SAVITRIBAI PHULE PUNE UNIVERSITY

(FORMERLY UNIVERSITY OF PUNE)

Four Year Degree Program in

Bachelor of Science (B.Sc)

with

Major: Cyber and Digital Science

(Faculty of Science & Technology)

Syllabi for

(For colleges Affiliated to Savitribai Phule Pune University)

Choice Based Credit System (CBCS) Syllabus

Under National Education Policy (NEP)

To be implemented from Academic Year 2025-26

Level:- 5.0 (Second Year) Sem:-III

Course Type	Course Code	Course Title	Credits		Teaching Scheme Hr/Week		Evaluation Scheme and Max Marks		
			TH	PR	TH	PR	CE	EE	Total
Major Core (4+2)	CDS-201-MJ	Ethical Hacking-I	2		2		15	35	50
	CDS-202-MJ	Cyber Ethics, Cyber Law & Cyber Policies	2		2		15	35	50
	CDS-203-MJP	Practical based on CDS201MJ		2		4	15	35	50
VSC(2)	CDS-221-VSC-P	Data Structure using Python		2		4	15	35	50
IKS	IKS-200-T	Computations in Ancient India	2		2		15	35	50
FP/OJT/CEP(2)	CDS-231-FP	Mini Project		2		4	15	35	50
Minor (2+2)	CDS-241-MN	Web Technology	2		2		15	35	50
	CDS-242-MNP	Practical based on CDS241MN		2		4	15	35	50
GE/OE(2)	OE-201-CDS-T OE-202-CDS-T OE-203-CDS-T	AI for Everyone I / Web design I / Digital Marketing I	2		2		15	35	50
AEC(2)	AEC-201-T	From University Basket	2		2		15	35	50
CC(2)	CC-201-T	From University Basket	2		2		15	35	50
Total			14	08	14	16			550

Level:- 5.0 (Second Year) Sem:-IV

Course Type	Course Code	Course Title	Credits		Teaching Scheme Hr/Week		Evaluation Scheme and Max Marks		
			TH	PR	TH	PR	CE	EE	Total
Major Core (4+2)	CDS-251-MJ	Ethical Hacking-II	2		2		15	35	50
	CDS-252-MJ	Advance Network Security	2		2		15	35	50
	CDS-253-MJP	Practical based on CDS251MJ		2		4	15	35	50
VSC(2)	CDS-271-VSC-P	Database management system		2		4	15	35	50
FP/OJT/ CEP(2)	CDS-281-FP	Mini Project		2		4	15	35	50
Minor (2+2)	CDS-291-MN	Advanced Web Technology	2		2		15	35	50
	CDS-292-MNP	Practical based on CDS291MN		2		4	15	35	50
GE/OE(2)	OE-251-CDS-T OE-252-CDS-T OE-253-CDS-T	AI for Everyone II / Web design II / Digital Marketing II	2		2		15	35	50
SEC(2)	SEC251CDS-T	Principals of operating System	2		2		15	35	50
AEC(2)	AEC-251-T	From University Basket	2		2		15	35	50
CC(2)	CC-251-T	From University Basket	2		2		15	35	50
Total			14	8	14	16			550

Detail Syllabus

B.Sc. Cyber & Digital Science

Sem III & IV

Savitribai Phule Pune University
As per NEP
S.Y.B.Sc. (Cyber and Digital Science)
CDS201MJ
Subject : Ethical Hacking - I

Teaching Scheme 2 Hours / week	**No. of Credit:** 02	**Examination Scheme** CA :15 marks UA: 35 marks

Prerequisites:
1. Fundamentals of Cyber Security
2. Fundamentals of OSI Model and TCP/IP Suite
3. Fundamentals of GNU/Linux Operating System

Course Objectives
1. Understand the fundamentals of Ethical Hacking and cyber security.
2. Learn reconnaissance and OSINT techniques for information gathering.
3. Perform network scanning, enumeration, and exploitation effectively.
4. Conduct vulnerability assessments and system hacking.
5. Explore web application security and penetration testing.

Course Outcomes: On completion of the course, student will be able to
CO1. Explain ethical hacking concepts and hacker types.
CO 2. Perform reconnaissance and OSINT techniques.
CO 3. Conduct network scanning and exploitation.
CO 4. Analyze system vulnerabilities and hacking methods.
CO 5. Identify and exploit web application vulnerabilities.

Course Contents

Unit 1	**Introduction to Ethical Hacking**	**4 hours**	**CO1**

1.1 What is Ethical Hacking?
1.2 Confidentiality Integrity Availability (C.I.A) Triad
1.3 Cyber security Threats & Attack Vectors
1.4 Types of Hackers
1.5 Ethical Hacking vs. Cyber crime
1.6 Ethical Hacking Process

Unit 2	**Foot printing, Reconnaissance & Open-Source Intelligence (OSINT)**	**4 Hours**	**CO 2**

2.1 Introduction to Reconnaissance
2.2 Passive vs. Active Reconnaissance
2.3 Introduction To Open Source Intelligence (OSINT)
2.4 Information Gathering/ Foot printing Techniques:
- 2.4.1 WHOIS Lookup, Reverse WHOIS
- 2.4.2 DNS Enumeration (Ns lookup, Dig)
- 2.4.3 Social Media Intelligence Gathering
- 2.4.4 Shodan & Censys for Internet-wide Scanning

