation

UNIT-IV

REVERSE ENGINEERING WITH DISASSEMBLERS AND DEBUGGERS

1. x86/x64 assembly language fundamentals for analysts
2. IDA Pro / Ghidra: control-flow graphs, decompilation
3. OllyDbg / x64dbg: breakpoints, code patching, anti-debugging bypass

UNIT-V

ADVANCED THREATS: ROOTKITS, RANSOMWARE, AND APT TECHNIQUES

1. Kernel-mode rootkit internals, DKOM, SSDT hooking
2. Ransomware encryption mechanisms and recovery strategies
3. APT case studies: lateral movement, living-off-the-land binaries (LOLBins)

REFERENCE BOOKS

1. Sikorski, M., & Honig, A. (2012). Practical Malware Analysis. No Starch Press.
2. Eilam, E. (2011). Reversing: Secrets of Reverse Engineering. Wiley.

3. Dinaburg, A., & Ruef, A. (2020). Practical Binary Analysis. No Starch Press.
4. MITRE ATT&CK Framework: https://attack.mitre.org/
5. Verizon. (2024). Data Breach Investigations Report (DBIR). Verizon Business.

RESEARCH METHODOLOGY IN CYBER SECURITY AND FORENSICS

L/T/P/C
2/-/-/2

Learning Outcome:

1. Explain the principles and stages of the research process applicable to cyber-security and forensics research.
2. Formulate research questions, hypotheses and appropriate research designs for security/forensics problems.
3. Apply qualitative and quantitative research methods and data-collection techniques relevant to the domain.
4. Prepare a scholarly research proposal and technical report following academic writing and citation standards.

UNIT-I

RESEARCH DESIGN AND PROBLEM FORMULATION

1. Identifying research gaps in cyber security and digital forensics
2. Formulating research questions, hypotheses, and objectives
3. Qualitative vs. quantitative vs. mixed-methods approaches

UNIT-II

LITERATURE REVIEW AND CITATION PRACTICES

1. Systematic literature review (SLR) methodology
2. Databases: IEEE Xplore, ACM Digital Library, Scopus, Google Scholar
3. Citation management: Zotero, Mendeley; APA / IEEE citation styles

UNIT-III

DATA COLLECTION AND EXPERIMENTAL DESIGN

1. Controlled experiments, case studies, surveys in security research
2. Dataset sourcing: CICIDS, CTU-13, UNSW-NB15, VirusTotal
3. Ethical considerations: responsible disclosure, IRB approval

UNIT-IV

STATISTICAL ANALYSIS AND INTERPRETATION

1. Descriptive and inferential statistics for security datasets
2. Machine learning evaluation metrics: accuracy, precision, recall, F1, ROC-AUC
3. Validity, reliability, and reproducibility of research findings

UNIT-V

ACADEMIC AND TECHNICAL WRITING

1. Conference and journal paper structure (IEEE, ACM templates)
2. Abstract, introduction, methodology, results, discussion, conclusion
3. Peer review process and responding to reviewer comments

REFERENCE BOOKS

1. Creswell, J. W. (2018). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (5th ed.). SAGE.
2. Vacca, J. R. (Ed.). (2021). Computer and Information Security Handbook (3rd ed.). Morgan Kaufmann.
3. Liao, Q., et al. (2016). Acing the Cybersecurity Job Interview. Syngress.
4. ACM / IEEE Paper Templates: https://www.acm.org/publications/proceedings-template

ENGLISH & COMMUNICATION SKILLS

L/T/P/C
2/-/-/2

Learning Outcome:

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.

REFERENCE BOOKS

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

COMPUTER FOUNDATION FOR SECURITY PROFESSIONALS

L/T/P/C
2/-/-/2

Learning Outcome:

1. Understand Computer Architecture and Hardware.
2. Master Operating System Fundamentals.
3. Apply the CIA Triad.
4. Analyze Networking and Communication Protocols.

UNIT-I

COMPUTER HARDWARE AND ARCHITECTURE BASICS

1. Processor and Memory: Understand CPU operations, registers, cache, and RAM (Random Access Memory) management.
2. Storage Systems: Learn hard disk architecture, solid-state drives (SSDs), and file system structures (NTFS, ext4).
3. Virtualization Concepts: Explore hypervisors, virtual machines (VMs), and containerization (Docker)

UNIT-II

OPERATING SYSTEM INTERNALS (WINDOWS & LINUX)

1. Command Line Interfaces (CLI): Master basic shell commands in Linux (Bash) and Windows (PowerShell/CMD).
2. Permissions and Access Control: Manage file permissions, user groups, and privilege escalation risks.
3. Process Management: Monitor active processes, services, and boot sequences.

UNIT-III

CORE COMPUTER NETWORKING

1. Network Models: Study the OSI and TCP/IP models and data encapsulation.
2. Protocols and Services: Understand TCP, UDP, DNS, DHCP, HTTP/HTTPS, and ICMP.
3. Network Hardware: Identify routers, switches, and basic firewall configurations

UNIT-IV

INTRODUCTION TO INFORMATION SECURITY PRINCIPLES

1. The CIA Triad: Learn confidentiality, integrity, and availability frameworks.
2. Threats and Vulnerabilities: Recognize common attack vectors, malware types (viruses, ransomware), and basic risk evaluation.
3. Defense Strategies: Implement defense-in-depth, password policies, and endpoint security basic

UNIT-V

BASIC CRYPTOGRAPHY AND SCRIPTING

1. Cryptographic Foundations: Distinguish symmetric vs. asymmetric encryption, hashing, and digital signatures.
2. Scripting Essentials: Use Python or Bash for basic automation and administrative tasks.

3. Peer review process and responding to reviewer comments

REFERENCE BOOKS

1. Ross J. Anderson: A classic and comprehensive resource focusing on security design principles, hardware, and real-world distributed systems.
2. Computer Security: Art and Science by Matt Bishop: A rigorous, detailed introduction to modern computer security theory paired with practical case studies.
3. Principles of Computer System Design by Jerome H. Saltzer and M. Frans Kaashoek: Explores core computer architecture concepts critical for understanding how secure systems are structured.

