ST. VINCENT PALLOTTI COLLEGE OF ENGINEERING & TECHNOLOGY,NAGPUR

(An autonomous institution affiliated to Rashtrasant Tukadoji Maharaj Nagpur University)

B. Tech. Scheme of Examination & Syllabus 2023-24 Computer Science and Engineering (Cyber Security)

SEMESTER VII

Sr No	Course Category	Course Code	Course Title	Hours per Week			Credits	Maximum Marks				Minimum passing Marks	No of Hours for ESE
				L	T	P		Mid Semester Examination	Continual Assessment	End Sem Examination	Total		
1	PCC	**23CS701T**	Cyber Forensics	**3**	**-**	**-**	**3**	**15**	**15**	**70**	**100**	**45**	**3**
2	PCC	**23CS701P**	Cyber Forensics Lab	**-**	**-**	**2**	**1**	**-**	**25**	**25**	**50**	**25**	**-**
3	PCC	**23CS702T**	Machine Learning for Cyber Security	**4**	**-**	**-**	**4**	**15**	**15**	**70**	**100**	**45**	**3**
4	PCC	**23CS702P**	Machine Learning for Cyber Security Lab	**-**	**-**	**2**	**1**	**-**	**25**	**25**	**50**	**25**	**-**
5	PEC	**23CS703T**	Program Elective-III	**3**	**-**	**-**	**3**	**15**	**15**	**70**	**100**	**45**	**3**
6	PCC	**23CS704P**	Network Protocol Engineering Lab	**-**	**-**	**2**	**1**	**-**	**25**	**25**	**50**	**25**	**-**
7	PCC	**23CS705P**	Security Operation Center Lab	**-**	**-**	**2**	**1**	**-**	**25**	**25**	**50**	**25**	**-**
8	ELC	**23CS706P**	Project - II	**-**	**-**	**4**	**2**	**-**	**50**	**50**	**100**	**50**	**-**
9	ELC	**23CS707P**	Summer / Winter Internship*	**-**	**-**	**-**	**2**	**-**	**50**	**-**	**50**	**25**	**-**
10	MDM	**23CS731M**	MDM – V (Refer MDM Basket)	**3**	**-**	**-**	**3**	**15**	**15**	**70**	**100**	**45**	**3**
			Total	**13**	**-**	**12**	**21**	**60**	**260**	**430**	**750**	**355**	

*** Summer / Winter Internship (Evaluation of Four weeks Internship Completion till 6th Semester)**

Program Elective - III	
23CS703T (i)	Threats and Malware Analysis
23CS703T (ii)	Information Security Audit and Monitoring
23CS703T (iii)	Information Security Analysis and Compliance using Big Data

Multidisciplinary Minor - V	
23CS731M	Web Security Analysis

		July 2026	**NEP 1.0**	**Applicable for 2026-27**
Chairman - BoS	**Dean – Academics**	**Date of Release**	**Version**	

ST. VINCENT PALLOTTI COLLEGE OF ENGINEERING & TECHNOLOGY, NAGPUR
(An autonomous institution affiliated to Rashtrasant Tukadoji Maharaj Nagpur University)
B. Tech. Scheme of Examination & Syllabus 2023-24
COMPUTER ENGINEERING AND ENGINEERING (CYBER SECURITY)

ARISE & SHINE

SEVENTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation			
						MSE	CA	ESE	Total
23CS701T	Cyber Forensics	3	-	-	3	15	15	70	100

Course Objectives	Course Outcomes
This course is intended 1. Analyze the core principles and techniques of cyber forensics and digital evidence management. 2. Apply standard procedures for evidence acquisition, analysis, and documentation. 3. Explore the tools and technologies used in the detection and investigation of cybercrimes. 4. Examine the legal and ethical aspects of cybercrime investigations.	**Students will be able to** 1. Comprehend the foundational concepts and scope of cyber forensics. 2. Analyzed and interpret digital evidence using appropriate forensic tools. 3. Document forensic activities in accordance with legal and professional standards. 4. Conduct forensic investigations in compliance with cyber laws and ethical practices. 5. Apply ethical principles in digital investigations and incident response planning.