Unit 3	Network Scanning, Enumeration & Exploitation	6 Hours	CO 3

3.1 Understanding Network Scanning
(TCP, UDP, SYN, ACK)
3.2 Using Nmap & Advanced Nmap Scripting Engine
3.3 OS Fingerprinting & Service Detection
3.4 Enumerating Network Services
(NetBIOS, SNMP, SMB)
3.5 Identifying Open Ports and Vulnerable Services
3.6 Evading Intrusion Detection Systems (IDS) & Firewalls
3.7 Network Traffic Analysis (Wireshark)
3.8 ARP Spoofing & MITM Attacks

Unit 4	Vulnerability Assessment & System Hacking	8 Hours	CO 4

4.1 Introduction to Vulnerability Scanning
4.2 Automated vs. Manual Vulnerability Analysis
4.3 Vulnerability Scanning Tools:

4.3.1 Nessus
4.3.2 OpenVAS

4.3.3 Nikto (for Web Servers)
4.4 Password Cracking Techniques:
4.4.1 Hash Cracking (John the Ripper, Hashcat)
4.4.2 Windows Password Extraction/ reset
4.4.3 Brute Force & Dictionary Attacks
4.5 Privilege Escalation Techniques(Windows & Linux)

Unit 5	Web Application Hacking & Exploitation	8 Hours	CO 5

5.1 Introduction to Web Vulnerabilities (OWASP Top 10)
5.2 SQL Injection (SQLi) - Manual & Automated Exploitation
5.3 Cross-Site Scripting (XSS) - Reflected, Stored & DOM-Based
5.4 Cross-Site Request Forgery (CSRF)
5.5 Remote File Inclusion (RFI) & Local File Inclusion (LFI)
5.6 Exploiting Content Management Systems (CMS)
5.7 Web Shell Injection & Command Execution
5.8 Bypassing Web Application Firewalls (WAF)

Reference Books:

1. The Basics of Hacking and Penetration Testing – Patrick Engebretson
2. Hacking: The Art of Exploitation (2nd Edition) – Jon Erickson
3. CEH Certified Ethical Hacker All-in-One Exam Guide – Matt Walker
4. Penetration Testing: A Hands-On Introduction to Hacking – Georgia Weidman

Savitribai Phule Pune University
As per NEP
S.Y.B.Sc. (Cyber and Digital Science)
CDS202MJ
Title: Cyber Ethics , Cyber Law & Cyber Policies

Teaching Scheme:	**No. of Credits: 02**	**Examination Scheme**
2 Hours / week		CA :15 marks UA: 35 marks

Prerequisites:
1. Basic Knowledge of Cyber Security
2. Fundamental Understanding of Information Technology
3. Basic Knowledge of Cyber Laws & Regulations

Course Objectives
1. Understand the fundamentals of cyber ethics and their role in digital behavior.
2. Explore various types of cybercrimes and analyze their legal and ethical implications.
3. Examine intellectual property rights (IPR) in cyberspace and their impact on digital content.
4. Analyze data protection and privacy laws to understand their importance in safeguarding digital information.
5. Evaluate national and international cyber policies to understand governance mechanisms in cyberspace.
6. Investigate emerging cyber threats and assess their implications on legal, ethical, and policy frameworks

Course Outcomes: On completion of the course, student will be able to
CO1. Principles of cyber ethics and apply them to real-world digital scenario
CO2. Identify and categorize cybercrimes while understanding the legal actions
CO3. Assess the role of IPR in protecting digital assets and preventing online fraud.
CO4. Analyze cyber security policies and frameworks implemented by governments and organizations.
CO5. Implementation of Policies in governments and organizations .Evaluate emerging cyber threats and propose legal and ethical solutions to mitigate risks.

Course Contents

Chapter 1	**Introduction to Cyber Space and Cyber Ethics**	**4 hours**	**CO1**

1.1 Definition and characteristics of cyberspace
1.2 Introduction to Cybercrime
1.3 Need Cyber laws: The Indian Context
1.4 Cybercrime and Information Security
1.5 Understanding cyber ethics and its importance
1.6 Moral, ethical, and legal issues in cyberspace
1.7 Professional ethics in information technology

Chapter 2	**Cyber Crimes and Legal Framework**	**8 hours**	**CO2**

2.1 Cybercrimes, Classification and types of cybercrimes
Classifications of Cybercrimes:
(E-Mail Spoofing, Spamming, Cyber defamation, Internet Time Theft, Salami Attack/Salami Technique, Data Diddling, Forgery, Web Jacking, Newsgroup, Spam/Crimes, Industrial Spying/Industrial Espionage, Hacking, Online Frauds, Computer Sabotage, Email Bombing/Mail Bombs, Computer Network Intrusions, Password Sniffing, Credit Card Frauds, Identity Theft)

2.2 Legal perspectives: Indian and global scenarios
2.3 Overview of the Information Technology Act, 2000
2.4 Amendments and their implications
2.5 Role of law enforcement agencies in combating cybercrime
2.6 Introduction to IT governance framework: COBIT, ISO/IEC 27001/27002

Chapter 3	**Intellectual Property Rights in Cyberspace**	**4 hours**	**CO3**

3.1 Understanding intellectual property in the digital age
3.2 Copyrights, trademarks, and patents online
3.3 Legal challenges in protecting digital content
3.4 Digital rights management and fair use policies
3.5 Case studies on IP infringement and resolutions

