Curriculum

For

1 Year Diploma

In

Cyber Security

Approved By :-
Centre for Curriculum Research & Development
Sindh Board of Technical Education, Karachi

Curriculum

For

One Year Diploma In Cybersecurity

Cybersecurity Course

Eligibility:	Minimum Matric
Duration:	1 Year

Certification:	Sindh Board of Technical Education (SBTE)

One Year Diploma in Cyber Security

Course Objective:

The Cybersecurity Course is designed to provide students with foundational and practical skills in the field of information security. The program aims to equip learners with the knowledge to protect computer systems, networks, and data from cyber threats, attacks, and unauthorized access. In addition to technical training, this course develops critical thinking, risk assessment, and problem-solving skills essential for cybersecurity professionals. Students will learn to adapt to the evolving threat landscape and use modern security tools to defend digital assets. The course encourages a deep understanding of security principles, ethical practices, and compliance standards.

Learning Outcomes:

By the end of this course, students will be able to:

- ✅ Understand the core principles, terminologies, and importance of cybersecurity
- ✅ Identify and analyze various types of cyber threats, malware, and attack vectors
- ✅ Implement basic network security controls like firewalls, VPNs, and IDS/IPS
- ✅ Harden operating systems and manage endpoint security
- ✅ Understand and apply fundamental cryptographic techniques
- ✅ Identify common application vulnerabilities (OWASP Top 10) and secure coding practices
- ✅ Manage user identities and access controls (IAM, MFA, RBAC)
- ✅ Understand security operations, incident response procedures, and digital forensics basics
- ✅ Conduct risk assessments and understand major compliance standards (ISO 27001, NIST, GDPR)
- ✅ Perform basic ethical hacking and penetration testing using common tools
- ✅ Understand emerging trends like AI in security, cloud security, and IoT security

Career & Job Market Opportunities:

Graduates of the Cybersecurity Course will have access to a wide range of job opportunities, including:

- Security Operations Center (SOC) Analyst
- Junior Network Security Administrator
- Vulnerability Assessment Analyst
- IT Security Support Specialist
- Cybersecurity Awareness Trainer
- Freelance Penetration Tester (Entry-Level)
- Compliance Assistant

This course lays a strong foundation for those interested in pursuing advanced cybersecurity certifications (like CEH, CompTIA Security+) or starting their career in the high-demand field of information security.

Certification by:

Sindh Board of Technical Education (SBTE) -- Recognized and valued across institutions and employers in Pakistan.

Recommended Books:

- "Cybersecurity for Beginners" - Raef Meeuwisse
- "Network Security Essentials" - William Stallings
- "The Web Application Hacker's Handbook" - Dafydd Stuttard and Marcus Pinto
- "Security Engineering" - Ross Anderson

Semester 1 Courses				
Sr. No.	**Course Title**	**Theory**	**Practical**	**Credit Hours**
CS-101	Introduction to Cybersecurity	2	3	3
CS-102	Network Security	2	3	3
CS-103	System and Endpoint Security	1	3	2
CS-104	Cryptography	2	3	3
CS-105	Application Security	1	3	2
CS-106	Functional English	2	0	2
	Total Credit Hours	**10**	**15**	**15**

Semester 2 Courses				
Sr. No.	**Course Title**	**Theory**	**Practical**	**Credit Hours**
CS-201	Identity and Access Management (IAM)	1	3	2
CS-202	Security Operations & Incident Response	2	3	3
CS-203	Risk Management and Compliance	2	0	2
CS-204	Ethical Hacking and Penetration Testing	2	3	3
CS-205	Emerging Trends in Cybersecurity	1	3	2
CS-206	Capstone Project	0	3	1
	Total Credit Hours	**8**	**15**	**13**

SINDH BOARD OF TECHNICAL EDUCATION, KARACHI

Diploma In Cybersecurity

Detail Course Outline

Duration: 6 Months (400 Hours) Total Marks 375

Semester-I

Subjects	Total Hours	Theory Hours	Practical Hours	Theory Marks	Practical Marks	Total Marks
Introduction to Cybersecurity	80	32	48	50	25	75
Network Security	80	32	48	50	25	75
System and Endpoint Security	64	16	48	25	25	50
Cryptography	80	32	48	50	25	75
Application Security	64	16	48	25	25	50
Functional English	32	32	0	50	0	50
	400	160	240	250	125	375

Detail Course Outline

Duration: 6 Months (368 Hours) Total Marks 325

Semester-II

Subjects	Total Hours	Theory Hours	Practical Hours	Theory Marks	Practical Marks	Total Marks
Identity and Access Management (IAM)	64	16	48	25	25	50
Security Operations & Incident Response	80	32	48	50	25	75
Risk Management and Compliance	32	32	0	50	0	50
Ethical Hacking and Penetration Testing	80	32	48	50	25	75
Emerging Trends in Cybersecurity	64	16	48	25	25	50
Capstone Project	48	0	48	0	25	25
	368	128	240	200	125	325

COURSE CODE: **CS-101**

COURSE TITLE: **Introduction to Cybersecurity**

T	P	C
2	3	3

Semester: 1st

Pre-requisite: Basic understanding of computer systems, networking fundamentals, and data representation.

Credit Hours: 3

This course provides a comprehensive foundation in cybersecurity, merging theoretical principles with the mathematical rigor required for modern cryptography. Students will explore the CIA triad, identify evolving threat landscapes, and master the fundamental mathematics—including modular arithmetic and inverse calculations—that secure global data exchange.

Course Objectives:

- Define cybersecurity and its critical role in a digitized society.
- Apply Modular Arithmetic, Inverse Calculations, and Prime Number Theory to cryptographic problems.
- Identify domains of cybersecurity (Network, Application, Information).
- Explain and implement the core principles of Confidentiality, Integrity, and Availability (CIA).
- Analyze real-world security incidents and develop defensive strategies.