Unit I: Introduction to Cyber Forensics	**[9 Hrs]**
Definition and scope of Cyber Forensics, Categories of cybercrime and digital evidence, Digital crime investigation process, Forensic readiness and lab setup, Chain of custody and integrity of evidence, Legal considerations in cyber forensics, Case Study: Introduction to a real-world cybercrime investigation.	
Unit II: Evidence Acquisition and Preservation	**[9 Hrs]**
Data acquisition techniques: live vs. static, Imaging tools and write blockers, Disk and file system analysis (FAT, NTFS, Ext), RAM and volatile memory analysis, Hashing techniques: MD5, SHA1, Evidence preservation and documentation, Lab: Creating and verifying forensic disk images.	
Unit III: Legal and Ethical Aspects of Risk Management	**[9 Hrs]**
Overview of forensic toolkits: FTK, Encase, Autopsy, Email and browser forensics, Log analysis and event correlation, Mobile device forensics basics, Steganography detection, Lab: Analysing browser cache and email headers	
Unit IV: Risk Analysis Techniques and Reporting	**[9 Hrs]**
Network traffic capture and analysis (Wireshark), IDS and firewall logs, Investigating insider threats and APTs, Malware behavior analysis basics. Memory dump analysis using Volatility, Case Study: Tracing a ransomware attack	
Unit V: Incident Response	**[9 Hrs]**
Cyber laws and forensic standards (IT Act, GDPR, HIPAA), Expert witness and courtroom presentation, Forensic report writing and documentation standards, Ethics in digital investigation, Lab: Drafting a forensic investigation report	

Text Books

S.N	Title	Authors	Edition	Publisher
1	Computer Forensics and Cyber Crime	Marjie T. Britz	4th Edition	Pearson
2	Guide to Computer Forensics and Investigations	Bill Nelson, Amelia Phillips, Chris Steuart	6th Edition	Cengage Learning

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Computer Forensics and Cyber Crime	Marjie T. Britz	4th Edition	Pearson
2	Guide to Computer Forensics and Investigations	Bill Nelson, Amelia Phillips, Chris Steuart	6th Edition	Cengage Learning

		July 2026	**NEP 1.0**	**Applicable for 2026-27**
Chairman - BoS	**Dean – Academics**	**Date of Release**	**Version**	

SEVENTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
23CS701P	Cyber Forensics Lab	-	-	2	1	25	25	50

Course Objectives	Course Outcomes
This course is intended 1. Analyse the principles and methodologies used in digital forensics and cyber investigations. 2. Identify and extract evidence from computers, mobile devices, and networks using forensic tools. 3. Ensure proper documentation, preservation, and presentation of digital evidence. 4. Gain knowledge of laws, ethics, and the legal framework related to cybercrime investigations.	**Students will be able to** 1. Comprehend the fundamental concepts of cyber forensics and digital evidence collection. 2. Utilize standard forensic tools to acquire and analyse data from digital devices. 3. Document forensic procedures to maintain the integrity and admissibility of evidence. 4. Apply forensics in real-world scenarios involving cybercrime investigations.

Experiment No.	Title of the Experiment
1	Introduction to Cyber Forensics and Setup of a Lab Environment
2	Acquisition and Imaging of Digital Evidence using FTK Imager
3	File Recovery and Metadata Extraction from a Windows System
4	Analyzing Web Browser Artefacts and Cache Files
5	Email Forensics: Header Analysis and Phishing Investigation
6	Memory Dump Analysis using Volatility Framework
7	Mobile Device Forensics using Open Source Tools
8	Network Packet Capture and Analysis using Wireshark
9	Detecting Hidden Files and Steganography Content
10	Reporting and Documentation of a Cyber Forensics Case Study
11	Legal Procedures and Chain of Custody Simulation

Text Books

S.N	Title	Authors	Edition	Publisher
1	Computer Forensics and Cyber Crime	Marjie T. Britz	4th Edition	Pearson
2	Guide to Computer Forensics and Investigations	Bill Nelson, Amelia Phillips, Chris Steuart	6th Edition	Cengage Learning

