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 2024-25

Savitribai Phule Pune University

B. Sc.(Cyber and Digital Science)

(To be implemented from Academic year 2024-2025)

Name of Program: Cyber and Digital Science

Introduction:

Digital and Cyber Forensics is a niche subject of modern studies which shall prepare students for professional work in business and industry, as well as government and law enforcement. Since Cybercrime has been on the rise in recent years, this course offers a special impetus and an excellent launch pad for those who are interested in becoming professionals' crime-fighters with rewarding career options.

Digital infrastructures and information networks have become crucial in any business activity. The information residing on these computers, networks, and in the cloud is a critical asset and should be secured. The impact of data loss or any downtime of the infrastructure is quite high. Hence, there is a need for heightened security measures to protect both infrastructure and data. The student shall learn the techniques to collect, preserve, analyze, and report digital evidence. It also opens a new avenue for research opportunities into forensics and security issues.

In the information era, digital technologies have opened up immense possibilities for economic and social change that is inclusive and sustainable. Designing and deploying digital technologies, analyzing human-computer interaction or big data will produce technological expertise as well as a nuanced understanding of the social, cultural, and economic aspects of the digital society. Students will gain insights into the design of digital technologies, and the policy challenges of deploying such technologies, with a broad-based training that will draw from computer science, engineering, research methods, management, economics and other social sciences, which will equip them with a rigorous

understanding of technologies for development and the development of technologies.

The Program is of Three Years duration with six semesters. It is a Full-Time Degree Program. The program will be based on the Choice-based credit system comprising 140 credit points.

Objectives:

- To strengthen the basics of the subject useful in selecting various career options.
- To make students aware of cybercrime and learn ways to handle them.
- To produce entrepreneurs who can work in the area of Cyber and Digital Forensics.
- **Eligibility**: Higher Secondary School Certificate (10 + 2) or its equivalent examination with English

OR

Three Year Diploma Course From The Board Of Technical Education Conducted By Government Of Maharashtra Or Its Equivalent

OR

Higher Secondary School Certificate (10 + 2) Examination with English and Vocational subject of +2 Level (MCVC)

PO No.	PO Outcomes
PO 1	Recognize and be comfortable with Linux administration, as it is important in modern IT environment.
PO 2	Acknowledge and implement action the modern IT world's needs in cyber security
PO 3	Develop creative skills, critical thinking , analytical skills and research to address the real world problems using cyber security skills.
PO 4	Understand the Concepts of cyber security, Networking, Digital Forensics and vulnerability testing and statistical techniques
PO 5	Applying the Concepts of Digital Communication, IOT and Digital Image Processing
PO 6	Determine and analyze software vulnerabilities and security solutions to reduce the risk of exploitation
PO 7	Learn needful programming languages such as C, Python,
PO 8	Establishing together cyber laws and cyber policies in order to comprehend the rules and regulations of the present IT environment
PO 9	To developing regulations and tactics for cyber security
PO 10	Applications, data, and cloud-based infrastructure are all safeguarded through cloud security.
PO 11	Understand security concepts including cyber threat intelligence, Block chain in cyber security, communication systems security, malware analysis, VAPT, IDS & IPS, and reporting of cybercrimes.

Savitribai Phule Pune University

Structure of UG Program as per NEP- 2020

Name of Program: - BSc(Cyber and Digital Science)

Major Course:- Cyber and Digital Science

Level:- 4.5 (First Year) Sem:-I

Course Type	Course Code	Course Code	Credits		Teaching Scheme Hr/Week		Evaluation Scheme & Max Marks		
			TH	PR	TH	PR	CE	EE	Total
Subject 1	CDS-101-MJ	Linux System Administration	2		2		20	30	50
Subject 2	CDS-102-MJ	Fundamental of C programming	2		2		20	30	50
Subject 3	CDS-103-MJ	Fundamentals of Computer	2		2		20	30	50
Subject 1 Practical	CDS-104-MJP	Practical based on CDS101MJ		2		4	20	30	50
Subject 2 Practical	CDS-105-MJP	Practical based on CDS102MJ		2		4	20	30	50
Subject 3 Practical	CDS-106-MJP	Practical based on CDS103MJ		2		4	20	30	50
IKS	IKS-101-CDS	Computing in ancient India	2		2		20	30	50
GE/OE	OE-101-CDS OE-102-CDS	Office Automation - I / Introduction to Google Tools - I	2		2		20	30	50
SEC	SEC-101-CDS	Fundamentals of Digital Communication.		2		4	20	30	50
AEC	AEC-101-MAR/HIN/ENG	MIL-I(Hindi) / MIL-I(Marathi) / English - I	2		2		20	30	50
VEC	VEC-101-ENV	EVS-I	2		2		20	30	50
TOTAL			14	08	14	16	220	330	550

Level:- 4.5 (First Year) Sem:-II

Course Type	Course Code	Course Code	Credits		Teaching Scheme Hr/Wee k		Evaluation Scheme and Max Marks		
			TH	PR	TH	PR	CE	EE	Total
Subject 1	CDS-151-MJ	Fundamentals of Cyber security	2		2		20	30	50
Subject 2	CDS-152-MJ	Network Security	2		2		20	30	50
Subject 3	CDS-153-MJ	Python Programming	2		2		20	30	50
Subject 1 Practical	CDS-154-MJP	Practical based on CDS151MJ		2		4	20	30	50
Subject 2 Practical	CDS-155-MJP	Practical based on CDS152MJ		2		4	20	30	50
Subject 3 Practical	CDS-156-MJP	Practical based on CDS153MJ		2		4	20	30	50
GE/OE	OE-152-CDS OE-153-CDS	Office Automation - II / Introduction to Google Tools - II	2		2		20	30	50
SEC	SEC-151-CDS	Statistical techniques for Computer Science **OR** Advance Excel		2		4	20	30	50
AEC	AEC-151-MAR/HIN/ENG	MIL-II(Hindi) / MIL-II(Marathi)/MIL-II (English - II)	2		2		20	30	50
VEC	VEC-151-ENV	EVS-II	2		2		20	30	50
CC	**CC-151 - T/P**	**University Basket**		**2**		**4**	**20**	**30**	**50**
TOTAL			14	08	12	20	220	330	550

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	CDS-201-MJ	Ethical Hacking-I	2		2		20	30	50
	CDS-202-MJ	Cyber Ethics, Cyber Law & Cyber Policies	2		2		20	30	50
	CDS-203-MJP	Practical based on CDS201MJ		2		4	20	30	50
VSC	CDS-221-VSC	Data Structure using Python		2		4	20	30	50
IKS	IKS-200-T	Indian Knowledge System in Computing	2		2		20	30	50
FP/OJT/CEP	CDS-231-FP	Mini Project		2		4	20	30	50
Minor	CDS-241-MN	Web Technology	2		2		20	30	50
	CDS-242-MNP	Practical based on CDS241MN		2		4	20	30	50
GE/OE	OE-201-CDS-T OE-202-CDS-T OE-203-CDS-T OE-204-CDS-T	AI for Everyone I / Web design I / Digital Marketing I/ Introduction to Cyber Security	2		2		20	30	50
AEC	AEC-201-T	From University Basket	2		2		20	30	50
CC	CC-201-T/P	From University Basket	2		2		20	30	50
Total			14	08	14	16	220	330	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	CDS-251-MJ	Ethical Hacking-II	2		2		20	30	50
	CDS-252-MJ	Advance Network Security	2		2		20	30	50
	CDS-253-MJP	Practical based on CDS251MJ		2		4	20	30	50
VSC	CDS-271-VSC-P	Database management system		2		4	20	30	50
FP/OJT/ CEP	CDS-281-FP	Mini Project		2		4	20	30	50
Minor	CDS-291-MN	Advanced Web Technology	2		2		20	30	50
	CDS-292-MNP	Practical based on CDS291MN		2		4	20	30	50
GE/OE	OE-251-CDS-T OE-252-CDS-T OE-253-CDS-T	AI for Everyone II / Web design II / Digital Marketing II	2		2		20	30	50
SEC	**SEC-251CDS -T**	**Principles of operating System**	**2**		**2**		**20**	**30**	**50**
AEC	AEC-251-T	From University Basket	2		2		20	30	50
CC	CC-251-T/P	From University Basket	2		2		20	30	50
Total			14	8	14	16	220	330	550

Level:-5.5(Third Year)Sem:-V

Course Type	Course Code	Course Code	Credits		Teaching Scheme Hr Week		Evaluation /Scheme and Max Marks		
			TH	PR	TH	PR	CE	EE	Total
Major Core	CDS-301-MJ	Digital Forensic-I	2		2		15	35	50
	CDS-302-MJ	Malware Analysis	2		2		15	35	50
	CDS-303-MJ	Cyber Threat Intelligence	2		2		15	35	50
	CDS-304-MJ	Attack Surface Analysis & Threat Modeling	2		2		15	35	50
	CDS-305-MJP	Practical based on CDS-301-MJ		2		4	15	35	50
	CDS-306-MJP	Practical based on CDS-302-MJ		2		4	15	35	50
Major Elective	CDS-307-MJ	**Web and Network Security Fundamentals**	2		2		15	35	50
	CDS-308-MJP	Practical based on CDS-307-MJ		2		4	15	35	50
	OR								
	CDS-309-MJ	Mobile Forensic	2		2		15	35	50
	CDS-310-MJP	Practical based on CDS-309-MJ		2		4	15	35	50
VSC	CDS-321-VSCP	**Linux and Web Server Hardening**		2		4	15	35	50
FP/OJT/ CEP	CDS-331-FP	Project		2		4	15	35	50
Minor	CDS-341-MN	**Data Analytics and Business Intelligence**	2		2		15	35	50
TOTAL			12	10	12	20	165	385	550

Level:-5.5(Third Year)Sem:-VI

Course Type	Course Code	Course Code	Credits		Teaching Scheme Hr Week		Evaluation / Scheme and Max Marks		
			TH	PR	TH	PR	CE	EE	Total
Major Core	CDS-351-MJ	Digital Forensic-II	2		2		15	35	50
	CDS-352-MJ	Vulnerability Assessment & Penetration Testing	2		2		15	35	50
	CDS-353-MJ	Cyber Crime & Reports	2		2		15	35	50
	CDS-354 MJ	Active Directory fundamentals and attacks	2		2		15	35	50
	CDS-355-MJP	Practical Based on CDS-351-MJ		2		4	15	35	50
	CDS-356-MJP	Practical Based on CDS-352-MJ		2		4	15	35	50
Major Elective	CDS-357-MJ	**Advanced Web Application Security**	2		2		15	35	50
	CDS-358-MJP	Practical Based on CDS-357-MJ		2		4	15	35	50
	OR								
	CDS-359-MJ	Fin-Tech Cyber Security	2		2		15	35	50
	CDS-360-MJP	Practical Based on CDS-359-MJ		2		4	15	35	50
FP/OJT/ CEP	CDS-381-OJT	On Job Training		4		8	30	70	100
VSC	CDS-391-VSC	Machine Learning for Data Analysis	2		2		15	35	50
TOTAL			12	10	12	20	165	385	550

Level:-6.0(FourthYear)Sem:-VII(Honors)

Course Type	Course Code	Course Code	Credits		Teaching Scheme Hr Week		Evaluation /Scheme and Max Marks		
			TH	PR	TH	PR	CE	EE	Total
Major Core	CDS-401-MJ	Malware Analysis II	2		2		15	35	50
	CDS-402-MJ	Intrusion Detection and Prevention System	2		2		15	35	50
	CDS-403-MJ	Digital Image Processing	2		2		15	35	50
	CDS-404-MJP	Practical Based on CDS-401-MJ		2		4	15	35	50
	CDS-405-MJP	Practical Based on CDS-402-MJ		2		4	15	35	50
Major Elective	CDS-408-MJ	Digital Payments and Its Security	2		2		15	35	50
	CDS-409-MJP	Practical Based on CDS-408-MJ		2		4	15	35	50
	OR								
	CDS-410MJ	Wireless Security	2		2		15	35	50
	CDS-411MJP	Practical Based on CDS-410-MJ		2		4	15	35	50
	OR								
	CDS-412-MJ	IT Act 2000 in Cyberspace	2		2		15	35	50
	CDS-413-MJP	Practical Based on CDS-412-MJ		2		4	15	35	50
Research Project	CDS - 471RP	Research Project		4		8	30	70	100
Research Methodology	CDS-472RM	Research Methodology	4		4		30	70	100
TOTAL			16	06	16	12	165	385	550

Level:-6.0(Fourth Year)Sem:-VIII(Honors)

Course Type	Course Code	Course Code	Credits		Teaching Scheme Hr Week		Evaluation /Scheme and Max Marks		
			TH	PR	TH	PR	CE	EE	Total
Major Core	CDS-451MJ	Mobile Application And Services	2		2		15	35	50
	CDS-452MJ	Incident Handling	2		2		15	35	50
	CDS-453MJ	Cyber Security Architecture	2		2		15	35	50
	CDS-454MJP	Practical Based on CDS-451-MJ		2		4	15	35	50
	CDS-455MJP	Practical Based on CDS-452-MJ		2		4	15	35	50
Major Elective	CDS-458MJ	Dark web and Cyber warfare	2		2		15	35	50
	CDS-459MJP	Practical Based on CDS-458MJ		2		4	15	35	50
	OR								
	CDS-460MJ	DecSecOps	2		2		15	35	50
	CDS-461MJP	Practical Based on CDS-460MJ		2		4	15	35	50
	OR								
	CDS-462MJ	Tools and Technology for Cyber Security	2		2		15	35	50
	CDS-463MJP	Practical Based on 462MJ		2		4	15	35	50
Research Project	CDS-481RM	Research Project		8		20	60	140	200
TOTAL			08	14	08	32	165	385	550

SEM I

Savitribai Phule Pune University
F.Y.B.Sc.(Cyber and Digital Science)

Subject Code : CDS101MJ
Subject :Linux System Administration

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / week	2	CE: 20 marks EE: 30 marks

Prerequisites

1. Familiarity with the terminal, shell, and command line interface

Course Objectives: -

- To make the students understand the Linux OS
- To acquaint them with the basic utilities of Linux
- To help them manage a network using Linux OS

Course Outcomes: - Student will be able to: -

- Demonstrate proficiency using the Linux command line and constructing shell scripts.
- Perform maintenance tasks, including user and system management.
- Install and configure system services.
- To install and implement Linux Operating Systems across the network.
- To manage and handle file permissions and other security aspects.

Course Contents

Chapter 1	**Introduction to Linux System Administration**	**6 hours**

Overview of Linux Operating System. Role of a Linux System Administrator. Understanding the Linux File System. Basic Shell Commands and Navigation.

Chapter 2	**Installation and Configuration**	**7 hours**

Linux Installation Methods.
Partitioning and File System Setup. User and Group Management.
Network Configuration and Troubleshooting.

Chapter 3	**Control Statements and Functions**	**6 hours**

Package Management with APT and YUM. Kernel Updates and System Reboots.
Log File Analysis and Troubleshooting. Monitoring System Performance.

Chapter 4	**Security and Access Control**	**5 hours**

User Authentication with PAM.
Firewalls and IP tables.
Secure Shell (SSH) Configuration.
Implementing SE Linux/App Armor for Mandatory Access Control.

Chapter 5	**Advanced Topics in Linux Administration**	**5 hours**

Automated Task Scheduling with Cron. Virtualization and Containerization (e.g. Docker). File and Directory Permissions.
Backup and Recovery Strategies.

Reference Books:

1. Linux System Administration, by Tom Adelstein, Bill Lubanovic, Released March 2007 Publisher(s): O'Reilly Media,ISBN: 9780596009526.
2. Pro Linux System Administration,by James Turnbull, Dennis Matotek, Peter Lieverdink,publisher(s): Apress, 2009,ISBN: 1430219130,9781430219132.
3. The Complete Guide to Linux System Administration by James S Walker, Released December 1,2004

Publisher(s):Course Technology Inc,ISBN: 0619216166,9780619216160

E-Books and Online Learning Material

1. https://www.w3schools.com/linux/
2. Linux Programming and Scripting: https://archive.nptel.ac.in/courses/117/106/117106113/

CDS-102MJ : Fundamentals of C Programming

Teaching Scheme2 Lectures / week	No. of Credits: 2	Examination Scheme CE :20 marks EE: 30 marks

Prerequisites: None

Course Objectives: -

1. To develop the basic concepts and terminology of programming in general.
2. To implements the algorithms and program in C language
3. To develop programming skills to a level such that problems of reasonable complexitycan be tackled successfully.

Course Outcomes: - Student will be able to :-

1. Devise computational strategies for developing applications
2. Develop applications (Simple to Complex) using C programming language

Course Contents

Unit 1	**C fundamentals**	**8 Lectures**

History of 'C' language, Features of C, Structure of C Program, C Character Set, Identifiers and Keywords, Variables and constants.
Data types- Basic data types, enumerated types, Type casting, Declarations, Expressions Operators and Expressions Unary and Binary arithmetic operators, Increment Decrement operators, Relational and logical operators, Bit wise operators, Assignment operators, Comma operator, size of operator, Ternary conditional operator, Precedence and associativity.

Unit 2	**Input Output Statements**	**5 lectures**

Input output functions:
printf, scanf functions, getchar, putchar, getch functions, gets, puts functions, Escapesequence characters, Format specifiers

Unit 3	**Control and Iterative structures**	**15 Lectures**

Decision making structures:- if, if-else, switch and conditional operator, Loop control structures:- while ,do while, for, Use of break and continue, Nested structures, Unconditional branching (goto statement).

Unit 4	**Functions**	**16 Lectures**

Concept of function, Advantages of Modular design,Standard library functions,
User defined functions:- declaration, definition, function call, parameter passing (by value), return statement.
Recursive functions.

Unit 5	**Arrays**	**16 Lectures**

Concept of array. Types of Arrays – One, Two and Multidimensional array.Array Operations - declaration, initialization, accessing array elements.
Memory representation of two-dimensional array (row major and column major)Passing arrays to function, bound checking

Reference Books:

1. C: the Complete Reference, Schildt Herbert, 4th edition, McGraw Hill
2. A Structured Programming Approach Using C, Behrouz A. Forouzan, Richard
    a. F. Gilberg, Cengage Learning India
3. The 'C' programming language, Brian Kernighan, Dennis Ritchie, PHI
4. Programming in C ,A Practical Approach, Ajay Mittal , Pearson
5. Programming with C, B. Gottfried, 3rdedition, Schaum's outline Series, Tata McGraw Hill.
6. Programming in ANSI C, E. Balagurusamy, 7th Edition, McGraw Hill.

Savitribai Phule Pune University
F.Y. B.Sc.(Cyber and Digital Science)
Subject Code : CDS103MJ

Subject : Fundamentals of Computers

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / week	2	CE :20 marks EE: 30 marks

Prerequisites

Course Objectives: -

- To study the basics of Computer System
- To learn how to configure computer devices
- To Learn Basic Commands of Operating system and application software

Course Outcomes: -

On completion of the course**, student will be able to–**

- Learn the fundamental concepts of computer science.
- Develop the logic of problem solving.
- Explain the needs of hardware and software required for a computation task.

Course Contents

Chapter 1	**Introduction to Computers**	**8 hours**

Introduction, Characteristics of Computers, Block diagram of computer
Types of computers and features- Mini Computers, Micro Computers, Mainframe Computers, Super Computers, Laptops and Tablets
Types of Programming Languages- Machine Languages, Assembly Languages, High Level Languages
Translators- Assembler, Compiler, Interpreter Data Organization- Drives, Files, Directories

Chapter 2	**Introduction to Computer Peripherals**	**7 hours**

Primary And Secondary storage devices
Primary storage devices – RAM, ROM, PROM, EPROM
Secondary Storage Devices - CD, HD, Pen drive
I/O Devices- Scanners, Digitizers, Plotters, LCD, Plasma
Display Pointing Devices –Mouse, Joystick, Touch Screen
Number Systems
Introduction to Binary, Octal,Hexadecimal system Conversion,
Simple Addition, Subtraction, Multiplication, Division

Chapter 3	**Operating System and its Services**	**5 hours**

Dos – History
Files and Directories
Internal and External Commands
Batch Files
Types of O.S.

Chapter 4	**Internet Network**	**4 hours**

Network definition
Common terminologies: LAN, WAN, Node, Host,
Workstation, bandwidth, Interoperability, Network administrator, network security
Network Components: Severs, Clients, Communication Media
Types of network: Peer to Peer, Clients Server

Chapter 5	**Introduction to Problem Solving**	**6 hours**

Concept: problem solving
Problem solving techniques (Trial & Error, Brainstorming, Divide & Conquer) Steps in problem solving (Define Problem, Analyze Problem, Explore Solution) Algorithms and Flowcharts (Definitions, Symbols)
Characteristics of an algorithm Simple Arithmetic Problems

Reference Books:

1. Computer Fundamentals by P.K. Sinha &Priti Sinha, 3rd edition, BPB pub.
2. Fundamental of Computers – By V. Rajaraman B.P.B. Publications
3. Computer Networks – By Tennenbum Tata MacGrow Hill Publication
4. How to solve it by Computer – R. G. Dromy
5. Introduction to algorithms – Cormen, Leiserson, Rivest, Stein

Books and Online Learning Material
https://www.geeksforgeeks.org/computer-fundamentals-tutorial/
https://www.javatpoint.com/computer-fundamaentals

Savitribai Phule Pune University
F.Y.B.Sc.(Cyber and Digital Science)
Practical based on CDS 101MJ
Linux System Administration(CDS104MJP)

Teaching Scheme 4 hours / week	No. of Credits 2	Examination Scheme CE: 20 marks EE: 30 marks

Prerequisites

Problem solving with Python

Course Objectives: -

To analyze fundamentals of the Linux operating system.

To analyses a problem and devise an algorithm to solve it.

Course Outcomes: - Student will be able to: -

Implement and administer a Linux Server.

Setup and manage policies.

Implement File Services.

Course Contents

Linux System Administration

Assignment 1: Introduction to Linux System Administration

a. Install a Linux distribution of your choice.
b. Explore and explain the file system hierarchy using basic shell Commands.
c. Create a new user and group, demonstrating user and group management.

Assignment 2: Installation and Configuration

a. Choose a different Linux installation method than in Question 1.
b. Perform a manual partitioning and file system setup during the installation.
c. Configure network settings and troubleshoot any connectivity issues.

Assignment 3: System Maintenance and Updates

a. Use APT or YUM to install, update, and remove packages on your system.
b. Analyze system logs to troubleshoot a specific issue (e.g., networking, package installation).
c. Monitor system performance using tools like top or htop.

Assignment 4: Security and Access Control

a. Configure user authentication using PAM.
b. Implement firewall rules using IP tables.
c. Secure SSH by modifying its configuration file.
d. Implement either SE Linux or App Armor for Mandatory Access Control.

Assignment 5: Advanced Topics in Linux Administration

a. Schedule automated tasks using Cron.
b. Install and run a Docker container, explaining the basics of containerization.
c. Set up file and directory permissions for a specific scenario.

Assignment 6: Installation and Configuration

a. Choose a different Linux distribution than in Question 2.
b. Perform an advanced partitioning scheme, including separate partitions for /, /home, and swap.Implement user and group quotas on specific directories to manage disk space usage.

Assignment 7: System Maintenance and Updates

a. Explore and demonstrate the process of upgrading the Linux kernel.
b. Analyze logs to identify and troubleshoot issues related to kernel updates.
c. Use performance monitoring tools to identify and rectify a performance bottleneck on the system

Reference Books:

1. Linux System Administration, by Tom Adelstein, Bill Lubanovic, Released March 2007 Publisher(s): O'Reilly Media,ISBN: 9780596009526.
2. Pro Linux System Administration,by James Turnbull, Dennis Matotek, PeterLieverdink,publisher(s): Apress, 2009,ISBN: 1430219130,9781430219132.
3. The Complete Guide to Linux System Administration by James S Walker, Released December 1,2004
4. Publisher(s):Course Technology Inc,ISBN: 0619216166,9780619216160

Savitribai Phule Pune University
F.Y.B.Sc.(Cyber and Digital Science) Title:
Practical based on CDS 102MJ
Fundamentals of C Programming (CDS105MJP)

Teaching Scheme4 hours / week	No. of Credits2	Examination Scheme CE: 20 marks EE: 30 marks

Course Objectives: -

1. To analyze fundamentals of the Basic C Programming.
2. To learn flow chart and algorithms
3. To develop the basic concepts and terminology of programming in general.