COURSE DURATION:

- Theory: 32 hours
- Practical / Lab: 48 hours

Learning Outcomes:

By the end of this course, students will be able to:

- Articulate the scope and importance of cybersecurity in professional environments.
- Solve complex modular equations and calculate modular inverses manually and via script.
- Differentiate between various cybersecurity domains and cryptographic protocols.
- Apply the CIA triad to evaluate and secure real-world technical scenarios.
- Critically Analyze major cyberattacks to prevent future vulnerabilities.

COURSE OUTLINE

Contents	Hours
1. Foundations of Cybersecurity	**4 + 6**
Definition, Purpose, and Components of a Secure System.	
2. The CIA Triad & Security Models	**4 + 6**
In-depth Confidentiality, Integrity, and Availability. Bell-LaPadula vs. Biba Models.	
3. Mathematical Foundations for Cryptography	**4 + 6**
Modular Arithmetic, Congruence, and the Euclidean Algorithm.	
4. Advanced Cryptographic Math	**4 + 6**
Multiplicative Inverses, Extended Euclidean Algorithm, and Fermat's Little Theorem.	
5. Cryptographic Systems	**4 + 6**
Symmetric (AES/DES) vs. Asymmetric (RSA/Diffie-Hellman), Hashing, and Digital Signatures.	
6. The Cyber Threat Landscape	**4 + 6**
Threat Actors, Attack Vectors, Malware (Ransomware, Trojans), and Social Engineering.	
7. Network & Application Security	**4 + 6**
Firewalls, IDS/IPS, VPNs, and the OWASP Top 10 vulnerabilities.	
8. Compliance, Ethics & Case Studies	**4 + 6**
Legal frameworks (GDPR, NIST), Ethics in Hacking, and Analysis of WannaCry/SolarWinds.	

Teaching Methodology:

- Lectures: Interactive sessions focused on theory and mathematical proofs.
- Problem-Solving Sets: Frequent drills on modular arithmetic and inverse calculations.
- Case Study Analysis: Group breakdowns of historical data breaches.
- Lab-Based Learning: Practical implementation of security tools and Python-based crypto scripts.

Recommended Books:

- "Cybersecurity Essentials" by Charles J. Brooks.
- "Introduction to Cybersecurity" by Noora Al-Mansoori.

LIST OF PRACTICALS

1. Identifying common malware types (Viruses, Worms, Trojans).
2. Simulating Phishing attacks for awareness training.
3. Analyzing DDoS attack vectors.
4. Exploring the CIA Triad in real-world scenarios.
5. Basic Firewall configuration.
6. Installing and updating Antivirus software.
7. Implementing basic Access Controls.
8. Data encryption basics for files.
9. Case study analysis of the WannaCry Ransomware.
10. Analysis of the Equifax Data Breach.
11. Reviewing the SolarWinds Supply Chain Attack.
12. Using basic network scanning tools.
13. Identifying threat actors and their motivations.
14. Verifying data integrity via checksums.
15. Evaluating compliance and trust indicators.
16. Assessing emerging threats in the current landscape.

COURSE CODE: **CS-102**
COURSE TITLE: **Network Security**

T	P	C
2	3	3

Semester: 1st
Pre-requisite: Basic knowledge of networking concepts, data communication, and network devices.

Credit Hours: 3

This course introduces essential network security concepts, including securing OSI/TCP-IP layers, configuring firewalls and VPNs, deploying IDS/IPS, and protecting wireless networks. Students gain practical skills to design and implement basic secure network architectures.

Course Objectives:

- Understand the OSI/TCP-IP model from a security perspective
- Learn the function and configuration of firewalls and VPNs
- Implement Intrusion Detection and Prevention Systems (IDS/IPS)
- Design basic secure network architectures
- Identify and mitigate common Wi-Fi security threats

COURSE DURATION:

- Theory: 32 hours
- Practical / Lab: 48 hours

Learning Outcomes:

- Explain how each layer of the network model can be secured
- Differentiate between network security devices and their purposes
- Configure a basic firewall rule set
- Design a simple secure network layout
- Secure a wireless network against common attacks

COURSE OUTLINE

Contents	Hours
1. OSI Model Overview for Security	**4 + 6**
1.1 Understanding OSI Layers	
1.2 Security Roles at Each Layer	
1.3 Common Threats per Layer	
2. Firewalls (Types, Configurations)	**4 + 6**
2.1 Firewall Types (Packet, Stateful, NGFW)	
2.2 Firewall Rules & Policies	
2.3 Network Segmentation with Firewalls	
3. Virtual Private Networks (VPNs)	**4 + 6**
3.1 VPN Types (Site-to-Site, Remote Access)	
3.2 Encryption & Tunneling Protocols	
3.3 VPN Use Cases & Limitations	
4. Intrusion Detection and Prevention Systems (IDS/IPS)	**4 + 6**
4.1 IDS vs IPS Differences	
4.2 Detection Methods (Signature, Anomaly)	
4.3 Deployment Architectures	
5. Proxy Servers and Network Address Translation (NAT)	**4 + 6**
5.1 Proxy Server Types & Uses	
5.2 NAT Types (SNAT, DNAT, PAT)	
5.3 Security Benefits of Proxy & NAT	
6. Secure Network Design Principles	**4 + 9**
6.1 Defense in Depth	
6.2 Network Segmentation & VLANs	
6.3 Zero Trust Architecture	
7. Wi-Fi Security (WPA2, WPA3, Threats)	**8 + 9**
7.1 Wi-Fi Encryption Standards	
7.2 Authentication Methods	
7.3 Common Wi-Fi Attacks & Mitigations	

Teaching Methodology:

- Lectures
- Lab simulations (e.g., Cisco Packet Tracer)
- Practical configuration exercises
- Demonstrations

Recommended Books:

- "CISSP Cert Guide" by Michael Gregg. (3rd Edition).