Chapter 4	**Data Protection and Privacy Laws**	**6 hours**	**CO4**

4.1 Importance of data protection in the digital era
4.2 Global data protection regulations: GDPR, CCPA, etc.
4.3 Indian data protection laws and policies
4.4 Challenges in implementing privacy laws
4.5 Case studies on data breaches and legal actions
4.6 Cybercrime and Punishment
4.7 Social computing and the associated challenges for organizations, Protecting people's privacy in the organization
4.8 Organizational guidelines for Internet usage and safe computing guidelines and computer usage policy

Chapter 5	**Cyber Policies and Governance**	**8 hours**	**CO5**

5.1 National and international cyber policies
5.2 Role of government and private sectors in cyber governance
5.3 Cyber Security Policy and Domains of Cyber Security Policy
5.4 Cyber security strategies and frameworks
5.5 Public-private partnerships in cyber security
5.6 Analysis of existing cyber policies and their effectiveness
5.7 The future of cyber laws and policies
5.8 Preparing for future cyber challenges
5.9 Case studies on recent cyber incidents and lessons learned

Reference Book:

1. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives–Nina Godbole,Sunit Belapure,Wiley:April2011India Publications Released.
2. Thomas R. Peltier, "Information Security policies and procedures: A Practitioner's Reference", 2nd Edition Prentice Hall, 2004.
3. Principles of Information Security, -Michael E Whitman, HerbertJMattord,3rdEdition, 2011.

Savitribai Phule Pune University
S.Y.B.Sc.(Cyber and Digital Science) Sem - III
Subject Code: CDS 221 VSC-P
Subject: Data Structure Using Python

Teaching Scheme	No. of Credits	Examination Scheme
4 hours / week	2	CE: 15 Marks EE: 35 Marks

Prerequisites:
- Knowledge of Python programming.
- Basic knowledge of algorithms and problem solving

Course Objectives:
1. Develop problem-solving skills using data structures and algorithms in Python.
2. Analyze and implement Linear and Non-linear Data Structures.
3. Develop the ability to design and implement efficient algorithms using appropriate data structures.
4. Understand the role of Python's built-in data structures like lists, tuples, sets, and dictionaries.

Course Outcomes:
On completion of the course, students will be able to:
CO1: Understand fundamental data structures and their importance in problem-solving.
CO2: Implement, manipulate, apply and analyze linear and non-linear data structures.
CO3: Develop efficient algorithms by utilizing appropriate searching and sorting techniques.
CO4: Solve real-world problems by selecting and implementing suitable data structures in Python.
CO5: Understand several ways of solving the same problem.

Course Contents

Chapter 1	Introduction to Data Structure, Sorting and Searching techniques	6 hours

1.1 Introduction to Data Structure, Concept, Need, Types
1.2 Algorithm Analysis: Definition, Characteristics, Space complexity, Time complexity, Best, Worst, Average Case Analysis
1.3 Asymptotic Notation: Big O, Omega Ω, Theta Θ
1.4 Sorting algorithms with efficiency: Bubble sort, Insertion sort, Merge sort, Quick Sort, Selection Sort.
1.5 Searching techniques: Linear Search, Binary search

Chapter 2	Stack and Queue	6 hours

Stack:
2.1 Introduction
2.2 Representation: Using Arrays
2.3 Operations: init(), push(), pop(), isEmpty(), isFull(), peek()
2.4 Application: String reversal, infix to postfix, infix to prefix, postfix evaluation
Queue:
2.5 Introduction
2.6 Representation: Using Arrays
2.7 Operations: init(), Insert(), Delete(), isEmpty(), isFull()

2.8 Types of Queues: Linear Queue, Circular Queue, Priority Queue.

Chapter 3	**Linked List**	**6 hours**

3.1 Introduction
3.2 Dynamic implementation of Linked List
3.3 Types of Linked List: Singly, Doubly, Singly Circular, Doubly Circular
3.4 Operations on Linked List: create, display, insert, delete, reverse, search, sort, concatenate, merge
3.5 Representation of stack and queue using linked list

Chapter 4	**Tree**	**6 hours**

4.1 Concept and Terminologies
4.2 Types of Trees: Binary Tree, Binary Search Tree, Expression Tree
4.3 Representation Dynamic
4.4 Operations on BST: Create, Insert, Delete, Search
4.5 Tree traversals: preorder, inorder, postorder (recursive)
4.6 Counting leaf, non-leaf & total nodes

Chapter 5	**Graph**	**6 hours**

5.1 Concept and terminologies
5.2 Graph Representation: Adjacency matrix, Adjacency list
5.3 Graph traversal: Breadth First Search and Depth First Search

Reference Books:

- "Introduction to Computing and Problem-Solving Using Python" by E. Balagurusamy
- "Problem Solving in Data Structure & Algorithms using Python" by Hemant Jain
- "Problem Solving with Algorithms and Data Structures using Python" by Bradley N. Miller and David L. Ranum

Savitribai Phule Pune University

S.Y.B.Sc. (Cyber and Digital Science)

Subject Code: CDS 241 MN

Subject: Web Technology

Teaching Scheme:	**No. of Credits: 2**	**Examination Scheme:**
2 hours / week		CE: 15 Marks UE: 35 Marks

Course Objectives:

- To Learn Core-PHP, Server-Side Scripting Language
- To Learn PHP with File handling & Database handling
- To Design dynamic and interactive Web pages.

