SBIT TECHMENTORS CURRICULUM CYBER SECURITY AND FORENSICS

TABLE OF CONTENTS

CYBER SECURITY AND FORENSICS

This program provides an in-depth exploration of the principles, practices, and technologies used in cybersecurity and digital forensics. It covers the fundamentals of securing networks, systems, and data from cyber threats while equipping students with the skills needed to investigate and respond to security breaches. Through a combination of theoretical knowledge and practical exercises, students will learn to identify vulnerabilities, implement robust security measures, and conduct thorough forensic investigations to uncover evidence of cybercrime. The course prepares students for careers in cybersecurity, forensics, and related fields, emphasizing real-world applications and hands-on experience.

SCHEME

Course Name: Cyber Security and Forensics

Duration: 9 Months (39 weeks)

S. No.	Paper Title	Lecture / Tutorial (per week)	Practical Classes (per week)	Total Hours (Lecture / Tutorial)	Total Hours (Practical Classes)	Total Credit
1	Introduction to Cybersecurity	3	10	20	50	3
2	Network Security	3	10	20	50	3
3	Application Security	4	11	26	68	4
4	Cryptography and Data Protection	3	10	20	50	3
5	Incident Response and Management	3	10	20	50	3
6	Digital Forensics	3	10	26	38	3
7	Capstone Project	1	5	18	144	6
Total				**150**	**450**	**25**

PROGRAM OUTCOMES

- Grasp Cybersecurity Fundamentals - Understand key cybersecurity concepts and assess various cyber threats and vulnerabilities.
- Secure Networks and Systems - Implement and manage network security measures, including firewalls, VPNs, and IDPS, and design secure network architectures.
- Develop and Secure Applications - Apply secure software development practices and mitigate common application vulnerabilities.
- Utilize Cryptography - Implement cryptographic techniques for data protection and manage cryptographic keys effectively.
- Respond to Cybersecurity Incidents - Develop and execute incident response plans and analyze incidents to improve future responses.
- Conduct Digital Forensic Investigations - Perform digital forensic investigations and analyze digital evidence across various platforms.
- Apply Knowledge in Real-World Scenarios - Execute a capstone project addressing a real-world cybersecurity or forensic problem and stay informed on emerging trends.
- Prepare for Professional Certification - Build the foundational skills necessary for certifications like CISSP, CEH, and EnCE.

LEARNING PATH VISUALIZATION

1) Introduction to Cybersecurity
2) Network Security
3) Application Security
4) Cryptography and Data Protection
5) Incident Response and Management
6) Digital Forensics
7) Capstone Project

MODULE 1: INTRODUCTION TO CYBERSECURITY

LEARNING OUTCOMES:

- Understand the key concepts and importance of cybersecurity.
- Identify various types of cyber threats and vulnerabilities.
- Familiarize with cybersecurity frameworks and standards.
- Conduct basic risk assessments and understand mitigation strategies.

TOPICS COVERED:

- Fundamentals of Cybersecurity
    - Definition, scope, and importance of cybersecurity.
    - Key concepts: Confidentiality, Integrity, Availability (CIA Triad).
    - Overview of cybersecurity domains: network, application, information, operational security.
- Types of Cyber Threats
    - Malware: Types (viruses, worms, trojans) and attack vectors.

- Social Engineering: Phishing, spear-phishing, and pretexting.
- Ransomware: How it works and prevention strategies.
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.
- Advanced Persistent Threats (APTs): Tactics, techniques, and procedures.

- Cybersecurity Frameworks and Standards
  - Overview of the NIST Cybersecurity Framework.
  - ISO/IEC 27001: Information Security Management.
  - CIS Controls: Basic, foundational, and organizational controls.
  - Introduction to GDPR, CCPA, and other regulatory frameworks.
- Risk Management and Assessment
  - Risk identification: Asset, threat, and vulnerability analysis.
  - Risk assessment methodologies: Qualitative and quantitative approaches.
  - Risk mitigation strategies: Avoidance, transference, mitigation, acceptance.

MODULE 2: NETWORK SECURITY

LEARNING OUTCOMES:

- Understand network security principles and the OSI model.
- Configure and manage firewalls and VPNs for secure communication.
- Implement and monitor IDPS to protect networks from intrusions.
- Design secure network architectures to safeguard information systems.