LIST OF PRACTICALS

1. OSI Model layer-by-layer security analysis.
2. Configuring Packet-filtering firewalls.
3. Implementing Stateful Inspection policies.
4. Next-Generation Firewall (NGFW) setup.
5. Network segmentation using VLANs.
6. Configuring Site-to-Site VPNs.
7. Setting up Remote Access VPNs.
8. Implementing Tunneling protocols.
9. IDS (Intrusion Detection System) deployment.
10. IPS (Intrusion Prevention System) configuration.
11. Signature-based vs. Anomaly-based detection labs.
12. Proxy Server setup and management.
13. Configuring Network Address Translation (NAT/PAT).
14. Designing a Secure Network Architecture.
15. Wi-Fi security: WPA2/WPA3 configuration.
16. Wireless attack mitigation (Rogue AP detection).

COURSE CODE: **CS-103**

COURSE TITLE: **System and Endpoint Security**

T	P	C
1	3	2

Semester: 1st

Pre-requisite: Basic understanding of operating systems, computer hardware, and system functions.

Credit Hours: 2

This course focuses on securing Windows and Linux systems through OS hardening, patch management, antivirus deployment, and endpoint protection. Students will gain hands-on experience with encryption, EDR, and application control to safeguard endpoints against modern threats.

Course Objectives:

- Harden Windows and Linux operating systems
- Implement and manage antivirus and anti-malware solutions
- Understand and apply patch management processes
- Utilize device encryption to protect data at rest
- Introduction to Endpoint Detection and Response (EDR)

COURSE DURATION:

- Theory: 16 hours
- Practical / Lab: 48 hours

Learning Outcomes:

- Harden an OS by disabling unnecessary services and configuring security settings
- Deploy and manage an antivirus solution
- Develop a basic patch management schedule
- Encrypt a disk drive using built-in OS tools
- Explain the role of EDR in modern security

COURSE OUTLINE

Contents	Hours
1. Operating System Hardening (Windows, Linux)	**2 + 6**
1.1 Disabling Unnecessary Services	
1.2 Configuring Secure Permissions	
1.3 Implementing Security Baselines (CIS, STIG)	
2. Antivirus and Anti-malware Tools	**2 + 6**
2.1 Signature-Based Detection	
2.2 Behavioral/Heuristic Analysis	
2.3 Real-Time Protection & Scanning	
3. Patch Management Strategies	**2 + 6**
3.1 Regular Update Scheduling	
3.2 Vulnerability Prioritization	
3.3 Testing & Deployment Methods	
4. Endpoint Detection and Response (EDR)	**2 + 6**
4.1 Endpoint Monitoring & Telemetry	
4.2 Threat Detection & Automated Response	
4.3 Incident Investigation Capabilities	
5. Device Encryption (BitLocker, LUKS)	**2 + 6**
5.1 Full-Disk vs File-Level Encryption	
5.2 Key Management & Recovery	
5.3 Encryption Policies & Compliance	
6. Application Whitelisting/Control	**2 + 9**
6.1 Allowlisting Trusted Applications	
6.2 Control of Execution Policies	
6.3 Preventing Unauthorized Software	
7. Practical Hardening Lab	**4 + 9**
7.1 Windows Hardening Exercises	
7.2 Linux Security Configuration Tasks	
7.3 Validation & Security Testing	

Teaching Methodology:

- Hands-on lab sessions
- Live demonstrations on VM environments
- Group projects

Recommended Books:

- "Endpoint Security" by Mark Stanislav.
- "Windows Security Baseline" (Technical Documentation) by Microsoft Docs.

LIST OF PRACTICALS

1. Windows OS hardening: disabling unnecessary services.
2. Linux OS hardening: configuring secure permissions.
3. Implementing CIS/STIG Security Baselines.
4. Antivirus deployment and real-time scanning.
5. Behavioral and Heuristic analysis testing.
6. Automating Patch Management updates.
7. Vulnerability prioritization labs.
8. Full-disk encryption using BitLocker.
9. Implementing LUKS for Linux disk encryption.
10. Endpoint Detection and Response (EDR) monitoring.
11. Investigating incidents via EDR telemetry.
12. Application Whitelisting and execution policies.
13. Managing File-level encryption.
14. Key management and recovery procedures.
15. Preventing unauthorized software execution.
16. Validation and security testing of hardened systems.

COURSE CODE: **CS-104**	**T**	**P**	**C**
COURSE TITLE: **Cryptography**	**2**	**3**	**3**

Semester: 1st

Pre-requisite: Basic knowledge of computer systems, data representation (number systems), and logical thinking.

Credit Hours: 3

This course introduces the fundamentals of cryptography, covering encryption, hashing, digital signatures, and SSL/TLS for secure communications. Students will gain practical skills in applying cryptographic methods, managing digital certificates, and ensuring data integrity.

Course Objectives:

- Understand the history and basic concepts of cryptography
- Differentiate between symmetric and asymmetric encryption
- Explain hashing algorithms and digital signatures
- Describe the role of SSL/TLS in securing web traffic
- Understand the components of Public Key Infrastructure (PKI)

COURSE DURATION:

- Theory: 32 hours
- Practical / Lab: 48 hours

Learning Outcomes:

- Encrypt and decrypt data using basic cryptographic tools
- Select appropriate cryptographic methods for a given scenario
- Verify data integrity using hashes
- Explain how HTTPS protects web communications
- Describe the process of issuing and managing digital certificates