Course Outcomes: -

On completion of the course, student will be able to:

CO1: Understand how to design static web pages & basics of PHP
CO2: Understand the concepts of functions and strings in PHP
CO3: Understand Use and Implementation of an array
CO4: Understand File concepts & how to make database connectivity with PHP

Course Contents

Unit 1	**Introduction to Web, HTML, CSS & PHP**	**9 hours**	**CO1**

1.1 WWW, Web server and Web browser, HTTP basics [HTTP Request, HTTP Response]
1.2 Client – Server Architecture
1.3 HTML - Tags and Attributes
1.4 Form & Table - Designing / Processing , Tables
1.5 Introduction to stylesheet
1.6 CSS- Concept, Types of CSS & ways to use CSS
1.7 Use of id and class attributes
1.8 PHP - Introduction to PHP
1.9 How does PHP work?
1.10 Lexical structure
1.11 Basic Programs.

Unit 2	**Functions & String**	**9 hours**	**CO2**

2.1 Function - Definition and function call
2.2 Types of parameters - Default parameters , Variable parameters, Missing parameters
2.3 Variable function
2.4 Anonymous function
2.5 Printing functions
2.6 Encoding and escaping functions
2.7 Encrypting and Decrypting Data
2.8 Introduction to String
2.9 Types of strings
2.10 Comparing, manipulating and searching string.
2.11 Regular expressions

Unit 3	**Arrays**	**5 hours**	**CO3**

3.1 - Types of Arrays
3.2 Identifying elements of an array
3.3 Storing data in arrays
3.4 Extracting multiple values
3.5 Converting between arrays and variables
3.6 Traversing arrays
3.7 Sorting Array Operations

Unit 4	**Files and Database handling**	**7 hours**	**CO4**

4.1 Working with files and directories
4.2Operations on Files - Opening and Closing, Getting information about file, Read/write to file, Splitting name and path from file, Rename and delete files
4.3 Reading and writing characters in file
4.4 Reading entire file
4.5 Random access to file data
4.6 Getting information on file
4.7 Using PHP to access a database
4.8 Relational databases and SQL

Reference Books :

1. HTML & CSS: The Complete Reference, Fifth Edition Author: Thomas A. Powell First published: 01 Jan 2010.
2. Programming PHP By Rasmus Lerdorf and Kevin Tatroe, O'Reilly publication
3. Beginning PHP 5 , Wrox publication
4. PHP web sevices, Wrox publication
5. Mastering PHP , BPB Publication
6. PHP for Beginners, SPD publication

Ref. Links

1. www.php.net.in
2. www.W3schools.com

Savitribai Phule Pune University

S.Y.B.Sc. (Cyber and Digital Science)

Subject Code: CDS 231 FP

Subject: Mini Project

Teaching Scheme: Practicals per week: 1 (4 hrs)	**No. of Credits: 2**	**Examination Scheme:** CE: 15 Marks UE: 35 Marks

Course Objectives:

The course is designed to teach-

- To provide students with hands-on experience in applying theoretical knowledge from cyber and digital science to real-world problems through project development.
- To encourage innovation and creativity in designing secure and efficient digital systems or cyber security solutions.
- To develop skills in using modern tools, platforms, and techniques relevant to areas such as ethical hacking, digital forensics, network security, and data protection.
- To cultivate the ability to identify, analyze, and solve complex problems in cyber security and digital systems through systematic project work.
- To enhance teamwork, project management, and communication skills through collaborative project execution and documentation.
- To prepare students for professional practice or further research by integrating industry-relevant standards, tools, and best practices in the mini project.

Course Outcomes: -

On completion of the course, student will be able to:

CO1: Apply fundamental concepts of cyber security and digital technologies to identify and define real-world problems.
CO2: Design and develop a practical solution using appropriate cyber and digital tools, techniques, or frameworks.
CO3: Demonstrate the ability to work independently or in teams to plan, implement, and evaluate a digital or cyber solution.
CO4: Analyze and interpret data or system behavior to ensure security, functionality, and compliance with ethical standards.
CO5: Communicate technical information effectively through documentation, presentations, and demonstrations.
CO6: Exhibit awareness of current trends, legal aspects, and best practices in cyber and digital science relevant to the project undertaken.

Course Contents

Unit	Description
1,2, 3	Introduction and Project Definition, Topic selection, Abstract of a project
4,5	Requirement Analysis , System Design , Tool & Technology Setup
6, 7, 8	Module Development – I Start coding initial modules (e.g., input handling, authentication, data collection). Module Development – II Develop core cyber security functions (e.g., encryption, threat detection, scanning).(if applicable)
9,10, 11	Testing & Debugging - Phase **I** Unit test initial modules. , Fix bugs and ensure data integrity and secure input validation. Prepare document flow of events
12 – 14	Integration of Modules, Testing & Debugging - Phase II ,Perform system-level testing.
15	Result Analysis, Report writing and Presentation of work

Guidelines for Field Project:

- Field projects may be executed in partnership with a host company/organization. They must be approved by the department offering this course or by the FP committee of the college
- Project can be in any domain from Cyber security, Ethical Hacking, Digital Forensic , Virtualization, Forensic Investigation
- Field project can be done individually or as a group of maximum 3 students
- A progress report (after every 12-15 hours of field work) should be maintained for the duration of the course.
- The domain of the field project should be related to the major course
- Students or groups will be assigned to faculty members who will act as project guides or mentors throughout this process.
- Field project should involve study of any real-life situation with a focus on measurement and quantification of the phenomenon/process/system/problem in society.
- A report should be submitted by each student (hard/soft copy) at the end of this course
- All projects should be typed on A4 sheets, Font Size 12, Times New Roman, one and a half spacing. The project report shall have appropriate chapter scheme and be presented in minimum of 15 pages.
- Upon completion of the FP program, students must submit a completion certificate duly signed by the faculty guide / mentor.