PRACTICAL: ADVANCED NETWORK SECURITY CONFIGURATION

L/T/P/C
-/-/4/2

Learning Outcome:

1. Configure firewalls, ACLs and secure network segmentation (DMZ) for enterprise infrastructure.
2. Implement VPN and IPSec tunnels for secure site-to-site and remote-access connectivity.
3. Deploy and test PKI/SSL-TLS certificates for secure communications.
4. Harden wireless network configurations against common attack vectors.

UNIT-I

Firewall rule-set configuration and ACL design for network segmentation.

UNIT-II

VPN and IPSec tunnel configuration for secure remote access.

UNIT-III

PKI deployment and SSL/TLS certificate configuration and testing.

UNIT-IV

802.1X, RADIUS and network access-control configuration.

UNIT-V

Wireless security hardening (WPA2/WPA3) and rogue access-point detection.

REFERENCE BOOKS

1. Vendor documentation (Cisco, Fortinet, pfSense); Stallings, W. (2022). Cryptography and Network Security. Pearson.

PRACTICAL: DIGITAL FORENSICS TOOLS

L/T/P/C
-/-/4/2

Learning Outcome:

1. Acquire forensic disk images using write-blockers and standard imaging tools.
2. Recover deleted files and analyse file-system artifacts using forensic suites (Autopsy/FTK/EnCase).
3. Perform memory acquisition and analysis using Volatility-based workflows.
4. Document forensic findings following chain-of-custody procedures.

UNIT-I

Forensic disk imaging and write-blocking procedures.

UNIT-II

File-system analysis and deleted-file recovery using Autopsy/FTK.

UNIT-III

Memory acquisition and Volatility-framework analysis.

UNIT-IV

Timeline reconstruction from file-system and log artifacts.

UNIT-V

Forensic report writing and chain-of-custody documentation.

REFERENCE BOOKS

1. Carrier, B. (2005). File System Forensic Analysis. Addison-Wesley; Ligh, M. H., et al. (2014). The Art of Memory Forensics. Wiley.

INTRODUCTION TO GITHUB & VERSION CONTROL

L/T/P/C
1/-/-/1

Learning Outcome:

1. Explain version-control concepts and the Git/GitHub workflow.
2. Create, manage and collaborate on repositories for security-research and tool-development projects.
3. Apply branching, merging and pull-request workflows in team-based development.
4. Document and maintain project code and research artifacts using GitHub best practices.

UNIT-I

Version-control fundamentals and Git installation/configuration.

UNIT-II

Repository creation, commits, branching and merging.

UNIT-III

Collaboration workflows – pull requests, code review, issue tracking.

UNIT-IV

Managing security-research code and datasets on GitHub responsibly.

UNIT-V

Documentation and project maintenance best practices.

REFERENCE BOOKS

1. Chacon, S., & Straub, B. (2019). Pro Git. Apress; GitHub official documentation.

MALLA REDDY VISHWAVIDYAPEETH

SCHOOL OF DIGITAL HEALTH SCIENCES AND TECHNOLOGY

MASTER OF SCIENCE (M.Sc.) IN DIGITAL FORENSICS AND CYBER SECURITY

Semester II

S.NO	SUBJECT	L	T	P	C
1	Penetration Testing and Vulnerability Assessment	3	-	-	3
2	Intrusion Detection and Prevention Systems	3	-	-	3
3	Security Auditing and Compliance	3	-	-	3
4	Network Forensics and Traffic Analysis	2	-	-	2
5	Cyber Security Regulations and Ethics	2	-	-	2
6	Open Source Intelligence (OSINT) and Threat Hunting	2	-	-	2
7	Practical: Penetration Testing Techniques	-	-	4	2
8	Practical: Security Auditing Techniques	-	-	4	2
9	Soft Skills and Professional Development	1	-	-	1
	TOTAL	**16**	**-**	**8**	**20**

SEMESTER-II

PENETRATION TESTING AND VULNERABILITY ASSESSMENT

L/T/P/C
3/-/-/3

Learning Outcome:

1. Explain the methodology, scope and legal/ethical boundaries of penetration testing engagements.
2. Perform vulnerability assessment and exploitation using standard penetration-testing toolkits.
3. Conduct network, web-application and wireless penetration tests.
4. Prepare a professional penetration-test report with prioritized, actionable remediation guidance.

UNIT-I

PENETRATION TESTING METHODOLOGY AND SCOPING

1. PTES, OWASP Testing Guide, NIST SP 800-115 frameworks
2. Rules of engagement, scope definition, and legal authorisation
3. Reconnaissance: passive (OSINT) and active (port scanning, banner grabbing)

UNIT-II

NETWORK AND INFRASTRUCTURE PENETRATION TESTING

1. Vulnerability scanning: Nessus, OpenVAS, Qualys
2. Exploitation: Metasploit Framework – modules, payloads, post-exploitation
3. Privilege escalation: local exploits, misconfigurations, credential harvesting

UNIT-III

WEB APPLICATION PENETRATION TESTING

1. OWASP Top 10 (2021): injection, XSS, IDOR, SSRF, broken access control
2. Tools: Burp Suite, OWASP ZAP, SQLMap, Nikto
3. API security testing and business logic vulnerabilities

UNIT-IV

WIRELESS AND SOCIAL ENGINEERING ATTACKS

1. WPA2 cracking: handshake capture, evil twin attacks (aircrack-ng)
2. Phishing, spear-phishing, vishing, and pretexting techniques
3. Physical security assessment and tailgating scenarios

UNIT-V

REPORTING AND REMEDIATION GUIDANCE

1. CVSS scoring and risk rating methodology
2. Penetration test report structure: executive summary and technical findings
3. Remediation recommendations and re-testing lifecycle

REFERENCE BOOKS

1. Weidman, G. (2014). Penetration Testing: A Hands-On Introduction to Hacking. No Starch Press.

2. Kennedy, D., et al. (2011). Metasploit: The Penetration Tester's Guide. No Starch Press.
3. OWASP Testing Guide v4.2: https://owasp.org/www-project-web-security-testing-guide/
4. Engebretson, P. (2013). The Basics of Hacking and Penetration Testing (2nd ed.). Syngress.
5. NIST SP 800-115 (2008). Technical Guide to Information Security Testing and Assessment.