COURSE OUTLINE

Contents	Hours
1. History and Basics of Cryptography	**4 + 6**
1.1 Early Ciphers (Caesar, Vigenère)	
1.2 Evolution to Modern Cryptography	
1.3 Core Goals (Confidentiality, Integrity, Authentication)	
2. Symmetric vs. Asymmetric Encryption	**4 + 6**
2.1 Symmetric Key Concepts (AES, DES)	
2.2 Asymmetric Key Concepts (RSA, ECC)	
2.3 Use Cases & Performance Differences	
3. Hashing Algorithms and Digital Signatures	**4 + 6**
3.1 Hash Function Properties (SHA, MD5)	
3.2 Digital Signature Creation & Verification	
3.3 Integrity & Non-Repudiation Uses	
4. SSL/TLS and HTTPS	**4 + 6**
4.1 TLS Handshake Process	
4.2 Certificate Validation	
4.3 Secure Communication in Web Browsing	
5. Public Key Infrastructure (PKI)	**4 + 6**
5.1 Certificate Authorities (CA)	
5.2 Key Pair and Certificate Management	
5.3 Revocation (CRL, OCSP)	
6. Cryptography in Everyday Applications	**6 + 9**
6.1 Secure Messaging (WhatsApp, Signal)	
6.2 Encrypted Storage & Backups	
6.3 Authentication Systems (2FA, Password Hashing)	
7. Cryptography Practical Exercises	**6 + 9**
7.1 Encrypting/Decrypting Data (OpenSSL Tools)	
7.2 Creating & Verifying Hashes	
7.3 Generating Keys and Certificates	

Teaching Methodology:

- Lectures
- Mathematical concept workshops
- Practical exercises with tools like OpenSSL
- Case studies

Recommended Books:

- "Everyday Cryptography" by Keith Martin. (Commonly used: 2nd Edition).
- "Applied Cryptography" by Bruce Schneier. (Commonly used: 20th Anniversary Edition).

LIST OF PRACTICALS

1. Practical implementation of Caesar and Vigenère ciphers.
2. Encrypting and decrypting data with AES (Symmetric).
3. Asymmetric key generation using RSA.
4. Elliptic Curve Cryptography (ECC) application.
5. Generating and verifying SHA-256 hashes.
6. MD5 hash collisions and properties.
7. Digital Signature creation and verification.
8. Managing the SSL/TLS handshake process.
9. Validating digital certificates.
10. HTTPS configuration for web browsing.
11. Setting up a Certificate Authority (CA).
12. Key Pair management and revocation (CRL/OCSP).
13. Secure Messaging simulations (WhatsApp/Signal protocols).
14. Encrypted storage and backup labs.
15. Password hashing and 2FA implementation.
16. Using OpenSSL for advanced crypto operations.

COURSE CODE: **CS-105**
COURSE TITLE: **Application Security**

T	P	C
1	3	2

Semester: 1st
Pre-requisite: Basic understanding of programming concepts, databases, and operating system fundamentals as covered in SSC and HSC Computer Science.
Credit Hours: 2

This course covers secure software development, emphasizing the OWASP Top 10 vulnerabilities, web and mobile application security, and fundamental secure coding practices. Students gain hands-on experience in identifying, testing, and mitigating common application security risks.

Course Objectives:

- Understand the Secure Software Development Lifecycle (SDLC)
- Identify and explain the OWASP Top 10 web vulnerabilities
- Perform basic testing for SQL Injection, XSS, and CSRF
- Recognize mobile application security challenges
- Apply fundamental secure coding principles

COURSE DURATION:

- Theory: 16 hours
- Practical / Lab: 48 hours

Learning Outcomes:

- List and describe the OWASP Top 10 risks
- Use basic tools to identify simple SQL Injection and XSS flaws
- Propose mitigations for common application vulnerabilities
- Differentiate between web and mobile app security concerns
- Write code snippets that avoid common security pitfalls

COURSE OUTLINE

Contents	Hours
1. Secure Software Development Lifecycle (SDLC)	**2 + 6**
1.1 Security Requirements & Planning	
1.2 Secure Design & Threat Modeling	
1.3 Secure Testing & Deployment	
2. Common Vulnerabilities (OWASP Top 10)	**2 + 6**
2.1 Injection Attacks	
2.2 Broken Authentication & Access Control	
2.3 Security Misconfigurations	
3. Web Application Security (SQL Injection, XSS, CSRF)	**2 + 6**
3.1 Identifying & Preventing SQL Injection	
3.2 Detecting Cross-Site Scripting (XSS)	
3.3 Mitigating Cross-Site Request Forgery (CSRF)	
4. Mobile App Security	**2 + 6**
4.1 Secure Data Storage & Permissions	
4.2 Mobile API Security	
4.3 Reverse Engineering Risks	
5. Secure Coding Practices	**2 + 6**
5.1 Input Validation & Sanitization	
5.2 Error Handling & Logging	
5.3 Avoiding Hardcoded Secrets	
6. Introduction to Static/Dynamic Analysis	**2 + 9**
6.1 Static Code Analysis Tools & Techniques	
6.2 Dynamic Application Testing	
6.3 Identifying and Fixing Detected Issues	
7. Vulnerability Scanning Lab	**4 + 9**
7.1 Setting Up Scanning Tools (e.g., Burp, Nessus)	
7.2 Running Vulnerability Assessments	
7.3 Analyzing Scan Reports & Mitigation Steps	

Teaching Methodology:

- Lectures
- Code review workshops
- Hands-on labs with vulnerable applications (e.g., OWASP WebGoat)
- Demonstrations

Recommended Books:

- "OWASP Testing Guide" by OW Foundation. (Commonly used: Version 4.2 or 5).

LIST OF PRACTICALS

1. Threat Modeling for software design.
2. Identifying SQL Injection vulnerabilities.
3. Practicing Cross-Site Scripting (XSS) detection.
4. Mitigating Cross-Site Request Forgery (CSRF).
5. Testing for Broken Authentication.
6. Analyzing Access Control flaws.
7. Security misconfiguration assessment.
8. Secure Input Validation and Sanitization coding.
9. Implementing secure Error Handling and Logging.
10. Avoiding hardcoded secrets in source code.
11. Mobile API security testing.
12. Reverse Engineering risks in mobile apps.
13. Static Code Analysis (SAST) tool usage.
14. Dynamic Application Security Testing (DAST).
15. Vulnerability scanning with Burp Suite.
16. Vulnerability scanning with Nessus.