Course Outcomes: - Student will be able to: -

1. Explore algorithmic approaches to problem solving
2. Develop modular programs using control structures and arrays in 'C'.

Practical 1*:* Use of data types, simple operators(expressions)

1. Accept temperatures in Fahrenheit(F)and print it in Celsius(C)and Kelvin (K)(Hint: C=5/9(F-32),K=C+273.15)
2. Accept initial velocity(u),acceleration(a)and time(t).Print the final velocity (v)and the distance (s) travelled. (Hint: $v = u + at$, $s = u + at^2$)
3. To calculate the area of square, rectangle, circle.
4. Accept two numbers and print arithmetic and harmonic mean of the two numbers(Hint:AM= (a+b)/2 , HM = ab/(a+b))
5. Accept three dimensions length (l), breadth(b) and height(h) of a cuboid andprint surface area and volume (Hint : surface area=2(lb+lh+bh), volume = lbh)

Practical 2*:* Use of decision making statements (if and if-else, nested structures)

1. Write a program to accept an integer and check if it is even or odd.
2. To find the maximum of two numbers and minimum of three numbers.
3. Writeaprogramtoacceptthreenumbersandcheckwhetherthefirstisbetween the other two numbers. Ex: Input 20 10 30. Output: 20 is between 10 and 30
4. Accept a character as input and check whether he character is a digit.(Check if it isin the range '0' to '9' both inclusive)
5. Writeaprogramtoacceptanumberandcheckifitisdivisibleby5and7.

Practical 3: Use of decision making statements (switch case)

1. Accept a single digit from the user and display it in words. For example, if digitentered is 9, display Nine.
2. Write a program, which accepts two integers and an operator as a character (+ - * /), performs the corresponding operation and displays the result.
3. Accept radius from the user and write a program having menu with the followingoptions and corresponding actions

	Actions
1.AreaofCircle	Compute area of circle and print
2.Circumferenceof Circle	Compute Circumference of circle and print
3.Volumeof Sphere	Compute Volume of Sphere and print

Practical 4: Use of simple loops, nested loops

1. Write a program that accepts a number and prints its first digit. Refer sample code1given above. Execute the program for different values.
2. Write a program that accepts numbers continuously as long as the number is positiveandprintsthesumofthenumbersread.Refersamplecode2given above. Execute the program for different values.
3. Write a program to accept n and display its multiplication table. Refer to samplecode3given above.
4. Writeaprogramtodisplayallprimenumbersbetween1andn.(n from user).

Practical 5: Use of standard library functions and menu driven programs

1. Write a program, which accepts a character from the user and checks if it is an alphabet, digit or punctuation symbol. If it is an alphabet, check if It is uppercase or lowercase and then change the case.
2. Write a menu driven program to perform the following operations till the user selects Exit.
   Acceptappropriatedataforeachoption.Usestandardlibraryfunctionsfrommath.h
   i. Sine ii. Cosine iii. Logic .e^x v. Square Root vi. Exit
3. Accept two complex numbers from the user (real part, imaginary part).Write amenu driven program to perform the following operations till the user selects Exit.
   i. ADD ii. SUBTRACT iii. MULTIPLY iv. EXIT

Practical 6: Use of user defined and recursive functions)

1. Write a function is Even, which accepts an integer as parameter and returns 1ifthenumberiseven, and 0otherwise. Use this function in main to accept n numbers and check if they are even or odd.
2. Write a function, which accepts a character and integer n as parameter and displays the next n characters.
3. Write are cursive C function to calculate the GCD of two numbers.
4. Write a recursive C function to calculate the factorial of the number.

Practical 7: Use of arrays(1-darrays)and functions

1. Write a program to accept n numbers in an array and calculate the average
2. Write a program to accept n numbers in an array and sort the array.
3. Write a program to accept n numbers in the range of 1 to 25 and count the frequency of occurrence of each number.

Practical 8: Use of multidimensional array(2-darrays)and functions

1. Write a program to accept a matrix A of size m X n and store its transpose in matrix B. Display matrix B. Write separate functions.
2. Write a program to add and multiply two matrices. Write separate functions to accept, display, add and multiply the matrices. Perform necessary checks before adding and multiplying the matrices.

Reference Books:

1. C: the Complete Reference, Schildt Herbert, 4th edition, McGraw Hill
2. A Structured Programming Approach Using C, Behrouz A. Forouzan, Richard F. Gilberg, Cengage Learning India
3. The 'C' programming language, Brian Kernighan, Dennis Ritchie, PHI
4. Programming in C ,A Practical Approach, Ajay Mittal , Pearson
5. Programming with C, B. Gottfried, 3rdedition, Schaum's outline Series, TataMcGraw Hill.
6. Programming in ANSI C, E. Balagurusamy, 7th Edition, McGraw Hill.

Savitribai Phule Pune University
F.Y.B.Sc.(Cyberand Digital Science)
Title: Practical based on CDS 103MJ

Fundamentals of Computer (CDS106MJP)

Teaching Scheme	No. of Credits	Examination Scheme
4 hours / week	2	CE: 20 marks EE: 30 marks

Course Objectives: -

1. To Know the Basics of Computers.
2. To Understand the Basics of Operating systems

Course Outcomes: - Student will be able to: -

1. Learn the fundamental concepts of computer science.
2. Develop the logic of problem solving

List of Sample practical's: Fundamentals of Computers

1. Write down the steps of installing Windows Operating System.
2. Write down the steps of installing Linux Operating System.
3. Write down the steps of creating a new file in Windows Operating System.
4. Write down the steps of creating a new file in Linux Operating System
5. Write down the steps for User Account and Group Management in Linux Operating System.
6. Write down the steps for User Account and Group Management in Windows Operating System.
7. Write down the steps to Hide the file and unhide the file in Windows Operating System.
8. File and folder management in Linux.
9. File and folder management in Windows.
10. Working with any five commands in command prompt (DOS).
11. Study about any five physical equipment used for networking.
12. Study of different internetworking devices in a computer network.
13. Explain about any five working of basic Networking Commands.
14. Study of basic network management commands
15. Write the steps to Assigning IP address to the PC and Connect to the computer.
16. Write the steps to connect the computer in Local Area Network.

17. Write the steps How to connect a network printer in Windows.

18. Write the steps How to setting to Local Area Network proxy Server.

Reference Books:

1. Fundamental of Computers – By V. Rajaraman B.P.B. Publications
2. Fundamental of Computers – By P. K. Sinha
3. Computer Today- By Suresh Basandra
4. Unix Concepts and Application – By Sumitabha Das
5. Computer Networks – By Tennenbum Tata MacGrow Hill Publication

Savitribai Phule Pune University F. Y. B.Sc.(Cyber and Digital Science) Subject Code : IKS-101CDS Subject : Computing in Ancient India		
Teaching Scheme 2 hours / week	No. of Credits 2	Examination Scheme CE :20 marks EE: 30 marks

Title of the Paper: Computing in Ancient India

Subject Code: IKS

Number of Credits: 2

Total number of Student Contact Hours: 30 hours

Session Duration: 1 Hour

Objectives:

- Discuss the rich heritage of mathematical temper of Ancient India
- Promote joyful learning of HISTORY

Contents:

Unit No	Unit Contents	Total No of Lectures	Text Books
1	Introduction and Overview of Ancient Science	**5**	**T1**
2	Binary numbers in Indian Antiquity	**8**	**T1**
3	The Katapayadi formula and modern hashing technique	**8**	**T1**
4	Panian Grammar and Formal language structures in theory and Indian logic	**8**	**T1**
5	Planets in Vedic Literature	**1**	**T1**

Outcomes:

With successful completion of this course, students will:

1. Improved critical thinking
2. New learning from Ancient India

Textbooks:

T.R.N. Rao, Subhash Kak, *Computing in Ancient India*, The Centre for Advanced Computer Studies, University of Southwestern Louisiana, 1998, ISBN 0-9666512-0-0

Savitribai Phule Pune University

BSc(Cyber and Digital Science)

Skill Enhancement Course

SEC 101 CDS Fundamentals of Digital Communication

(Practical)

Teaching Scheme	No. of Credits	Examination Scheme
Practical:4 hours / week	2	CA: 20 marks UA: 30 marks

Prerequisite: Students are expected to know the concepts studied in following course:

1. Analogue and Digital Communication
2. Electronics Devices and circuits
3. Mobile communication

Course Objectives:

- To make the student familiar with electronic components
- To learn the steps in electronic circuits through simulation and hardware implementation.
- To learn about various wireless & cellular communication networks.
- To make students familiar with mathematical interpretation related to the fundamentals of analog and digital communication systems.
- To impart knowledge regarding concepts of AM, FM modulation and detection.

Course Outcomes:

- On completion of the course, students will be able to interpret and summarize the specifications of different passive, active and Integrated components required to build electronic circuits.
- To solve problems on Number systems and their representation
- To familiarize with logic gates and applications in combinational and sequential circuits.
- To identify the importance of different blocks in electronic communication systems.
- Understand the working principles of mobile networks and Contrast different types of telecommunication networks.

Assignment : 1 Introduction to Basic components of Electronics.

1. Introduction to electronics, analog and digital communication, Introduction to active and passive components (Registers, capacitors, Inductor, Switch, Transformer, Diode ,etc..) Identify, measure value

Assignment :2 Introduction to Devices for electronics measurements

1. Difference between device and components, Different electronics measurement devices CRO , Function Generator, DMM and its functions.

Assignment :3 Study of Logic Gates (Verification of Truth tables)

1. Introduction, Logic Gates: AND, OR, NOT, NOR, NAND gates, symbols and their Truth tables.

Assignments :4 Study of Half Adder and Full Adder using Logic Gates.

1. Combinational Circuits :Implementation of half adder, full adder

Assignment :5 Study of Decimal to BCD/ (Binary) Converter.

1. Number Systems: Decimal, Binary, Octal, Hexadecimal, Binary Coded Decimal number,inter-conversions.

Assignment :6 Study of read and write action of RAM

1. Introduction to memory, types Volatile , non volatile , RAM, ROM, Implementation of RAM

Assignment:7 Study of Amplitude Modulation

1. Elements of Communication system, Types of communication: simplex, half duplex, full duplex,baseband and broadband, Serial communication: asynchronous and synchronous, Modulation ,types(AM)

Assignment:8 Study of Pulse code Modulation

1. Need of modulation and demodulation, Digital Modulation technique-PCM.

Assignment :9 Error detection and correction using Hamming Code

1. Error detection, Error correction methods, hamming code, limitation

Assignment :10 Study of Mobile hardware (Study Experiment)

1. Basic block diagram of mobile hardware, applications of each block

Assignment :11 Mobile communication(GSM)(Study Experiment)

1. Basic cellular systems, cells, Concept of frequency reuse channels, Handoff GSMsystem architecture

Text Books:

1. Modern Digital and Analog Communication Systems, B.P. Lathi and Z. Ding (adapted by H. M. Gupta) Oxford University Press 4th Edition.
2. Communication Systems, Simon Haykin, John Wiley and Sons, 4th Edition
3. Principles of Communication Systems, Herbut Taub, Donald L. Schilling and Goutam Saha, Tata McGraw Hill, 4th Edition.

Reference Books:

1. Digital Communications: Fundamentals and Applications, Bernard Sklar, PHPTR NJ.
2. Analog and Digital Communication, T.L. Singal, McGraw Hill Education.
3. Modern Digital Electronics | 5th Edition. R P Jain

Open Elective

Savitribai Phule Pune University
F.Y.B.Sc.(Cyber and Digital Science)
Subject Code : OE101CDS
Subject : Office Automation I

Teaching Scheme	**No. of Credits :** 2	**Examination Scheme**
2 hours / week		CE: 20 marks EE: 30 marks

Prerequisites :
1. Basic Computer Awareness
2. Fundamental Operating System Knowledge
3. Basic Internet Skills

Course Objectives :-

- To introduce basic office automation tools
- To develop document creation and formatting skills
- To perform data handling using spreadsheets
- To understand presentation tools
- To enhance digital office productivity skills

Course Contents

Unit 1	**Introduction to Office Automation**	**6 hours**

Concept of Office Automation ,Types of Office Automation Tools
Introduction to Operating System (Windows/Linux basics) ,
File Management: Create, Rename, Delete, Copy, Move files
Basics of GUI and Desktop Environment
Introduction to Office Suites (MS Office / LibreOffice / Google Workspace)

Unit 2	**Word Processing (MS Word)**	**6 Lecture**

Introduction to Word Processing Software
Creating, Saving, Opening Documents
Editing Text (Cut, Copy, Paste, Find, Replace)
Formatting:
Font, Paragraph, Alignment

Bullets & Numbering

Page Setup (Margins, Orientation, Size)
Insert:
Tables, Images, Shapes

Header, Footer & Page Number **Printing Documents**		
Unit 3	**Spreadsheet (MS Excel)**	**6 Lectures**
Introduction to Spreadsheet Workbook & Worksheet concepts Data Entry and Editing Formatting Cells (Number, Alignment, Font) Basic Formulas: SUM, AVERAGE, COUNT, MIN, MAX Cell Referencing (Relative & Absolute) Creating Charts (Bar, Pie, Line) Sorting and Filtering Data		
Unit 4	**Presentation Tools (MS PowerPoint)**	**6 Lectures**
Introduction to Presentation Software Creating Slides and Layouts Adding Text, Images, Audio, Video Slide Formatting and Themes Transitions and Animations Slide Show Setup Preparing Professional Presentations		
Unit 5	**Internet & Online Office Tools**	**6 Lectures**
Basics of Internet and Web Browsers Search Techniques (Google Search Tips) Email: Creating Email Account Sending, Receiving, Attachments Introduction to Cloud-based Tools: Google Docs Google Sheets Google Slides Online Collaboration and Sharing **Cyber Safety in Office Work**		

Reference Books:

1. **Microsoft Office 365 Step by Step – Joan Lambert**
2. **Computer Fundamentals and Office Automation – S. K. Basandra**
3. **Introduction to Computers – Peter Norton**
4. **MS Office Complete Reference – BPB Publications**
5. **Practical Computer Literacy – June Jamrich Parsons**

E-Books and Online Learning Material

1. Microsoft Learn (Official Tutorials)
2. NPTEL – Computer Fundamentals Courses
3. Spoken Tutorial – IIT Bombay (Office Tools)
4. LibreOffice Official Documentation
5. TutorialsPoint – MS Office

Savitribai Phule Pune University
F.Y. B.Sc.(Cyber and Digital Science)
Subject Code : OE102CDS
Subject : Introduction to Google Tools I

Teaching Scheme	**No. of Credits**	**Examination Scheme**
2 hours / week	2	CE: 20 marks EE: 30 marks

Prerequisites :
1. Basic Computer Awareness
2. Fundamental Operating System Knowledge
3. Basic Internet Skills

Course Objectives:-

- To introduce students to cloud-based tools
- To develop skills in using Google Workspace applications
- To enable collaboration and online document management
- To improve digital productivity and communication
- To understand secure usage of online tools

Course Contents

Unit 1	**Introduction to Google Workspace**	**6 hours**

Introduction to Cloud Computing
Overview of Google Workspace
Creating and Managing Google Account
Navigating Google Workspace Interface
Introduction to Google Drive
File Upload, Download, Organization (Folders)

Unit 2	**Google Docs**	**6 Lecture**

Introduction to Google Docs
Creating and Editing Documents
Text Formatting (Font, Paragraph, Alignment)
Insert:

Tables, Images, Links

Page Setup and Printing
Sharing and Collaboration (Comments, Suggestions)

Unit 3	**Google Sheets**	**6 Lectures**

Introduction to Google Sheets
Data Entry and Formatting
Basic Formulas:
SUM, AVERAGE, COUNT
Creating Charts
Sorting and Filtering Data
Sharing and Collaborative Editing

Unit 4	Google Slides	6 Lectures

Introduction to Google Slides
Creating Presentations
Adding Text, Images, Audio, Video
Themes and Layouts
Transitions and Animations
Presenting and Sharing Slides

Unit 5	Google Forms & Communication Tools	6 Lectures

Introduction to Google Forms
Creating Forms and Surveys
Question Types and Validation
Collecting and Viewing Responses
Introduction to Gmail
Sending Emails with Attachments
Basics of Online Collaboration & Cyber Safety

Reference Books:

1. **Google Workspace for Beginners** – Tech Demystified
2. **Cloud Computing Basics** – Rajkumar Buyya
3. **Internet & Web Technologies** – Uttam K. Roy
4. **Computer Fundamentals** – P.K. Sinha
5. **Digital Literacy and Computer Applications** – Ramesh Bangia

E-Books and Online Learning Material

1. Google Workspace Learning Center
2. NPTEL – Cloud Computing Courses
3. Spoken Tutorial IIT Bombay – Google Tools Tutorials
4. Tutorials Point – Google Docs/Sheets
5. Coursera – Google Workspace Courses

SEM-II

Savitribai Phule Pune University
F.Y.B.Sc.(Cyber and Digital Science)
Subject Code : CDS151MJ

Subject :Fundamentals of Cyber Security

Teaching Scheme	No. of Credits 2	Examination Scheme
2 hours / week		CE: 20 marks EE: 30 marks

Prerequisites

1. **Computers Basics**
2. **Basics of networking**

Course Objectives: -

- To prepare students with the technical knowledge and skills needed to protect and defend computer systems and networks.
- To develop students can identify the current Computer security and breaches

Course Outcomes: - Student will be able to: -

- Analyze and evaluate the cyber security needs of an organization.
- Measure the performance and troubleshoot cyber security systems.
- To introduce the current cyber related activities

Course Contents

Chapter 1	**Introduction to Cybersecurity**	**5 hours**

Overview of Cybersecurity
Definition and significance of cyber security Evolution and historical context of cyber security
Cyber Threat Landscape
Understanding the current threat landscape
Types of cyber threats: malware, phishing, ransomware, etc.
Key Principles of Cybersecurity
Confidentiality, integrity, availability (CIA Triad)Defense-in-depth and layered security
Risk Management in Cybersecurity
Identifying and assessing cyber security risks Strategies for risk mitigation and management
Legal and Ethical Considerations
Overview of cyber security laws and regulations Ethical responsibilities in cybersecurity

Chapter 2	**Basics of Networking and Security**	**8 hours**

Networking Fundamentals
Introduction to networking concepts Basics of TCP/IP and network protocols
Common Network Attacks
Types of network attacks: eavesdropping, man-in-the-middle, DoSReal-world examples and case studies
Network Security Technologies
Firewalls, intrusion detection/prevention systems (IDS/IPS)Virtual Private Networks (VPNs) for secure communication
Wireless Network Security
Risks associated with wireless networks
Securing Wi-Fi networks against unauthorized access
Securing Network Devices
Best practices for securing routers, switches, and other devicesImplementing access controls and monitoring

Chapter 3	Operating System Security	8 hours

Basics of Operating System Security Key security features in operating systems User account management and access controls
Patch Management
Importance of software updates
Strategies for effective patch management
Antivirus and Anti-malware Protection
Role of antivirus software in Cyber security Evaluating and selecting antivirus solutions
Encryption and Secure Boot
Securing data through encryption Ensuring a secure boot process
Endpoint Security

Chapter 4	Web Security	5 hours

Web Application Security Basics
Common vulnerabilities in web applications Best practices for secure coding
Secure Web Browsing
Safe browsing habits and precautions
Recognizing and avoiding phishing attacks
HTTPS and SSL/TLS
Importance of encrypted communication on the web
Configuring and implementing SSL/TLS for websites

Web Security Tools and Testing
Introduction to web security tools (e.g., OWASP ZAP)
Conducting security assessments and penetration testing

Web Security Policies and Compliance
Developing and enforcing web security policies
Compliance with industry standards (e.g., PCI DSS)

Chapter 5	**Security Best Practices and Emerging Trends**	**4 hours**

Security Awareness and Training
Importance of cybersecurity education
Creating a security-aware organizational culture

Incident Response and Management
Developing an incident response plan
Conducting incident response exercises and simulations

Cloud Security Fundamentals
Understanding security considerations in cloud environments
Shared responsibility model and best practices

Threat Intelligence and Information Sharing
Role of threat intelligence in cyber security
Participating in information sharing communities

Future Trends in Cybersecurity
Exploring emerging technologies and challenges
Continuous learning and adapting to evolving threats

Reference Books:

1. Computer Security Basics by by Rick Lehtinen , Publisher : O'Reilly Media; 2nd edition (23 June 2006); CBS PUBLISHERS & DISTRIBUTORS PVT. LTD 01149347068, ISBN-10 : 0596006691, 978-0596006693.

2. Fundamentals of Computer Security by Josef Pieprzyk ,Thomas Hardjono ,Jennifer Seberry , Publisher : Springer; Softcover reprint of hardcover 1st ed. 2003 edition (1 December 2010), ISBN : 3642077137, 978-3642077135.

CDS-152 MJ : Network Security		
Teaching Scheme 2 Lectures / week	**No. of Credits:2**	**Examination Scheme** CE :20 marks EE: 30 marks

Prerequisites: Computer Fundamentals and Networking

Course Objectives: -

1. To prepare students with basic networking concept.
2. To understand process of data communication using protocols and standards
3. To learn various topologies and applications of network.
4. To understand the concept of network layer, transport layer and application layer

Course Outcomes: - Student will be able to :-

1. Understand the concept of OSI Reference Model and TCP/IP.
2. To know the components of the Network Security.
3. Understand top down approach of data communication from one user to another user
4. To detect the IP address and route.

Course Contents

Unit 1	Network Fundamental and Security	Lectures 10

Introduction to OSI Model with all layers
TCP/IP Protocol Suite
Introduction Attacks on Computers and Computer Security
Need for Security,Security Attacks (Active and Passive attacks) , Services and Mechanisms Network Security, Network Security Model, Internet Standards and RFCs , Symmetric Key Cryptography, Introduction to Modern Symmetric Key Ciphers- DES, Blowfish, IDEA, AES, RC5, Modes of operation of Modern Symmetric Key Ciphers, Asymmetric Key Cryptography – RSA, Digital signatures and Digital Certificates, Certificate Authority and key management Kerberos, X.509 Directory Authentication Service.

Unit 2	User Authentication and security at Application and Transport Layer	Lectures 6

Pretty Good Privacy (PGP) and S/MIME.
User Authentication
Remote User-Authentication Principles, Remote User-Authentication Using Symmetric Encryption, Remote User-Authentication Using Asymmetric Encryption.

Application Layer Security:
Email privacy: PGP and S/MIME , SSL Architecture –Handshake ,Change Cipher Space, Alert And Record Protocols, SSL Message Formats – Transport Layer Security
Transport Level Security:
Transport Layer Security, HTTPS, Secure Shell (SSH)

Unit 3	Network Layer Security and IP Security	Lectures 8

Network Layer Security:
Modes – Two Security Protocols , Security Association, Security Policy, Internet Key Exchange System Security: Description , Buffer Overflow And Malicious Software(Viruses and Related Threats, Virus Counter measures,) , Malicious Programs
IP Security: Overview of IP Security (IPSec) , IP Security Architecture, Modes of Operation Security Associations (SA), Authentication Header (AH) , Encapsulating Security Payload (ESP), Internet Key Exchange

Unit 4	Firewall And security in Mobile and IoT	Lectures 7

Firewalls: The Need for firewalls, Firewall Characteristics, Types of Firewalls
Firewall Design principles, Trusted Systems, Intruders, Intrusion Detection Systems.
Firewall Biasing, Firewall location and configuration, Virtual Private Networks
Security In Mobile And Iot: Security and Threats To SDN, Cloud Security
Security Issues and Risks, Data Protection, Security As A Service, Addressing Cloud Security
IOT, Security Framework

Reference Books:

1. Behrouz A Forouzan, Cryptography and Network Security , McGraw-Hill Education, 2011
2. Network Security and Cryptography: Bernard Menezes, CENGAGE Learning
3. William Stallings, Network Security Essentials: Applications and Standards, Prentice Hall India, 4th Edition
4. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud" William Stallings Publisher: Addison-Wesley 2015
5. William Stallings, Cryptography and Network Security: Principles and Standards, Prentice Hall India, 3rd Edition, 2003

Savitribai Phule Pune University
F.Y.B.Sc. (Cyber and Digital Science)

Subject Code: CDS153MJ
Subject: Python Programming

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / week	2	CE: 20 Marks UE: 30 Marks

Prerequisites:

- Knowledge of procedure oriented programming language.