INTRUSION DETECTION AND PREVENTION SYSTEMS

L/T/P/C
3/-/-/3

Learning Outcome:

1. Explain the architecture and detection techniques of intrusion detection and prevention systems (IDS/IPS).
2. Configure signature-based and anomaly-based detection rules for network and host-based IDS/IPS.
3. Analyse security alerts and correlate events to identify true and false positives.
4. Evaluate IDS/IPS deployment strategies for enterprise and critical-infrastructure networks.

UNIT-I

IDS/IPS ARCHITECTURES AND DETECTION METHODOLOGIES

1. Signature-based, anomaly-based, and stateful protocol analysis
2. Network-based (NIDS) vs. host-based (HIDS) deployment
3. Sensor placement, traffic mirroring (SPAN/TAP)

UNIT-II

SNORT AND SURICATA RULE DEVELOPMENT

1. Snort rule syntax: header, options, alert generation
2. Suricata multi-threading, EVE JSON logging
3. Custom rule writing for zero-day and APT indicators

UNIT-III

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

1. SIEM architecture: data ingestion, normalisation, correlation
2. Splunk: SPL queries, dashboards, alerts
3. ELK Stack (Elasticsearch, Logstash, Kibana): pipeline configuration

UNIT-IV

THREAT HUNTING AND BEHAVIOURAL ANALYTICS

1. Hypothesis-driven hunting methodology
2. UEBA (User and Entity Behaviour Analytics)
3. Threat hunting with Sigma rules and MITRE ATT&CK navigator

UNIT-V

EVASION TECHNIQUES AND IDS BYPASS

1. Fragmentation, polymorphism, and protocol-level evasion
2. Encrypted C2 traffic and domain fronting
3. Strategies to harden detection capabilities against evasion

REFERENCE BOOKS

1. Bejtlich, R. (2004). The Tao of Network Security Monitoring. Addison-Wesley.
2. Sanders, C., & Smith, J. (2013). Applied Network Security Monitoring. Syngress.

3. Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems. NIST SP 800-94.
4. Chuvakin, A., Schmidt, K., & Phillips, C. (2012). Logging and Log Management. Syngress.

SECURITY AUDITING AND COMPLIANCE

L/T/P/C
3/-/-/3

Learning Outcome:

1. Explain security-auditing methodologies and compliance frameworks (ISO 27001, NIST CSF, PCI-DSS).
2. Plan and conduct a security audit of an organizational IT environment.
3. Assess regulatory and compliance gaps against applicable standards and frameworks.
4. Prepare an audit report with risk ratings and compliance-remediation recommendations.

UNIT-I

SECURITY AUDIT FRAMEWORKS AND STANDARDS

1. ISO/IEC 27001:2022 – ISMS requirements and Annex A controls
2. NIST Cybersecurity Framework (CSF) 2.0 – Identify, Protect, Detect, Respond, Recover
3. PCI-DSS, HIPAA, SOC 2 – industry-specific compliance requirements

UNIT-II

AUDIT PLANNING AND EVIDENCE COLLECTION

1. Audit scope, objectives, and risk-based approach
2. Evidence types: interviews, observation, documentation review, re-performance
3. Sampling techniques and audit trail analysis

UNIT-III

VULNERABILITY MANAGEMENT AND RISK ASSESSMENT

1. Asset inventory and criticality classification
2. Qualitative and quantitative risk assessment (FAIR, OCTAVE)
3. Patch management lifecycle and SLA metrics

UNIT-IV

IT GOVERNANCE, RISK, AND COMPLIANCE (GRC) TOOLS

1. GRC platforms: ServiceNow GRC, RSA Archer, MetricStream
2. Policy lifecycle management and exception handling
3. Third-party vendor risk assessment

UNIT-V

AUDIT REPORTING AND CONTINUOUS COMPLIANCE

1. Audit finding classification: critical, high, medium, low
2. Management response and remediation tracking
3. Continuous monitoring: automated compliance dashboards

REFERENCE BOOKS

1. Cannon, D. (2019). CISA Certified Information Systems Auditor Study Guide (4th ed.). Sybex.
2. IT Governance Institute. (2019). COBIT 2019 Framework. ISACA.

3. ISO/IEC 27001:2022. Information Security Management Systems – Requirements.
4. NIST Cybersecurity Framework 2.0: https://www.nist.gov/cyberframework
5. Peltier, T. R. (2016). Information Security Policies, Procedures, and Standards. CRC Press.

NETWORK FORENSICS AND TRAFFIC ANALYSIS

L/T/P/C
2/-/-/2

Learning Outcome:

1. Explain the principles and tools of network forensics and traffic analysis.
2. Capture and analyse network traffic to reconstruct security incidents.
3. Correlate SIEM/log data to identify patterns of network-based attacks.
4. Present network-forensic findings in a structured investigative report.