COURSE CODE: **CS-106**
COURSE TITLE: **Functional English**

T	P	C
2	0	2

Semester: 1st
Pre-requisite: Basic proficiency in English reading, writing, and comprehension skills at the secondary school level.
Credit Hours: 2

This course develops technical communication skills for IT and cybersecurity professionals, focusing on clear report writing, effective presentations, and professional documentation. Students will practice incident reporting, technical vocabulary, and professional communication in both written and oral formats.

Course Objectives:

- Improve technical writing for reports and documentation
- Build vocabulary specific to IT and cybersecurity
- Develop skills for presenting technical information clearly
- Practice writing clear and concise incident reports
- Participate in professional discussions and meetings

COURSE DURATION:

- Theory: 32 hours

Learning Outcomes:

- Write effective technical reports and documentation
- Deliver clear and confident presentations on technical topics
- Articulate cybersecurity concepts in written and oral form
- Write a standard incident response report
- Communicate professionally in a team environment

COURSE OUTLINE

Contents	Hours
1. Technical Writing Essentials	**4**
1.1 Clarity and Conciseness in Documentation	
1.2 Structuring Reports and Manuals	
1.3 Using Visuals and Formatting Effectively	
2. IT and Cybersecurity Vocabulary	**4**
2.1 Key Terminologies (Malware, Encryption, Firewall)	
2.2 Acronyms and Abbreviations (IDS, VPN, PKI)	
2.3 Contextual Usage in Reports and Communication	
3. Writing Incident Reports and Documentation	**4**
3.1 Recording Facts Accurately and Objectively	
3.2 Structuring Incident Reports (What, When, How, Impact)	
3.3 Recommendations and Follow-Up Actions	
4. Email Etiquette for Professionals	**4**
4.1 Clear Subject Lines and Professional Tone	
4.2 Structuring Messages for Readability	
4.3 Handling Sensitive or Confidential Information	
5. Oral Communication and Presentation Skills	**4**
5.1 Effective Public Speaking Techniques	
5.2 Using Visual Aids and Slides	
5.3 Engaging the Audience and Handling Questions	
6. Interview Practice for Tech Roles	**6**
6.1 Common Technical and Behavioral Questions	
6.2 Presenting Skills and Experience Clearly	
6.3 Practicing Problem-Solving and Case Scenarios	
7. Writing a Security Policy Brief	**6**
7.1 Purpose and Audience of Policy Briefs	
7.2 Summarizing Security Risks and Recommendations	
7.3 Formatting and Professional Presentation	

Teaching Methodology:

- Interactive sessions
- Writing workshops
- Role-play and presentations
- Peer reviews

Recommended Books:

- "Technical Writing for IT Professionals" by Ellen Lange.
- "Writing for Computer Science" by Justin Zobel.

SEMESTER II

COURSE CODE: **CS-201**

COURSE TITLE: **Identity and Access Management (IAM)**

T	P	C
1	3	2

Semester: 2nd

Pre-requisite: Basic understanding of computer systems, databases, networking concepts, and user account management fundamentals.

Credit Hours: 2

This course covers the fundamentals of Identity and Access Management (IAM), including authentication, authorization, RBAC, SSO, and privileged access management. Students will gain practical skills in implementing secure access controls, multi-factor authentication, and user lifecycle management.

Course Objectives:

- Differentiate between authentication, authorization, and accounting
- Implement and manage strong password policies and MFA
- Design and apply Role-Based Access Control (RBAC) models
- Understand Identity Providers (IdP) and Single Sign-On (SSO)
- Introduction to Privileged Access Management (PAM)

COURSE DURATION:

- Theory: 16 hours
- Practical / Lab: 48 hours

Learning Outcomes:

- Design a basic RBAC model for an organization
- Configure a multi-factor authentication solution
- Explain the flow of an SSO transaction
- Manage user lifecycles (provisioning, de-provisioning)
- Justify the need for privileged access management

COURSE OUTLINE

Contents	Hours
1. Authentication vs. Authorization	**2 + 6**
1.1 Difference Between Authentication and Authorization	
1.2 Common Authentication Methods (Passwords, Biometrics)	
1.3 Access Control Mechanisms	
2. Password Policies and Multi-Factor Authentication (MFA)	**2 + 6**
2.1 Strong Password Guidelines and Best Practices	
2.2 Implementing Multi-Factor Authentication	
2.3 Password Management Tools and Techniques	
3. Role-Based Access Control (RBAC)	**2 + 6**
3.1 Defining Roles and Permissions	
3.2 Assigning Users to Roles	
3.3 Monitoring and Reviewing Role Access	
4. Identity Providers (IdP) and Single Sign-On (SSO)	**2 + 6**
4.1 Understanding Identity Providers	
4.2 Implementing Single Sign-On Solutions	
4.3 Security Benefits and Challenges	
5. Privileged Access Management (PAM)	**2 + 6**
5.1 Managing Administrative and High-Privilege Accounts	
5.2 Tools for PAM Implementation	
5.3 Monitoring and Auditing Privileged Access	
6. User Lifecycle Management	**2 + 9**
6.1 User Provisioning and Onboarding	
6.2 Role Changes and Access Modification	
6.3 Offboarding and Access Revocation	
7. IAM Implementation Project	**4 + 9**
7.1 Planning and Designing IAM Solutions	
7.2 Deployment and Configuration Steps	
7.3 Testing, Monitoring, and Optimization	

Teaching Methodology:

- Lectures
- Lab simulations (e.g., configuring Active Directory/MFA)
- Case studies
- Group projects

Recommended Books:

- "Identity and Access Management" by Bill Mann.
- "Microsoft Azure AD Documentation" (Technical Resource).

COURSE CODE: **CS-202**

COURSE TITLE: **Security Operations & Incident Response**

T	P	C
1	3	2

Semester: 2nd

Pre-requisite: Basic knowledge of operating systems, networking fundamentals, and introductory cybersecurity concepts.