Contents of the Report:

The contents of the report may include the following sections (can be modified as per the case under study):

1. Title page
2. Certificate by the Institute
3. Certificate by Mentor
4. Student's Declaration
5. Acknowledgement
6. Abstract (In 50-100 words)
7. Introduction: Background and rationale (2-5 pages), Objectives (3-5 Objectives)
8. Methodology: Study design, Data collection method, Data analysis techniques (if applicable)
9. Design of the case study
10. Conclusion
11. References
12. Appendices (if any)

Evaluation:

Mentors / Guides may use the following to evaluate a field project.

i. Field visit completion (if any)
ii. Objectives, Literature Review, Methodology
iii. Methods used for collecting requirements and data
iv. Data Analysis (if any)
v. Conclusion and Recommendations
vi. Attendance and interaction
vii. Overall Report quality
viii. Presentation and communication skills

Savitribai Phule Pune University
As per NEP
S.Y.B.Sc. (Cyber and Digital Science)
CDS251MJ
Subject: Ethical Hacking - II

Teaching Scheme 2 Hours / week	**No. of Credits:** 02	**Examination Scheme** CA :15 marks UA: 35 marks

Prerequisites:
1. Fundamentals of Cyber Security
2. Basics of Ethical hacking
3. understanding of network

Course Objectives:
1. Understand wireless and IoT security vulnerabilities.
2. Use Metasploit for system exploitation.
3. Learn social engineering and phishing techniques.
4. Analyze malware and perform reverse engineering.
5. To Basic understanding of penetration Testing

Course Outcomes: On completion of the course, student will be able to:
1. Demonstrate wireless and IoT hacking skills.
2. Exploit systems using Metasploit.
3. Perform ethical social engineering attacks.
4. Analyze and reverse-engineer malware.
5. Understanding of how penetration works

Course Contents

Unit 1	**Wireless & IoT Hacking**	**6 Hours**	**CO 1**

1.1 Understanding Wireless Encryption (WEP, WPA, WPA2, WPA3)
1.2 Wireless Network Sniffing(Wireshark, Airodump-ng)
1.3 Cracking Wi-Fi Networks with Aircrack-ng & Wifite
1.4 Rogue Access Points & Evil Twin Attacks
1.5 Bluetooth Hacking & Exploitation
1.6 IoT Device Security & Exploitation
1.7 IoT Network Protocols

Unit 2	**Exploiting Systems Using Metasploit**	**8 Hours**	**CO 2**

2.1 Introduction to Metasploit Framework
2.2 Creating Exploits & Payloads with Msfvenom
2.3 Exploiting Windows & Linux Systems
2.4 Post-Exploitation Techniques:
  2.4.1Privilege Escalation
  2.4.2 Data Exfiltration
  2.4.3 Persistence & Covering Tracks
2.5 Writing Custom Exploits

Unit 3	Social Engineering & Phishing Attacks	6 Hours	CO 3

3.1 Social Engineering Techniques
3.2 Crafting Malicious Attachments
3.3 Phishing Attacks:
- 3.3.1 Spear Phishing vs. Mass Phishing
- 3.3.2 Creating Fake Websites for Credential Harvesting
- 3.3.3 Advanced Phishing Tools (Evilginx2, Gophish)

3.4 SMS & Voice Phishing (Vishing)
3.5 USB-based Attacks (Rubber Ducky, BadUSB)

Unit 4	Malware Analysis & Reverse Engineering	5 Hours	CO 4

4.1 Types of Malware (Viruses, Worms, Trojans, Ransomware)
4.2 Static vs. Dynamic Analysis of Malware
4.3 Using Sandboxes for Malware Analysis
4.4 Reverse Engineering Basics

Unit 5	Penetration Testing	5 Hours	CO 5

5.1 Phases of Penetration Testing (Planning, reconnaissance, Scanning, Exploitation, Reporting)
5.2 Black Box vs. White Box Testing
5.3 Simulating Advanced Persistent Threats (APT)
5.4 Red Team vs. Blue Team vs. Purple Team Exercises
5.5 Writing a Professional Penetration Testing Report
5.6 Legal & Ethical Considerations in Ethical Hacking

Reference Books:

1. Hacking: The Art of Exploitation by Jon Erickson
2. The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws by Dafydd Stuttard and Marcus Pinto
3. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy by Patrick Engebretson
4. Penetration Testing: A Hands-on Introduction to Hacking by Georgia Weidman

Savitribai Phule Pune University
S.Y.B.Sc. (Cyber and Digital Science)
CDS252 MJ
Title: Advance Network Security

Teaching Scheme	**No. of Credits: 02**	**Examination Scheme**
2 Hours / week		CA :15 marks UA: 35 marks

Prerequisites:

1. Basic knowledge of Networking and ISO/OSI model.
2. Basic knowledge of security concepts, authentication, and access control.
3. Knowledge of Linux and Windows security concepts

Course Objectives

1. Understand the fundamental concepts of network security and its importance in modern communication.
2. Explore various cryptographic techniques and their role in securing data transmission.
3. Analyze different network security protocols and their implementation.
4. Study intrusion detection and prevention mechanisms for securing networks.
5. Examine security challenges in web applications and API security.