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Computer Forensics and Cyber Crime	Marjie T. Britz	4th Edition	Pearson
2	Guide to Computer Forensics and Investigations	Bill Nelson, Amelia Phillips, Chris Steuart	6th Edition	Cengage Learning

		July 2026	NEP 1.0	Applicable for 2026-27
Chairman - BoS	Dean – Academics	Date of Release	Version	

SEVENTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation			
						MSE	CA	ESE	Total
23CS702T	Machine Learning for Cyber Security	4	-	-	4	15	15	70	100

Course Objectives	Course Outcomes
This course is intended to provide: 1. Explain the foundational concepts of Machine Learning (ML) and their relevance to cyber security applications. 2. Explore various ML techniques such as supervised, unsupervised, and reinforcement learning for solving security problems. 3. Analyze real-world cyber security datasets using ML algorithms to detect anomalies, intrusions, malware, and phishing attacks.	**Student will be able to:** 1. Explain the fundamental concepts of machine learning and its integration into cyber security systems. 2. Apply supervised learning for cyber threat classification tasks. 3. Implement unsupervised learning algorithms and anomaly detection techniques to identify irregular patterns and threats in network traffic. 4. Design and evaluate machine learning models by performing feature engineering and using appropriate evaluation metrics in a cyber-security context. 5. Analyze real-world case studies of cyber threat detection and propose ML-driven solutions for identifying threats

Unit-I	**10 Hrs**
Introduction to Machine Learning: Definitions, Overview of machine learning and cyber security, Application areas of machine learning in cyber security, Challenges and limitations of machine learning in cyber security, Types (Supervised, Unsupervised, Reinforcement Learning), Role of ML in Cyber Security, Comparison of traditional vs. ML-based security systems, Basics of Data Preprocessing for Cyber Security, Overview of popular ML tools: Scikit-learn, Pandas, NumPy.	
Unit-II	**9 Hrs**
Supervised Learning Concepts: Labels, Features, Training & Testing, Classification Algorithms: Decision Trees, Random Forests, Logistic Regression, and Support Vector Machines (SVM), k-Nearest Neighbors (k-NN). Application: Intrusion Detection Systems (IDS), Evaluation Metrics: Accuracy, Precision, Recall, F1-Score and Confusion Matrix.	
Unit-III	**9 Hrs**
Unsupervised Learning Concepts: Clustering and Dimensionality Reduction, Clustering Algorithms: K-Means Clustering, DBSCAN, Hierarchical Clustering, Anomaly Detection Techniques: Isolation Forest One-Class SVM. Dimensionality Reduction: PCA (Principal Component Analysis) and Case Study: Detecting abnormal behavior in network traffic.	
Unit-IV	**8 Hrs**
Importance of Feature Engineering in Cyber Security, Feature Selection Techniques, Feature Extraction Techniques, Model Evaluation in Cyber Contexts: ROC curve, AUC.	
Unit-V	**9 Hrs**
Types of cyber threats: malware, phishing, DDoS, insider threats, etc., Traditional vs AI-based Threat Detection Systems, ML Pipeline in Security: Data Collection, Feature Engineering, Model Deployment, Case studies.	

Text Books

S.N	Title	Authors	Edition	Publisher
1	Machine Learning and Security: Protecting Systems with Data and Algorithms	Clarence Chio, David Freeman	Second	O'Reilly Media, 2018
2	Hands-On Machine Learning for Cybersecurity	Soma Halder, Sinan Ozdemir	Third	Packt Publishing

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Machine Learning for Cybersecurity Cookbook	Emmanuel Tsukerman	Second	Packt Publishing, 2019
2	Applied Machine Learning for Cybersecurity	Aihua Liu	Third	Springer

SEVENTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
23CS702P	Machine Learning for Cyber Security Lab	-	-	2	1	25	25	50