UNIT-I

NETWORK EVIDENCE AND CAPTURE METHODOLOGY

1. Full-packet capture vs. NetFlow/IPFIX collection
2. Legal aspects of network evidence collection
3. Tools: Wireshark, tcpdump, NetworkMiner, Zeek (Bro)

UNIT-II

PROTOCOL ANALYSIS FOR FORENSICS

1. HTTP/S, DNS, SMB, FTP, SMTP traffic dissection
2. Detecting data exfiltration via DNS tunnelling, steganography
3. Encrypted traffic analysis (JA3/JA3S, JARM fingerprinting)

UNIT-III

INTRUSION ANALYSIS FROM PACKET DATA

1. Reconstructing attack timelines from PCAP
2. Identifying C2 beacon patterns and lateral movement
3. Case study: analysing a real-world breach PCAP dataset

UNIT-IV

WIRELESS NETWORK FORENSICS

1. 802.11 frame analysis, BSSID/SSID mapping
2. Detecting rogue APs and deauthentication attacks
3. Bluetooth and ZigBee evidence collection

REFERENCE BOOKS

1. Davidoff, S., & Ham, J. (2012). Network Forensics: Tracking Hackers through Cyberspace. Prentice Hall.
2. Kozierok, C. M. (2005). The TCP/IP Guide. No Starch Press.
3. Zeek Network Security Monitor Documentation: https://docs.zeek.org/

CYBER SECURITY REGULATIONS AND ETHICS

L/T/P/C
2/-/-/2

Learning Outcome:

1. Explain national and international cyber-security laws, regulations and data-protection frameworks.
2. Apply the IT Act 2000 and DPDP Act provisions to cyber-security and forensics practice.
3. Analyse ethical dilemmas in security research, vulnerability disclosure and investigation.
4. Evaluate organizational compliance obligations under applicable cyber-security regulations.

UNIT-I

LEGAL FRAMEWORKS IN CYBER SECURITY

1. Information Technology Act 2000 & Amendment 2008 (India)
2. Computer Fraud and Abuse Act (CFAA – USA), NIS2 Directive (EU)
3. International conventions: Budapest Convention on Cybercrime

UNIT-II

DATA PROTECTION AND PRIVACY LAWS

1. GDPR – principles, data subject rights, controller/processor obligations
2. India's Digital Personal Data Protection Act 2023
3. Cross-border data transfer mechanisms: SCCs, adequacy decisions

UNIT-III

ETHICS IN CYBER SECURITY AND FORENSICS

1. Professional ethics codes: (ISC)², EC-Council, ISACA
2. Responsible disclosure vs. full disclosure: case studies
3. Ethical dilemmas: privacy vs. security, attribution of nation-state attacks

UNIT-IV

INTELLECTUAL PROPERTY AND CYBER CRIMES

1. Software copyright, patents, trade secrets, and cyber theft
2. Types of cyber crime: fraud, identity theft, cyber terrorism
3. Law enforcement collaboration: CERT-In, Interpol, FBI CISA

REFERENCE BOOKS

1. Remy, J. (2021). Cyber Law and Ethics (2nd ed.). Jones & Bartlett Learning.
2. Ministry of Electronics & IT. (2023). Digital Personal Data Protection Act, 2023. Government of India.
3. Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. JDFSL.

OPEN SOURCE INTELLIGENCE (OSINT) AND THREAT HUNTING

L/T/P/C
2/-/-/2

Learning Outcome:

1. Explain OSINT collection methodologies and tools for cyber-security intelligence gathering.
2. Apply the MITRE ATT&CK framework to structure and guide threat-hunting activities.
3. Conduct proactive threat-hunting exercises using OSINT and internal telemetry data.
4. Evaluate and prioritize threat-intelligence findings for security-operations decision-making.

UNIT-I

OSINT FUNDAMENTALS AND METHODOLOGY

1. OSINT sources: social media, WHOIS, Shodan, Censys, Pastebin
2. Structured OSINT process: collection, processing, analysis, dissemination
3. Legal and ethical boundaries of OSINT investigations

UNIT-II

OSINT TOOLS AND TECHNIQUES

1. Maltego: link analysis and entity relationships
2. theHarvester, Recon-ng, SpiderFoot automation
3. Dark web OSINT: onion sites, Tor anonymity considerations

UNIT-III

CYBER THREAT INTELLIGENCE (CTI) LIFECYCLE

1. Strategic, operational, tactical, and technical intelligence
2. Threat intelligence platforms (TIPs): MISP, OpenCTI, ThreatConnect
3. Indicator of Compromise (IoC) sharing: STIX/TAXII standards

UNIT-IV

PROACTIVE THREAT HUNTING

1. Hunting maturity model and hypothesis creation
2. Hunting techniques: stack counting, clustering, frequency analysis
3. Building a threat hunting programme in a SOC environment

REFERENCE BOOKS

1. Bazzell, M. (2023). Open Source Intelligence Techniques (10th ed.). Independently Published.
2. MISP Project: https://www.misp-project.org/
3. CISA. (2023). Cyber Threat Intelligence Sharing: Best Practices. CISA Publications.
4. Semester III – Course Syllabi

PRACTICAL: PENETRATION TESTING TECHNIQUES

L/T/P/C
-/-/4/2

Learning Outcome:

1. Perform reconnaissance and vulnerability scanning of target networks/applications.
2. Exploit identified vulnerabilities using standard penetration-testing frameworks.
3. Conduct web-application penetration testing (OWASP Top-10 based).
4. Prepare a professional penetration-test report with remediation recommendations.

UNIT-I

Reconnaissance and vulnerability scanning (Nmap, Nessus/OpenVAS).

UNIT-II

Exploitation using Metasploit and related frameworks.

UNIT-III

Web-application penetration testing (Burp Suite, OWASP ZAP).

UNIT-IV

Wireless penetration testing techniques.

UNIT-V

Penetration-test reporting and remediation prioritization.

REFERENCE BOOKS

1. Weidman, G. (2014). Penetration Testing: A Hands-On Introduction to Hacking. No Starch Press; OWASP Testing Guide.

PRACTICAL: SECURITY AUDITING TECHNIQUES

L/T/P/C
-/-/4/2

Learning Outcome:

1. Plan and execute a security audit against ISO 27001/NIST CSF control sets.
2. Conduct configuration and compliance audits of systems and networks.
3. Use automated compliance-scanning tools to assess security posture.
4. Prepare an audit report with risk ratings and remediation timelines.

UNIT-I

Audit planning and control-framework mapping (ISO 27001, NIST CSF).

UNIT-II

Configuration auditing of servers, endpoints and network devices.

UNIT-III

Automated compliance scanning and reporting tools.

UNIT-IV

Risk rating and prioritization of audit findings.