Course Objectives:

1. To define the structure and components of a Python program.
2. To acquaint with data types, input/output statements, decision making, looping and functions in Python.
3. To learn how to use Lists, Tuples, Sets and Dictionaries in Python programs.
4. To design object- oriented programs using classes in Python.

Course Outcomes:

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

1. Devise algorithms, implement, test, debug and execute programs in the Python language.
2. Demonstrate Python programming skills for problems that require the writing of well documented programs including use of the logical constructs of the language.
3. Apply the problem-solving skills using different data structures in Python.
4. Develop an application using functions, classes and built-in modules of Python.

Course Contents

Chapter 1	**Fundamentals of Python Programming**	**6 hours**

Introduction to Python
Features and Applications of Python
Comments, identifiers and reserved words in Python
Data types in Python, Data type conversion
Python print function and input function
Python operators (arithmetic, comparison, assignment, bitwise, logical, Membership,identity), operator precedence
Indentation in Python
Conditional Statements, loop statements, control statements (break, continue, pass)

Chapter 2	**Built-in Data Structures in Python**	**8 hours**

Python List - concept, declaration, inserting, updating, deleting and accessing elements, built-in operators and functions, indexing and slicing elements
Python Tuple - concept, creating and accessing elements, Tuple operators and built-in Tuple functions
Python Set - concept, declaration, inserting, updating, deleting and accessing elements, Set operations
Python Dictionary - concept, declaration, inserting, updating, deleting elements and

different ways of accessing Dictionary elements, built-in functions, Dictionary properties
Python data structure conversion

Chapter 3	Strings and Arrays	6 hours

Concept of String
Types of String (Single quotes, Double quotes, Triple quotes) Creating and accessing String
String operators
Python standard String handling functions Concept of Array
Creating and accessing Array elements
Array Operations (Traverse, Insertion, Deletion, Search and Update) Built-in Array methods

Chapter 4	Functions and Object Oriented Concepts	6 hours

Defining and calling function
Function arguments - required arguments, default arguments, keyword arguments, variable- length arguments
Scope of variable - basic rules
Order of arguments (positional & keyword) void function and lambda functions Recursion
Object oriented programming concept
Python Classes and Objects, accessing members Python Constructor
Data hiding
Class variables, instance variables, class methods and static methods

Chapter 5	Introduction to Python modules and Libraries	4 hours

Introduction to built in modules in Python(OS, random, math, datetime, calendar, sys, collections, statistics)
Introduction to Python libraries (NumPy, Pandas, Matplotlib)

Reference Books:

1. Beginning Python: From Novice to Professional, Magnus Lie Hetland, Apress
2. Beginning Programming with Python for Dummies Paperback – 2015 by John Paul Mueller

E-Books and Online Learning Material

1. https://www.javatpoint.com/python-tutorial
2. https://www.tutorialspoint.com/python/index.htm
3. https://www.geeksforgeeks.org/python-programming-language/

Savitribai Phule Pune University
F.Y.B.Sc.(Cyber and Digital Science)
Practical course based on CDS151MJ

Fundamentals of Cyber Security
(CDS154MJP)

Teaching Scheme	No. of Credits	Examination Scheme
4 hours / week	2	CE: 20 marks EE: 30 marks

Course Objectives: -

1. To prepare students with the technical knowledge and skills needed to protect and defend computer systems and networks.
2. To develop students can identify the current Computer security and breaches

Course Outcomes: - Student will be able to: -

1. Understand and explore the basics of Computer Networks and Various Protocols
2. Administrate a network and schedule flow of information .
3. Examine the network security issues in Mobile and ad hoc networks.
4. Demonstrate the TCP/IP and OSI fashions with merits and demerits.
5. Evaluate the shortest path by using Routing algorithms.

Course Contents

Practical Assignment 1: Network Security Basics:

1. Set up a basic network topology using virtualization software.
2. Implement and configure a firewall to control incoming and outgoing traffic.
3. Use network monitoring tools to identify and analyze network activities.

Practical Assignment 2: Operating System Security

1. Harden the Windows/Linux operating system by configuring user accounts and access controls.
2. Implement security measures such as enabling firewalls and updating system patches.
3. Use antivirus software to scan for and remove potential threats.

Practical Assignment 3: Web Security

1. Identify and fix common vulnerabilities in a web application (e.g., SQL injection, cross-sitescripting).
2. Configure SSL/TLS for a website to ensure secure communication.
3. Use web security tools like OWASP ZAP to perform security assessments.

Practical Assignment 4: Wireless Network Security

1. Secure a Wi-Fi network by implementing WPA2/WPA3 encryption.
2. Configure a wireless intrusion detection system (WIDS) to monitor wireless traffic.
3. Investigate and respond to a simulated wireless security incident.

Practical Assignment 5: Endpoint Security

1. Install and configure endpoint security solutions on different operating systems.
2. Conduct malware analysis on a provided sample and propose mitigation strategies.
3. Implement and test device encryption on a selected device.

Practical Assignment 6: Incident Response and Management

1. Develop an incident response plan for a simulated security incident.
2. Simulate a security incident and follow the incident response plan.
3. Conduct a post-incident analysis and propose improvements to the plan.

Practical Assignment 7: Security Awareness and Training

1. Design and deliver a brief security awareness presentation.
2. Create and conduct a phishing simulation to assess user awareness.
3. Evaluate the effectiveness of security training materials.

Practical Assignment 8: Security Best Practices and Emerging Trends

1. Explore and implement security best practices for cloud environments.
2. Securely configure an IoT device and assess its security.
3. Research and present on emerging trends in cybersecurity.

Reference Books:

1. Computer Security Basics by by Rick Lehtinen , Publisher : O'Reilly Media; 2nd edition (23 June 2006); CBS PUBLISHERS & DISTRIBUTORS PVT. LTD 01149347068, ISBN-10 : 0596006691, 978-0596006693.
2. Fundamentals of Computer Security by Josef Pieprzyk ,Thomas Hardjono ,Jennifer Seberry , Publisher Springer; Softcover reprint of hardcover 1st ed. 2003 edition (1 December 2010), ISBN : 3642077137,978-3642077135.

Savitribai Phule Pune University
F.Y.B.Sc.(Cyber and Digital Science)
Practical course based on CDS152MJ

Network Security (CDS155MJP)

Teaching Scheme	No. of Credits	Examination Scheme
4 hours / week	2	CE: 20 marks EE: 30 marks

Course Contents

Course Objectives: -

To prepare students with basic networking concept.
To understand process of data communication using protocols and standards
To learn various topologies and applications of network.
To understand the concept of network layer, transport layer and application layer

Course Outcomes: - Student will be able to :-

Understand the concept of OSI Reference Model and TCP/IP.
To know the components of the Network Security.
Understand top down approach of data communication from one user to another user
To detect the IP address and route.

Assignment No 1: Implement following commands in Linux in python and write their output :

1. hostname
2. hostname–d
3. hostname –f
4. hostname–I
5. ping
6. netstat
7. netstat –a
8. dig
9. host
10. netstat –at
11. netstat–au
12. netstat –l

Assignment No 2: Implement following commands in Linux in python and write their output :

1. netstat–lt
2. netstat–lu
3. netstat–s
4. netstat–st
5. iwconfig
6. netstat –su
7. traceroute,tracepath
8. ifconfig
9. ifconfig–a
10. ifconfigeth()

11. nslookup
12. telnet

Assignment No 3:Study the following Network Devices in Detail and write their functions:

1. Repeater
2. Hub
3. \Switch
4. Bridge
5. Router
6. Gateway

Assignment No *04 :* Study of LAN environment:

Study the concept of MAC addresses, IP addresses.

A. Find out in formation about the network in your lab and fill in details below:

1. Total Number of computers in your lab:
2. Finddetailsofany5computers:

MAC address	IPaddress	LANspeed	hostname

1. Are the IP addresses assigned to the machines statically or dynamically?
2. Does the network have a DHCP server?
3. If yes, what is the address of the server?

Assignment No 5 Router Basic Commands and Security Configuration

1. CISCO IOS Configuration Router Basic Commands
2. Security Configuration, Operation and Verification in IOS,
3. Running and Start-up Configuration.

Assignment No 6 Static Routing

1. Configure Static Routing Configuration in Sample Network

Assignment No 7 Dynamic Routing using Protocols

1. Configuring Dynamic Routing using RIPv1 and RIPv2 Protocol
2. Configuring Dynamic Routing using OSPF Protocol

Assignment No 8 Remote Management using Network Protocols

1. Configuring and Verifying TELNET and SSH

Assignment No 9 Switch Configuration

1. Configure and verify Switch Configuration
2. Configuring and verifying Access Control List.

Assignment No 10 Data Encryption

1. Encrypt data using Cryptographic Tools –Truecrypt
2. Implementation of Stegnography

Assignment No 11 Network Security Configuration

1. Configuring Firewall
2. Configuring VPN

Reference Books:

1. Behrouz A Forouzan, Cryptography and Network Security , McGraw-Hill Education, 2011
2. Network Security and Cryptography: Bernard Menezes, CENGAGE Learning
3. William Stallings, Network Security Essentials: Applications and Standards, Prentice HallIndia, 4th Edition
4. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud" William Stallings Publisher: Addison-Wesley 2015
5. William Stallings, Cryptography and Network Security: Principles and Standards, PrenticeHall India, 3rd Edition, 2003

Savitribai Phule Pune University
F.Y. B.Sc.(Cyber and Digital Science)
Practical course based on CDS153MJ

Python Programming (CDS156 MJP)

Teaching Scheme 4 hours / week	No. of Credits2	Examination Scheme CE: 20 marks EE: 30 marks

Course Contents

Course Objectives:

1. To define the structure and components of a Python program.
2. To learn how to use Lists, Tuples, Sets and Dictionaries in Python programs.
3. To design object oriented programs using classes in Python.

Course Outcomes:

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

1. Devise algorithms, implement, test, debug and execute programs in the Python language.
2. Apply the problem-solving skills using different data structures in Python.
3. Develop an application using functions, classes and built-in modules of Python.

Assignment 1: Write a Python program to:

1. Get a string from a given string where all occurrences of its first character have been changed to '$', except the first character itself.

Assignment 2: Write a Python program to:

1. Change a given string to a new string where the first and last characters have been exchanged.

Assignment 3: Write a Python program to:

1. Remove the nth index character from a non-empty string.

Assignment 4: Write a Python program to:

1. Sort(ascending and descending) dictionary by value.

Assignment 5: Write a Python program to:

1. Shuffle and print a specified list.

Assignment 6: Write a Python program to:

1. Merge two python dictionaries.

Assignment 7: Write a Python program to:

1. Accept a string and calculate the number of digits, letters and other characters.

Assignment 8: Write a Python program to:

1. Write a program that takes two digits m(row) and n(column) as input and generates a two-dimensional array. Read the elements and display the array.

Assignment 9: Write a Python program to:

1. Write a program that accepts a range of numbers (n to m) and list down all the even/odd numbers to be printed in a comma separated sequence.

Assignment 10: Write a Python program to:

1. A function that generates all the factors of a number.

Assignment 11: Write a Python program to:

1. Function to find the sum of digits of a number.

Assignment 12: Write a Python program to:

1. Function to find GCD/LCM of 2 numbers.

Assignment 13: Write a Python program to:

1. Function to concatenate two strings.

Assignment 14: Write a Python program to:

1. Program to display Fibonacci series using recursion.

Assignment 15: Write a Python program to:

1. Convert decimal to binary using recursion.

Assignment 16: Write a Python program to:

1. Calculate the number of upper-case letters and lower-case letters in a string. Import the module to calculate number of upper-case letters and lower-case letters from a string input by the user.

Assignment 17: Write a Python program to:

1. Take a list and return a new list with unique elements of the first list. Import the module and input a list to find the unique elements in a list.

Assignment 18: Write a Python program to:

1. Capitalize each word in a file.

Assignment 19: Write a Python program to:

1. Delete comment lines from a file.

Assignment 20: Write a Python program to:

1. Search a word and replace with another word for all the occurrences.

Assignment 21: Write a Python program to:

1. A program to read a file in reverse order. The last sentence should be read first and continue till the first sentence is read.

Assignment 22: Write a Python program to:

1. Insert a sentence into a specified position of a file

Reference Books:

1 Beginning Python: From Novice to Professional, Magnus Lie Hetland, Apress
2 Beginning Programming with Python for Dummies Paperback – 2015 by John Paul Mueller

E-Books and Online Learning Material

1 https://www.javatpoint.com/python-tutorial
2 https://www.tutorialspoint.com/python/index.htm

Savitribai Phule Pune University
F.Y.B.Sc.(Cyber and Digital Science)
Subject Code : SEC151CDS
Subject : Statistical techniques for Computer Science

Teaching Scheme	No. of Credits	Examination Scheme
4 hours / week	2	CE: 20 marks EE: 30 marks

Prerequisites

1. To get good idea to brush up on the foundational knowledge you'll need in the course and you may refresh your algebraic skills in advance

Course Objectives: -

1. To tabulate and make frequency distribution of the given data.
2. To use various graphical and diagrammatic techniques and interpret.
3. To compute various measures of central tendency, dispersion,
4. To compute the relation between variables and prediction values using correlation and regression.

Course Outcomes: - Student will be able to: -

1. Handling raw data and understand the nature of the data
2. How to represent data by graphical methods.
3. Install and configure system services.
4. Predict the values in correlation & regression and interpret to take decision.

Course Contents

Chapter 1	**Data Condensation and Presentation of Data**	**7 hours**

Raw data, variable, discrete variable, continuous variable, constant, attribute with illustration. Classification, methods of classification.
Frequency Distribution - Discrete and Continuous frequency distribution.
Graphs & Diagrams - Histogram, Frequency polygon, Frequency curve, Pie-Diagram, Bar Diagram, Multiple bar Diagram, Sub-divided bar diagram, Percentage bar diagram.
Construction of frequency distribution, diagrams and graphs using MS Excel/python.

Chapter 2	**Measures of Central Tendency**	**8 hours**

Concept and meaning of Measure of Central Tendency, Requirements of good Measure of Central Tendency.
Arithmetic Mean (A.M) for discrete and continuous frequency distribution, Merits & Demerits
Median for discrete and continuous frequency distribution, Merits & Demerits
Mode for discrete and continuous frequency distribution, Merits & Demerits
Empirical Relation between mean, median and mode.
Measures of central tendency using MS Excel/python. Numerical Problems.

Chapter 3	**Measures of Dispersion**	**7 hours**

Concept and meaning of Measure of dispersion, Requirements of good Measure of dispersion.
Types of Measure of Dispersion- Absolute & Relative Measure
dispersion Range, Coefficient of Range
Standard Deviation (S.D.), Variance, Coefficient of Variation (C.V)
Measures of dispersion using MS Excel/Python
Numerical Problems

Chapter 4	**Correlation & Regression Analysis (for bivariate data)**	**8 hours**

Concept and meaning of Correlation, Types of correlation.
Methods to study Correlation: Scatter Diagram, Karl- Pearson correlation
coefficient Numerical Problems on Correlation
Concept and meaning of regression, lines of regression equation of Y on X and X on Y.
Regression coefficients, properties of regression coefficients
Correlation, Regression using MS Excel/Python
Numerical problems on Regression.

Reference Books:

1. Statistical Methods, George W. Snedecor, William G, Cochran, John Wiley &sons
2. Fundamentals of Applied Statistics (3rd Edition), Gupta and Kapoor, S.Chand and Sons, New Delhi, 1987.
3. Draper, N. R. and Smith, H. (1998). Applied Regression Analysis, John Wiley, ThirdEdition

E-Books and Online Learning Material

1. http://eclm.unipune.ac.in/Search.aspx?subid=480&catid=1 .
2. http://ndl.iitkgp.ac.in/

Savitribai Phule Pune University
F.Y.B.Sc.(Cyber and Digital Science)

Subject Code : SEC151CDS
Subject : Advance Excel

Teaching Scheme	No. of Credits	Examination Scheme
4 hours / week	2	CE: 20 marks EE: 30 marks

Prerequisites

1. Understanding and using the AutoFilter feature
2. Knowing what a PivotTable is and how to build one

Course Objectives: -

1. Acquire knowledge of data validation, conditional formatting, and charting techniques to improve data visualization.
2. Develop advanced Excel skills to enhance efficiency and reduce risk in data management and analysis.

Course Outcomes: - Student will be able to: -

1. Creation, management, and formatting pivot tables and pivot charts
2. Students will be able to Create pivot tables and pivot charts.

Course Contents

Chapter 1	**Advanced Functions and Formulas**	**5 hours**

Introduction to Advanced Excel Functions*
Overview of advanced functions: VLOOKUP, HLOOKUP, INDEX, MATCH, OFFSET,etc.
Application scenarios for each function. Nested Functions and Formula Auditing*
Creating nested functions for complex calculations.
Utilizing the Formula Auditing tools for error checking and tracing.Array Formulas*
Understanding array formulas and their applications. Building and using array formulas for efficient data analysis.
Data Validation and Dynamic Lists* Implementing data validation rules for data accuracy.
Creating dynamic dropdown lists for enhanced data entry.Practical Assignment: Advanced Functions*
Solve real-world business problems using advanced Excel functions. Design and implement formulas for data analysis and decision-making.

Chapter 2	**Data Analysis and Pivot Tables**	**8 hours**

Importing and Transforming Data Importing data from external sources.
Transforming and cleaning data using Power Query.
Pivot Tables Basics*
Introduction to Pivot Tables and Pivot Charts. Creating basic Pivot Tables for data summarization.Advanced Pivot Table Techniques*
Grouping and filtering data in Pivot Tables. Using calculated fields and items for custom calculations.Slicers and Timelines* Creating and using slicers for interactive data analysis.Implementing timelines for date-based filtering.
Practical Assignment: Data Analysis with Pivot Tables* Analyze a dataset using Pivot Tables and advanced techniques.
Create dynamic dashboards with multiple Pivot Tables and visualizations.

Chapter 3	**Advanced Data Visualization**	**8 hours**

Conditional Formatting*
Applying advanced conditional formatting rules. Creating heatmaps and data bars for visual analysis.
Sparklines and Trendlines*
Implementing sparklines for compact data visualizations.Adding trendlines to analyze data trends.
Custom Charts and Graphs*
Creating custom charts with advanced formatting options.Combining different chart types in a single chart.
Power View and Power Map*
Introduction to Power View for interactive data exploration.Utilizing Power Map for geographical data visualization.
Practical Assignment: Data Visualization Project*
Design and implement a comprehensive data visualization project.
Present insights using advanced Excel charts and visualizations.

Chapter 4	**Excel Automation with Macros**	**5 hours**

Introduction to Macros and VBA*
Overview of Excel Macros and Visual Basic for Applications (VBA).Recording and editing basic macros.
Variables and Control Structures in VBA*Declaring and using variables in VBA.
Implementing control structures: loops and conditional statements.User Forms and Interactivity*
Creating user forms for data input.Adding interactivity to macros.
Error Handling and Debugging*
Implementing error handling in VBA. Debugging and troubleshooting macros.
Practical Assignment: Macro Automation Project*
Develop and implement a macro to automate a specific business process.Test and debug the macro for efficiency.

Chapter 5	**Advanced Excel Tips and Tricks**	**4 hours**

Excel Shortcuts and Productivity Hacks*
Essential keyboard shortcuts for efficient Excel usage.Productivity hacks for everyday tasks.
Advanced Data Validation Techniques* Dynamic data validation using named ranges.
Creating cascading dropdown lists for complex data entry.
Advanced Charting Techniques* Advancedformatting options for Excel charts.
Creating combination charts and dual-axis charts.
Collaborative Editing and Review* Enabling and using track changes in Excel.
Collaborative editing with multiple users.
Practical Assignment:
Excel Mastery Project*
Apply advanced Excel skills to solve a complex problem or analyze a substantial dataset.
Present the findings using a combination of charts, formulas, and data visualizations

Reference Books:

1. Mastering Advanced Excel, by published by BPB Publications ,ISBN NO: 935551865X, 978-9355518651
2. Advanced Excel with VBA Macros, by Swarup Das, publisher Blue Rose Publishers; 1st edition(6 October 2020), ISBN NO: 9390380316 , 978-9390380312.

E-Books and Online Learning Material

3. https://trumpexcel.com/learn-excel/-- Learn Excel.

Open Elective

Savitribai Phule Pune University
F.Y.B.Sc.(Cyber and Digital Science)
Subject Code : OE152CDS
Subject : Office Automation II

Teaching Scheme	**No. of Credits**	**Examination Scheme**
2 hours / week	2	CE: 20 marks EE: 30 marks

Prerequisites :

1. Basic Computer Awareness
2. Fundamental Operating System Knowledge
3. Basic Internet Skills

Course Objectives:-

1. To develop advanced skills in office automation tools
2. To apply automation techniques in documents and spreadsheets
3. To enhance data analysis and reporting skills
4. To introduce collaborative and cloud-based working
5. To improve professional productivity

Course Contents

Unit 1	**Advanced Word Processing**	**6 hours**

Styles and Themes
Templates and Document Formatting
Mail Merge (Letters, Labels, Emails)
Table of Contents and Index
Track Changes and Comments
Document Protection and Security

Unit 2	**Advanced Spreadsheet Techniques**	**6 Lecture**

Advanced Functions:

IF, VLOOKUP, HLOOKUP

COUNTIF, SUMIF

Data Validation
Conditional Formatting
Pivot Tables and Pivot Charts
What-if Analysis (Goal Seek)
Data Protection and Sheet Security

Unit 3	Database Handling in Spreadsheet	6 Lectures
Creating and Managing Data Tables Sorting and Advanced Filtering Subtotals and Grouping Data Forms Import/Export Data Introduction to Data Analysis Tools		
Unit 4	**Advanced Presentation Tools**	**6 Lectures**
Slide Master and Custom Layouts Advanced Animations and Transitions Embedding Audio, Video, Hyperlinks SmartArt and Infographics Presentation Tips and Design Principles Exporting and Sharing Presentations		
Unit 5	**Cloud Computing & Office Automation Tools**	**6 Lectures**
Introduction to Cloud Computing Cloud Storage (Google Drive, OneDrive) Collaboration Tools: Real-time editing Sharing & Permissions Online Forms (Google Forms basics) Introduction to Automation Tools: Macros (basic concept) Cyber Security in Office Automation		

Reference Books:

1. **Microsoft Office 365 Step by Step** – Joan Lambert
2. **Excel 2019 Bible** – Michael Alexander & Richard Kusleika
3. **Mastering Microsoft Office** – Lonnie E. Moseley
4. **Office 2019 All-in-One for Dummies** – Peter Weverka
5. **Computer Fundamentals and Office Automation** – S. K. Basandra

E-Books and Online Learning Material

1. Microsoft Learn (Official Tutorials)
2. Google Workspace Learning Center
3. NPTEL – Digital Literacy Courses
4. LibreOffice Documentation
5. Tutorials Point – Advanced Excel & Office

Savitribai Phule Pune University
F.Y. B.Sc.(Cyber and Digital Science)
Subject Code : OE153CDS
Subject : Introduction to Google Tools II

Teaching Scheme	**No. of Credits**	**Examination Scheme**
2 hours / week	2	CE: 20 marks EE: 30 marks

Prerequisites :
1. Basic Computer Awareness
2. Fundamental Operating System Knowledge
3. Basic Internet Skills

Course Objectives:-

1. To enhance advanced skills in Google Workspace tools
2. To introduce automation and add-ons in Google applications
3. To develop collaborative and data analysis abilities
4. To use Google tools in academic and professional environments
5. To ensure secure and efficient cloud usage

Course Contents

Unit 1	Advanced Google Drive & Collaboration	**6 hours**

Advanced features of Google Drive
File sharing permissions and access control
Version history and file recovery
Managing shared drives
Offline access and synchronization
Collaboration tools and real-time editing

Unit 2	**Advanced Google Docs**	**6 Lecture**

Advanced features of Google Docs
Using Templates and Styles
Table of Contents and Document Outline
Voice Typing and Add-ons
Comments, Suggestions, and Version Control
Document publishing and sharing

Unit 3	**Advanced Google Sheets**	**6 Lectures**

Advanced features of Google Sheets
Functions:
IF, VLOOKUP, COUNTIF, SUMIF

Data Validation and Conditional Formatting
Pivot Tables and Charts
Data Analysis and Reporting
Introduction to Macros (Recording basics)

Unit 4	Advanced Google Forms & Data Handling	6 Lectures

Advanced features of Google Forms
Creating quizzes and auto-grading
Response validation and branching
Linking Forms with Sheets
Data collection and analysis
Sharing and embedding forms

Unit 5	Google Tools Ecosystem & Productivity	6 Lectures

Introduction to Google Calendar
Introduction to Google Meet
Task Management using Google Tasks
Integration between Google Tools
Introduction to Add-ons and Extensions
Cyber Security & Privacy in Cloud Tools

Reference Books:

1. **Google Workspace: The Missing Manual** – Nancy Conner
2. **Cloud Computing Concepts** – Rajkumar Buyya
3. **Mastering Google Apps** – Mark Collins
4. **Digital Literacy and Computer Applications** – Ramesh Bangia
5. **Computer Fundamentals and Applications** – P.K. Sinha

E-Books and Online Learning Material

1. Google Workspace Learning Center
2. NPTEL – Cloud & IT Courses
3. Spoken Tutorial IIT Bombay
4. Coursera – Google Workspace Courses
5. TutorialsPoint

SEM III

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

Teaching Scheme 2 Hours / week	No. of Credit 02	Examination Scheme CA : 20 marks UA: 30 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
1. Explain ethical hacking concepts and hacker types.
2. Perform reconnaissance and OSINT techniques.
3. Conduct network scanning and exploitation.
4. Analyze system vulnerabilities and hacking methods.
5. Identify and exploit web application vulnerabilities.