Course Outcomes: On completion of the course, student will be able to

CO1: Understand Advanced Network Security Concepts
CO2: Understand Cryptographic Techniques
CO3: Secure Network Architectures and Protocols also Identify and Mitigate Cyber Threats
CO4: Implement Network Security Devices
CO5: Implement Security Policies and Risk Management and Investigate and Respond to Security Incidents

Course Contents

Chapter 1	**Introduction to Network Security**	**4 hours**	**CO1**

1.1 Basics of Network Security
1.2 Security Goals: Confidentiality, Integrity, Availability (CIA)
1.3 Security Threats and Attacks: Malware, Phishing, DoS/DDoS
1.4 Security Policies and Risk Management
OSI Security Architecture

Chapter 2	**Cryptographic Techniques**	**8 hours**	**CO2**

2.1 Cryptography, plain text and cipher text, cipher key,
2.2 Categories of cryptography-Symmetric key, asymmetric key
2.3 Key Exchange Mechanisms (Diffie-Hellman)

2.4 Symmetric key cryptography

2.5.1 Traditional ciphers – substitution cipher, shift cipher, Transposition cipher
2.5.2 Simple Modern ciphers-XOR, Rotation cipher, s-box, p-box
2.5.3 Modern round ciphers-DES
2.5.4 Mode of operation-ECB,CBC,CFB,OFB

2.6 Asymmetric key cryptography-RSA Security Services

2.6.1 Message confidentiality-With Symmetric key cryptography, with asymmetric key cryptography
2.6.2 Message integrity-Document and fingerprint, message and message digest
2.6.3 Message authentication-MAC,HMAC

2.6.4 Digital signature
2.6.5 Entity Authentication-Passwords, Fixed passwords challenge-response

Chapter 3	Network Security Protocols	8 hours	CO3

3.1 Secure Socket Layer (SSL) & Transport Layer Security (TLS)
- 3.1.1 SSL services
- 3.1.2 Security parameters
- 3.1.3 Sessions and connections
- 3.1.4 Transport layer security

3.2 Internet Protocol Security (IPSec)
- 3.2.1 Two modes
- 3.2.2 Two security protocols
- 3.3.3 Services provided by IPSec
- 3.3.4 Security association

3.3Virtual Private Networks (VPNs)
3.4Wireless Security Protocols (WEP, WPA, WPA2, WPA3)

Chapter 4	Intrusion Detection and Prevention	4 hours	CO4

4.1 Firewalls: Types and Configurations
4.2 Intrusion Detection Systems (IDS) & Intrusion Prevention Systems (IPS)
4.3 Honeypots and Honeynets
4.1 Security Information and Event Management (SIEM)

Chapter 5	Web & API Security	6 hours	CO5

5.1 OWASP Top 10 Security Risks
5.2 Secure Authentication and Authorization (OAuth, JWT)
5.3 Secure API Design and Implementation
5.4 Web Application Firewalls (WAF)
5.5 Emerging Threats and Security Trends
- 5.5.1 Cloud Security and Zero Trust Architecture
- 5.5.2 AI and Machine Learning in Cyber security

Reference Book:

1. Behourz A Forouzan, Cryptography And Network Security, McGraw Hill Education, 2015. 2.William Stallings,Cryptography And Network Security,Prentice Hall, 2018.
3. Atul Kahate,Cryptography And Network Security, TMH, 2019.
4. Cryptography and Network Security: Principles and Practice, William Stallings, 7th edition, Pearson Education
5. Network Security Essentials: Applications and Standards (For VTU), William Stallings, 3rd edition, Pearson Education

Savitribai Phule Pune University
S.Y.B.Sc. (Cyber and Digital Science)
CDS-271-VSC-P
Title: Database Management System

Teaching Scheme : 4 hours 20min / week	**No. of Credits: 2**	**Examination Scheme** CA:15 marks UA:35 marks

Course Objectives: -The course should enable the student:

1. Learn how to design databases using ER and EER models to represent real-world scenarios.
2. Gain hands-on experience in creating and modifying databases, tables, and constraints.
3. Develop skills to insert, update, delete, and retrieve data using SQL.
4. Learn how to use joins, sub queries, and set operations for complex data retrieval.
5. Implement views and indexing techniques to improve query performance.

Course Outcome: The students should be able to

CO1: Construct ER and EER diagrams for real-world applications.
CO2: Create and manage databases using DDL commands effectively.
CO3: Perform DML operations and write optimized queries using SELECT statements.
CO4: Execute joins, sub queries, and set operations for efficient data analysis.
CO5: Apply indexing and views to optimize database operations.