Course Objectives	Course Outcomes
This course is intended 1. Understand the fundamental concepts of machine learning and their role in modern cyber security systems. 2. Apply supervised and unsupervised machine learning techniques to detect, classify, and analyze cyber threats. 3. Develop and evaluate machine learning models for cyber security applications using appropriate datasets, features, and performance metrics. 4. Analyze adversarial machine learning threats and ethical challenges associated with deploying ML-based cyber defense solutions.	**Students will be able to** 1. Explain core machine learning concepts, workflows, and tools used in cyber security applications. 2. Implement supervised machine learning algorithms to classify cyber threats such as malware, phishing, and intrusions. 3. Apply unsupervised learning and anomaly detection techniques to identify abnormal patterns in network and system data. 4. Design, evaluate, and interpret machine learning models for cyber security while considering adversarial attacks and ethical implications.

Experiment No.	Title of the Experiment
1	Install and explore Python, NumPy, Pandas, Matplotlib, and Scikit-learn. Load a basic cyber dataset and inspect features.
2	Perform data cleaning, handling missing values, normalization, encoding categorical features using a network security dataset.
3	Train a supervised ML model to classify malware vs benign files and evaluate accuracy.
4	Build and compare Decision Tree and Random Forest models on IDS datasets (e.g., KDD/NSL-KDD).
5	Extract features from phishing datasets and apply Support Vector Machine for classification.
6	Apply unsupervised learning to cluster normal and abnormal network traffic patterns.
7	Detect outliers and anomalies in network traffic using density-based clustering.
8	Apply PCA on high-dimensional cyber datasets to reduce features and visualize attack patterns.
9	Evaluate classification models using confusion matrix, ROC curve, and AUC score in cyber security context.
10	Analyze adversarial attacks, model poisoning, evasion techniques, and discuss ethical challenges in ML-based cyber defense.

Text Books

S.No.	Title	Authors	Edition	Publisher
1	Machine Learning and Security: Protecting Systems with Data and Algorithms	Clarence Chio, David Freeman	Second Edition	O'Reilly Media
2	Hands-On Machine Learning for Cybersecurity	Soma Halder, Sinan Ozdemir	Third Edition	Packt Publishing

Reference Books

S.No.	Title	Authors	Edition	Publisher
1	Machine Learning for Cybersecurity Cookbook	Emmanuel Tsukerman	Second Edition	Packt Publishing
2	Applied Machine Learning for Cybersecurity	Aihua Liu	Third Edition	Springer

Chairman - BoS	Dean – Academics	July 2026 Date of Release	NEP 1.0 Version	Applicable for 2026-27

SEVENTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation			
						MSE	CA	ESE	Total
23CS703T(i)	PE –III Threat and Malware Analysis	3	-	-	3	15	15	70	100

Course Objectives	Course Outcomes
This course is intended 1. To identify malware types based on static & behavioral analysis 2. To determine malware types & capabilities 3. To evaluate potential threat from malware activity	**Student will be able to:** 1. Understand CTI concepts, threat types, and intelligence lifecycle models. 2. Apply structured intelligence frameworks like MITRE ATT&CK and STIX for threat reporting. 3. Analyze CTI implementation using OSINT tools and organizational strategies. 4. Apply static and dynamic malware analysis using appropriate lab setups. 5. Evaluate malware detection techniques using signature and non-signature-based methods.

Unit-I — **9 Hrs**

Introduction to Cyber Threat Intelligence (CTI) Essential Terminology, Types of Threats, APTs & IoCs, Where to Begin? The Intelligence Cycle, The Diamond Model, Cyber Kill Chain, Cyber Threat Lifecycles& Frameworks

Unit-II — **9 Hrs**

Structured intelligence and business planning, MITRE ATT&CK Framework , STIX Language, Intelligence Reporting, Intelligence Report Structure, Collection Sources, Threat Intelligence Budgeting, Intelligence Analysts

Unit-III — **9 Hrs**

CTI Implementation Organizational Footprint, Primary Considerations for CTI Implementation, Developing the Core CTI Team, Introduction to OSINT, OSINT Platforms, OSINT Research Technologies, CTI Prioritization

Unit-IV — **9 Hrs**

Introduction to Malware Analysis History, Types of Malwares, Types of Malware Analysis, Malware Analysis Lab Setup, Static Malware Analysis, Dynamic Malware Analysis

Unit-V — **9 Hrs**

Malware Detection Techniques: Signature-based techniques: malware signatures, packed malware signature, metamorphic and polymorphic malware signature Non-signature based techniques: similarity-based techniques, machine-learning methods, invariant inferences.