Unit	Course Contents	Hours	CO
1	**Introduction to Ethical Hacking**	**4**	**CO 1**

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

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

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

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)

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 Book:

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)

CDS203MJP

Title: Practical Based CDS201MJ-Ethical Hacking - I

Teaching Scheme 2 Hours / week	No. of Credit 02	Examination Scheme CA :20 marks UA: 30 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. Understanding Ethical Hacking & Lab Setup
2. Footprinting, Reconnaissance & OSINT
3. Network Scanning, Enumeration & Exploitation
4. Vulnerability Assessment & System Hacking
5. Web Application Hacking & Exploitation

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

1. Fundamentals of Ethical Hacking & Lab Configuration
2. Information Gathering & Open-Source Intelligence (OSINT)
3. Network Scanning, Attack Simulation & Exploitation
4. System Security Analysis & Vulnerability Exploitation
5. Web Security Testing & Web Application Exploitation

Unit	Course Contents	CO
Unit 1	**Introduction to Ethical Hacking & Lab Setup**	**CO 1**

Install & configure Kali Linux on VirtualBox/VMware
Set up a penetration testing lab (Metasploitable2, DVWA, Windows 10)
Learn basic Linux commands for hacking & security testing
Configure network settings for ethical hacking practice
Understand and use essential hacking tools (Nmap, Metasploit, Wireshark)

Unit 2	**Footprinting, Reconnaissance & OSINT**	**CO 2**

Perform WHOIS lookup on a target domain

Extract DNS records using nslookupand dig

Use Google Dorking to find sensitive information

Conduct passive reconnaissance using Shodan & Censys

Perform social media intelligence gathering using OSINT tools (theHarvester, Maltego)

Enumerate email addresses & phone numbers from a website

Use Recon-ng framework for automated reconnaissance

Unit 3	**Network Scanning, Enumeration & Exploitation**	**CO 3**

Perform a network scan using Nmap (TCP, UDP, SYN, FIN scans)
Enumerate open ports and running services on a target system
Perform OS fingerprinting & service detection
Scan and exploit SMB services using enum4linux & Metasploit.
Enumerate SNMP information using Nmap
Capture network packets using Wireshark
Perform ARP spoofing & Man-in-the-Middle (MITM) attack using Bettercap

Unit 4	**Vulnerability Assessment & System Hacking**	**CO 4**

Perform vulnerability scanning using Nessus/OpenVAS
Scan web applications for vulnerabilities using Nikto
Crack password hashes using John the Ripper & Hashcat
Extract Windows passwords using Mimikatz
Perform brute-force login attacks using Hydra
Exploit weak file permissions for privilege escalation (Linux & Windows)
Create a backdoor using Netcat

Unit 5	**Web Application Hacking & Exploitation**	**CO 5**

Identify OWASP Top 10 vulnerabilities in a test web application
Perform SQL Injection to extract data from a database
Exploit XSS (Reflected, Stored & DOM-Based) to steal session cookies
Perform Cross-Site Request Forgery (CSRF) attack
Exploit Local File Inclusion (LFI) & Remote File Inclusion (RFI) vulnerabilities
Crack website login using Burp Suite Intruder
Bypass Web Application Firewall (WAF) using tampered requests

Note: Perform All this topic on try hack me also for home practice

Reference Book:

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 Credit	Examination Scheme
2 Hours / week	02	CA :20 marks UA: 30 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
1. Principles of cyber ethics and apply them to real-world digital scenario
2. Identify and categorize cybercrimes while understanding the legal actions
3. Assess the role of IPR in protecting digital assets and preventing online fraud.
4. Analyze cyber security policies and frameworks implemented by governments and organizations.
5. 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
Subject: Data Structure Using Python

Teaching Scheme	No. of Credits	Examination Scheme
4 hours / week	2	CE: 20 Marks EE: 30 Marks

Prerequisites:
1. Knowledge of Python programming.
2. 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:
1. Understand fundamental data structures and their importance in problem-solving.
2. Implement, manipulate, apply and analyze linear and non-linear data structures.
3. Develop efficient algorithms by utilizing appropriate searching and sorting techniques.
4. Solve real-world problems by selecting and implementing suitable data structures in Python.
5. 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) Sem III

Sub Code: IKS-200-T

Title: Indian Knowledge System in Computing

Objective:

1. To introduce Vedic mathematical techniques and their relevance to modern computational methods.
2. To understand Nyaya's logical framework and its application in reasoning and AI.
3. To explore the algorithmic structure of Panini's grammar and Chandasastra's binary system in computational linguistics and mathematics.
4. To explore real-world applications of IKS concepts in computational sciences.

Learning Outcomes:

By the end of the course, students will:

1. Understand the computational foundations of Indian Knowledge Systems by applying Vedic mathematical techniques in problem-solving.
2. Use Nyaya's logical reasoning in AI and decision-making.
3. Explore the connection between **Panini's** grammar and NLP technologies.
4. Recognize the applications of IKS in modern computing fields.

Unit 1: Vedic Mathematics & Computational Thinking (8 Hours)

1.1 Introduction to Vedic Mathematics: Origins and importance in ancient India, Sutras and their logical foundation

1.2 Basic Arithmetic using Vedic Methods: Addition, subtraction, multiplication, and division tricks

1.3 Algebraic Applications of Vedic Mathematics: Squaring, square roots, cube roots, and factorization

Unit 2: Introduction to Nyaya (Indian Logic) (8 Hours)

2.1 Introduction to Nyaya Philosophy: Introduction to Nyaya (Indian Logic), Overview of Indian philosophical schools, Importance of Nyaya in logical reasoning, Types of reasoning (Anumana, Pramana, etc.)

2.2 Nyaya's Four Sources of Knowledge (Pramaṇa): Perception, inference, comparison, verbal testimony

2.3 Types of Argumentations in Nyaya

Vada (truth-based), Jalpa (debate-focused), Vitanda (criticism)

2.4 Applications in AI & Machine Learning**:** Logical reasoning models, expert systems, and rule-based AI

Unit 3: Panini's Astadhyayi & Chandasāstra (8 Hours)

3.1 Introduction to Panini's Astadhyayi: Historical background and linguistic importance

3.2 Rule-Based System of Sanskrit Grammar: Sutras, meta-rules, recursion, and transformations

3.3 Chandasastra's Binary logic and combinatorial techniques

Unit 4: Applications of IKS in Computer Science (6 Hours)

4.1 Mind and cognition in Samkhya and Yoga: AI insights

4.2 Machine Learning and Indian philosophies: Understanding of human cognition in Indian philosophical schools (Advaita, Samkhya and Yoga)

4.3 Cryptography and Security: Ancient cryptographic methods in Kautilya's Arthashastra, protecting information: analogies from Indian traditions.

Recommended Books:

1. Vedic Mathematics, Jagadguru Swami Bharati Krishna Tirtha, Motilal Banarsidass Publishing House, New Delhi.
2. "The Power of Vedic Maths" – Atul Gupta, JAICO publishing
3. Nyaya Theory of Knowledge" – S.C. Vidyabhusana
4. "A Primer of Indian Logic" – Kuppuswami Sastri, Hassell Street Press.2021
5. "Indian Logic: A Reader" – Jonardon Ganeri
6. "Aṣṭādhyāyī of Pāṇini" (Volumes 1 & 2) – Rama Nath Sharma, Munshirm Manoharlal publication
7. "Panini: His Work and Its Traditions" – George Cardona, Motilal Banarsidass Publishing House
8. "The Mathematics of Metre" – Satyanarayana Das
9. "Samkhya and Science" – Debabrata Sen Sharma
10. Explores the cognitive science aspects of Samkhya and Yoga in AI research.
11. "AI and Indian Philosophy" – Sangeet Kedia
12. "Kautilya's Arthashastra" – R. Shamasastry (Translation)
13. "History of Indian Cryptography" – Subhash Kak
14. Discusses coded messages, steganography, and security concepts in ancient India.
15. Saubhagya Vardhan, AI in Land of Vedas, Notion Press, 2023

	Savitribai Phule Pune University **S.Y.B.Sc. (Cyber and Digital Science)** **Subject Code: CDS 241MN** **Subject: Web Technology**	
Teaching Scheme: 2 hours / week	**No. of Credits: 2**	**Examination Scheme :** **CE: 20 Marks** **UE: 30 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:

CO1: Explain the basic concepts of the World Wide Web, HTTP protocol, and client-server architecture.
CO2: Design and structure web pages using HTML elements, forms, tables, and CSS for styling.
CO3: Develop client-side interactivity using JavaScript including event handling and string operations.
CO4: Develop server-side scripts using PHP including functions, control structures, and string manipulation techniques.
CO5: Apply array handling techniques in PHP for storing, accessing, and manipulating data efficiently.
CO6: Perform file handling operations in PHP such as reading, writing, renaming, and accessing file information.

Course Contents

Unit 1	**Introduction to Web, HTML and CSS**	**4 hours**

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
CSS- Concept, Types of CSS & ways to use CSS

Unit 2	**Introduction to JavaScript**	**6 hours**

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

Unit 3	**Introduction to PHP**	**10 hours**

3.1 Introduction to PHP
3.2 How does PHP work?
3.3 Lexical structure –Basic program, Control structure
3.4 Function - Definition and function call
3.5 Types of parameters - Default parameters , Variable parameters, Missing parameters
3.6 Variable function
3.7 Anonymous function
3.8 Printing functions
3.9 Introduction to String
3.10 Types of strings
3.11 Comparing, manipulating and searching string
3.12 Regular expressions

Unit 4	**Arrays**	**5 hours**

4.1 Types of Array
4.2 Identifying elements of an array
4.3 Storing data in arrays
4.4 Extracting multiple values
4.5 Converting between arrays and variables
4.6 Traversing arrays
4.7 Sorting
4.8 Array Operations

Unit 5	**File Handling**	**5 hours**

5.1 Working with files and directories
5.2 Operations on Files - Opening and Closing, Getting information about file, Read/write to file, Splitting name and path from file, Rename and delete files
5.3 Reading and writing characters in file
5.4 Reading entire file
5.5 Random access to file data
5.6 Getting information on file

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

OPEN ELECTIVE

Savitribai Phule Pune University
S.Y.B.Sc. (Cyber and Digital Science)
Subject Code: OE-201-CDS-T
Subject Name: AI for Everyone - I

Teaching Scheme:	No. of Credits:	Examination Scheme:
2 hours / week	**2**	CA:20 Marks UA: 30 Marks

Course Objectives: -

1. Understand the basics of artificial intelligence and its subfields.
2. Explore real-world applications of AI across different industries.
3. Gain insights into the ethical, social, and economic implications of AI.
4. Develop an appreciation for the potential of AI to drive innovation and transformation.

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

CO1: Define and explain the fundamental concepts and subfields of AI.
CO2: Identify real-world applications of AI across various industries.
CO3: Analyze the ethical, social, and economic implications of AI.
CO4: Recognize the potential of AI to drive innovation and transformation in different domains.

Course Contents

Unit 1	**Introduction to Artificial Intelligence**	**6 hours**	**CO1**

1.1 Definition and scope of AI
1.2 Historical overview and key milestones
1.3 Differentiating AI from human intelligence
1.4 Types of AI tools: Text, image, audio, video, coding, and automation.
1.5 Where to find free AI tools? (Google AI, OpenAI, Hugging Face, etc.)

Unit 2	**AI Subfields and Technologies**	**6 hours**	**CO2**

2.1 Machine learning: Supervised, unsupervised, and reinforcement learning
2.2 Deep learning and neural networks
2.3 Natural language processing (NLP) and computer vision

Unit 3	**Applications of AI**	**6 hours**	**CO3**

3.1 AI in healthcare: Diagnosis, treatment, and medical imaging
AI in finance: Fraud detection, algorithmic trading, and risk assessment
AI in transportation: Autonomous vehicles and traffic optimization
AI in customer service and chatbots
AI in education: Personalized learning and intelligent tutoring systems

Unit 4	**Ethical and Social Implications of AI**	**6 hours**	**CO4**

4.1 Bias and fairness in AI systems.
4.2 Privacy and data protection concerns
4.3 Impact of AI on employment and the workforce
4.4 AI and social **ineq**uality

Unit 5	AI Writing Assistants Tools	6 hours	CO5
5.1 ChatGPT (OpenAI) 5.2 Google Gemini (Bard AI) 5.3 Claude AI (Anthropic) 5.4 Perplexity AI 5.5 Rytr			
Reference Books:			
1. **Artificial Intelligence: A Guide for Thinking Humans"** – Melanie Mitchell 2. **The AI Revolution in Medicine: GPT-4 and Beyond"** – Peter Lee, Carey Goldberg, Isaac Kohane 3. **AI 2041: Ten Visions for Our Future"** – Kai-Fu Lee, Chen Qiufan 4. **The Business of AI: AI Technologies and How to Leverage Them for Business Success"** – Anirudh Koul 5. **AI-Powered Marketing: Harness the Future of Marketing with AI"** – Peter Gentsch 6. **The AI Marketing Handbook"** – Ryan McKenzie			

Savitribai Phule Pune University
S.Y.B.Sc.(Cyber and Digital Science)
Subject Code : OE-202-CDS-T
Subject : Web Design I

Teaching Scheme	**No. of Credits**	**Examination Scheme**
2 hours / week	2	CE: 20 marks EE: 30 marks

Prerequisites :

- Basic computer knowledge and the ability to work with files.
- Knowledge and understanding of Internet

Course Objectives:-

1. To learn HTML tags and programming concepts and techniques.
2. To develop the ability to logically plan and develop web pages.
3. To learn writing and debugging HTML code.
4. To learn to design table, frames etc.

Course Outcomes

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

1. Learn and use the HTML Tags.
2. Understand and resolves errors in HTML codes.
3. Design and develop the page using HTML codes.
4. Implement and develop Web pages

Course Contents

Unit 1	**Introduction to Web Design**	**8 hours**

1.1 Introduction
1.2 Working of the Internet.
1.3 Role of Web Servers, Clients(Communication)
1.4 Web Browsers
1.5 Working of the Internet, Intranet and WWW
1.6 E-Mail Servers and Protocols
1.7 E-mail Clients and Web Based Mail Access using Browser
1.8 Messenger Services and Clients(Chat)
1.9 Advantages and Disadvantages of Internet
1.10 Concept of effective Web Design (Web site, classification of website, Advantages and Disadvantages. Of website)
1.11 Fundamental Principles of Web page design and issues

Unit 2	**Getting Started with HTML**	**6 Lecture**

2.1 Introduction to scripting Languages

2.2 HTML Editing Tools

2.3 WYSISYG Authoring Tools

2.3.1 HTML Script

2.3.2 Basic HTML Document Structure

2.3.3 Common HTML Tags and its attributes

2.3.4 Design HTML Tags

2.3.5 Text Formatting and Styles

2.3.6 Images and Graphics

2.3.7 Button, Formatting and Style

2.3.8 Lists

2.3.9 Hyperlinks

2.4 Multimedia

2.5 Frames

2.6 HTML Forms

2.7 Linking Web pages

2.8 Publishing Web Pages

Unit 3	**Tables**	**6 Lectures**

3.1 Table Structure
3.2 Table tags
3.3 Affecting table appearance
3.4 Table troubleshooting
3.5 Tips and tricks
3.6 Standard table templates
3.7 Multipart images in tables

Unit 4	**Frame / Forms**	**6 Lectures**

4.1. Introduction to frames
4.2. Basic frameset structure
4.3. The frame function, appearance and Targeting frames.
4.4. The Inline (Floating) frames and Frame design tips and tricks
4.5. Forms: FORM elements, FORM attributes, Unconventional use of FORM elements
4.8. Demystifying CGI , Retrieving parameter value using getParameter () method

Case Studies	**4 hours**

Case study 1: Creation of forms, small case study to create HTML pages using all the above learnt techniques.
Case study 2: Creation of Forms layout designing by using div element with CSS property
Case study 3: Create Multiple Web pages link them to publish a small website.

Reference Books:

1.Computer Programming For Beginners:Learn The Basics Of HTML5-Joseph Connor
2. The Complete Reference HTML & CSS-Fifth Edition-Thomas A.Powell
3. Learning Web Design: A beginner's Guide to HTML, CSS, Javascript, and Web Graphics - Jennifer Robbins
4. HTML5: The Missing Manual - Matthew MacDonald.

Semester III					
Semester No.	**Course Code**	**Type of Course**	**Course Title**	**Credits**	**Hours/Week**
III	OE-204-CDS-T	OE (Open Elective)	Introduction to Cyber Security	2	2

Course Objectives	
1	Understand basic concepts and terms in cyber security.
2	Learn about privacy and related legal protections.
3	Grasp fundamental encryption principles.
4	Understand basics of Cyber laws and Indian IT Act.

Course Outcome	
CO1	Define and explain essential cybersecurity concepts, threats, and preventive strategies.
CO2	Interpret privacy principles and identify relevant laws and regulations protecting digital data.
CO3	Apply basic encryption methods to secure data and understand their role in cybersecurity.
CO4	Good understanding of cyberlaws, cybercrime and punishments in Indian Scenario.

Unit	**Title and Contents**	**No. of Lecture Hours**
1	**Chapter 1: Introduction to Cyber Crime and Cyber Security** 1.1 Introduction 1.2 Cybercrime:Definition and significance of cybersecurity, Evolution and historical context of cybersecurity 1.3 Cybercrime and Information Security 1.4 Who are Cybercriminals? 1.5 Hackers and Types of Hackers 1.6 Types of Cybercrimes: E-Mail Spoofing, Spamming, Cyber defamation, Internet Time Theft, Salami Attack/Salami Technique, Data Diddling, Forgery, Web Jacking, Newsgroup, Spam/Crimes Emanating from Usenet Newsgroup, Industrial Spying/Industrial Espionage, Hacking, Online Frauds, Computer Sabotage, Email Bombing/Mail Bombs, Computer Network Intrusions, Password Sniffing, Credit Card Frauds, Identity Theft 1.7 Vulnerability, Threats, and Harmful Acts 1.8 CIA Triad	**15**

2	**Chapter 2:- Cybercrime Tools, Techniques and Cyber Laws** 2.1 Introduction 2.2 Proxy Servers and Anonymizers 2.3 Phishing 2.4 Password Cracking 2.5 Keyloggers and Spyware 2.6 Virus and Worms 2.7 Trojan Horses and Backdoors 2.8 Steganography 2.9 DoS and DDoS Attacks 2.10 SQL Injection 2.11 Introduction: Cyber Laws 2.12 Cybercrime and the Legal Landscape around the World 2.13 Why Do We Need Cyberlaws: The Indian Context 2.14 The Indian IT Act 2.14.1 Challenges to Indian Law and Cybercrime Scenario in India 2.14.2 Digital Signatures and the Indian IT Act, Amendments to the Indian IT Act 2.15 Cybercrime and Punishment 2.16 Cyberlaw, Technology and Students: Indian Scenario	**15**

Reference Material
Reference Books

Sr. No.	Title of the Book	Author/s	Publication	Place
1	Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives	Nina Godbole, Sunit Belapure	Wiley	April 2011 India Publications Released.
2	Principles of Information Security. 3rd Edition, 2011.	Michael E Whitman, Herbert J Mattord	Cengage Learning	20 Channel Center Street, Boston, MA 02210 USA
3	Computer Security: Principles and Practice, 3rd edition	William Stallings and Lawrie Brown	Pearson	Boston, Massachusetts, USA
4	Cyber Security Essentials	James Graham Richard Howard Ryan Olson	Auerbach Publications	United States of America

Other Learning Material
E- Resource:

1) Swayam – Cyber Security Course (by NPTEL/IIT Madras) https://nptel.ac.in/courses/106106248
2) Swayam – Cyber laws https://onlinecourses.swayam2.ac.in/cec25_cs04/preview

सावित्राब फुले पुणे विदाप्प, पुणे
[Savitribai Phule Pune University, Pune]

अभ्ासमक
पदविका / पदि, ि२-२ (सत-३ ि ४)
विर् – कराप् (AEC) (शैकवणक
ि२ २०२५-२६ पासून) [Level 5.0, UG
Degree, Year-II] (w.e.f. academic
year 2025-26)

कराप् विर्ाचा पुनरवचि अभ्ासमक - जून २०२५ पासून

Ability Enhancement Course: Marathi
AEC : Marathi

S. Y. BSc (Cyber & Digital Science)

U.G. कराप् – वृि्ि (सत-३) अभ्ासक [Level 5.0]			
Course Type	Ability Enhancement Course AEC - कराप् (Marathi)	Credits- 2 (Theory)	Weeks- 15 Hours- 30
AEC-201-MAR	भारा आवण ज्िनव्िवार	Int. Marks 15	Ext. Marks 35

अभ्ासपवतकेविर्् :

सदर अभ्यससपत्र िक भाषेर स्वस, भयषयपेप्ितिप्् प्ध पसदयि, भयषरचत ्य् आपि ्ैपिप््र, भयषयभ्यसयचत अगर् अभयषयभ्यसयचत आश्ि्य, भयषय आपि जत्ेव््वयर ्यच्यिती सरससरसंध, व्ववयार् भयषय, ियसत् सयपवत्यचत भयषय, ीपीि सयपवत्यचत भयषय स्वस, ्य्ीते भयषय, सारभयषय ्चर स्वस् आश्ि्य स्जेकारण्यस ्दि वोई.

अभ्ासपवतकेच् उव्दे :

१. भाषेर स्वस् ्य् ्यचय सारच् ्वे धीर
२. जत्ेव््वयरयेनसयर भयषरचय ्यसर् ब्रेनसयर पेयि वोियन्च प्यरयचर आ्ीे ्वे धीर.
३. ्रयठत भयषरचय सारभयषय सयसरक आपि ि्ैीत सयसरक प््रयस जीक **घरिर**
४. ्रयठत भयषरच्य उस्ोजेयत् ्ौित्यचय प््रयस सयधिर.