UNIT-V

Audit report writing and stakeholder communication.

REFERENCE BOOKS

1. ISO/IEC 27001:2022 standard documentation; NIST Cybersecurity Framework (CSF) publications.

SOFT SKILLS AND PROFESSIONAL DEVELOPMENT

L/T/P/C
1/-/-/1

Learning Outcome:

1. Demonstrate effective professional communication in technical and client-facing security contexts.
2. Apply teamwork and collaboration skills relevant to SOC/incident-response team environments.
3. Practise resume-building, interview preparation and professional networking for the cyber-security industry.
4. Demonstrate time-management and stress-management techniques suited to high-pressure security operations.

UNIT-I

Professional communication and client/stakeholder reporting.

UNIT-II

Teamwork and collaboration in SOC/incident-response settings.

UNIT-III

Resume building, interview skills and professional networking.

UNIT-IV

Time-management and stress-management for high-pressure security roles.

UNIT-V

Professional ethics and workplace conduct in cyber security.

REFERENCE BOOKS

1. Covey, S. R. (2020). The 7 Habits of Highly Effective People. Simon & Schuster; industry professional-development resources.

MALLA REDDY VISHWAVIDYAPEETH

SCHOOL OF DIGITAL HEALTH SCIENCES AND TECHNOLOGY

MASTER OF SCIENCE (M.Sc.) IN DIGITAL FORENSICS AND CYBER SECURITY

Semester III

S.NO	SUBJECT	L	T	P	C
1	Cyber Security Incident Response and Disaster Recovery	3	-	-	3
2	Cloud Security and Virtualization Security	3	-	-	3
3	Cyber Law and Ethical Hacking	3	-	-	3
4	Mobile and IoT Forensics	2	-	-	2
5	AI and Machine Learning in Cyber Security	2	-	-	2
6	Practical: Incident Response Implementation	-	-	6	3
7	Practical: Cloud Security Implementation	-	-	6	3
8	Seminar: Emerging Threats and Case Studies	1	-	-	1
	TOTAL	**14**	**-**	**12**	**20**

SEMESTER-III

CYBER SECURITY INCIDENT RESPONSE AND DISASTER RECOVERY

L/T/P/C

3/-/-/3

Learning Outcome:

1. Explain the incident-response lifecycle and disaster-recovery/business-continuity planning principles.
2. Develop and test an incident-response plan for a simulated organizational security incident.
3. Coordinate incident containment, eradication and recovery activities.
4. Evaluate disaster-recovery strategies and business-continuity plans for organizational resilience.

UNIT-I

INCIDENT RESPONSE LIFECYCLE (NIST SP 800-61)

1. Phases: Preparation, Detection & Analysis, Containment, Eradication, Recovery, Lessons Learned
2. Building an Incident Response Team (CSIRT/SOC) and runbooks
3. Incident classification, severity levels and escalation procedures

UNIT-II

DETECTION AND TRIAGE

1. Alert triage workflow: true positive vs. false positive management
2. Endpoint detection and response (EDR): CrowdStrike, Microsoft Defender for Endpoint
3. Threat scoring: CVSS, risk-based prioritisation

UNIT-III

CONTAINMENT, ERADICATION, AND RECOVERY

1. Network isolation, account lockout, and system quarantine strategies
2. Malware eradication: re-imaging, registry cleaning, persistence removal
3. Backup strategies: 3-2-1 rule, immutable backups, RTO/RPO objectives

UNIT-IV

BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING

1. BCP/DRP frameworks: ISO 22301, NIST SP 800-34
2. Disaster recovery testing: tabletop, functional, and full-scale exercises
3. Cloud DR: cross-region failover, geo-redundancy, chaos engineering

UNIT-V

POST-INCIDENT ACTIVITIES AND LESSONS LEARNED

1. Root cause analysis (RCA) and timeline reconstruction
2. Evidence preservation for legal proceedings
3. KPIs: MTTD, MTTR, number of incidents and trend analysis

REFERENCE BOOKS

1. Cichonski, P., et al. (2012). Computer Security Incident Handling Guide. NIST SP 800-61 Rev. 2.
2. Luttgens, J., Pepe, M., & Mandia, K. (2014). Incident Response & Computer Forensics (3rd ed.). McGraw-Hill.
3. ISO 22301:2019. Business Continuity Management Systems – Requirements.
4. Swanson, M., et al. (2010). Contingency Planning Guide for Federal Information Systems. NIST SP 800-34.

CLOUD SECURITY AND VIRTUALIZATION SECURITY

L/T/P/C
3/-/-/3

Learning Outcome:

1. Explain cloud-computing and virtualization architectures and their associated security risks.
2. Configure identity, access-management and network-security controls in cloud environments.
3. Assess virtualization-security threats (hypervisor attacks, VM escape) and mitigation strategies.
4. Evaluate cloud-security compliance frameworks and shared-responsibility models across providers.

UNIT-I

CLOUD COMPUTING ARCHITECTURE AND SHARED RESPONSIBILITY

1. IaaS, PaaS, SaaS deployment models and security implications
2. Shared responsibility model: AWS, Azure, GCP comparative analysis
3. Cloud service agreements, SLA security clauses, and compliance

UNIT-II

IDENTITY AND ACCESS MANAGEMENT IN CLOUD

1. IAM policies, roles, and least privilege in AWS/Azure/GCP
2. Multi-factor authentication, federated identity (SAML, OIDC)
3. Privileged access management (PAM) and just-in-time access

UNIT-III

CLOUD NETWORK AND DATA SECURITY

1. VPC architecture, security groups, NACLs, and cloud firewalls
2. Encryption at rest and in transit: KMS, HSM, TLS enforcement
3. Cloud DLP, CASB solutions, and data classification

UNIT-IV

CONTAINER AND KUBERNETES SECURITY

1. Docker security: image scanning, rootless containers, seccomp/AppArmor
2. Kubernetes RBAC, network policies, pod security standards
3. CI/CD pipeline security: DevSecOps, shift-left scanning (Trivy, Snyk)

UNIT-V

CLOUD FORENSICS AND INCIDENT RESPONSE

1. Collecting cloud logs: AWS CloudTrail, Azure Monitor, GCP Audit Logs
2. Challenges of volatile cloud evidence and multi-tenant environments
3. Cloud-native SIEM: AWS Security Hub, Microsoft Sentinel

REFERENCE BOOKS

1. Winkler, V. J. R. (2011). Securing the Cloud: Cloud Computer Security Techniques and Tactics. Syngress.
2. CSA. (2023). Cloud Controls Matrix v4. Cloud Security Alliance.