Text Books

S.N	Title	Authors	Edition	Publisher
1	Cyber Threat Intelligence: The No-Nonsense Guide for CISOs and Security Managers	Aaron Roberts.	First Edition	Apress Publishing.
2	TheThreat Intelligence Handbook: APractical Guidefor SecurityTeamsto UnlockingthePower ofIntelligence.	Chris Pace	First Edition	Cyber EdgePress

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Learning Malware Analysis	Monappa K A	First Edition	Packt Publishing
2	Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software	by Michael Sikorski & Andrew Honig.	First Edition	No Starch Press

SEVENTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation			
						MSE	CA	ESE	Total
23CS703T(iii)	PE – III Information Security Analysis and Compliance using Big Data	3	-	-	3	15	15	70	100

Course Objectives	Course Outcomes
This course is intended 1. Understand security principles, risk analysis, and compliance needs in big-data environments. 2. Analyze threats across data ingestion, storage, processing, sharing, and reporting layers. 3. Apply protection methods such as encryption, masking, access control, logging, and monitoring. 4. Prepare students for security, governance, and compliance roles in data-driven industries.	**Students will be able to** 1. Identify threats, vulnerabilities, and key risk scenarios in big data architectures. 2. Apply encryption, masking, tokenization, and secure data at rest/in transit controls. 3. Implement identity, access management, and secure service perimeter controls for Hadoop/Spark/Cloud. 4. Design and operate monitoring, logging, and audit pipelines for data activity. 5. Apply privacy governance, DPIA, and audit practices for secure data management.

Unit I - Big Data Security Foundations (concepts & architecture)	**[9 Hrs]**
Big data characteristics & architectures (HDFS, YARN, Spark, Kafka, NoSQL), threat model for big data, CIA in big data context, data lifecycle and classification, key industry use cases and security drivers.	
Unit II - Data Protection Techniques	**[9 Hrs]**
Encryption at rest and in transit (key management basics), column/field level encryption, tokenization, data masking & anonymization techniques (k anonymity, differential privacy overview), secure ingestion and ETL considerations.	
Unit III - Identity, Access and Perimeter Controls	**[9 Hrs]**
Kerberos, LDAP/Active Directory integration, Access Control, RBAC vs ABAC for big data, Apache Ranger/Atlas/Knox overview, secrets management, network segmentation, API gateway considerations.	
Unit IV - Monitoring, Detection and Incident Response	**[9 Hrs]**
Data activity monitoring (user/file/row level), logging best practices (centralized log pipelines, retention), SIEM integration, anomaly detection basics for data access patterns, forensics and containment in big data clusters.	
Unit V - Compliance, Governance and Secure Design	**[9 Hrs]**
Data retention & lifecycle governance, data protection impact assessment (DPIA), privacy by design, audits & evidence collection, case studies & industry best practices.	

Text Books

S.N	Title	Authors	Edition	Publisher
1	Securing Hadoop and Big Data Platforms	William J. Buchanan	1st	CRC Press
2	Big Data Security and Privacy: Emerging Issues and Solutions	Ashok Kumar Das, Joaquín García-Alfaro, et al.	1st	Springer

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Security and Privacy in Big Data: Challenges and Solutions	R. K. P. Subramanian, S. K. Gupta, et al.	1st	CRC Press
2	Information Security and IT Risk Management	Edward Amoroso	2nd	CRC Press

SEVENTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
23CS704P	Network Protocol Engineering Lab	-	-	2	1	25	25	50