अभ्ासक :

घटक	ि्पश्ल	शे्क	घड्ाळ् ि्ास
१	**भारेचे सिवप ि का्** १.१ भयषय स्वसचचय १.२ भयषरचत पेप्ित : प्ध पसदयि १.३ भयषयवसर : ्ौपि् आपि पीपिि (भयषय आपि पीसत) १.४ भयषरचत ्य् आपि ्ैपिप््र १.५ भयषयभ्यसयचत अगर् अभयषयभ्यसयचत आश्ि्य	१	१५
२	**भारा आवण ज्िनव्िवार : परसपरसरं** २.१ व्ववयार् भाषेर स्वस २.२ ियसत् सयपवत्यच्य भाषेर स्वस २.३ ीपीि सयपवत्यच्य भाषेर स्वस २.४ ्य्ीते भाषेर स्वस २.५ सारभयषय : स्वस् आश्ि्य	१	१५

अभ्ासपवतकेच् अध््न वनषपप् (COs) :

्या अभ्ासपवतकेि्या अध््नाि्ून विदाय्ा्कध्े पुढ्ल ककिाचा विकास वोबल,

Cognitive Ability	Course Outcomes	Teaching Learning Method
Co-1 Remember	भयर स्वस, ्ैपिप््र आपि ्य् ्यप्प्त ्यपवित सयगिय ्रही.	व्याये
Co-2 Understanding	भयषय आपि जत्ेव््वयर ्यचर आ्ी वोही.	व्याये, स्-अध््े
Co-3 Applying	जत्ेव््वयरयेनसयर भयषरच्य ्यसर ्रण्यत परीय पळरी.	्यचे, ीि
Co-4 Analyzing	भयषय आपि जत्ेव््वयरयच्य सदभयि प्शरषिक्रिय प््पसि **वोही.**	आ् प्शरषि
Co-5 Evaluating	भयषरच्य प्ध शिस्रती उस्ोजे प्प् स्ज प््पसि **वोही.**	रसगवि
Co-6 Creating	्रयठत भयषरच्य उस्ोजेयत् ्ौि्यच्य अभ्यसयिक अेनभ््यडितचत ्ीय आ्गि वोही.	स्-अेनभयर सयदरत्रि

U.G. कराप् – वृि्ृ िर (सत-४) अभ्ासक [Level 5.0]			
Course Type	Ability Enhancement Course AEC - कराप् (Marathi)	Credits- 2 (Theory)	Weeks-15 Hours-30
AEC-251-MAR	भारा आवण सिादकौशल्े	Int. Marks 15	Ext. Marks 35

अभ्ासपवतकेविर्् :

सदर अभ्यससपत्र िक भयषय आपि भयपष् ्ौील ्यचर स्वस ्शवसंध, प्यिभयषयप्ष् ंरि पे्, भयषय आपि स्यद्ौील ्यचर स्वस् शवसंध, पयरप्् स्यद्ौील िसच्च पगि स्यद्ौील स्जेक घरिय ्रिती.

अभ्ासपवतकेच् उव्दे :

१. भयषरच्य स्वसयचय ्शभयपष््ौील्यचय सारच् ्वे घरि.
२ .जत्ेव््वयरयेनसयर भयपष््ौील्यच्य ्यसरयचर स्वस ्रीक घरि.
३ .जत्ेव््वयरयेनसयर स्यद्ौील्यचय सारच् ्वे घरि.
४. भयपष््ौील् स्थद्ौील ्यच्यिती सरससर सयवच्यचर आ्ीे ्वे घरि.
५ .भयपष् ्ौील् स्थद्ौील ्यचर उस्ोजेयत् ्ौील्यचय प््यस सयधिर.

अभ्ासक :

घटक	िपश्ल	शो्क	घड्ाळ् िास
१	**भारा आवण भावरक कौशल्े : सिवप ि सवसरं** १.१ भयषय : उचचयरि आपि ंरि १.२ भयषय : शृि आपि सभयषि १.३ भयषय : पीसत आपि ंरि (प्यिभयषयप्ष् ंरि पे््) १.४ ंरिप्ष् ेत्े ियस्ी् **क**ेय	१	१५
२	**भारा आवण सिादकौशल्े : सिवप ि सवसरं** २.१ पयरप्् स्यद्ौील : शृि, ्यचे, सभयषि, भयषि, पचि, ंरि २.२ पगि स्यद्ौील : सयरयि ंरि, भयषयिर, ्लसेय प्सियर, पे्स्देयत् स्थद्यत् ंरि, ्नीयिि ंरि	१	१५

अभ्ासपवतकेच् अध््न वनषपप् (COs) :

ा अभ्ासपवतकेिा अध््नािून विदाय्ाकध्े पुढ्ल ककिाचा विकास वोबल,

Cognitive Ability	Course Outcomes	Teaching Learning Method
Co-1 Remember	भयषय आपि भयपष् ौिल यचर स्वस् ्वसंधय प्पत यपवित सयगिय रडी.	व्या्ये, स्-अध्े
Co-2 Understanding	भयषय आपि स्यद्ौिल यचर स्वस् ्वसंध यचर आ्े वोडी.	व्या्ये, सयपक्त्यस्यचर यचे
Co-3 Applying	पयरप् स्यद्ौिल्यचय यसर रण्यचत पररिय प्ळरी.	सयदरत्रि
Co-4 Analyzing	पगि स्यद्ौिल्यच्य सदभयि प्शरषिक्िय प््पसि वोडी.	उिा् प्शरषि
Co-5 Evaluating	भयषय आपि स्यद्ौिल प्प् रज प््पसि वोडी.	रसगवि
Co-6 Creating	भयपष् ौिल् स्यद्ौिल यचर उस्ोजे रण्यचर ौिल् अ्गि वोडी.	स्-अेनभ्चर सयदरत्रि

सदभ गर :

१. ियसेव््वयरयि रयठत (रस्य: स्वस: पपर्य) भयषय सचयीेयी्, ियस्ी् फोटो प्पि नदियी, सुतरि १९९७.
२. ैिरत, डॉ. अिो् ऊ्, सेरव्धे प्यिे, सुतरि १ जयेर्यरत २०००.
३. गतिय्तत, यध् ोवोळ्, ौज प्यिे, नंई १ जयेर्यरत २००४.
४. सृजेयत् ीरि, आेद सयटती, सद्धय प्यिे, सुतरि २००५ .
५. व्वयार् रयठत भयषय, िरपदेत ोपविर, सेरव्धे प्यिे, सुतरि १ जयेर्यरत २००८.
६. व्यससतठ, वयदर् यळक, अकर्ये् प्यिे, सुतरि २०११.
७. जयपवरयि ियस, डॉ.देय िरडत्र, सेरव्धे प्यिे, सुतरि १ जयेर्यरत २०१३.
८. सयंर- सस्ृित, डॉ. रि िखर, स्यि प्यिे पय. पी. औरगयंयद, १ जयेर्यरत २०१५.
९. व्वयार् रयठत, सयठ्सनसि, सुतरि प्दयसतठ प्यिे, सुतरि
१०. ंयित्चत रकर, ििरय् चववयि वयरयष् नप्दयसतठ, ेयपि.
११. रयठतपत्र पदरत, शत.ेय. चयफर र, सेरव्धे प्यिे, सुतरि
१२. रयठत ीरि यगदपि्य, यपस्े िरि, रयज् रयठत प्यस ससरय, नंई
१३. उस्ोपजि अभ्यसर्, रयठत भयषरचत स्यद्ौिल, िििरय् वयरयष् नप्दयसतठ, ेयपि.
१४. व्वयार् रयठत- डॉ. ल्यि यर, डॉ. द.पद.सनडर, पेरयीत प्यिे, सुतरि
१५. रयठत सयपवत् : यवत ीरिध, डॉ. सनधय्र िरीयर, स्वस प्यिे,औरगयंयद.
१६. व्वयार् रयठत, डॉ. ीतीय गोप्ीर, डॉ. जशत सयटिर, सेरव्धे प्यिे, सुतरि
१७. व्वयार् उस्ोपजि रयठत आपि पसयर्यध्यचत यिैीत : ससयद् - डॉ. सदतस सयगळर, डय्ड सप्ीर् िशस, सुतरि
१८. भ््र सनदर रयठत भयषय, डॉ. द. पद. सनडर, ॅजरपसट् प्यिे, सुतरि
१९. सत्यारिचय स्भय, ी. े. गोिीर, सुतरि प्दयसतठ प्यिे, सुतरि
२०. सत्यारिय : स्वस आपि पचप्रसय, वस्तर जोधळर, सनप्धय प्यिे, सुतरि
२१. भयषयिर त्यसय, ल्यि यळर, अजीत सोिि, पपि्य प्यिे, सुतरि
२२. ेभयरि, व्वयार् रयठत प्िरषय्, ऑगसट-सपटट, १९८२, पयर सयठियीय, यई.
२३. व्वयार् रयठत- ी.रय.ेपसरयंयद्र, फड् प्यिे, ोल्हापूर .

२४. भयषयपचिे, डॉ. ्रि् वरि्नि,स्यळ प्यिे, सत्रि

२५. भयपष् सजे आपि उस्ोजे, ग्स रयजे, पिदर अरि, सयटती गो्टरशर, द्य प्यिे, सत्रि

२६. ्रयठत भयषय : आज आपि उदय, अपीं ग्ळत, द्य प्यिे, सत्रि

२७. फीचर रपटग, पसशे्न ्यर अ्ीक ्र, शतप्दय प्यिे, सत्रि

२८. जयपवरयितचर ्न,्रि् ्रळ्.

२९. कदिसयठत ीरि, ्रि् ्रळ्.

SEM IV

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

Teaching Scheme 2 Hours / week	No. of Credit 02	Examination Scheme CA :20 marks UA: 30 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

Unit	Course Contents	Hours	CO
1	**Wireless & IoT Hacking**	4 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

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:
- 2.4.1 Privilege Escalation
- 2.4.2 Data Exfiltration
- 2.4.3 Persistence & Covering Tracks

2.5 Writing Custom Exploits

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)			
4	**Malware Analysis & Reverse Engineering**	**5 Hours**	**CO 4**
1.1 Types of Malware (Viruses, Worms, Trojans, Ransomware) 1.2 Static vs. Dynamic Analysis of Malware 1.3 Using Sandboxes for Malware Analysis 1.4 Reverse Engineering Basics			
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 Book:

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
As per NEP
S.Y.B.Sc. (Cyber and Digital Science)
CDS253MJP
Title:Practical based on CDS251MJ
Ethical Hacking - II

Teaching Scheme 4 Hours / week	No. of Credit 02	Examination Scheme CA :20 marks UA: 30 marks

Prerequisites:
1. Basic knowledge of Linux and Windows operating systems.
2. Understanding of networking concepts (TCP/IP, ports, protocols).
3. Familiarity with cybersecurity fundamentals and ethical hacking principles.
4. Experience with command-line tools and scripting (Bash, Python preferred).

Course Objectives
1. Understand and exploit vulnerabilities in wireless and IoT networks.
2. Utilize Metasploit for system exploitation and post-exploitation techniques.
3. Execute social engineering attacks, phishing campaigns, and bypass security controls.
4. Analyze malware behavior, perform reverse engineering, and debug malicious code.
5. Conduct advanced penetration testing and red team operations to assess security defenses.

Course Outcomes: On completion of the course, student will be able to
1. Capture, analyze, and crack Wi-Fi traffic using advanced tools.
2. Exploit vulnerabilities in IoT devices and misconfigured systems.
3. Use Metasploit for penetration testing, payload execution, and credential dumping.
4. Execute social engineering attacks and bypass multi-factor authentication.
5. Perform malware analysis, reverse engineering, and sandbox-based investigations.
6. Simulate real-world attacks, bypass security measures, and generate professional reports.

Unit	Course Contents	CO
Unit 1	**Wireless & IoT Hacking**	**CO 1**
	Capture Wi-Fi traffic using Airodump-ng Crack WEP/WPA2 Wi-Fi passwords using Aircrack-ng De-authenticate clients from a Wi-Fi network using Aireplay-ng Perform Evil Twin attack to steal Wi-Fi credentials Exploit Bluetooth vulnerabilities using Hciconfig & Bluesniff Extract firmware from an IoT device for vulnerability analysis Exploit a misconfigured IoT device (Smart Camera, Router, or Smart Plug)	
Unit 2	**Exploiting Systems Using Metasploit**	**CO 2**

Perform a Metasploit scan for vulnerable services
Exploit a Windows system using Metasploit & Meterpreter
Generate & execute a payload using Msfvenom
Maintain persistence using Metasploit post-exploitation modules
Extract system credentials using Hashdump & Credential Dumping
Exploit an unpatched Linux service using Metasploit

Unit 3	Social Engineering & Phishing Attacks	CO 3

Create a phishing email using GoPhish
Clone a login page to capture credentials using Social Engineering Toolkit (SET)
Bypass 2FA using Evilginx2
Execute a Rubber Ducky USB attack
Perform a voice phishing (vishing) attack simulation

Unit 4	Malware Analysis & Reverse Engineering	CO 4

Perform static analysis on a malware sample using PE Studio
Use Wireshark to analyze malware network activity
Introduction to IDA Pro
Intro to OllyDbg
Extract strings from malware using stringscommand

Unit 5	Penetration Testing	CO 5

Conduct a full penetration test on a network (reconnaissance to exploitation)
Perform a red team exercise against a secure environment
Use Scapy to create fragmented packets and observe how a firewall handles them
Write a professional penetration testing report with remediation steps

Note: Perform All this topic on try hack me also for home practice

Reference Book:

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
As per NEP
S.Y.B.Sc. (Cyber and Digital Science)
CDS252 MJ
Title: Advance Network Security

Teaching Scheme 2 Hours / week	No. of Credit 02	Examination Scheme CA :20 marks UA: 30 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
1. Understand Advanced Network Security Concepts
2. Understand Cryptographic Techniques
3. Secure Network Architectures and Protocols also Identify and Mitigate Cyber Threats
4. Implement Network Security Devices
5. 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-221-VSC-P
Title: Database Management System

Teaching Scheme 4 hours / week	No. of Credits: 2	Examination Scheme CA:20 marks UA: 30 marks

Course Objectives: -The course should enable the student:

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

Course Outcome: The students should be able to

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

Practical Assignment:

Module 1: Database Design and ER Model

1. **Database Concepts and Normalization**
2. **Understanding ER Models**
    - Create an ER diagram for a case study (e.g., Hospital Management, Online Shopping, and Library System).
    - Identify entities, attributes, relationships, and cardinality.

Module 2: SQL Basics – Data Definition and Constraints

2. **Creating and Modifying Databases (DDL Commands)**
    - Create a database and define multiple tables with appropriate data types.
    - Implement primary key, foreign key, unique, not null, check, and default constraints.
    - Alter tables (add/drop/rename columns, modify constraints).
    - Drop tables and databases.
    - Truncate

Module 3: Data Manipulation and Retrieval

3. **Data Insertion, Modification, and Deletion (DML Commands)**
    - Insert single and multiple records into tables.
    - Update specific and multiple records.
    - Delete specific and all records.

4. **Querying Data using SELECT Statements**
    - Use various SQL operators (AND, OR, BETWEEN, NOT, IN, IS NULL, LIKE).
    - Apply aggregate functions (AVG, COUNT, MAX, MIN, and SUM).
    - Use DISTINCT, ORDER BY, GROUP BY, HAVING.

Module 4: Advanced SQL – Joins and Sub queries

5. **Working with Joins**
    - Perform different types of joins:
        - Inner Join
        - Left, Right, and Full Outer Joins
        - Self-Join
6. **Sub queries and Set Operations**
    - Write nested queries using SELECT, INSERT, UPDATE, and DELETE.
    - Use set operations: UNION, UNION ALL, INTERSECT, EXCEPT.

Module 5: Views and Indexing

7. **Views and Indexing for Performance Optimization**
    - Create and manage views (CREATE VIEW, UPDATE VIEW, and DROP VIEW).
    - Implement indexing (Single-level, Multi-level).
    - Compare query performance with and without indexing.

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.
- MySQL: The Complete Reference, Vikram Vaswani, McGraw Hill Professional, 2004

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)
CDS-291-MN: Advanced Web Technology

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / week	**2**	CA:20 marks UA: 30 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 Learn Database connectivity using PHP
4. To Learn AJAX to make our application more dynamic.
5. 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: Interpret and formulate XML queries.
CO3: To learn database handling with PHP.
CO4: Learn to build website AJAX framework
CO5: Understand 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	**XML**	**6 hours**	**CO2**

2.1 What is XML?
2.2 XML document Structure
2.3 PHP and XML
2.4 XML parser
2.5 The document object model (DOM)
2.6 DOM Events(onmouseup, onmousedown, onclick, onload, onmouseover, onmouseout).
2.7 The simple XML extension
2.8 Changing a value with simple XML

Chapter 3	**Database Connectivity**	**6 hours**	**CO3**

3.1 **Introduction to MySQL and Database Concepts**
Overview of relational databases, tables, fields, and SQL basics (SELECT, INSERT, UPDATE, DELETE).
3.2 **Connecting PHP with MySQL Database**
Using mysqli_connect () or PDO to establish a connection to the database.
3.3 **Executing SQL Queries from PHP**

Performing SQL operations using mysqli_query () or PDO::query(), handling query results.

3.4 **Fetching and Displaying Data**
Retrieving data using mysqli_fetch_assoc(), mysqli_fetch_array() or PDO fetch methods.

3.5 **Error Handling and Security Measures**
Using prepared statements (mysqli_prepare() or PDO::prepare()) to prevent SQL injection and handle database errors securely.

3.6 PEAR DB basics

Chapter 4	**Introduction of AJAX**	**6 hours**	**CO4**

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

Chapter 5	**NodeJS**	**8 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)

SEC251CDSP-241: Principles of Operating Systems

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / week	**2**	CA:20 marks UA: 30 marks

Prerequisites
1. Basics of mathematics

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**	**8 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, SRTF,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	**Memory Management**	**7 hours**	
5.1 Background – Basic hardware, Address binding, Logical versus physical address space, Swapping 5.2 Contiguous Memory Allocation –First Fit, Best Fit, Worst Fit, Fragmentation, types of fragmentation, Compaction 5.3 Paging and Segmentation – Basic Concepts 5.4 Demand paging 5.6 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			

Open Elective

Savitribai Phule Pune University

S.Y.B.Sc. (Computer Science) - Sem –IV

Course Type:GE/OE. Course Code: OE-253-CS-T

Course Title: Digital Marketing II

Teaching Scheme	No. of Credits	Examination Scheme
02 Hours /Week	2	IE :20 Marks UE:30Marks

Prerequisites

- Digital marketing requires creativity and problem-solving abilities.
- Experience with social media platforms (Facebook, Instagram, Twitter, LinkedIn, etc.) is beneficial, as digital marketing

Course Objectives

- To understand Digital Marketing as the most powerful marketing tool.
- To Learn to create digital marketing artworks.
- To use social media sites like Facebook, Instagram, Twitter, LinkedIn, and others to raise sales, engage customers, and establish your brand.

Course Outcomes

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

CO1: Understand and learn marketing strategies and results effectively to stakeholders.

CO2: Assess and enhance digital marketing campaigns' return on Investment.

CO3: Analyze and implement practical experience with industry-standard digital marketing tools.

CO4: Analyze and use variety of social media channels to create and interact with communities, raise awareness of a brand.

Course Contents

Chapter1	**Online Consumer Behavior Analysis**	**8 Hours**

1.1 Consumer Behavior

1.2 Segmentation and Targeting online customers

1.3 Psychological Responses

1.4 Social Trends

Chapter2	**Social Media Marketing**	**8 Hours**

2.1. Social Media Sites

2.2. - Influence of Social Media Marketing

2.3. Power of Social Media

2.4. Monetization through Social Media

Chapter3	Future of Digital Marketing	8 Hours
3.1. Use of Artificial Intelligence (AI) in Digital Marketing. 3.2. Common use of household gadgets for online marketing. 3.3. Digital Marketing strategies.		
Case Study		**6 Hours**
Case Study 1 Experiential Learning: Creating a website. Case Study 2 Online Consumer Behavior Analysis for an E-Commerce Fashion Brand		
Reference Books:		
1 Digital Marketing: Nitin Kamat, Chinmay Kamat (Himalaya Publishing House) 2 "Digital Marketing for Dummies" by Ryan Deiss and Russ Henneberry 3 "Influence: The Psychology of Persuasion" by Robert B. Cialdini 4 "Social Media Marketing Workbook: How to Use Social Media for Business" by Jason McDonald		

Savitribai Phule Pune University
S.Y.B.Sc.(Cyber and Digital Science)
Subject Code : OE-252-CDS-T
Subject : Web Design II

Teaching Scheme 2 hours / week	**No. of Credits** 2	**Examination Scheme** CE: 20 marks EE: 30 marks

Prerequisites :

- Knowledge and understanding of HTML is essential for structuring web pages.
- Basic design principles can enhance your web design abilities.
- Knowledge of programming concepts like variables, loops, and functions can be helpful
- when learning JavaScript.

Course Objectives:-

1. To learn to define the structure and content of XML documents using XML.
2. To know and learning how to use the DOM to access and manipulate XML data within

3. applications.
4. To prepare the learners with the fundamentals of CSS programming and scripting languages.
5. Learners should know how to create and interact with web pages effectively, develop static
6. and dynamic websites, and understand how they work together.

Course Outcomes

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

4. **Learn and use the CSS to design Webpages.**
5. **Understand Linking and publishing of Web pages.**
6. **Plan, design and implement webpages.**
7. **Develop a dynamic web pages using JavaScript (client side programming).**

Course Contents

Unit 1	**CSS(Cascading Style Sheet)**	**8 hours**

1.1. Introduction of CSS and its Syntax

1.2. Ways to Insert CSS and Background image handling

1.3. Background colour management using CSS

1.4. Text and Font management using CSS

1.5. Managing Hyperlinks and List using CSS

1.6. Designing Borders and Outline

1.7. Setting Page Margin using CSS

Unit 2	**XML(Extensible Markup Language)**	**8 Lecture**

2.1. XML Namespaces and Infoset and Document Type

2.2. Definitions (DTDs)

2.3. XML Schemas and XML-Parser

2.4. Data Modeling, Document and Object Model (DOM)

2.5. Displaying XML with XSLT

Unit 3	**Introduction to JavaScript**	**8 Lectures**

3.1. Concept of Script, Types of Scripts, Scripting Languages

3.2. Introduction to JavaScript.

3.3. Variables, identifier and Operator, Control structure.

3.4. Examples on JavaScript Operators.

3.5. Functions

3.6. Event Handling in JavaScript with examples.

Case Studies	**6 hours**

Case study 1: Creation of forms, small case study to create HTML pages using all the above learnt techniques.
Case study 2: Redesigning the Website of a Small Business.
Case study 3: Create a Styled Web Page for a Coffee Shop.

Reference Books:

1.1. Learning Web Design: A beginner's Guide to HTML, CSS, Javascript, and Web Graphics -
Jennifer Robbins
2. HTML5: The Missing Manual - Matthew MacDonald
3. HTML and JavaScript – Ivan Bayross
4. Mastering HTML, CSS &Javascript Web Publishing

Savitribai Phule Pune University
S.Y.B.Sc. (Cyber and Digital Science)
Subject Code: OE-251-CDS-T
Subject Name: AI for Everyone - II

Teaching Scheme: 2 hours / week	No. of Credits: **2**	Examination Scheme: CA:20 Marks UA: 30 Marks

Course Objectives: -

1. Understand the basics of artificial intelligence and its subfields.
2. Explore real-world applications of AI across different industries.
3. Gain insights into the ethical, social, and economic implications of AI.
4. Develop an appreciation for the potential of AI to drive innovation and transformation.

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

CO1: To understand different types if AI Models
CO2: To understand content optimization using AI.
CO3: To understand Animations and motions in AI
CO4: To understand Transcription of text using AI
CO5: To Understand uses of AI in Data Science.