3. AWS Security Best Practices Whitepaper: https://aws.amazon.com/security/
4. Rice, J. (2020). Hacking the Cloud (2nd ed.). No Starch Press.
5. NIST SP 800-190. (2017). Application Container Security Guide.

CYBER LAW AND ETHICAL HACKING

L/T/P/C
3/-/-/3

Learning Outcome:

1. Explain the legal framework governing cyber crime, digital evidence and ethical hacking in India and globally.
2. Apply ethical-hacking methodologies within a defined legal and authorization framework.
3. Analyse case law and precedents relevant to cyber-crime prosecution and digital evidence.
4. Evaluate the legal and ethical implications of offensive-security engagements and vulnerability disclosure.

UNIT-I

CYBER LAW FRAMEWORKS – INDIAN AND INTERNATIONAL

1. IT Act 2000: Sections 43, 66, 66A-F, 67, 69, 70 – offences and penalties
2. IPC provisions applicable to cyber crime: 420, 463, 468
3. International cyber law: UNCITRAL, UNODC guidelines, mutual legal assistance treaties (MLATs)

UNIT-II

ETHICAL HACKING PRINCIPLES AND AUTHORISATION

1. Difference between ethical hacking and criminal activity
2. Bug bounty programmes: HackerOne, Bugcrowd – scope and responsible disclosure
3. Certification landscape: CEH, OSCP, GPEN, CPENT

UNIT-III

ADVANCED EXPLOITATION TECHNIQUES

1. Buffer overflow, format string, use-after-free exploit development
2. Shellcode writing, NOP sleds, return-oriented programming (ROP)
3. Active Directory attacks: Kerberoasting, Pass-the-Hash, DCSync

UNIT-IV

SOCIAL ENGINEERING AND PHYSICAL SECURITY

1. Phishing simulation tools: Gophish, King Phisher
2. Physical penetration testing: badge cloning, lock picking (legally authorised)
3. Insider threat modelling and behavioural indicators

UNIT-V

CASE STUDIES IN CYBER CRIME AND LEGAL PROCEEDINGS

1. Notable Indian cyber crime cases and court judgements
2. Digital evidence standards: Sections 65A & 65B of the Indian Evidence Act
3. Interaction with law enforcement: FIR filing, CERT-In reporting obligations

REFERENCE BOOKS

1. Anand, V. K. (2019). Cyber Laws in India. Universal Law Publishing.

2. Harper, A., et al. (2011). Gray Hat Hacking (4th ed.). McGraw-Hill.
3. Engebretson, P. (2013). The Basics of Hacking and Penetration Testing. Syngress.
4. Ministry of Law & Justice. (2000). Information Technology Act, 2000 (as amended). Government of India.

MOBILE AND IOT FORENSICS

L/T/P/C
2/-/-/2

Learning Outcome:

1. Explain mobile-device and IoT architectures and their forensic-acquisition challenges.
2. Perform logical and physical acquisition of mobile-device data using standard forensic tools.
3. Analyse IoT device artifacts and network traffic for forensic evidence.
4. Prepare a forensic report documenting mobile/IoT evidence and analysis findings.

UNIT-I

MOBILE DEVICE FORENSICS

1. Android forensics: ADB, JTAG, chip-off extraction methods
2. iOS forensics: logical, file system, and full file system acquisition
3. Mobile forensics tools: Cellebrite UFED, Oxygen Forensics, Magnet AXIOM

UNIT-II

MOBILE APP AND DATA ANALYSIS

1. SQLite database forensics: contacts, messages, app data
2. Social media artefacts: WhatsApp, Telegram encryption and evidence recovery
3. Cloud-synced data recovery: iCloud, Google Drive artefacts

UNIT-III

IOT ARCHITECTURE AND ATTACK SURFACES

1. IoT protocol stack: MQTT, CoAP, Zigbee, Z-Wave vulnerabilities
2. Firmware extraction and analysis: binwalk, Firmwalker
3. Shodan-based IoT reconnaissance and threat assessment

UNIT-IV

IOT FORENSIC INVESTIGATION TECHNIQUES

1. Smart home device forensics: Amazon Echo, Google Nest log analysis
2. Industrial IoT (ICS/SCADA) forensics considerations
3. IoT evidence chain of custody and reporting standards

REFERENCE BOOKS

1. Bommisetty, S., Tamma, R., & Mahalik, H. (2014). Practical Mobile Forensics. Packt Publishing.
2. Lee, S., & Lim, H. (2018). Internet of Things Forensics. Journal of Forensic Sciences.
3. Cellebrite. (2023). Mobile Forensics Best Practices. Cellebrite Publications.
4. ENISA. (2022). Guidelines for Securing IoT. European Union Agency for Cybersecurity.

AI AND MACHINE LEARNING IN CYBER SECURITY

L/T/P/C
2/-/-/2

Learning Outcome:

1. Explain applications of artificial intelligence and machine learning in cyber-security defence and detection.
2. Apply ML techniques for anomaly detection, malware classification and phishing detection.
3. Evaluate adversarial-AI risks and techniques used to evade ML-based security systems.
4. Assess the ethical and operational considerations of deploying AI-driven security solutions.