Course Objectives	Course Outcomes
This course is intended 1. Understand the differences between IT and OT networks, including their architecture and security requirements. 2. Familiarize with industry-standard tools for asset discovery, threat detection, and network monitoring in OT environments. 3. Apply cybersecurity frameworks and standards like IEC 62443 to design secure OT systems. 4. Develop hands-on skills in configuring network security measures including VLANs, firewalls, RBAC, and intrusion detection systems. 5. Plan and implement proactive OT cybersecurity practices including risk assessment, incident response, and patch management.	**Students will be able to** 1. Differentiate between IT and OT network architectures and identify unique security requirements for OT systems. 2. Demonstrate the ability to use tools like Armis, Nozomi, and Claroty CTD for asset classification and threat detection in OT environments. 3. Apply IEC 62443 zoning, conduits, and risk assessment principles to secure an industrial control system. 4. Configure and monitor OT security protocols using tools such as Wireshark, VLANs, firewalls, and Snort for network defense. 5. Design an effective incident response plan and implement system hardening techniques for enhanced OT cybersecurity posture.

Expt. No.	Title of the Experiment
1	Compare IT vs OT Network Architecture and Security Requirements
2	Discover and Classify OT Assets Using Armis
3	Apply IEC 62443 Zoning and Conduit Concepts to a Sample OT System
4	Perform a Risk Assessment Based on IEC 62443-3-2 Guidelines
5	Configure Role-Based Access Control in an ICS Simulation (IEC 62443-3-3 SR 1.1)
6	Detect ICS Threats Using Nozomi Guardian (Simulated)
7	Analyze Threat Alerts Using Claroty Continuous Threat Detection (CTD)
8	Monitor OT Protocols (Modbus/DNP3) Using Wireshark
9	Implement VLANs and Firewalls to Segment an OT Network
10	Deploy Snort for Intrusion Detection in an Industrial Control Network
11	Design an Incident Response Plan for an OT Cybersecurity Scenario
12	Simulate Patch Management and System Hardening for OT Devices

Text Books

S.No.	Title	Authors	Edition	Publisher
1	Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems	Eric D. Knapp, Joel Langill	-	Syngress
2	Practical Industrial Internet of Things Security: A practitioner's guide to securing connected industries	Sravani Bhattacharjee, Gaurav Belani	-	Packt Publishing

Reference Books

S.No.	Title	Authors	Edition	Publisher
1	Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS	Tyson Macaulay & Bryan L. Singer	7th Edition	CRC Press
2	The Industrial Cybersecurity Handbook: A Practical Guide to Securing Your Organization's OT and ICS Environment	P.E. David J. Teumim	10th Edition	ISA (International Society of Automation)

		July 2026	NEP 1.0	Applicable for 2026-27
Chairman - BoS	Dean – Academics	Date of Release	Version	

SEVENTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
23CS705P	Security Operation Center Lab	-	-	2	1	25	25	50

Course Objectives	Course Outcomes
This course is intended 1. To understand the working of a Security Operations Center (SOC) by studying SIEM, log monitoring, endpoint security, network monitoring, and incident management workflows. 2. To develop practical skills in security monitoring and threat detection using tools such as Wazuh, Splunk, Sysmon, Zeek, Suricata, Wireshark, and Elastic Stack. 3. To perform incident investigation and response by analyzing logs, detecting suspicious activity, mapping attacks to MITRE ATT&CK;, and preparing incident response reports. 4. To apply digital forensics and threat intelligence techniques for malware triage, phishing investigation, endpoint forensic analysis, IOC extraction, and security case documentation.	**Students will be able to** 1. Understand the architecture, functions, and workflow of a Security Operations Center using SIEM, endpoint monitoring, network monitoring, and incident response tools. 2. Configure and operate security monitoring tools such as Wazuh, Splunk, Sysmon, Zeek, Suricata, Wireshark, and Elastic Stack for log collection and analysis. 3. Analyze and detect security incidents including brute-force attacks, web attacks, phishing attempts, Malware indicators, abnormal network traffic, and endpoint compromise. 4. Apply threat hunting, MITRE ATT&CK; mapping, digital forensics, IOC extraction, and incident reporting Techniques to complete SOC-based investigations.