Course Contents

Unit 1	**Advanced AI Fundamentals & Trends**	**6 hours**	**CO1**

1.1 Deep Dive into AI, Machine Learning & Deep Learning
1.2 Types of AI Models: Generative AI, NLP, Computer Vision, Reinforcement Learning
1.3 Latest AI Trends: AGI, Large Language Models (LLMs), and multimodal AI
1.4 Exploring AI Frameworks & APIs: OpenAI, Hugging Face, Google AI

Unit 2	**AI for Advanced Text & Content Creation**	**6 hours**	**CO2**

2.1 AI for Long-form Writing & Reports
2.2 Automating Research & Citation Management
2.3 AI for SEO & Content Optimization
2.4 Using AI for Professional Emails & Business Writing

Unit 3	**Advanced AI for Image & Video Processing**	**6 hours**	**CO3**

3.1 AI Image Generation Beyond Basics
3.2 Deepfake Technology & Ethical Concerns
3.3 AI Video Editing & Creation
3.4 AI Animation & Motion Capture

Unit 4	**AI in Audio, Speech, and Music**	**6 hours**	**CO4**

4.1 Advanced AI Voice Cloning & Speech Synthesis
4.2 AI for Podcasting & Audiobooks
4.3 Music Composition with AI
4.4 Speech-to-Text & AI Transcription

Unit 5	**AI for Coding, Development & Automation**	**6 hours**	**CO5**

5.1 AI-Powered Code Generation & Debugging
5.2 AI for No-Code & Low-Code Development
5.3 Automating Workflows & AI Agents

5.4 AI in Data Science & Analytics
Reference Books:
1. **Artificial Intelligence: A Modern Approach** – Stuart Russell & Peter Norvig. 2. **Practical AI for Business Leaders** – Anand S. Rao 3. **AI-Powered Automation Handbook** – Will Kelly 4. **AI for Content Creators: How to Use AI Tools for Writing and Marketing** – Rob Lennon 5. **Human Compatible: Artificial Intelligence and the Problem of Control** – Stuart Russell

SEM V

Semester: V

DIGITAL FORENSIC – I

Programme Name :	**B.Sc. Cyber and Digital Science**
Class :	**T. Y. B.Sc Cyber and Digital Science**
Semester :	V
Course Type :	Major Core (Theory)
Course Code :	CDS-301-MJ
Course Title :	Digital Forensic – I
No. of Credits :	02
No. of Teaching Hours :	30

A. Rationale:

Digital Forensics is a crucial subject in cyber security that focuses on the identification, preservation, analysis, and presentation of digital evidence. This course introduces students to the fundamental concepts and tools used in digital forensic investigations. It provides knowledge of forensic processes, legal considerations, and techniques for analyzing data from computers and digital storage devices. The course prepares students to handle cybercrime investigations and supports roles in cybersecurity, law enforcement, and incident response.

B. INDUSTRY / EMPLOYER EXPECTED OUTCOME:

- Develops practical skills in handling digital evidence and forensic tools
- Prepares students for roles such as digital forensic analyst, cybersecurity analyst, and incident responder
- Enhances ability to investigate cybercrimes and analyze digital data securely
- Builds understanding of legal procedures and ethical practices in digital investigations

C. COURSE OUTCOMES (COs):

CO1–CO6 correspond to Bloom's Taxonomy levels as:
CO1 (Remember), CO2 (Understand), CO3 (Apply), CO4 (Analyze), CO5 (Evaluate), and CO6 (Create)

Course Outcome Table:

CO No.	Course Outcome Statement
CO1	Recall the fundamentals of digital forensics, cybercrime, and the forensic investigation process.
CO2	Explain types of digital evidence, data acquisition methods, and forensic tools.
CO3	Apply forensic techniques to collect and preserve digital evidence from storage devices.
CO4	Analyze file systems, deleted files, and digital artifacts using forensic tools.
CO5	Evaluate different forensic methods and tools for investigation scenarios.
CO6	Create forensic reports and document findings following legal and professional standards.

D. Syllabus

Unit	Course Contents	Hours	CO
1	**Introduction to Digital Forensics**	4	1
	1.1 What is Digital Forensics? 1.2 Need and Importance in Cyber Security 1.3 Types of Cyber Crimes 1.4 Digital Forensic Investigation Process 1.5 Roles and Responsibilities of Forensic Investigator		
2	**Digital Evidence & Acquisition**	4	2
	2.1 Concept of Digital Evidence 2.2 Types and Characteristics of Digital Evidence 2.3 Chain of Custody 2.4 Evidence Handling Procedures 2.5 Data Acquisition Techniques (Live and Dead) 2.6 Disk Imaging and Cloning 2.7 Tools: FTK Imager, dd		
3	**File Systems & Disk Analysis**	6	3
	3.1 Introduction to File Systems (FAT, NTFS, EXT) 3.2 Disk Structure and Partitioning 3.3 File Allocation and Storage Mechanism 3.4 Metadata and Timestamp Analysis 3.5 Deleted File Recovery Techniques 3.6 Introduction to Autopsy Tool		
4	**Forensic Tools & Investigation Techniques**	8	4

	4.1 Overview of Digital Forensic Tools 4.2 Autopsy and EnCase Basics 4.3 FTK Tool Usage 4.4 Disk Analysis and Keyword Searching 4.5 Registry Analysis Basics 4.6 Log File Analysis		
5	**Network & Email Forensics**	**8**	**5**
	5.1 Introduction to Network Forensics 5.2 Packet Capturing using Wireshark (Basic) 5.3 Network Log Analysis 5.4 Email Structure and Header Analysis 5.5 Web Browser Forensics Basics		
6	**Reporting and Case Studies**	**6**	**6**
	6.1 Importance of Documentation 6.2 Forensic Report Writing Format 6.3 Evidence Presentation Basics 6.4 Legal Admissibility of Digital Evidence 6.5 Case Study on Cybercrime Investigation		

Reference Books:

- Digital Forensics and Incident Response – Jason T. Luttgens
- Guide to Computer Forensics and Investigations – Bill Nelson
- Computer Forensics: Principles and Practices – Linda Volonino
- Practical Digital Forensics – Niranjan Reddy

PRACTICAL BASED ON DIGITAL FORENSICS – I

Programme Name :	**B.Sc. Cyber and Digital Science**
Class :	**T. Y. B.Sc Cyber and Digital Science**
Semester :	V
Course Type :	Major Core Practical
Course Code :	CDS-305-MJP
Course Title :	Practical Based on 301MJ (Digital Forensics - I)
No. of Credits :	02

A. Rationale:

This practical course is designed to provide hands-on experience in digital forensic investigation techniques. It enables students to apply theoretical knowledge gained in Digital Forensics – I through real-world tasks such as evidence acquisition, disk analysis, and forensic tool usage. The course strengthens practical skills required for cybercrime investigation and digital evidence handling.

B. INDUSTRY / EMPLOYER EXPECTED OUTCOME:

- Develops practical skills in handling digital forensic tools
- Prepares students for roles such as forensic analyst and incident responder
- Enhances ability to investigate and analyze digital evidence
- Builds problem-solving skills in real-world forensic scenarios

C. COURSE OUTCOMES (COs):

CO No.	Course Outcome Statement
CO1	Perform basic digital forensic investigation tasks using tools
CO2	Acquire and preserve digital evidence from storage devices
CO3	Analyze file systems and recover deleted data
CO4	Investigate system logs and user activity
CO5	Evaluate forensic tools and investigation techniques
CO6	Prepare basic forensic reports

D. COURSE STRUCTURE AND CONTENTS:

Practical 1: Introduction to Digital Forensics (6 hours)

- Install and set up forensic tools (Autopsy, FTK Imager)
- Explore digital forensic environment
- Activity: Identify types of digital evidence

Practical 2: Disk Imaging and Acquisition (4 hours)

- Create disk image using FTK Imager
- Perform live vs dead acquisition
- Activity: Verify integrity using hash values

Practical 3: File System Analysis (4 hours)

- Analyze FAT/NTFS file systems
- Explore file structure and metadata
- Activity: Identify hidden and system files

Practical 4: Deleted File Recovery (4 hours)

- Recover deleted files using Autopsy
- Analyze recovered artifacts
- Activity: Document recovered evidence

Practical 5: Log and Registry Analysis (4 hours)

- Analyze system logs and registry
- Identify user activity
- Activity: Detect suspicious actions

Practical 6: Network & Email Forensics (4 hours)

- Capture packets using Wireshark
- Analyze email headers
- Activity: Identify phishing attempt

E. SUGGESTED MICRO PROJECT / ASSIGNMENT:

- Prepare forensic investigation report on a simulated cybercrime
- Analyze a disk image and extract evidence
- Document findings with screenshots

F. GENERAL / OVERALL EXPECTATIONS:

1. Students will gain hands-on experience in forensic tools
2. Students will analyze and interpret digital evidence
3. Students will perform basic cybercrime investigation
4. Students will develop reporting and documentation skills
5. Students will apply theoretical knowledge in practical scenarios

MALWARE ANALYSIS

Programme Name	**B.Sc. Cyber and Digital Science**
Class	**T. Y. B.Sc Cyber and Digital Science**
Semester	V
Course Type	Major Core (Theory)
Course Code	CDS-302-MJ
Course Title	Malware Analysis
Credits	02
Hours	30

A. Rationale:

Malware Analysis is an essential subject in cybersecurity that focuses on understanding, detecting, and analyzing malicious software. This course introduces students to various types of malware, their behavior, and techniques used by attackers. It provides knowledge of basic static and dynamic analysis methods along with hands-on exposure to analysis tools. The course prepares students to identify, analyze, and respond to malware threats in cybersecurity operations.

B. INDUSTRY / EMPLOYER EXPECTED OUTCOME:

- Develops skills in identifying and analyzing different types of malware
- Prepares students for roles such as malware analyst and cybersecurity analyst
- Enhances ability to detect and respond to malware-based attacks
- Builds understanding of safe analysis environments and ethical practices

C. COURSE OUTCOMES (COs):

CO No.	Course Outcome Statement
CO1	Recall the fundamentals of malware, its types, and lifecycle.
CO2	Explain malware analysis techniques, tools, and safe environments.
CO3	Apply basic static and dynamic analysis methods.
CO4	Analyze malware behavior and system impact.

CO5	Evaluate malware detection techniques and security measures.
CO6	Create basic malware analysis reports and document findings.

D. Syllabus

Unit	Course Contents	Hours	CO
Unit 1	**Introduction to Malware Analysis**	**4**	**2**
	1.1 What is Malware? 1.2 Types of Malware 1.3 Malware vs Vulnerability vs Exploit 1.4 Malware Lifecycle 1.5 Objectives of Malware Analysis		
Unit 2	**Analysis Setup & Techniques**	**4**	**2**
	2.1 Safe Malware Analysis Environment 2.2 Virtual Machines (VMware, VirtualBox) 2.3 Sandboxing Basics 2.4 Static vs Dynamic Analysis 2.5 File Hashing (MD5, SHA) 2.6 Tools: Strings, PEiD		
Unit 3	**Static Malware Analysis**	**6**	**3**
	3.1 Executable File Structure Basics (PE Format Introduction) 3.2 File Property and Header Analysis 3.3 Strings Analysis 3.4 Identifying Packed and Obfuscated Files 3.5 Tools: PEview, Detect It Easy		
Unit 4	**Dynamic Malware Analysis**	**8**	**4**
	4.1 Behavior Analysis Basics 4.2 Monitoring Processes (Process Explorer) 4.3 File and Registry Changes 4.4 Network Activity Analysis (Wireshark) 4.5 Basic Sandbox Analysis 4.6 Introduction to Process Monitor (ProcMon)		
Unit 5	**Malware Techniques and Detection**	**8**	**5**
	5.1 Code Obfuscation Basics 5.2 Packing and Unpacking Concepts 5.3 Rootkits and Keyloggers 5.4 Malware Persistence Mechanisms 5.5 Signature-Based and Behavior-Based Detection 5.6 Introduction to Antivirus Detection Techniques		
Unit 6	**Reporting and Case Study**	**6**	**6**
	6.1 Malware Analysis Report Writing 6.2 Indicators of Compromise (IOCs) 6.3 Malware Classification Basics		

	6.4 Case Study of Malware Attack 6.5 Basic Prevention Techniques 6.6 Introduction to Threat Intelligence Integration

Reference Books:

- Practical Malware Analysis – Michael Sikorski & Andrew Honig
- Malware Analyst's Cookbook – Michael Hale Ligh
- Learning Malware Analysis – Monnappa K A
- The Art of Memory Forensics – Michael Hale Ligh

PRACTICAL BASED ON MALWARE ANALYSIS

Programme Name :	**B.Sc. Cyber and Digital Science**
Class :	**T. Y. B.Sc Cyber and Digital Science**
Semester :	V
Course Type :	Major Core Practical
Course Code :	CDS-306-MJP
Course Title :	Practical based on CDS - 302MJ (Malware Analysis)
No. of Credits :	02

A. Rationale:

This practical course provides hands-on experience in analyzing malicious software using basic static and dynamic analysis techniques. It enables students to safely investigate malware behavior in controlled environments using virtual machines and analysis tools. The course strengthens practical skills required to detect, analyze, and respond to malware threats in real-world cybersecurity scenarios.

B. INDUSTRY / EMPLOYER EXPECTED OUTCOME:

- Develops skills in identifying and analyzing malware behavior
- Prepares students for roles such as malware analyst and SOC analyst
- Enhances ability to work in secure analysis environments
- Builds knowledge of malware detection and response techniques

C. COURSE OUTCOMES (COs):

CO No.	Course Outcome Statement
CO1	Perform malware analysis in a safe environment
CO2	Identify different types of malware and their behavior
CO3	Apply static and dynamic analysis techniques
CO4	Analyze system and network activity caused by malware
CO5	Evaluate malware detection and prevention techniques
CO6	Prepare basic malware analysis reports

D. COURSE STRUCTURE AND CONTENTS:

Practical 1: Malware Analysis Environment Setup (6 hours)

- Install VirtualBox / VMware
- Setup isolated lab environment
- Configure snapshots and rollback
- Activity: Create secure malware lab

Practical 2: Basic Static Analysis (4 hours)

- Use tools: Strings, PEiD, Detect It Easy
- Analyze file properties and hashes (MD5, SHA)
- Activity: Identify suspicious file indicators

Practical 3: Advanced Static Analysis (4 hours)

- Analyze PE file structure
- Identify packed or obfuscated files
- Activity: Compare clean vs malicious files

Practical 4: Dynamic Analysis (4 hours)

- Execute malware in sandbox environment
- Monitor using Process Explorer
- Activity: Observe process behavior

Practical 5: System and Network Monitoring (4 hours)

- Monitor file, registry changes (ProcMon)
- Capture traffic using Wireshark
- Activity: Identify malicious network activity

Practical 6: Reporting and Case Study (4 hours)

- Document findings
- Identify Indicators of Compromise (IOCs)
- Activity: Create malware analysis report

E. SUGGESTED MICRO PROJECT / ASSIGNMENT:

- Analyze a sample malware and prepare report
- Compare static vs dynamic analysis results
- Identify behavior and attack pattern

F. GENERAL / OVERALL EXPECTATIONS:

- Students will gain hands-on experience in malware analysis
- Students will understand malware behavior and impact
- Students will use analysis tools effectively
- Students will develop investigation and reporting skills
- Students will work in secure and controlled environments

CYBER THREAT INTELLIGENCE

Programme Name :	**B.Sc. Cyber and Digital Science**
Class :	**T. Y. B.Sc Cyber and Digital Science**
Semester :	V
Course Type :	Major Core (Theory)
Course Code :	CDS-303-MJ
Course Title :	Cyber Threat Intelligence
No. of Credits :	02
No. of Teaching Hours :	30

A. Rationale:

Cyber Threat Intelligence focuses on collecting, analyzing, and interpreting threat data to understand cyber attacks. This subject introduces students to intelligence concepts, threat actors, and modern cyber threats. It helps in developing the ability to identify and respond to cyber incidents using intelligence-driven approaches.

B. INDUSTRY / EMPLOYER EXPECTED OUTCOME:

- Develops skills in collecting and analyzing threat intelligence
- Prepares students for roles such as SOC analyst and threat analyst
- Enhances ability to identify threat actors and attack patterns
- Builds understanding of proactive cybersecurity strategies

C. COURSE OUTCOMES (COs):

CO No.	Course Outcome Statement
CO1	Recall the fundamentals of cyber threat intelligence.
CO2	Explain threat intelligence lifecycle and data sources.
CO3	Apply techniques to collect and process threat data.
CO4	Analyze threat data to identify patterns and indicators.
CO5	Evaluate intelligence sources and security decisions.

Unit	Course Contents	Hours	CO
1	**Introduction to CTI**	4	1
	1.1 What is Cyber Threat Intelligence 1.2 Importance in Cyber Security 1.3 Types of Threat Intelligence 1.4 Threat Landscape 1.5 Threat Actors		
2	**Intelligence Lifecycle**	4	2
	2.1 Threat Intelligence Lifecycle 2.2 Data Collection Methods 2.3 Data Processing 2.4 Intelligence Analysis 2.5 Intelligence Sharing		
3	**Data Collection & Tools**	6	3
	3.1 Data Collection Techniques 3.2 Indicators of Compromise (IOCs) 3.3 Threat Intelligence Platforms 3.4 Tools: MISP, OpenCTI, VirusTotal 3.5 Data Correlation Basics		
4	**Threat Analysis**	8	4
	4.1 Threat Analysis Techniques 4.2 Network and Malware-based Analysis 4.3 Behavioral Analysis 4.4 Introduction to MITRE ATT&CK 4.5 Identifying Attack Patterns		
5	**Security Operations**	8	5
	5.1 Intelligence Sharing Basics 5.2 Role in SOC 5.3 Incident Response using CTI 5.4 Threat Hunting Basics 5.5 Integration with SIEM		
6	**Reporting and Trends**	6	6
	6.1 Threat Intelligence Reporting 6.2 Risk Assessment Basics 6.3 Decision Making using CTI 6.4 Case Studies 6.5 Emerging Trends in CTI		

Reference Books:

- Cyber Threat Intelligence – Kerry E. Paterson
- The Threat Intelligence Handbook – Recorded Future
- Intelligence-Driven Incident Response – Scott J. Roberts
- Practical Threat Intelligence and Data-Driven Threat Hunting – Valentina Palacín

Semester: V

ATTACK SURFACE ANALYSIS & THREAT MODELING

Programme Name :	**B.Sc Cyber and Digital Science**
Class :	**T. Y. B.Sc Cyber and Digital Science**
Semester :	V
Course Type :	Major Core (Theory)
Course Code :	CDS-304-MJ
Course Title :	Attack Surface Analysis & Threat Modeling
No. of Credits :	02
No. of Teaching Hours :	30

A. Rationale:

Attack Surface Analysis and Threat Modeling are essential components of modern cybersecurity practices. This subject introduces students to the concepts of identifying system vulnerabilities, analyzing attack surfaces, and understanding potential threats in applications, networks, and systems. The course helps learners develop a proactive security mindset by understanding risks before attacks occur. It prepares students for roles related to secure system design, risk analysis, and cybersecurity assessment.

B. INDUSTRY / EMPLOYER EXPECTED OUTCOME:

- Develops skills in identifying and analyzing attack surfaces
- Prepares students for roles such as security analyst and risk analyst
- Enhances ability to identify threats and vulnerabilities in systems
- Builds understanding of secure design and threat mitigation practices

C. COURSE OUTCOMES (COs):

CO No.	Course Outcome Statement
CO1	Recall basic concepts of attack surfaces and threat modeling.
CO2	Explain threats, vulnerabilities, and risk assessment concepts.

CO3	Apply attack surface analysis techniques to systems and applications.
CO4	Analyze security threats using threat modeling approaches.
CO5	Evaluate security risks and mitigation strategies.
CO6	Create basic threat models and security assessment reports.

D. Syllabus

Unit	Course Contents	Hours	CO
1	**Introduction to Attack Surface Analysis**	**4**	**1**
	1.1 Introduction to Cyber Attack Surface 1.2 Types of Attack Surfaces 1.3 Entry Points and Exposure 1.4 Importance of Attack Surface Reduction 1.5 Basic Security Concepts		
2	**Fundamentals of Threat Modeling**	**4**	**2**
	2.1 Introduction to Threat Modeling 2.2 Threats, Vulnerabilities and Risks 2.3 Threat Actors and Attack Vectors 2.4 Security Objectives 2.5 Risk Assessment Basics		
3	**Attack Surface Identification**	**6**	**3**
	3.1 Network Attack Surface 3.2 Application Attack Surface 3.3 User and Physical Attack Surface 3.4 Asset Identification 3.5 Tools for Surface Analysis (Basic Overview)		
4	**Threat Modeling Techniques**	**8**	**4**
	4.1 STRIDE Model Basics 4.2 DREAD Risk Assessment Basics 4.3 Data Flow Diagrams (DFD) 4.4 Identifying Threat Scenarios 4.5 Threat Prioritization		
5	**Risk Mitigation and Security Controls**	**8**	**5**

	5.1 Security Controls Overview 5.2 Secure Design Principles 5.3 Access Control Basics 5.4 Vulnerability Mitigation 5.5 Incident Prevention Techniques		
6	**Reporting and Case Studies**	**6**	**6**
	6.1 Threat Modeling Documentation 6.2 Attack Surface Assessment Report 6.3 Case Study Analysis 6.4 Risk Evaluation 6.5 Best Practices in Threat Modeling		

Reference Books:

7. Threat Modeling: Designing for Security – Adam Shostack
8. The Web Application Hacker's Handbook – Dafydd Stuttard
9. Security Engineering – Ross Anderson
10. OWASP Threat Modeling Guide

Web & Network Security Fundamentals

Programme Name :	**B.Sc. Cyber and Digital Science**
Class :	**T. Y. B.Sc Cyber and Digital Science**
Semester :	V
Course Type :	Major Elective (Theory)
Course Code :	CDS-307-MJ
Course Title :	Web and Network Security Fundamentals
No. of Credits :	02
No. of Teaching Hours :	30

A. Rationale:

Web and Network Security Fundamentals is an essential subject in cybersecurity that focuses on protecting web applications and network infrastructure from cyber threats. This course introduces students to basic networking concepts, web technologies, and common vulnerabilities found in real-world systems. It helps students understand how cyber attacks are performed and how basic security measures are implemented to prevent them. The subject builds a strong foundation for advanced topics such as penetration testing, secure coding, and network defense.

B. INDUSTRY / EMPLOYER EXPECTED OUTCOME:

- Develops understanding of network architecture and web application structure
- Prepares students for roles such as network security analyst and web security analyst
- Enhances ability to identify common web and network vulnerabilities
- Builds knowledge of basic security tools and defensive techniques

C. COURSE OUTCOMES (COs):

CO1–CO6 correspond to Bloom's Taxonomy levels as:
CO1 (Remember), CO2 (Understand), CO3 (Apply), CO4 (Analyze), CO5 (Evaluate), CO6 (Create)

Course Outcome Table:

CO No.	Course Outcome Statement
CO1	Recall the basic concepts of web and network security and common cyber threats.

CO2	Explain web application components, network models, and common vulnerabilities.
CO3	Apply basic tools and techniques to identify web and network security issues.
CO4	Analyze network traffic and web application behavior to detect security issues.
CO5	Evaluate security measures, configurations, and risk factors in web and network systems.
CO6	Create simple security configurations and basic reports for web and network protection.

Syllabus

Unit	Course Contents	Hours	CO
1	**Introduction to Web and Network Security**	**4**	**1**
	1.1 Basics of Networking (LAN, WAN, Internet) 1.2 OSI and TCP/IP Models Overview 1.3 Introduction to Web Applications 1.4 Need for Web and Network Security 1.5 Common Cyber Threats		
2	**Web Application Fundamentals**	**4**	**2**
	2.1 HTTP and HTTPS Protocols 2.2 Structure of Web Applications 2.3 Client-Server Architecture 2.4 Introduction to Web Vulnerabilities 2.5 OWASP Top 10 Overview		
3	**Network Security Fundamentals**	**6**	**3**
	3.1 Firewalls and Types 3.2 Intrusion Detection and Prevention Systems (IDS/IPS) 3.3 VPN Basics 3.4 Network Scanning using Nmap 3.5 Packet Analysis using Wireshark		
4	**Web and Network Attacks**	**8**	**4**
	4.1 SQL Injection Basics 4.2 Cross-Site Scripting (XSS) Basics 4.3 Phishing and Social Engineering 4.4 Denial of Service (DoS) Overview 4.5 Basic Traffic and Log Analysis		
5	**Security Measures and Best Practices**	**8**	**5**
	5.1 Secure Configuration of Systems 5.2 Password Policies and Authentication Methods 5.3 Basics of Encryption (SSL/TLS) 5.4 Patch Management and Updates 5.5 Risk Assessment Basics		

6	**Practical Implementation and Reporting**	**6**	**6**
	6.1 Introduction to Tools (Burp Suite, Nikto) 6.2 Basic Vulnerability Scanning 6.3 Secure Web Application Practices 6.4 Basic Network Security Setup 6.5 Preparing Simple Security Report		

Reference Books:

- Web Application Hacker's Handbook – Dafydd Stuttard & Marcus Pinto
- Network Security Essentials – William Stallings
- Computer Networking: A Top-Down Approach – James F. Kurose & Keith W. Ross
- OWASP Testing Guide (Open Web Application Security Project)

PRACTICAL BASED ON WEB & NETWORK SECURITY FUNDAMENTALS

Programme Name :	**B.Sc. Cyber and Digital Science**
Class :	**T. Y. B.Sc Cyber and Digital Science**
Semester :	V
Course Type :	Major Elective Practical
Course Code :	CDS-308-MJP
Course Title :	Practical based on Web and Network Security Fundamentals (CDS-307MJ)
No. of Credits :	02

A. Rationale:
This practical course provides hands-on experience in web and network security concepts. It enables students to perform basic security testing, network analysis, and vulnerability identification using industry tools. The course helps learners understand real-world attack techniques and defensive measures, preparing them for roles in network security and web application security.