Credit Hours: 2

This course introduces Security Operations Center (SOC) practices, including SIEM monitoring, incident response, digital forensics, and basic malware analysis. Students will gain hands-on experience in detecting, investigating, and documenting security incidents within a controlled environment.

Course Objectives:

- Understand the role and functions of a SOC
- Use Security Information and Event Management (SIEM) for monitoring
- Follow a structured incident response lifecycle
- Perform basic digital forensic tasks on a system
- Understand the fundamentals of malware analysis

COURSE DURATION:

- Theory: 16 hours
- Practical / Lab: 48 hours

Learning Outcomes:

- Monitor a simulated SIEM dashboard for alerts
- Document an incident using a standard response plan
- Perform basic forensic imaging and data collection
- Analyze a system for indicators of compromise (IOCs)
- Write a basic incident report

COURSE OUTLINE

Contents	Hours
1. Security Information and Event Management (SIEM)	**2 + 6**
1.1 Collecting and Aggregating Security Logs	
1.2 Real-Time Monitoring and Alerting	
1.3 Correlation and Reporting for Threat Detection	
2. SOC Operations and Monitoring	**2 + 6**
2.1 Roles and Responsibilities in a SOC	
2.2 Continuous Monitoring of Networks and Systems	
2.3 Escalation Procedures and Reporting	
3. Incident Detection and Response Lifecycle	**2 + 6**
3.1 Identifying and Prioritizing Security Incidents	
3.2 Containment, Eradication, and Recovery Steps	
3.3 Post-Incident Analysis and Lessons Learned	
4. Digital Forensics Basics (Imaging, Evidence Handling)	**2 + 6**
4.1 Creating Forensic Images of Systems and Drives	
4.2 Preserving Evidence Integrity	
4.3 Legal and Procedural Considerations	
5. Malware Analysis Fundamentals	**2 + 6**
5.1 Static and Dynamic Analysis Techniques	
5.2 Identifying Malware Behavior and Signatures	
5.3 Tools for Malware Investigation	
6. Threat Hunting Introduction	**2 + 9**
6.1 Proactive Search for Threats in Networks	
6.2 Using Indicators of Compromise (IOCs)	
6.3 Documenting and Reporting Threat Findings	
7. Incident Response Tabletop Exercise	**4 + 9**
7.1 Simulating Security Incidents	
7.2 Team Coordination and Decision-Making	
7.3 Reviewing Actions and Improving Response Plans	

Teaching Methodology:

- Lectures
- Hands-on labs with SIEM tools (e.g., Splunk Free)
- Simulation exercises (tabletops)
- Forensic practicals on VM images

Recommended Books:

- "Incident Response & Computer Forensics" by Kevin Mandia. (Commonly used: 3rd Edition).
- "The Essential Guide to SIEM" by Splunk.

LIST OF PRACTICALS

1. Configuring Authentication vs. Authorization.
2. Implementing Multi-Factor Authentication (MFA).
3. Designing Role-Based Access Control (RBAC) models.
4. Defining user roles and permission sets.
5. Active Directory user management.
6. Implementing Single Sign-On (SSO) solutions.
7. Identity Provider (IdP) integration.
8. Privileged Access Management (PAM) implementation.
9. Monitoring and auditing privileged accounts.
10. User lifecycle: Provisioning and Onboarding.
11. User lifecycle: Role changes and modifications.
12. User lifecycle: Offboarding and Revocation.
13. Strong password policy enforcement.
14. Biometric authentication labs.
15. Access Control Mechanism reviews.
16. IAM solution testing and optimization.

COURSE CODE: **CS-203**

COURSE TITLE: **Risk Management and Compliance**

T	P	C
2	0	2

Semester: 2nd

Pre-requisite: Basic understanding of computer systems, networking fundamentals, operating systems, and the software development life cycle (SDLC) gained from Matriculation / Intermediate Computer Science studies.

Credit Hours: 2

This course covers cybersecurity risk management, business continuity, disaster recovery, and compliance with major standards like ISO 27001, NIST, GDPR, and PCI-DSS. Students will learn to assess risks, develop BCP/DRP plans, and ensure alignment with regulatory and business requirements.

Course Objectives:

- Conduct a basic cybersecurity risk assessment
- Develop a Business Impact Analysis (BIA) and Business Continuity Plan (BCP)
- Create a Disaster Recovery Plan (DRP)
- Understand key provisions of major compliance standards (ISO 27001, NIST, GDPR, PCI-DSS)
- Map controls to compliance requirements

COURSE DURATION:

- Theory: 32 hours

Learning Outcomes:

- Identify, assess, and prioritize IT risks
- Develop core components of a BCP and DRP
- Differentiate between various compliance frameworks
- Perform a gap analysis against a simple control set
- Explain the importance of compliance to business goals

COURSE OUTLINE

Contents	Hours
1. Risk Assessment and Management	**4**
1.1 Identifying and Evaluating Risks	
1.2 Risk Mitigation Strategies	
1.3 Risk Monitoring and Review	
2. Business Impact Analysis (BIA)	**4**
2.1 Identifying Critical Business Functions	
2.2 Assessing Financial and Operational Impacts	
2.3 Prioritizing Recovery Efforts	
3. Business Continuity Planning (BCP)	**4**
3.1 Developing Continuity Strategies	
3.2 Resource and Staff Allocation	
3.3 Testing and Updating BCP Plans	
4. Disaster Recovery Planning (DRP)	**4**
4.1 Backup and Recovery Solutions	
4.2 Recovery Time Objective (RTO) and Recovery Point Objective (RPO)	
4.3 DRP Testing and Validation	
5. Compliance Standards: ISO 27001, NIST CSF	**4**
5.1 Understanding ISO 27001 Requirements	
5.2 Implementing NIST Cybersecurity Framework Controls	
5.3 Continuous Compliance Monitoring	
6. Data Privacy Regulations: GDPR, PDPL	**6**
6.1 Personal Data Protection Principles	
6.2 Rights of Data Subjects	
6.3 Compliance and Enforcement Measures	
7. Industry Standards: PCI-DSS, HIPAA	**6**
7.1 Payment Card Data Security Requirements	
7.2 Health Information Security Requirements	
7.3 Audits, Reporting, and Penalties	

Teaching Methodology:

- Lectures
- Case studies of real breaches and compliance failures
- Group workshops to develop BCP/DRP documents
- Research assignments

Recommended Books:

- "Risk Management for Cybersecurity" by Gregory Allen.
- "COBIT 5" (Framework) by IT Governance Institute.