TOPICS COVERED:

- Network Security Fundamentals
  - Understanding the OSI model and its relevance to security.
  - TCP/IP protocols and their vulnerabilities.
- Firewalls and VPNs
  - Types of firewalls: Packet filtering, stateful inspection, proxy firewalls.
  - VPN fundamentals: IPsec, SSL/TLS VPNs, and their applications.
  - Configuring firewalls for secure network access.
- Intrusion Detection and Prevention Systems (IDPS)
  - Difference between IDS and IPS.
  - Types of IDPS: Signature-based, anomaly-based, hybrid systems.
  - Deployment strategies: Network-based vs. host-based IDPS.
- Secure Network Design
  - Principles of network segmentation and zoning.
  - Implementing DMZs (Demilitarized Zones) for added security.
  - Network security monitoring and log management.

MODULE 3: APPLICATION SECURITY

LEARNING OUTCOMES:

- Understand the Secure Software Development Lifecycle (SDLC).

- Identify and mitigate common application vulnerabilities.
- Conduct penetration testing and vulnerability scanning.
- Implement security measures in DevOps environments.

TOPICS COVERED:

- Secure Software Development Lifecycle (SDLC)
  - Integrating security into each phase of the SDLC.
  - Secure coding practices: Input validation, error handling, and session management.
  - Code review and security testing techniques.
- Common Application Vulnerabilities
  - Overview of the OWASP Top 10 vulnerabilities.
  - SQL Injection: How it works and how to prevent it.
  - Cross-Site Scripting (XSS): Types, impact, and mitigation strategies.
  - Cross-Site Request Forgery (CSRF): Understanding and prevention.
- Penetration Testing and Vulnerability Scanning
  - Difference between vulnerability scanning and penetration testing.
  - Tools for vulnerability scanning: Nessus, OpenVAS, and others.
  - Penetration testing methodologies: Reconnaissance, exploitation, post-exploitation.
- Security in DevOps
  - Introduction to DevSecOps: Integrating security into DevOps practices.
  - Automating security testing in CI/CD pipelines.
  - Infrastructure as Code (IaC) security best practices.

MODULE 4: CRYPTOGRAPHY AND DATA PROTECTION

LEARNING OUTCOMES:

- Understand the basic principles of cryptography and encryption techniques.
- Apply cryptographic protocols to secure data communication.
- Manage cryptographic keys and implement PKI.
- Protect data through encryption and other data protection strategies.

TOPICS COVERED:

- Fundamentals of Cryptography
  - Introduction to cryptographic principles: Confidentiality, integrity, authenticity.
  - Symmetric encryption: Algorithms (AES, DES), key management.
  - Asymmetric encryption: RSA, ECC, key exchange mechanisms.
  - Hash functions: MD5, SHA family, applications in integrity verification.
- Cryptographic Protocols
  - SSL/TLS: Secure communication protocols, handshake process.
  - IPsec: Modes (transport, tunnel), applications in VPNs.
  - PGP/GPG: Email encryption, signing, and verification.
  - Overview of blockchain and cryptographic primitives used in blockchain technology.
- Key Management

- Public Key Infrastructure (PKI): Components, architecture, and deployment.
- Digital certificates: Types (SSL, Code Signing), issuing and revocation processes.
- Hardware Security Modules (HSMs) and their role in key management.

- Data Protection Techniques
  - Encryption techniques for data at rest: Full disk encryption, file/folder encryption.
  - Encrypting data in transit: SSL/TLS, VPNs, secure email.
  - Data masking and tokenization techniques.
  - Implementing Data Loss Prevention (DLP) solutions.

MODULE 5: INCIDENT RESPONSE AND MANAGEMENT

LEARNING OUTCOMES:

- Develop and implement an effective incident response plan.
- Detect and monitor cyber threats using SIEM and other tools.
- Respond to and contain cybersecurity incidents effectively.
- Conduct post-incident analysis to improve future incident response.

TOPICS COVERED:

- Incident Response Fundamentals
  - Overview of incident response lifecycle: Preparation, detection, containment, eradication, recovery, lessons learned.
  - Developing an incident response plan: Roles, responsibilities, communication channels.
  - Incident response team (IRT): Structure, roles, and responsibilities.
- Threat Detection and Monitoring
  - Security Information and Event Management (SIEM): Features, deployment, and best practices.
  - Log analysis: Techniques, tools, and common log sources.
  - Threat intelligence: Sources, integration, and application in detection.
- Incident Handling and Containment
  - Containment strategies: Isolating affected systems, preventing lateral movement.
  - Eradication techniques: Removing malware, closing vulnerabilities.
  - Recovery: Restoring systems to normal operation, verifying system integrity.
- Post-Incident Analysis
  - Conducting a root cause analysis: Techniques and tools.
  - Incident reporting: Creating actionable and detailed incident reports.
  - Continuous improvement: Updating response plans based on analysis.