UNIT-I

AI/ML FOUNDATIONS FOR SECURITY APPLICATIONS

1. Supervised, unsupervised, and reinforcement learning paradigms
2. Feature engineering for security datasets (CICIDS2017, NSL-KDD)
3. Python ML stack: scikit-learn, TensorFlow, PyTorch for security

UNIT-II

INTRUSION DETECTION WITH ML

1. Binary and multi-class classification of network traffic
2. Random Forest, XGBoost, LSTM for anomaly detection
3. Handling class imbalance: SMOTE, cost-sensitive learning

UNIT-III

MALWARE CLASSIFICATION AND DETECTION

1. Static feature extraction: PE imports, entropy, n-grams
2. Dynamic feature extraction: system call sequences, API call graphs
3. Deep learning for malware: CNN on binary visualisation

UNIT-IV

ADVERSARIAL ML AND AI SECURITY

1. Adversarial examples: FGSM, PGD attacks on classifiers
2. Model poisoning, backdoor attacks, and defences
3. Explainable AI (XAI) in security: SHAP, LIME for forensic decisions

REFERENCE BOOKS

1. Geron, A. (2022). Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow (3rd ed.). O'Reilly.
2. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
3. Sommer, R., & Paxson, V. (2010). Outside the Closed World: ML in Network Intrusion Detection. IEEE S&P.
4. Apruzzese, G., et al. (2022). The Role of Machine Learning in Cybersecurity. Digital Threats: Research and Practice.
5. Semester IV – Course Syllabi

PRACTICAL: INCIDENT RESPONSE IMPLEMENTATION

L/T/P/C
-/-/6/3

Learning Outcome:

1. Set up and configure an incident-response toolkit and playbooks.
2. Detect, contain and eradicate a simulated security incident.
3. Perform post-incident recovery and root-cause analysis.
4. Document the incident-response process and lessons learned.

UNIT-I

Incident-response toolkit setup and playbook development.

UNIT-II

Simulated incident detection and containment exercises.

UNIT-III

Eradication and recovery procedures.

UNIT-IV

Root-cause analysis and post-incident review.

UNIT-V

Incident documentation and reporting to stakeholders.

REFERENCE BOOKS

1. NIST SP 800-61 Computer Security Incident Handling Guide; SANS Incident Handler's Handbook.

PRACTICAL: CLOUD SECURITY IMPLEMENTATION

L/T/P/C
-/-/6/3

Learning Outcome:

1. Configure identity and access management (IAM) policies in a cloud environment.
2. Implement network-security controls (security groups, VPC/VNet configuration) in the cloud.
3. Configure logging, monitoring and threat-detection services in a cloud platform.
4. Assess and remediate cloud-security misconfigurations using automated tools.

UNIT-I

IAM policy configuration and least-privilege access design.

UNIT-II

Virtual network and security-group configuration.

UNIT-III

Cloud logging, monitoring and threat-detection service configuration.

UNIT-IV

Container and virtualization security configuration.

UNIT-V

Automated cloud-security posture assessment and remediation.

REFERENCE BOOKS

1. AWS/Azure/GCP official security documentation; Cloud Security Alliance (CSA) guidance documents.

SEMINAR: EMERGING THREATS AND CASE STUDIES

L/T/P/C
1/-/-/1

Learning Outcome:

1. Present and critically analyse a recent, real-world cyber-security or forensics case study.
2. Evaluate emerging threat trends (ransomware-as-a-service, supply-chain attacks, AI-driven attacks).
3. Facilitate structured discussion and peer critique on emerging cyber-security topics.
4. Synthesize lessons learned from case studies into recommendations for organizational practice.

Each student/group selects and presents a seminar on a recent cyber-security incident or emerging-threat trend (e.g., a major ransomware campaign, supply-chain compromise, nation-state APT operation, or AI-driven attack), followed by structured peer discussion and faculty critique.

REFERENCE BOOKS

1. Recent reports from CERT-In, MITRE, Verizon DBIR, and peer-reviewed cyber-security journals/conference proceedings selected by the student and approved by the course coordinator.

MALLA REDDY VISHWAVIDYAPEETH

SCHOOL OF DIGITAL HEALTH SCIENCES AND TECHNOLOGY

MASTER OF SCIENCE (M.Sc.) IN DIGITAL FORENSICS AND CYBER SECURITY

Semester IV

S.NO	SUBJECT	L	T	P	C
1	Advanced Malware Analysis and Reverse Engineering	3	-	-	3
2	Cyber Threat Intelligence and Hunting	3	-	-	3
3	Digital Forensics and Cyber Security Project Management	2	-	-	2
4	Thesis / Research Project	-	-	1	2
	TOTAL	**8**	**-**	**-**	**20**

SEMESTER-IV

ADVANCED MALWARE ANALYSIS AND REVERSE ENGINEERING

L/T/P/C
3/-/-/3

Learning Outcome:

1. Perform advanced static and dynamic analysis of obfuscated and packed malware samples.
2. Reverse-engineer advanced malware families including fileless malware and APT toolsets.
3. Develop detection and mitigation strategies for advanced persistent threats.
4. Automate malware-analysis workflows using scripting and analysis frameworks.

UNIT-I

ADVANCED STATIC ANALYSIS AND CODE RECOVERY

1. Deobfuscation: custom XOR, base64 chaining, VM-based protectors
2. Ghidra scripting: automating decompilation and struct recovery
3. Identifying and recovering from heavy packing (Themida, VMProtect)

UNIT-II

ADVANCED DYNAMIC ANALYSIS AND ANTI-ANALYSIS BYPASS

1. Anti-debugging: IsDebuggerPresent, timing checks, hardware breakpoints bypass
2. Anti-VM detection evasion in analysis environments
3. Process injection: DLL injection, process hollowing, reflective PE loading

UNIT-III

EXPLOIT DEVELOPMENT AND VULNERABILITY RESEARCH

1. Stack and heap exploitation: BOF, heap spray, use-after-free
2. DEP/ASLR/CFG bypass techniques and ROP chain construction
3. Fuzzing methodologies: AFL++, libFuzzer, WinAFL for vulnerability discovery

UNIT-IV

THREAT ACTOR ATTRIBUTION AND MALWARE FAMILIES

1. Code similarity analysis: BinDiff, diaphora for malware lineage
2. Tracking APT malware families: Lazarus, Turla, APT28 toolsets
3. Deception technologies: honeypots (T-Pot) and malware lure analysis

UNIT-V

CAPSTONE MALWARE CASE STUDY

1. End-to-end analysis of a complex, multi-stage malware sample
2. Documenting Indicators of Compromise (IoCs) and YARA rules
3. Producing a professional threat analysis report

REFERENCE BOOKS

1. Sikorski, M., & Honig, A. (2012). Practical Malware Analysis. No Starch Press.
2. Anley, C., et al. (2007). The Shellcoder's Handbook (2nd ed.). Wiley.