LIST OF PRACTICALS

1. Collecting and aggregating security logs in SIEM.
2. Monitoring SIEM dashboards (e.g., Splunk).
3. Real-time alerting and threat detection correlation.
4. Escalation procedures and SOC reporting.
5. Incident containment and eradication steps.
6. Post-incident analysis and lessons learned.
7. Creating forensic images of drives.
8. Evidence handling and integrity preservation.
9. Static malware analysis techniques.
10. Dynamic malware analysis (Sandboxing).
11. Identifying Indicators of Compromise (IOCs).
12. Proactive Threat Hunting in networks.
13. Documenting incident reports.
14. Incident Response Tabletop Exercises.
15. Forensic practicals on VM images.
16. Team coordination and decision-making simulations.

COURSE CODE: **CS-204**

COURSE TITLE: **Ethical Hacking and Penetration Testing**

T	P	C
2	3	3

Semester: 2nd

Pre-requisite: Fundamental knowledge of computer systems, networking concepts, operating systems, and programming basics (especially C/C++) acquired through Matriculation / Intermediate Computer Science studies.

Credit Hours: 3

This course introduces the fundamentals of ethical hacking and penetration testing, covering legal considerations, reconnaissance, vulnerability scanning, and exploitation techniques. Students will work hands-on with industry tools to identify security weaknesses and produce professional penetration testing reports.

Course Objectives:

- Understand the ethics and legal aspects of penetration testing
- Follow a structured penetration testing methodology (e.g., PTES)
- Use reconnaissance and scanning tools (e.g., Nmap)
- Utilize exploitation frameworks (e.g., Metasploit)
- Write a professional penetration testing report

COURSE DURATION:

- Theory: 32 hours
- Practical / Lab: 48 hours

Learning Outcomes:

- Perform passive and active reconnaissance
- Conduct network and vulnerability scanning
- Execute basic exploits against known vulnerabilities
- Document findings and suggest remediation steps
- Write a comprehensive penetration test report

COURSE OUTLINE

Contents	Hours
1. Basics of Ethical Hacking and Legal Frameworks	**4 + 6**
1.1 Ethical Hacking Concepts and Objectives	
1.2 Legal Considerations and Authorization	
1.3 Types of Assessments and Engagement Rules	
2. Penetration Testing Execution Standard (PTES) Phases	**4 + 6**
2.1 Pre-Engagement Interactions	
2.2 Intelligence Gathering and Vulnerability Analysis	
2.3 Exploitation, Post-Exploitation, and Reporting	
3. Reconnaissance and Scanning Tools (Nmap, Nessus)	**4 + 6**
3.1 Network Discovery and Port Scanning	
3.2 Vulnerability Scanning and Assessment	
3.3 Interpreting and Validating Scan Results	
4. Exploitation Tools (Metasploit, Burp Suite)	**4 + 6**
4.1 Exploit Development and Execution	
4.2 Web Application Testing with Burp Suite	
4.3 Payloads, Sessions, and Advanced Techniques	
5. Post-Exploitation Techniques	**4 + 6**
5.1 Privilege Escalation and Lateral Movement	
5.2 Persistence Mechanisms	
5.3 Data Extraction and Cleanup	
6. Vulnerability Assessment vs. Penetration Testing	**6 + 9**
6.1 Purpose and Scope Differences	
6.2 Methodology and Tools	
6.3 Reporting and Risk Prioritization	
7. Report Writing and Remediation	**6 + 9**
7.1 Documenting Findings and Evidence	
7.2 Communicating Technical Issues to Stakeholders	
7.3 Recommending Fixes and Security Improvements	

Teaching Methodology:

- Lectures
- Extensive hands-on labs in a virtual lab environment (e.g., Kali Linux)
- Capture The Flag (CTF) exercises
- Project-based learning

Recommended Books:

- "The Basics of Hacking and Penetration Testing" by Patrick Engebretson. (Commonly used: 2nd Edition).
- "Penetration Testing" by Georgia Weidman.

LIST OF PRACTICALS

1. Passive reconnaissance and OSINT gathering.
2. Active reconnaissance using Nmap.
3. Network discovery and port scanning.
4. Vulnerability scanning with Nessus.
5. Interpreting and validating scan results.
6. Exploitation with Metasploit Framework.
7. Web application testing with Burp Suite.
8. Generating and executing payloads.
9. Privilege Escalation on Linux/Windows.
10. Lateral Movement within a network.
11. Establishing persistence mechanisms.
12. Data extraction and cleanup procedures.
13. Capture The Flag (CTF) challenges.
14. Writing a professional penetration test report.
15. Communicating technical issues to stakeholders.
16. Recommending security fixes and remediations.

COURSE CODE: **CS-205** **T P C**

COURSE TITLE: **Emerging Trends in Cybersecurity** **1 3 2**

Semester: 2nd

Pre-requisite: Basic understanding of computer systems, networking fundamentals, digital logic, and general cybersecurity concepts gained from secondary / intermediate-level computer science studies.

Credit Hours: 2

This course explores emerging cybersecurity domains, including AI/ML for threat detection, cloud security, DevSecOps, IoT protection, and blockchain vulnerabilities. Students gain practical knowledge of modern security practices and hands-on experience with cloud platforms, automated security, and next-generation threat mitigation.