Experiment No.	Title of the Experiment
1	Design and Deploy a Mini Security Operations Center using SIEM
2	Windows Attack Detection using Sysmon and SIEM
3	Detect and Respond to SSH/RDP Brute Force Attacks
4	Analyze Web Server Logs for Suspicious Web Attacks
5	Conduct Threat Hunting using MITRE ATTACK; Framework
6	Perform Safe Malware Triage and Static Analysis
7	Deploy Network IDS and Analyze Suspicious Traffic using Zeek and Suricata
8	Investigate a Phishing Email using Email Headers and Threat Intelligence
9	Perform Endpoint Forensic Investigation after Security Incident
10	End-to-End SOC Case Investigation and Incident Response Simulation

Text Books

S.No.	Title	Authors	Edition	Publisher
1	Blue Team Handbook: SOC, SIEM and Threat Hunting	Don Murdoch	Second Edition	Independently Published
2	The Practice of Network Security Monitoring	Richard Bejtlich	Third Edition	McGraw Hill Education

Reference Books

S.No.	Title	Authors	Edition	Publisher
1	The Art of Memory Forensics	Michael Hale Ligh, Andrew Case, Jamie Levy, Aaron Walters	First Edition	John Wiley & Sons
2	Cybersecurity Blue Team Toolkit	Nadean H. Tanner	First Edition	John Wiley & Sons

		July 2026	NEP 1.0	Applicable for 2026-27
Chairman - BoS	Dean – Academics	Date of Release	Version	

SEVENTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation			
						MSE	CA	ESE	Total
23CS731M	MDM - V Web Security Analysis	3	-	-	3	15	15	70	100

Course Objectives	Course Outcomes
This course is intended 1. Identify common web security threats and vulnerabilities. 2. Analyze web applications for security weaknesses. 3. Identify and assess various types of web security vulnerabilities. 4. Utilize appropriate tools and methodologies to assess and test web security. 5. Develop strategies to mitigate web security risks and protect against potential attacks.	**Student will be able to:** 1. Analyze web applications for security weaknesses. 2. Conduct comprehensive security assessments of web applications. 3. Apply appropriate tools and techniques for web security testing and analysis. 4. Implement effective mitigation strategies to address identified vulnerabilities. 5. Enhance overall web application security.

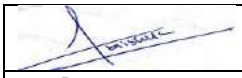
Unit-I	**9 Hrs**
Introduction to Web Security: Understanding web security concepts and principles, overview of common web security threats and attack vectors, introduction to web application architecture and potential vulnerabilities.	
Unit-II	**9 Hrs**
Web Application Vulnerabilities: Common web application vulnerabilities (e.g., Cross-Site Scripting, SQL Injection, CSRF), techniques for identifying and exploiting web vulnerabilities, best practices for securing web applications	
Unit-III	**9 Hrs**
Security Analysis Techniques: Methods for assessing and analyzing web security, introduction to web application testing methodologies, hands-on exercises for identifying and assessing web vulnerabilities.	
Unit-IV	**9 Hrs**
Web Security Testing Tools: Overview of popular web security testing tools (e.g., Burp Suite, OWASP ZAP, Nmap), practical demonstrations and lab exercises, integration of tools into the web security analysis process.	
Unit-V	**9 Hrs**
Mitigation Strategies and Best Practices: Strategies for mitigating web security vulnerabilities, best practices for secure web application development, case studies and real-world examples.	

Text Books

S.N	Title	Authors	Edition	Publisher
1	The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws	Dafydd Stuttard, Marcus Pinto	2nd Edition,	No Starch Press
2	Web Security Testing Cookbook	Paco Hope, Ben Walther	1st Edition,	O'Reilly Media

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Web Application Security: A Beginner's Guide	Bryan Sullivan,	1st Edition,	McGraw-Hill Education
2	Web Application Security: A Comprehensive Guide for Beginners	Bhushan Bhange, Dr. Anjali Khiwadkar,	1st Edition,	Packt Publishing

		July 2026	NEP 1.0	Applicable for 2026-27
Chairman - BoS	Dean – Academics	Date of Release	Version	