B. INDUSTRY / EMPLOYER EXPECTED OUTCOME:

- **Develops skills in basic web and network security testing**
- **Prepares students for roles such as network security analyst and SOC analyst**
- **Enhances ability to identify vulnerabilities and analyze network traffic**
- **Builds knowledge of security tools and defensive practices**

C. COURSE OUTCOMES (COs):

CO No.	Course Outcome Statement
CO1	Perform basic network and web security testing tasks
CO2	Identify common web and network vulnerabilities
CO3	Apply tools for scanning and traffic analysis
CO4	Analyze network packets and web application behavior
CO5	Evaluate security configurations and mitigation techniques
CO6	Prepare basic security assessment reports

D. COURSE STRUCTURE AND CONTENTS:

Practical 1: Networking Basics and Setup (6 hours)

- Configure basic network settings
- Verify connectivity using ping, traceroute
- Activity: Setup small network environment

Practical 2: Network Scanning (4 hours)

- Perform scanning using Nmap
- Identify open ports and services
- Activity: Analyze scan results

Practical 3: Packet Analysis (4 hours)

- Capture traffic using Wireshark
- Analyze packets and protocols
- Activity: Identify suspicious traffic

Practical 4: Web Application Testing (4 hours)

- Use tools: Burp Suite (Basic), Nikto
- Intercept HTTP requests
- Activity: Identify basic vulnerabilities

Practical 5: Security Configuration (4 hours)

- Configure firewall (basic rules)
- Apply password policies
- Activity: Secure system configuration

Practical 6: Vulnerability Scanning and Reporting (4 hours)

- Perform basic vulnerability scan
- Document findings
- Activity: Prepare security report

E. SUGGESTED MICRO PROJECT / ASSIGNMENT:

- Perform vulnerability scan on test system
- Analyze captured network traffic
- Prepare report on identified vulnerabilities

F. GENERAL / OVERALL EXPECTATIONS:

1. Students will perform basic security testing tasks
2. Students will analyze network and web traffic
3. Students will use security tools effectively
4. Students will identify vulnerabilities and risks
5. Students will develop reporting and documentation skills

MOBILE FORENSICS

Programme Name :	**B.Sc. Cyber and Digital Science**
Class :	**T. Y. B.Sc Cyber and Digital Science**
Semester :	V
Course Type :	Major Elective (Theory)
Course Code :	CDS-309-MJ
Course Title :	Mobile forensic
No. of Credits :	02
No. of Teaching Hours :	30

A. Rationale:

Mobile forensics focuses on the identification, acquisition, and analysis of data from mobile devices such as smartphones and tablets. With the increasing use of mobile devices in daily life, they have become a major source of digital evidence in cybercrime investigations. This subject introduces students to mobile operating systems, data storage, and forensic tools used to extract and analyze data. It helps learners understand real-world investigation scenarios and prepares them for roles in digital forensics and cyber investigation.

B. INDUSTRY / EMPLOYER EXPECTED OUTCOME:

- Develops skills in mobile device investigation and evidence handling
- Prepares students for roles such as digital forensic analyst
- Enhances ability to analyze mobile data and recover evidence
- Builds understanding of mobile security and forensic tools

C. COURSE OUTCOMES (COs):

CO No.	Course Outcome Statement
CO1	Recall basic concepts of mobile forensics and mobile device architecture.
CO2	Explain mobile operating systems and data storage mechanisms.
CO3	Apply techniques to acquire and extract data from mobile devices.
CO4	Analyze mobile device data for forensic investigation.

CO5	Evaluate forensic tools and mobile investigation methods.
CO6	Create basic forensic reports based on mobile data analysis.

Syllabus

Unit	Course Contents	Hours	CO
1	**Introduction to Mobile Forensics**	**4**	**1**
	1.1 Overview of Mobile Forensics 1.2 Types of Mobile Devices 1.3 Mobile Operating Systems (Android, iOS Basics) 1.4 Importance of Mobile Evidence 1.5 Challenges in Mobile Forensics		
2	**Mobile Device Architecture**	**4**	**2**
	2.1 Mobile Hardware Components 2.2 SIM, Memory and Storage 2.3 File Systems in Mobile Devices 2.4 Data Storage Locations 2.5 Mobile Security Features		
3	**Data Acquisition Techniques**	**6**	**3**
	3.1 Logical and Physical Acquisition 3.2 Manual Acquisition Methods 3.3 Backup Extraction 3.4 Introduction to Mobile Forensic Tools 3.5 Data Preservation Techniques		
4	**Mobile Data Analysis**	**8**	**4**
	4.1 Call Logs and Contacts Analysis 4.2 SMS and Messaging Analysis 4.3 Application Data Analysis 4.4 Media Files and Document Analysis 4.5 Location and GPS Data Analysis		
5	**Tools and Investigation**	**8**	**5**
	5.1 Tools: Cellebrite, Oxygen, Autopsy (Overview) 5.2 Mobile Forensic Toolkits 5.3 Evidence Handling Procedures 5.4 Chain of Custody Basics 5.5 Legal and Ethical Considerations		
6	**Reporting and Case Study**	**6**	**6**
	6.1 Mobile Forensic Report Writing 6.2 Documentation Techniques 6.3 Case Study Analysis 6.4 Evidence Presentation 6.5 Best Practices in Investigation		

Reference Books:

- Mobile Forensic Investigations – Lee Reiber
- Android Forensics – Andrew Hoog
- Practical Mobile Forensics – Satish Bommisetty
- Digital Forensics with Open Source Tools – Cory Altheide

Practical based on Mobile Forensics

Programme Name :	**B.Sc. Cyber and Digital Science**
Class :	**T. Y. B.Sc Cyber and Digital Science**
Semester :	V
Course Type :	Major Elective Practical
Course Code :	CDS-310-MJP
Course Title :	Practical based on Mobile Forensics (CDS-309MJ)
No. of Credits :	02

A. Rationale:

This practical course provides hands-on experience in mobile forensic investigation techniques. It enables students to acquire, extract, and analyze data from mobile devices using forensic tools and methods. The course helps learners understand real-world mobile investigation scenarios and prepares them for roles in digital forensics and cybercrime investigation.

B. INDUSTRY / EMPLOYER EXPECTED OUTCOME:

- Develops skills in mobile device investigation and evidence handling
- Prepares students for roles such as mobile forensic analyst
- Enhances ability to extract and analyze mobile data
- Builds knowledge of forensic tools and mobile security

C. COURSE OUTCOMES (COs):

CO No.	Course Outcome Statement
CO1	Perform mobile forensic acquisition and analysis tasks
CO2	Identify mobile device data types and storage locations
CO3	Apply techniques to extract data from mobile devices
CO4	Analyze mobile artifacts such as messages, logs, and media
CO5	Evaluate tools and methods used in mobile forensics
CO6	Prepare mobile forensic investigation reports

D. COURSE STRUCTURE AND CONTENTS:

Practical 1: Introduction to Mobile Forensics (6 hours)

- Overview of mobile forensic tools
- Setup mobile analysis environment
- Activity: Identify types of mobile evidence

Practical 2: Mobile Device Acquisition (4 hours)

- Logical acquisition techniques
- Backup extraction methods
- Activity: Extract basic device data

Practical 3: Data Extraction and Analysis (4 hours)

- Analyze call logs, SMS, contacts
- Examine application data
- Activity: Identify user activity

Practical 4: Media and File Analysis (4 hours)

- Analyze images, videos, documents
- Recover deleted files (basic)
- Activity: Identify hidden data

Practical 5: Location and Network Data Analysis (4 hours)

- Analyze GPS/location data
- Examine network connections
- Activity: Track device activity

Practical 6: Reporting and Case Study (4 hours)

- Prepare forensic report
- Document findings and evidence
- Activity: Case study analysis

E. SUGGESTED MICRO PROJECT / ASSIGNMENT:

- Analyze mobile backup data and prepare report
- Extract and document user activity
- Perform basic forensic investigation on sample data

F. GENERAL / OVERALL EXPECTATIONS:

1. Students will perform mobile forensic investigations
2. Students will analyze and interpret mobile data
3. Students will use forensic tools effectively
4. Students will identify digital evidence from mobile devices
5. Students will develop reporting and documentation skills

Linux and Web Server Hardening

Programme Name :	**B.Sc. Cyber and Digital Science**
Class :	**T. Y. B.Sc Cyber and Digital Science**
Semester :	V
Course Type :	VSC (Theory)
Course Code :	CDS-321-VSCP
Course Title :	Linux and Web Server Hardening
No. of Credits :	02
No. of Teaching Hours :	60

A. Rationale:

Linux and Web Server Hardening is an essential subject that focuses on securing operating systems and web servers against cyber threats. This course introduces students to Linux system security, user management, access control, and web server configuration. It helps students understand how to secure servers in real-world environments using best practices. The subject prepares learners for roles in system administration, network security, and server management.

B. INDUSTRY / EMPLOYER EXPECTED OUTCOME:

- Develops skills in securing Linux systems and web servers
- Prepares students for roles such as system administrator and security analyst
- Enhances ability to configure and manage secure server environments
- Builds knowledge of server hardening techniques and best practices

C. COURSE OUTCOMES (COs):

CO No.	Course Outcome Statement
CO1	Recall basic concepts of Linux systems and server security.
CO2	Explain Linux security mechanisms and web server configuration.
CO3	Apply techniques to secure Linux systems and web servers.
CO4	Analyze system logs and server activities for security issues.

CO5	Evaluate security configurations and hardening methods.
CO6	Create secure Linux and web server configurations.

Syllabus

Unit	Course Contents	Hours	CO
1	**Introduction to Linux Security**	**4**	**1**
	1.1 Basics of Linux Operating System 1.2 Linux File System Structure 1.3 User and Group Management 1.4 Permissions and Access Control 1.5 Need for System Security		
2	**Linux Hardening Techniques**	**4**	**2**
	2.1 Password Policies 2.2 File Permissions and Ownership 2.3 Secure Shell (SSH) Configuration 2.4 Firewall Basics (iptables, ufw) 2.5 System Updates and Patch Management		
3	**Web Server Basics**	**6**	**3**
	3.1 Introduction to Web Servers 3.2 Apache and Nginx Overview 3.3 Server Installation and Configuration 3.4 Virtual Hosting Basics 3.5 Server Logs		
4	**Web Server Hardening**	**8**	**4**
	4.1 Securing Apache/Nginx 4.2 SSL/TLS Configuration 4.3 Directory Listing and Access Control 4.4 Protecting Against Common Attacks 4.5 Log Monitoring and Analysis		
5	**Monitoring and Security Tools**	**8**	**5**
	5.1 Intrusion Detection Basics 5.2 Log Monitoring Tools 5.3 Fail2Ban Overview 5.4 System Monitoring Tools 5.5 Backup and Recovery		
6	**Best Practices and Case Study**	**6**	**6**
	6.1 Linux Security Best Practices 6.2 Server Hardening Checklist 6.3 Case Study on Server Attack 6.4 Incident Handling Basics 6.5 Secure Deployment Practices		

Reference Books:

- Linux Hardening in Hostile Networks – Kyle Rankin
- Practical Linux Security Cookbook – Tajinder Kalsi
- Web Server Security – Dinesh Goyal
- Linux Administration Handbook – Evi Nemeth

PROJECT / HANDS-ON TRAINING (CDS-331-FP)

Programme Name :	**B.Sc. Cyber and Digital Science**
Class :	**T. Y. B.Sc Cyber and Digital Science**
Semester :	V
Course Type :	Project / Field Project
Course Code :	CDS-331-FP
Course Title :	Project
No. of Credits :	02

A. Rationale:

The project course is designed to provide students with an opportunity to apply theoretical and practical knowledge gained throughout the semester in a real-world scenario. It enables students to work on cybersecurity-related problems, develop solutions, and enhance their analytical, technical, and research skills. The course prepares students for industry-level problem solving and project execution.

B. INDUSTRY / EMPLOYER EXPECTED OUTCOME:

- Develops problem-solving and analytical skills
- Prepares students for real-world cybersecurity projects
- Enhances research, development, and documentation skills
- Builds teamwork and project management abilities

C. COURSE OUTCOMES (COs):

CO No.	Course Outcome Statement
CO1	Identify and define a cybersecurity problem or project topic
CO2	Understand project requirements and plan implementation
CO3	Apply technical skills to develop a solution
CO4	Analyze results and validate project outcomes

CO5	Evaluate effectiveness of the implemented solution
CO6	Prepare and present project report and documentation

D. COURSE STRUCTURE AND CONTENTS:

Phase 1: Project Selection and Planning (6 hours)
- Identify project domain (Forensics, Web Security, Malware, etc.)
- Define problem statement
- Prepare project proposal

Phase 2: Design and Development (8 hours)
- Design system architecture
- Implement project using tools/technologies
- Develop working model

Phase 3: Testing and Validation (6 hours)
- Test project functionality
- Identify and fix issues
- Validate results

Phase 4: Documentation and Reporting (6 hours)
- Prepare project report
- Include diagrams, screenshots
- Document methodology

Phase 5: Presentation and Evaluation (4 hours)
- Present project to panel
- Demonstrate working
- Answer questions

E. SUGGESTED PROJECT AREAS:
- Phishing Detection System
- Malware Analysis Tool
- Network Traffic Analyzer
- Web Vulnerability Scanner
- Digital Forensic Toolkit
- Password Strength Checker

F. GENERAL / OVERALL EXPECTATIONS:
1. Students will complete a working cybersecurity project
2. Students will apply practical and theoretical knowledge
3. Students will develop problem-solving skills
4. Students will improve documentation and presentation skills
5. Students will gain industry-level project experience

Data Analytics and Business Intelligence

Programme Name :	**B.Sc. Cyber and Digital Science**
Class :	**T. Y. B.Sc Cyber and Digital Science**
Semester :	**V**
Course Type :	**Minor (Theory)**
Course Code :	**CDS-341-MN**
Course Title :	**Data Analytics and Business Intelligence**
No. of Credits :	**02**
No. of Teaching Hours :	**30**

A. Rationale:

Data Analytics and Business Intelligence focuses on analyzing data to support decision-making processes in organizations. This subject introduces students to data analysis techniques, visualization, and business intelligence tools. It helps students understand how data is used to identify trends, patterns, and insights. The course prepares learners for roles in data analysis, business intelligence, and decision support systems.

B. INDUSTRY / EMPLOYER EXPECTED OUTCOME:

- **Develops skills in data analysis and interpretation**
- **Prepares students for roles such as data analyst and business analyst**
- **Enhances ability to visualize and present data insights**
- **Builds knowledge of business intelligence tools and techniques**

C. COURSE OUTCOMES (COs):

CO No.	Course Outcome Statement
CO1	Recall basic concepts of data analytics and business intelligence.
CO2	Explain data processing, analysis, and visualization techniques.
CO3	Apply tools to analyze and visualize data.
CO4	Analyze data to identify patterns and trends.

CO5	Evaluate data-driven decisions and insights.
CO6	Create reports and dashboards for business intelligence.

Syllabus

Unit	Course Contents	Hours	CO
1	**Introduction to Data Analytics**	**4**	**1**
	1.1 What is Data Analytics 1.2 Types of Data 1.3 Data Analytics Process 1.4 Applications of Data Analytics 1.5 Importance in Business		
2	**Data Processing and Preparation**	**4**	**2**
	2.1 Data Collection Methods 2.2 Data Cleaning 2.3 Data Transformation 2.4 Data Storage Concepts 2.5 Introduction to Databases		
3	**Data Analysis Techniques**	**6**	**3**
	3.1 Descriptive Analysis 3.2 Basic Statistical Concepts 3.3 Data Aggregation 3.4 Introduction to Excel for Analysis 3.5 Data Filtering and Sorting		
4	**Data Visualization**	**8**	**4**
	4.1 Importance of Visualization 4.2 Charts and Graphs 4.3 Dashboard Basics 4.4 Tools: Excel, Power BI (Overview) 4.5 Interpreting Visual Data		
5	**Business Intelligence Concepts**	**8**	**5**
	5.1 Introduction to BI 5.2 BI Architecture 5.3 Data Warehousing Basics 5.4 Reporting Tools 5.5 Decision Support Systems		
6	**Reporting and Case Study**	**6**	**6**
	6.1 Report Preparation 6.2 Data Interpretation 6.3 Business Case Studies 6.4 Decision Making using Data 6.5 Future Trends in BI		

Reference Books:

- Data Science for Business – Foster Provost
- Business Intelligence Guidebook – Rick Sherman
- Data Analytics Made Accessible – Anil Maheshwari
- Microsoft Power BI Guide

SEM VI

Semester VI

Digital Forensics – II

Programme Name :	B.Sc. Cyber and Digital Science
Class :	T. Y. Cyber and Digital Science
Semester :	VI
Course Type :	Major Core (Theory)
Course Code :	CDS-351-MJ
Course Title :	Digital Forensics – II
No. of Credits :	02
No. of Teaching Hours :	30

A. Rationale:

Digital Forensics – II is an advanced continuation of Digital Forensics – I and focuses on modern forensic investigation techniques used in real-world scenarios. This subject introduces students to advanced areas such as memory forensics, mobile forensics, and cloud forensics. It also covers evidence correlation, timeline analysis, and handling complex cyber incidents. The course helps students develop practical investigation skills and prepares them for professional roles in digital forensics, incident response, and cybercrime investigation.

B. INDUSTRY / EMPLOYER EXPECTED OUTCOME:

- Develops advanced skills in digital forensic investigation and evidence handling
- Prepares students for roles such as digital forensic analyst and incident responder
- Enhances ability to analyze memory, mobile, and cloud-based evidence
- Builds knowledge of advanced forensic tools and real-world investigation techniques

C. COURSE OUTCOMES (COs):

Course Outcome Table:

CO No.	Course Outcome Statement
CO1	Recall advanced concepts of digital forensics and modern investigation techniques.
CO2	Explain memory, mobile, and cloud forensic techniques.

CO3	Apply advanced forensic tools for evidence acquisition and analysis.
CO4	Analyze digital evidence from multiple sources and environments.
CO5	Evaluate forensic methods and tools for complex investigation scenarios.
CO6	Create detailed forensic reports and present findings for legal and professional use.

D. Syllabus

Unit	Course Contents	Hours	CO
1	**Advanced Digital Forensics Concepts**	**4**	**1**
	1.1 Review of Digital Forensics Fundamentals 1.2 Advanced Forensic Investigation Process 1.3 Types of Advanced Digital Forensics 1.4 Challenges in Digital Investigations 1.5 Legal and Ethical Considerations (Advanced)		
2	**Memory and Live Forensics**	**4**	**2**
	2.1 Introduction to Memory Forensics 2.2 RAM Acquisition Techniques 2.3 Live System Forensics 2.4 Memory Artifacts Analysis 2.5 Tools: Volatility (Basics)		
3	**Mobile Device Forensics**	**6**	**3**
	3.1 Introduction to Mobile Forensics 3.2 Mobile Data Acquisition Methods 3.3 Android Forensics Basics 3.4 Mobile Artifacts (Call logs, SMS, App data) 3.5 Tools: Oxygen, Autopsy (Mobile Module)		
4	**Cloud and Network Forensics**	**8**	**4**
	4.1 Introduction to Cloud Forensics 4.2 Cloud Data Acquisition Challenges 4.3 Log Analysis in Cloud Environments 4.4 Advanced Network Forensics 4.5 Correlation of Multiple Evidence Sources		
5	**Advanced Investigation Techniques**	**8**	**5**
	5.1 Timeline Analysis 5.2 Event Reconstruction 5.3 Anti-Forensics Techniques 5.4 Detection of Anti-Forensics 5.5 Case-Based Investigation Approach		
6	**Reporting and Legal Procedures**	**6**	**6**
	6.1 Advanced Forensic Report Writing 6.2 Expert Witness and Court Procedures 6.3 Evidence Presentation Techniques 6.4 Legal Compliance and Standards 6.5 Real-world Case Studies		

Reference Books:

- Digital Forensics and Incident Response – Jason T. Luttgens
- Guide to Computer Forensics and Investigations – Bill Nelson
- The Art of Memory Forensics – Michael Hale Ligh
- Mobile Forensic Investigations – Lee Reiber
- Cloud Forensics – Paul T. Jaeger

PRACTICAL BASED ON DIGITAL FORENSICS – II

Programme Name :	**B.Sc. Cyber and Digital Science**
Class :	**T. Y. B.Sc Cyber and Digital Science**
Semester :	VI
Course Type :	Major Core Practical
Course Code :	CDS-355-MJP
Course Title :	Practical based on Digital Forensics – II (CDS-351MJ)
No. of Credits :	02

A. Rationale:

This practical course provides advanced hands-on experience in digital forensic investigation techniques. It enables students to analyze complex digital evidence such as memory data, network artifacts, and system logs. The course prepares learners for real-world forensic investigations and incident response scenarios.

B. INDUSTRY / EMPLOYER EXPECTED OUTCOME:

- Develops advanced forensic investigation skills
- Prepares students for roles such as forensic analyst and incident responder
- Enhances ability to analyze complex digital evidence
- Builds expertise in forensic tools and reporting

C. COURSE OUTCOMES (COs):

CO No.	Course Outcome Statement
CO1	Perform advanced forensic data acquisition techniques
CO2	Analyze memory and system artifacts
CO3	Apply forensic tools for investigation
CO4	Analyze network and log-based evidence
CO5	Evaluate forensic investigation processes
CO6	Prepare detailed forensic reports

D. COURSE STRUCTURE AND CONTENTS:

Practical 1: Advanced Evidence Acquisition (6 hours)

- Live and remote acquisition
- Memory acquisition tools
- Activity: Capture memory dump

Practical 2: Memory Forensics (4 hours)

- Analyze RAM using tools (Volatility basic)
- Identify running processes
- Activity: Extract artifacts

Practical 3: Log and Timeline Analysis (4 hours)

- Analyze system logs
- Create timeline of events
- Activity: Identify suspicious activity

Practical 4: Network Forensics (4 hours)

- Capture and analyze packets
- Identify attack patterns
- Activity: Investigate network traffic

Practical 5: Advanced File and Artifact Analysis (4 hours)

- Analyze browser artifacts
- Recover hidden data
- Activity: Extract user activity

Practical 6: Reporting and Case Study (4 hours)

- Prepare detailed forensic report
- Document investigation steps
- Activity: Case study analysis

E. SUGGESTED MICRO PROJECT / ASSIGNMENT:

- Analyze memory dump and prepare report
- Perform full forensic investigation on sample case
- Create timeline-based analysis

F. GENERAL / OVERALL EXPECTATIONS:

1. Students will perform advanced forensic investigations
2. Students will analyze memory and network data
3. Students will use advanced forensic tools
4. Students will develop reporting and analysis skills
5. Students will handle real-world forensic scenarios

Vulnerability Assessment & Penetration Testing

Programme Name :	B.Sc. Cyber and Digital Science
Class :	T. Y. B.Sc. Cyber and Digital Science
Semester :	VI
Course Type :	Major Core (Theory)
Course Code :	CDS-352-MJ
Course Title :	Vulnerability Assessment & Penetration Testing
No. of Credits :	02
No. of Teaching Hours :	30

A. Rationale:

Vulnerability Assessment and Penetration Testing (VAPT) is a critical area in cybersecurity that focuses on identifying, analyzing, and mitigating security vulnerabilities in systems, networks, and web applications. This subject provides students with advanced knowledge of security testing methodologies, tools, and techniques used in real-world environments. It helps students understand

how attackers exploit vulnerabilities and how organizations defend against such threats. The course prepares students for professional roles in penetration testing, security auditing, and vulnerability management.