MODULE 6: DIGITAL FORENSICS

LEARNING OUTCOMES:

- Understand the fundamental principles of digital forensics.
- Use forensic tools to recover and analyze digital evidence.
- Conduct forensic investigations in network and cloud environments.

- Apply mobile forensics techniques to extract and analyze data from devices.

TOPICS COVERED:

- Introduction to Digital Forensics
  - Overview of digital forensics: History, importance, and legal considerations.
  - Types of digital forensics: Computer, network, mobile, cloud forensics.
  - Legal and ethical considerations in forensic investigations.
- Forensic Tools and Techniques
  - Disk imaging: Tools (FTK Imager, dd), techniques, and importance.
  - Data recovery: Techniques for recovering deleted, fragmented, or encrypted files.
  - Forensic analysis: Tools (EnCase, Autopsy), methodologies, and reporting.
- Network and Cloud Forensics
  - Network forensics: Capturing and analyzing network traffic, tools (Wireshark, tcpdump).
  - Investigating network intrusions: Techniques, tracing attackers.
  - Cloud forensics: Challenges, evidence acquisition, and tools.
- Mobile Device Forensics
  - Mobile device architecture: Operating systems (iOS, Android), file systems.
  - Techniques for acquiring mobile data: Logical, physical, file system extractions.
  - Analyzing mobile data: Call logs, messages, GPS data, app usage.

MODULE 7: CAPSTONE PROJECT

LEARNING OUTCOMES:

- Develop and present a comprehensive cybersecurity or forensic solution.
- Stay informed on emerging trends and technologies in cybersecurity.
- Understand the future direction of digital forensics.
- Prepare for professional certifications in cybersecurity and forensics.

TOPICS COVERED:

- Comprehensive Security Audit of a Small Business Network
  - Conduct a thorough security audit of a small business's IT infrastructure. Identify vulnerabilities, assess risks, and provide a detailed report with recommendations for improving the security posture.
- Design and Implementation of a Secure Web Application
  - Develop a web application with built-in security features. Implement measures to protect against common threats such as SQL injection, XSS, and CSRF. Include secure coding practices and demonstrate vulnerability testing.
- Incident Response Simulation and Analysis
  - Create a simulated cyber-attack on a fictional organization, then lead an incident response exercise. Document the detection, containment, eradication, and recovery processes, and provide a post-incident analysis with lessons learned.
- Digital Forensics Investigation of a Cybercrime Case

- Perform a digital forensic investigation based on a mock cybercrime scenario. Recover and analyze digital evidence from multiple sources, such as computers, mobile devices, or networks, and present findings in a legal report format.

- Development of a Custom Intrusion Detection System (IDS)
  - Design and implement a custom IDS for a network. Use machine learning or rule-based approaches to detect and prevent unauthorized activities. Test the system's effectiveness against different types of attacks.
- Implementation of a Zero Trust Security Architecture
  - Design and implement a Zero Trust security model for an organization's IT infrastructure. Document the process of moving from a traditional security model to Zero Trust, including identity management, network segmentation, and continuous monitoring.
- Cryptographic Analysis and Implementation of a Secure Communication System
  - Develop a secure communication system using cryptographic techniques. Implement encryption, decryption, and key management processes, and demonstrate the system's ability to protect data confidentiality and integrity during transmission.

ATTENDANCE AND EVALUATION

Attendance: 75% of all mandatory classes/mini projects

Evaluation: Score from assignments, mini-projects, online quiz (20 min tests every week), and a final exam.

Evaluation Scheme

Assessment Type	Total Count	Best of	Points / Assessment	Total Points
Quizzes	24	22	5	110
Lab Assignments	24	20	3	60
Mini Projects	24	23	10	230
Final Exams	6	6	100	600
Capstone	1	1	400	400
			Total	1400

Grading Scheme

Letter Grade	Percentage Range
A+	90% - 100%
A	70% - 89%
B+	50% - 69%
B	40% - 49%
C	0% - 40%

Certificate of Completion Criteria:

- Secure more than **40% marks** overall
- Maintain at least **75% attendance** as per the policy

Certificate of Participation Criteria:

- Secure less than **40% marks** overall
- Maintain at least **50% attendance** as per the policy

C Grade: Only participation certificate

Capstone evaluation: Based on the final presentation during the campus visit/online session.