Course Contents

Unit 1	**Database Design and ER Model** 1.1 Understanding ER and EER Models 1.1.1 Create an ER diagram for a case study (e.g., Hospital Management, Online Shopping, and Library System). 1.1.2 Identify entities, attributes, relationships, and cardinality. 1.2 Convert the ER diagram into an EER diagram using generalization, specialization, and aggregation.	6 Hours	CO1

Unit 2	**SQL Basics – Data Definition and Constraints** 2.1 Creating and Modifying Databases (DDL Commands) 2.1.1 Create a database and define multiple tables with appropriate data types. 2.1.2 Implement primary key, foreign key, unique, not null, check, and default constraints. 2.1.3 Alter tables (add/drop/rename columns, modify constraints). 2.1.4 Drop tables and databases. 2.1.5 Truncate	6 Hours	CO2
Unit 3	**Data Manipulation and Retrieval** 3.1 Data Insertion, Modification, and Deletion (DML Commands) 3.1.1 Insert single and multiple records into tables. 3.1.2 Update specific and multiple records. 3.1.3 Delete specific and all records. 3.2 Querying Data using SELECT Statements 3.3 Use various SQL operators (AND, OR, BETWEEN, NOT, IN, IS NULL, LIKE). 3.4 Apply aggregate functions (AVG, COUNT, MAX, MIN, and SUM). 3.4 Use DISTINCT, ORDER BY, GROUP BY, HAVING.	7 Hours	CO3
Unit 4:	**Advanced SQL – Joins and Sub queries** 4.1 Working with Joins 4.1.1 Perform different types of joins: 4.1.1.1 Inner Join 4.1.1.2 Left, Right, and Full Outer Joins 4.1.1.3 Self-Join 4.2 Sub queries and Set Operations 4.3 Write nested queries using SELECT, INSERT, UPDATE, and DELETE. 4.4 Use set operations: UNION, UNION ALL, INTERSECT, EXCEPT.	6 Hours	CO4
Unit 5:	**Views and Indexing** 5.1 Views and Indexing for Performance Optimization 5.1.1 Create and manage views (CREATE VIEW, UPDATE VIEW, and DROP VIEW). 5.1.2 Implement indexing (Single-level, multi-level). 5.2 Compare query performance with and without indexing.	5 Hours	CO5

Reference Books :

- Beginning Databases with PostgreSQL: From Novice to Professional, Richard Stones, Neil Matthew, ISBN:9781590594780
- Henry F. Korth, Abraham Silberschatz, S. Sudarshan, “Database System Concepts”, Tata McGraw-Hill Education
- Data base Management Systems, Raghu Ramakrishnan, Johannes Gehrke, McGraw Hill Education (India) Private Limited, 3rd Edition.

Websites for Reference:

1. NPTEL Online Course: https://nptel.ac.in/courses/106/105/106105175/
2. MIT Open Courseware (Databases): https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-830-database-systems-fall-2010/
3. Stanford Online - Databases Course: https://online.stanford.edu/courses/cs145-introduction-databases
4. Khan Academy - SQL Tutorial: https://www.khanacademy.org/computing/computer-programming/s
5. https://www.w3schools.com/sql/
6. https://www.geeksforgeeks.org/dbms/
7. https://www.tutorialspoint.com/dbms/index.htm
8. https://mode.com/sql-tutorial/

Savitribai Phule Pune University

S.Y.B.Sc. (Cyber and Digital Science)

Subject Code: CDS 281 FP
Subject: Mini Project

Teaching Scheme: Practicals per week: 1 (4 hrs)	**No. of Credits: 2**	**Examination Scheme:** CE: 15 Marks UE: 35 Marks

Course Objectives:

The course is designed to teach-

- To provide students with hands-on experience in applying theoretical knowledge from cyber and digital science to real-world problems through project development.
- To encourage innovation and creativity in designing secure and efficient digital systems or cyber security solutions.
- To enhance teamwork, project management, and communication skills through collaborative project execution and documentation.
- To prepare students for professional practice or further research by integrating industry-relevant standards, tools, and best practices in the mini project.

Course Outcomes: -

On completion of the course, student will be able to:
CO1: Design and develop a practical solution using appropriate cyber and digital tools, techniques, or frameworks.
CO2: Demonstrate the ability to work independently or in teams to plan, implement, and evaluate a digital or cyber solution.
CO3: Analyze and interpret data or system behavior to ensure security, functionality, and compliance with ethical standards.
CO4: Communicate technical information effectively through documentation, presentations, and demonstrations.
CO5: Exhibit awareness of current trends, legal aspects, and best practices in cyber and digital science relevant to the project undertaken.

Course Contents

Unit	**Description**
1,12	Implementation of the case studied in semester III
13,14	Reports generated (if any), experiences while undergoing the course
15	Report writing and Presentation of work via demos of developed project

Savitribai Phule Pune University
S.Y.B.Sc. (Cyber and Digital Science)
CDS-291-MN: Advanced Web Technologies Syllabus

Teaching Scheme:	**No. of Credits:**	**Examination Scheme:**
2 hours / week	**2**	CA:15 marks UA: 35 marks

Prerequisites

1. HTML5, CSS3
2. Core PHP

Course Objectives: -

1. To Learn different technologies used at client Side Scripting Language
2. To Learn XML and XML parsers.
3. To One PHP framework for effective design of web application.
4. To Learn JavaScript to create web pages.
5. To Learn AJAX to make our application more dynamic.
6. To Learn basic concepts of NodeJS

Course Outcomes: - On completion of the course, student will be able to–

CO1: Understand concepts like setting response headers , PHP error handling etc.
CO2: Use of JavaScript to create web page
CO3: Interpret and formulate XML queries
CO4: Learn to build website AJAX framework
CO5: Understand the JavaScript and technical concepts behind Node JS..

Course Contents

Chapter 1	**Introduction to Web Techniques**	**4 hours**	**CO1**

1.1 Variables
1.2 Server information Processing forms
1.3 Setting response headers
1.4 Maintaining state
1.5 PHP error handling

Chapter 2	**JavaScript**	**8 hours**	**CO2**

2.1 Basic syntax of JavaScript
2.2 Data types and variables
2.3 Functions and events [onclick, onchange, onload]
2.4 Popup boxes
2.5 String methods [indexof, lastindexof, search, replace, match]
2.6 Regular expression

Chapter 3	**XML**	**8 hours**	**CO3**

3.1 What is XML?
3.2 XML document Structure
3.3 PHP and XML
3.4 XML parser
3.5 The document object model (DOM)
3.6 DOM Events (onmouseup, onmousedown, onclick, onload, onmouseover, onmouseout).