Course Objectives:

- Evaluate the use of AI and Machine Learning in cybersecurity defense and offense
- Identify key security responsibilities and tools in cloud platforms (IaaS, PaaS, SaaS)
- Understand the principles and practices of DevSecOps
- Analyze the security architecture and vulnerabilities of IoT devices
- Explore the security implications of blockchain and decentralized systems

COURSE DURATION:

- Theory: 16 hours
- Practical / Lab: 48 hours

Learning Outcomes:

- Discuss the pros and cons of using AI for threat detection
- Configure a basic security group in a cloud platform
- Integrate a simple security scan into a CI/CD pipeline
- Identify common attack vectors for IoT devices
- Explain how blockchain provides integrity and its potential security issues

COURSE OUTLINE

Contents	Hours
1. AI and Machine Learning in Cybersecurity	**2 + 6**
1.1 Threat Detection Using AI/ML	
1.2 Behavioral Analytics and Anomaly Detection	
1.3 Automation of Security Operations	
2. Cloud Security (Shared Responsibility Model, AWS/Azure/GCP Security)	**2 + 6**
2.1 Understanding the Shared Responsibility Model	
2.2 Cloud Security Best Practices per Provider	
2.3 Data Protection, Identity, and Access Management in Cloud	
3. DevSecOps: Integrating Security into DevOps	**2 + 6**
3.1 Shift-Left Security Practices	
3.2 Automated Security Testing in CI/CD	
3.3 Secure Code Review and Monitoring	
4. IoT Security Challenges and Protocols	**2 + 6**
4.1 IoT Device Vulnerabilities and Risks	
4.2 Secure Communication Protocols	
4.3 Monitoring and Firmware Update Practices	
5. Blockchain Security & Cryptocurrency Threats	**2 + 6**
5.1 Blockchain Security Principles	
5.2 Smart Contract Vulnerabilities	
5.3 Cryptocurrency Fraud and Attack Types	
6. Zero Trust Architecture	**2 + 6**
6.1 Core Principles of Zero Trust	
6.2 Identity and Device Verification	
6.3 Micro-Segmentation and Network Access Control	
7. The Future Cybersecurity Landscape	**4 + 12**
7.1 Emerging Threats and Attack Vectors	
7.2 Advancements in Security Technologies	
7.3 Preparing for Next-Generation Cybersecurity Challenges	

Teaching Methodology:

- Lectures
- Research presentations
- Cloud platform free-tier labs
- Discussion forums on emerging threats

Recommended Books:

- "Security for Cloud Native Applications" by O'Reilly (Multiple authors/Whitepapers).
- "Whitepapers" by AWS, Azure, and GCP

LIST OF PRACTICALS

1. AI/ML for threat detection simulations.
2. Behavioral analytics and anomaly detection.
3. Automation of security operations.
4. Configuring Cloud Security Groups (AWS/Azure).
5. Shared Responsibility Model implementation.
6. Cloud Data Protection and IAM.
7. Shift-Left security practices in development.
8. Integrating security scans into CI/CD pipelines.
9. Automated Secure Code Review.
10. IoT device vulnerability assessment.
11. Secure IoT communication protocols.
12. IoT firmware update and monitoring practices.
13. Blockchain security principle analysis.
14. Smart Contract vulnerability testing.
15. Zero Trust Architecture: Identity verification.
16. Micro-segmentation and network access control.

COURSE CODE: **CS-206**
COURSE TITLE: **Capstone Project**

T	P	C
0	3	1

Semester: 2nd
Credit Hours: 1

This capstone course enables students to apply their cumulative cybersecurity knowledge in a comprehensive project, managing all phases from planning to execution. Students will demonstrate proficiency with tools, techniques, and professional documentation while presenting and defending their findings.

Course Objectives:

- Apply comprehensive cybersecurity knowledge to a complex project
- Manage a cybersecurity project from planning to execution and reporting
- Demonstrate proficiency with multiple security tools and techniques
- Develop professional-level documentation and presentation skills
- Solve unforeseen challenges and adapt methodologies as needed

COURSE DURATION:

- Practical / Lab: 48 hours

Learning Outcomes:

- Plan and execute a multi-faceted cybersecurity project
- Synthesize information from various domains (network, app, system)
- Produce a professional report and presentation on findings
- Defend methodology and conclusions in an oral presentation
- Demonstrate readiness for entry-level cybersecurity roles

COURSE OUTLINE

Contents	Hours
1. Project Scoping and Proposal Writing	**6**
1.1 Defining Project Objectives and Deliverables	
1.2 Identifying Scope, Constraints, and Stakeholders	
1.3 Writing a Clear and Structured Proposal	
2. Project Management for Security	**6**
2.1 Planning and Scheduling Tasks	
2.2 Resource Allocation and Risk Management	
2.3 Tracking Progress and Adjusting Plans	
3. Execution of Technical Work (e.g., Pen Test, Policy Creation, IR Simulation)	**6**
3.1 Performing Security Assessments or Implementations	
3.2 Following Standard Operating Procedures and Best Practices	
3.3 Documenting Actions and Maintaining Evidence	
4. Data Analysis and Synthesis	**6**
4.1 Collecting and Organizing Project Data	
4.2 Analyzing Findings and Identifying Patterns	
4.3 Synthesizing Results into Actionable Insights	
5. Report Writing and Executive Summary	**6**
5.1 Structuring Technical Reports Clearly	
5.2 Writing Concise Executive Summaries	
5.3 Including Recommendations and Supporting Evidence	
6. Final Presentation Preparation	**9**
6.1 Designing Clear and Engaging Slides	
6.2 Rehearsing Delivery and Timing	
6.3 Anticipating Questions and Preparing Answers	
7. Project Demonstration and Defense	**9**
7.1 Presenting Technical Work to Stakeholders	
7.2 Demonstrating Key Findings and Solutions	
7.3 Responding to Feedback and Questions	

Teaching Methodology:

- Project-based learning
- Mentor meetings and guidance
- Independent research and work
- Peer reviews

Recommended Books:

- N/A (Guided by previous course materials and mentor advice)