3. Seitz, J. (2021). Black Hat Python (2nd ed.). No Starch Press.
4. MITRE ATT&CK Software Database: https://attack.mitre.org/software/

CYBER THREAT INTELLIGENCE AND HUNTING

L/T/P/C
3/-/-/3

Learning Outcome:

1. Explain the cyber-threat-intelligence lifecycle and intelligence-sharing frameworks.
2. Develop and apply threat-hunting hypotheses using the MITRE ATT&CK framework and internal telemetry.
3. Analyse advanced persistent threat (APT) campaigns and attacker tactics, techniques and procedures (TTPs).
4. Produce actionable threat-intelligence reports for organizational decision-making.

UNIT-I

THREAT INTELLIGENCE PROGRAMME DESIGN

1. Intelligence requirements definition and collection planning
2. Source evaluation: reliability and credibility ratings
3. Intelligence sharing communities: ISACs, FS-ISAC, H-ISAC

UNIT-II

ADVANCED CTI ANALYSIS TECHNIQUES

1. Diamond Model of Intrusion Analysis for attribution
2. TTP mapping to MITRE ATT&CK and D3FEND
3. Malware family clustering: Malpedia, VirusTotal Intelligence, CAPE sandbox

UNIT-III

STRATEGIC AND GEOPOLITICAL THREAT INTELLIGENCE

1. Nation-state actor profiles: Russia, China, North Korea, Iran
2. Hacktivism, cyber terrorism, and hybrid warfare
3. Briefing executives: translating technical threat data into business risk

UNIT-IV

AUTOMATED THREAT HUNTING PIPELINES

1. Jupyter notebooks for threat hunting at scale
2. Velociraptor: endpoint querying and hunting artefacts
3. Automated IoC ingestion and SOAR playbook integration (Palo Alto XSOAR)

REFERENCE BOOKS

1. Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-Driven Computer Network Defence. Lockheed Martin.
2. MISP Project and STIX/TAXII Documentation: https://oasis-open.github.io/cti-documentation/
3. CrowdStrike. (2024). Global Threat Report. CrowdStrike Holdings.
4. Caltagirone, S., Pendergast, A., & Betz, C. (2013). The Diamond Model of Intrusion Analysis. DTIC.

DIGITAL FORENSICS AND CYBER SECURITY PROJECT MANAGEMENT

L/T/P/C

2/-/-/2

Learning Outcome:

1. Explain project-management principles and frameworks applicable to cyber-security and forensics projects.
2. Plan and manage a security-operations or forensic-investigation project, including resource and risk planning.
3. Apply project-management tools to track cyber-security project deliverables, timelines and budgets.
4. Evaluate project outcomes and communicate results to technical and executive stakeholders.

UNIT-I

PROJECT MANAGEMENT FUNDAMENTALS FOR SECURITY PROJECTS

1. PMBOK and PRINCE2 frameworks applied to security engagements
2. Agile and Scrum methodologies in cyber security teams
3. Stakeholder management, scope control, and change management

UNIT-II

MANAGING DIGITAL FORENSICS ENGAGEMENTS

1. Engagement lifecycle: scoping, contracting, NDA, final report delivery
2. Resource planning: personnel, licensing, lab infrastructure costs
3. Quality assurance: peer review of forensic findings and second opinions

UNIT-III

BUILDING AND MATURING A SECURITY OPERATIONS CENTRE (SOC)

1. SOC models: in-house, MSSP, hybrid – cost-benefit analysis
2. SOC maturity models (SOC-CMM) and capability roadmap
3. Key metrics: alert volume, MTTD, MTTR, analyst utilisation

UNIT-IV

COMMUNICATION, REPORTING, AND EXECUTIVE ENGAGEMENT

1. Executive cyber security reporting: dashboards and risk heat maps
2. Crisis communications during a major incident
3. Vendor and third-party security management

REFERENCE BOOKS

1. PMI. (2021). A Guide to the Project Management Body of Knowledge (PMBOK Guide), 7th ed. PMI.
2. Axelos. (2017). PRINCE2 Agile. Axelos.
3. SANS Institute SOC Survey Reports (Annual). SANS Publications.
4. Talabis, M., & Martin, J. (2012). Information Security Risk Assessment Toolkit. Syngress.

THESIS / RESEARCH PROJECT

L/T/P/C
-/-/-/12

Learning Outcome:

1. Formulate an original research problem in digital forensics or cyber security with a clear research question.
2. Design and execute an appropriate research methodology, including data collection and analysis.
3. Produce a written dissertation presenting original findings in accordance with academic and ethical standards.
4. Defend the research work through an oral viva-voce before a committee including an external expert.

UNIT-I

RESEARCH PROJECT

1. Students undertake an independent research investigation in the domain of Digital Forensics or Cyber Security.
2. Typical project tracks include: novel intrusion detection systems, malware analysis automation, cloud forensics tooling, legal-technical analysis of cyber crime cases, or AI-driven threat hunting.
3. Deliverables: research proposal, mid-term progress report, final dissertation (~15,000 words), and oral viva voce.

REFERENCE BOOKS

1. Creswell, J. W. (2018). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (5th ed.). SAGE.
2. Zobel, J. (2015). Writing for Computer Science (3rd ed.). Springer.
3. IEEE Transactions on Information Forensics and Security (journal): https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=10206