3.7 The simple XML extension
3.8 Changing a value with simple XML

Chapter 4	AJAX	6 hours	CO4

4.1 Introduction of AJAX
4.2 AJAX web application model
4.3 AJAX –PHP framework Performing
4.4 AJAX validation Handling XML data using php and AJAX
4.5 Connecting database using php and AJAX

Chapter 5	NodeJS	4 hours	CO5

5.1 Introduction to Node JS
5.2 What is Node JS?
5.3 Advantages of Node JS
5.4 Traditional Web Server Model
5.5 Node.js Process Model
5.6 Install Node.js
5.7 Working in REPL
5.8 Module and Module types
5.9 What is NPM ?
5.10 Adding dependency in package .json

Reference Books:

1. Web Technologies, Black Book, Dreamtech Press
2. Web Applications : Concepts and Real World Design, Knuckles, Wiley-India
3. Internet and World Wide Web How to program, P.J. Deitel & H.M. Deitel Pearson Education
4. Programming PHP By Rasmus Lerdorf and Kevin Tatroe, O'Reilly publication

E-Books and Online Learning Material

1. https://www.w3schools.com
2. https://wwwtutorialspoint.com
3. https://www.php.net

Savitribai Phule Pune University
S.Y.B.Sc. (Cyber and Digital Science)
Subject Code: SEC251CDS-T
Title: Principles of Operating Systems

Teaching Scheme	**No. of Credits**	**Examination Scheme**
2 hours / week	**2**	CA:15 marks UA: 35 marks

Prerequisites

1. Basics of mathematics
2. Fundamental of Computer

Course Objectives: -

1. To understand the concept of operation system and its principle
2. To study the various functions and services provided by operating system
3. To understand the concept of process, memory, deadlock handling
4. To study the different methods of CPU Scheduling, Disk Scheduling and Page replacements algorithms

Course Outcomes: - On completion of the course, student will be able to–

CO1. Basic concepts of operating System.
CO2. Processes and CPU Scheduling by operating system, Threads
CO3. Synchronization in process and threads by operating system
CO4. Deadlock
CO5. Disk scheduling Mechanism
CO6. Memory management by operating system using with the help of various schemes like demand paging

Course Contents

Chapter 1	**Introduction to Operating System and Structure**	**3 hours**	**CO1**

1.1 Operating Systems Overview- system Overview and Functions of operating systems
1.2 Operating system Services, Operating system structure
1.3 Types of Operating Systems - Time-Sharing Systems, Personal Computer Systems, Parallel Systems, Distributed Systems, Real Time Systems,
1.4 System calls Types of System calls and their working.

Chapter 2	**Processes and CPU Scheduling**	**6 hours**	**CO2**

2.1 Process & Thread Concept – The processes, Process states, Process control block, Thread
2.2 Process Scheduling – Scheduling queues, Schedulers, context switch
2.3 Scheduling Concepts- CPU-I/O burst cycle, Scheduling Criteria, CPU scheduler
2.4 Scheduling Algorithms – Types of Scheduling-preemptive and non-preemptive , FCFS, SJF, LJF, Priority scheduling, Round-robin scheduling,

Chapter 3	**Process Synchronization**	**4 hours**	**CO3**

3.1 Principles Of Concurrency, Cooperating Process,
3.2 Critical Section Problem
3.2 Mutual Exclusion, Progress, Bounded Wait

3.4 Semaphores
3.3 Message Passing
3.4 Classic Problems of Synchronization – The bounded buffer problem, The reader writer problem, The dining philosopher problem

Chapter 4	**Deadlock**	**8 hours**	**CO4**

4.1 Deadlock Characterization – Necessary conditions
4.2 Deadlock Handling Methods-
4.2.1 Prevention
4.2.2 Deadlock Avoidance - Safe state, Resource Allocation graph algorithm, Banker's Algorithm
4.2.3 Deadlock Detection and Recovery from Deadlock – Process termination, Resource preemption
4.2.4 Ignorance

Chapter 5	**Disk scheduling**	**3 hours**

5.1 Overview of disk structure
5.2 Disk Scheduling Algorithms- FCFS Scheduling, SSTF Scheduling, SCAN, CSCAN Scheduling, LOOK, CLOOK Scheduling,

Chapter 6	**Memory Management**	**6 hours**

6.1 Background – Basic hardware, Address binding, Logical versus physical address space, Swapping
6.2 Contiguous Memory Allocation –First Fit, Best Fit, Worst Fit, Fragmentation, types of fragmentation, Compaction
6.3 Paging and Segmentation – Basic Concepts
6.4 Demand paging
6.6 Page replacement – FIFO, Optimal, LRU, MRU,LFU,MFU

Reference Books:

1. Operating System Concepts by Silberschatz, Galvin, Wiley publication
2. Operating Systems: Internals and Design Principles, Seventh Edition, William Stallings, PEARSON
3. Modern Operating Systems by Andrew Tanenbaum, Prentice-Hall
4. Operating Systems by Deitel, Deitel and Choffnes, Pearson Education