B. INDUSTRY / EMPLOYER EXPECTED OUTCOME:

- Develops practical skills in identifying and assessing system vulnerabilities
- Prepares students for roles such as penetration tester and security analyst
- Enhances ability to perform security testing using industry tools
- Builds understanding of risk assessment and vulnerability management

C. COURSE OUTCOMES (COs):

Course Outcome Table:

CO No.	Course Outcome Statement
CO1	Recall concepts of vulnerability assessment and penetration testing.
CO2	Explain VAPT methodologies, tools, and testing processes.
CO3	Apply tools and techniques to identify vulnerabilities in systems and networks.

CO4	Analyze vulnerabilities and security weaknesses in different environments.
CO5	Evaluate security risks and recommend mitigation strategies.
CO6	Create detailed vulnerability assessment and penetration testing reports.

Syllabus

Unit	Course Contents	Hours	CO
1	**Introduction to VAPT**	**4**	**1**
	1.1 Basics of Vulnerability Assessment 1.2 Basics of Penetration Testing 1.3 Difference between VA and PT 1.4 Types of Penetration Testing 1.5 Legal and Ethical Considerations		
2	**VAPT Methodology**	**4**	**2**
	2.1 VAPT Lifecycle 2.2 Information Gathering Techniques 2.3 Scanning and Enumeration 2.4 Vulnerability Identification 2.5 Tools: Nmap, Nikto		
3	**Web Application Testing**	**6**	**3**
	3.1 SQL Injection Testing 3.2 Cross-Site Scripting (XSS) Testing 3.3 Authentication Testing 3.4 Session Management Testing 3.5 Tools: Burp Suite, OWASP ZAP		
4	**Network Penetration Testing**	**8**	**4**
	4.1 Network Scanning Techniques 4.2 Service Enumeration 4.3 Exploitation Basics 4.4 Password Attacks Basics 4.5 Tools: Metasploit (Basic), Hydra 4.6 Traffic Analysis		
5	**Risk Assessment and Mitigation**	**8**	**5**
	5.1 Risk Assessment Concepts 5.2 Vulnerability Scoring (CVSS Basics) 5.3 Patch Management 5.4 Secure Configuration Practices 5.5 Security Controls and Mitigation		
6	**Reporting and Case Study**	**6**	**6**
	6.1 VAPT Report Writing 6.2 Documentation and Evidence Collection 6.3 Vulnerability Classification 6.4 Case Study on Security Testing 6.5 Remediation Techniques		

Reference Books:

- Penetration Testing: A Hands-On Introduction to Hacking – Georgia Weidman
- The Web Application Hacker's Handbook – Dafydd Stuttard
- Network Security Assessment – Chris McNab
- OWASP Testing Guide

PRACTICAL BASED ON VULNERABILITY ASSESSMENT & PENETRATION TESTING (VAPT)

Programme Name :	**B.Sc. Cyber and Digital Science**
Class :	**T. Y. B.Sc Cyber and Digital Science**
Semester :	VI
Course Type :	Major Core Practical
Course Code :	CDS-356-MJP
Course Title :	Practical based on Vulnerability Assessment & Penetration Testing
No. of Credits :	02

A. Rationale:

This practical course provides hands-on experience in identifying, analyzing, and exploiting security vulnerabilities in systems and applications. It enables students to perform vulnerability assessment and basic penetration testing using industry tools. The course prepares learners to understand real-world attack techniques and implement security measures.

B. INDUSTRY / EMPLOYER EXPECTED OUTCOME:

- Develops skills in vulnerability assessment and penetration testing
- Prepares students for roles such as penetration tester and security analyst
- Enhances ability to identify and exploit system vulnerabilities
- Builds knowledge of security tools and mitigation techniques

C. COURSE OUTCOMES (COs):

CO No.	Course Outcome Statement
CO1	Perform vulnerability scanning on systems and networks
CO2	Identify common security vulnerabilities
CO3	Apply penetration testing techniques
CO4	Analyze vulnerabilities and exploit results
CO5	Evaluate security risks and mitigation strategies
CO6	Prepare vulnerability assessment and penetration testing reports

D. COURSE STRUCTURE AND CONTENTS:

Practical 1: Lab Setup and Introduction (6 hours)

- Setup Kali Linux environment
- Configure target machines (Metasploitable / DVWA)
- Activity: Create testing lab

Practical 2: Network Scanning (4 hours)

- Use Nmap for scanning
- Identify open ports and services
- Activity: Analyze scan results

Practical 3: Vulnerability Scanning (4 hours)

- Use tools: OpenVAS / Nessus (basic)
- Identify vulnerabilities
- Activity: Generate vulnerability report

Practical 4: Exploitation Basics (4 hours)

- Use Metasploit Framework
- Perform basic exploitation
- Activity: Gain access to target system

Practical 5: Web Application Testing (4 hours)

- Test vulnerabilities (SQLi, XSS basic)
- Use tools: Burp Suite
- Activity: Identify web vulnerabilities

Practical 6: Reporting and Mitigation (4 hours)

- Document findings
- Suggest mitigation techniques
- Activity: Prepare VAPT report

E. SUGGESTED MICRO PROJECT / ASSIGNMENT:

- Perform vulnerability assessment on test system
- Analyze and document vulnerabilities
- Prepare penetration testing report

F. GENERAL / OVERALL EXPECTATIONS:

1. Students will perform vulnerability assessment tasks
2. Students will identify and exploit vulnerabilities
3. Students will use penetration testing tools effectively
4. Students will analyze security risks
5. Students will develop reporting and documentation skills

Cyber Crime & Reports

Programme Name :	B.Sc. Cyber and Digital Science
Class :	T. Y. B.Sc. Cyber and Digital Science
Semester :	VI
Course Type :	Major Core (Theory)
Course Code :	CDS-353-MJ
Course Title :	Cyber Crime & Reports
No. of Credits :	02
No. of Teaching Hours :	30

A. Rationale:

Cyber Crime & Reports is an important subject in cybersecurity that focuses on understanding various types of cybercrimes, their investigation, and reporting procedures. This course introduces students to cybercrime laws, digital evidence handling, and documentation required in legal and professional environments. It helps students understand how cyber incidents are reported, investigated, and presented in court. The subject prepares learners for roles in cybercrime investigation, law enforcement support, and cybersecurity compliance.

B. INDUSTRY / EMPLOYER EXPECTED OUTCOME:

- Develops knowledge of different types of cybercrimes and investigation procedures
- Prepares students for roles in cybercrime investigation and legal support
- Enhances ability to document and report cyber incidents professionally
- Builds understanding of cyber laws, compliance, and legal frameworks

C. COURSE OUTCOMES (COs):

Course Outcome Table:

CO No.	Course Outcome Statement
CO1	Recall concepts of cybercrime, types, and legal frameworks.
CO2	Explain cybercrime investigation processes and legal procedures.
CO3	Apply techniques for handling and documenting digital evidence.
CO4	Analyze cybercrime cases and investigation reports.

CO5	Evaluate legal, ethical, and compliance aspects in cybercrime cases.
CO6	Create professional cybercrime reports and documentation.

Syllabus

Unit	Course Contents	Hours	CO
1	**Introduction to Cyber Crime**	**4**	**1**
	1.1 Definition of Cyber Crime 1.2 Types of Cyber Crimes 1.3 Cyber Crime Trends 1.4 Impact of Cyber Crimes 1.5 Overview of Cyber Laws		
2	**Cyber Laws and Legal Framework**	**4**	**2**
	2.1 IT Act (India) Overview 2.2 Cyber Law Provisions 2.3 Legal Procedures in Cybercrime Investigation 2.4 Roles of Law Enforcement Agencies 2.5 Digital Evidence and Legal Issues		
3	**Cyber Crime Investigation Process**	**6**	**3**
	3.1 Investigation Methodology 3.2 Evidence Collection Techniques 3.3 Evidence Preservation 3.4 Chain of Custody 3.5 Use of Forensic Tools in Investigation		
4	**Analysis of Cyber Crimes**	**8**	**4**
	4.1 Case Analysis Techniques 4.2 Financial Cyber Crimes 4.3 Identity Theft and Fraud 4.4 Social Media Crimes 4.5 Email and Phishing Attacks 4.6 Incident Analysis		
5	**Legal and Ethical Issues**	**8**	**5**
	5.1 Privacy and Data Protection 5.2 Ethical Issues in Cyber Investigation 5.3 Compliance Requirements 5.4 Cyber Security Policies 5.5 Legal Challenges in Cybercrime Cases		
6	**Reporting and Documentation**	**6**	**6**
	6.1 Cyber Crime Report Writing 6.2 FIR and Complaint Documentation 6.3 Evidence Documentation 6.4 Case Report Preparation 6.5 Court Presentation Basics		

Reference Books:

- Cyber Law – Pavan Duggal
- Cyber Crimes and Law – Nina Godbole
- Guide to Computer Forensics and Investigations – Bill Nelson
- Information Technology Act, 2000 (India)

Semester: VI

ACTIVE DIRECTORY FUNDAMENTALS AND ATTACKS

Programme Name :	**B.Sc. Cyber and Digital Science**
Class :	**T. Y. B.Sc Cyber and Digital Science**
Semester :	VI
Course Type :	Major Core (Theory)
Course Code :	CDS-354-MJ
Course Title :	Active Directory Fundamentals and Attacks
No. of Credits :	02
No. of Teaching Hours :	30

A. Rationale:

Active Directory is one of the most widely used identity and access management systems in enterprise environments. This subject introduces students to the fundamentals of Active Directory, including domain structure, authentication, group policies, and user management. It also covers common attack techniques targeting Active Directory environments and basic defensive measures. The course helps learners understand enterprise security concepts and prepares them for roles in system administration, SOC operations, and cybersecurity.

B. INDUSTRY / EMPLOYER EXPECTED OUTCOME:

- Develops understanding of Active Directory architecture and administration
- Prepares students for roles such as SOC analyst and system administrator
- Enhances ability to identify common Active Directory attacks
- Builds knowledge of authentication, access control, and AD security practices

C. COURSE OUTCOMES (COs):

CO No.	Course Outcome Statement
CO1	Recall basic concepts of Active Directory and domain services.
CO2	Explain Active Directory structure, authentication, and policies.
CO3	Apply Active Directory management and configuration techniques.

CO4	Analyze common Active Directory attack methods and vulnerabilities.
CO5	Evaluate security controls and mitigation techniques in AD environments.
CO6	Create basic security assessment and incident reports for AD systems.

D. Syllabus

Unit	Course Contents	Hours	CO
1	**Introduction to Active Directory**	**4**	**1**
	1.1 Introduction to Active Directory 1.2 Domain, Forest and Tree Concepts 1.3 Active Directory Components 1.4 Roles of Domain Controller 1.5 Importance of Active Directory in Enterprises		
2	Authentication and Policies	4	2
	2.1 Authentication Basics 2.2 Kerberos Authentication Overview 2.3 LDAP Basics 2.4 Group Policy Basics 2.5 User and Access Management		
3	Active Directory Administration	6	3
	3.1 User and Group Management 3.2 Organizational Units (OU) 3.3 Password and Account Policies 3.4 Active Directory Tools Overview 3.5 Basic AD Configuration		
4	Active Directory Attacks	8	4
	4.1 Password Attacks Basics 4.2 Pass-the-Hash Overview 4.3 Kerberoasting Basics 4.4 Privilege Escalation Concepts 4.5 Enumeration Techniques		
5	Security and Mitigation	8	5
	5.1 Hardening Active Directory 5.2 Access Control Best Practices 5.3 Monitoring and Logging		

	5.4 Incident Detection Basics 5.5 Security Policies and Updates		
6	Reporting and Case Studies	6	6
	6.1 Active Directory Security Assessment 6.2 Incident Documentation 6.3 Attack Case Studies 6.4 Mitigation Strategies 6.5 Best Practices for AD Security		

Reference Books:

Active Directory Administration Cookbook – Sander Berkouwer
The Practice of Network Security Monitoring – Richard Bejtlich
Blue Team Handbook – Don Murdoch
Microsoft Active Directory Documentation

Advanced Web Application Security

Programme Name :	B.Sc. Cyber and Digital Science
Class :	T. Y. B.Sc. Cyber and Digital Science
Semester :	VI
Course Type :	Major Elective (Theory)
Course Code :	CDS-357-MJ
Course Title :	Advanced Web Application Security
No. of Credits :	02
No. of Teaching Hours :	30

A. Rationale:

Advanced Web Application Security is a specialized subject that focuses on securing modern web applications against sophisticated cyber attacks. This course builds upon fundamental web security concepts and introduces advanced vulnerabilities, exploitation techniques, and secure development practices. Students will learn how attackers target web applications and how to identify, test, and mitigate these vulnerabilities using industry-standard tools. The subject prepares learners for roles in web security testing, application security, and penetration testing.

B. INDUSTRY / EMPLOYER EXPECTED OUTCOME:

- Develops advanced skills in identifying and testing web application vulnerabilities
- Prepares students for roles such as web application security tester and penetration tester
- Enhances ability to perform secure coding and vulnerability mitigation
- Builds expertise in industry tools used for web security testing

C. COURSE OUTCOMES (COs):

Course Outcome Table:

CO No.	Course Outcome Statement
CO1	Recall advanced web application security concepts and attack types.
CO2	Explain advanced web vulnerabilities and secure coding practices.
CO3	Apply tools and techniques to test and exploit web application vulnerabilities.

CO4	Analyze web application behavior to identify security flaws.
CO5	Evaluate security controls and mitigation techniques for web applications.
CO6	Create detailed web application security testing reports.

Syllabus

Unit	Course Contents	Hours	CO
1	**Advanced Web Security Concepts**	**4**	**1**
	1.1 Review of Web Security Fundamentals 1.2 Advanced Threat Landscape for Web Applications 1.3 Web Application Architecture Overview 1.4 Secure Development Lifecycle (SDLC) 1.5 OWASP Top 10 (Detailed Overview)		
2	**Advanced Web Vulnerabilities**	**4**	**2**
	2.1 Advanced SQL Injection 2.2 Cross-Site Scripting (Advanced) 2.3 Cross-Site Request Forgery (CSRF) 2.4 File Upload Vulnerabilities 2.5 Authentication and Session Attacks		
3	**Web Application Testing Techniques File Systems & Disk Analysis**	**6**	**3**
	3.1 Manual Testing Techniques 3.2 Automated Testing Tools 3.3 Parameter Tampering 3.4 Input Validation Testing 3.5 Tools: Burp Suite (Advanced), OWASP ZAP		
4	**Exploitation Techniques**	**8**	**4**
	4.1 Exploiting SQL Injection 4.2 Exploiting XSS 4.3 Exploiting File Upload Issues 4.4 Session Hijacking 4.5 Privilege Escalation in Web Apps 4.6 Logic-Based Attacks		
5	**Security Controls and Secure Coding**	**8**	**5**
	5.1 Input Validation Techniques 5.2 Secure Authentication Mechanisms 5.3 Session Management Security 5.4 Web Application Firewalls (WAF) 5.5 Secure Coding Best Practices		
6	**Reporting and Case Study**	**6**	**6**
	6.1 Web Security Testing Report Writing 6.2 Vulnerability Classification 6.3 Risk Assessment Basics 6.4 Case Study of Web Application Attack 6.5 Remediation Techniques		

Reference Books:

- The Web Application Hacker's Handbook – Dafydd Stuttard & Marcus Pinto
- OWASP Testing Guide – Open Web Application Security Project
- Web Application Security – Andrew Hoffman
- Penetration Testing – Georgia Weidman

CDS-357-MJP PRACTICAL BASED ON ADVANCED WEB APPLICATION SECURITY

Programme Name :	**B.Sc. Cyber and Digital Science**
Class :	**T. Y. B.Sc Cyber and Digital Science**
Semester :	VI
Course Type :	Major Elective Practical
Course Code :	CDS-358-MJP
Course Title :	Practical based on Advanced Web Application Security (CDS 357MJ)
No. of Credits :	02

A. Rationale:

This practical course provides hands-on experience in advanced web application security testing techniques. It enables students to identify, analyze, and exploit web vulnerabilities using industry-standard tools. The course focuses on real-world attack scenarios and secure coding practices, preparing learners for roles in web security and penetration testing.

B. INDUSTRY / EMPLOYER EXPECTED OUTCOME:

- Develops skills in advanced web application security testing
- Prepares students for roles such as web security analyst and penetration tester
- Enhances ability to identify and exploit web vulnerabilities
- Builds knowledge of secure coding and mitigation techniques

C. COURSE OUTCOMES (COs):

CO No.	Course Outcome Statement
CO1	Perform advanced web security testing tasks
CO2	Identify complex web application vulnerabilities
CO3	Apply advanced testing tools and techniques
CO4	Analyze web application behavior and attack patterns
CO5	Evaluate security controls and mitigation strategies
CO6	Prepare detailed web security assessment reports

D. COURSE STRUCTURE AND CONTENTS:

Practical 1: Advanced Lab Setup (6 hours)

- Setup testing environment (DVWA, OWASP Juice Shop)
- Configure proxy tools (Burp Suite)
- Activity: Setup secure testing lab

Practical 2: Advanced Authentication Testing (4 hours)

- Test authentication mechanisms
- Analyze session management issues
- Activity: Identify authentication flaws

Practical 3: Injection Attacks (4 hours)

- Perform SQL Injection (advanced scenarios)
- Command Injection basics
- Activity: Exploit input validation flaws

Practical 4: Client-Side Attacks (4 hours)

- Cross-Site Scripting (Stored, Reflected)
- DOM-based XSS basics
- Activity: Execute XSS attacks

Practical 5: Access Control Testing (4 hours)

- Broken Access Control testing
- Privilege escalation basics
- Activity: Bypass access controls

Practical 6: Reporting and Secure Practices (4 hours)

- Document vulnerabilities
- Suggest mitigation strategies
- Activity: Prepare security report

E. SUGGESTED MICRO PROJECT / ASSIGNMENT:

- Perform security testing on web application
- Identify and document vulnerabilities
- Prepare detailed security assessment report

F. GENERAL / OVERALL EXPECTATIONS:

- Students will perform advanced web security testing
- Students will identify complex vulnerabilities
- Students will use security tools effectively
- Students will analyze and secure web applications
- Students will develop reporting and documentation skills

Fin-Tech Cyber Security

Programme Name :	B.Sc. Cyber and Digital Science
Class :	T. Y. B.Sc. Cyber and Digital Science
Semester :	VI
Course Type :	Major Elective (Theory)
Course Code :	CDS-359-MJ
Course Title :	Fin-Tech Cyber Security
No. of Credits :	02
No. of Teaching Hours :	30

A. Rationale:

Fin-Tech Cyber Security focuses on securing financial technologies such as online banking, digital payments, and financial platforms. This subject introduces students to risks, threats, and security mechanisms used in financial systems. It helps students understand how financial transactions are protected and how cyber attacks target banking and payment systems. The course prepares learners for roles in financial cybersecurity, fraud detection, and secure digital transactions.

B. INDUSTRY / EMPLOYER EXPECTED OUTCOME:

- Develops knowledge of financial systems and cybersecurity risks
- Prepares students for roles in banking security and fraud analysis
- Enhances ability to identify and prevent financial cyber attacks
- Builds understanding of secure payment systems and compliance

C. COURSE OUTCOMES (COs):

CO No.	Course Outcome Statement
CO1	Recall basic concepts of financial technologies and cyber security risks.
CO2	Explain digital payment systems and financial security mechanisms.
CO3	Apply techniques to secure financial transactions and systems.
CO4	Analyze cyber threats targeting financial platforms.

CO5	Evaluate security measures and fraud detection techniques.
CO6	Create reports on financial cyber security incidents and solutions.

Syllabus

Unit	Course Contents	Hours	CO
1	**Introduction to Fin-Tech Security**	**4**	**1**
	1.1 Introduction to Fin-Tech 1.2 Digital Banking Systems 1.3 Payment Systems Overview 1.4 Financial Cyber Threats 1.5 Importance of Fin-Tech Security		
2	**Digital Payment Systems**	**4**	**2**
	2.1 UPI and Online Payments 2.2 Credit/Debit Card Systems 2.3 Payment Gateways 2.4 Encryption in Financial Systems 2.5 Authentication Mechanisms		
3	**Financial Threats and Attacks**	**6**	**3**
	3.1 Phishing and Fraud Attacks 3.2 Card Skimming 3.3 Online Banking Attacks 3.4 Malware in Financial Systems 3.5 Identity Theft		
4	**Security Measures in Fin-Tech**	**8**	**4**
	4.1 Secure Payment Protocols 4.2 Multi-Factor Authentication 4.3 Fraud Detection Systems 4.4 Risk Management Techniques 4.5 Transaction Monitoring		
5	**Compliance and Regulations**	**8**	**5**
	5.1 RBI Guidelines (Overview) 5.2 PCI-DSS Standards 5.3 Data Protection in Finance 5.4 Legal Compliance 5.5 Risk Assessment		
6	**Case Study and Reporting**	**6**	**6**
	6.1 Financial Fraud Case Studies 6.2 Incident Reporting 6.3 Investigation Techniques 6.4 Risk Analysis Reports 6.5 Future Trends in Fin-Tech Security		

Reference Books:

- Financial Cybersecurity Risk Management – Thomas J. Parenty
- Cybersecurity in Banking – Joe Grant
- Digital Payments and FinTech – Indian Institute Publications
- PCI-DSS Documentation

CDS-358-MJP PRACTICAL BASED ON FIN-TECH CYBER SECURITY

Programme Name :	**B.Sc. Cyber and Digital Science**
Class :	**T. Y. B.Sc Cyber and Digital Science**
Semester :	VI
Course Type :	Major Elective Practical
Course Code :	CDS-360-MJP
Course Title :	Practical based on Fin-Tech Cyber Security (CDS-359MJ)
No. of Credits :	02

A. Rationale:

This practical course provides hands-on experience in cybersecurity practices related to financial technology systems. It enables students to understand and analyze security mechanisms used in digital payments, banking systems, and financial applications. The course prepares learners to identify threats, analyze transactions, and implement security measures in fintech environments.

B. INDUSTRY / EMPLOYER EXPECTED OUTCOME:

- Develops skills in securing financial applications and systems
- Prepares students for roles such as fintech security analyst
- Enhances ability to analyze digital transactions and fraud patterns
- Builds knowledge of payment security and compliance standards

C. COURSE OUTCOMES (COs):

CO No.	Course Outcome Statement
CO1	Perform basic security analysis of fintech systems
CO2	Identify threats in digital payment systems
CO3	Apply techniques to analyze financial transactions
CO4	Analyze fraud patterns and security risks
CO5	Evaluate security controls in fintech applications
CO6	Prepare reports on fintech security analysis

D. COURSE STRUCTURE AND CONTENTS:

Practical 1: Introduction to Fin-Tech Systems (6 hours)

- Overview of digital payment systems
- Understand UPI, wallets, banking apps
- Activity: Analyze transaction flow

Practical 2: Payment Security Analysis (4 hours)

- Study encryption in transactions
- Understand SSL/TLS basics
- Activity: Analyze secure communication

Practical 3: Fraud Detection Basics (4 hours)

- Identify suspicious transactions
- Analyze fraud patterns
- Activity: Detect anomalies in dataset

Practical 4: Application Security Testing (4 hours)

- Analyze fintech application security
- Identify vulnerabilities
- Activity: Basic security testing

Practical 5: Compliance and Risk Management (4 hours)

- Study PCI-DSS basics
- Understand risk assessment
- Activity: Evaluate system security

Practical 6: Reporting and Case Study (4 hours)

- Document findings
- Analyze real-world fintech case
- Activity: Prepare security report

E. SUGGESTED MICRO PROJECT / ASSIGNMENT:

- Analyze fintech transaction dataset
- Identify fraud or suspicious activity
- Prepare report with findings

F. GENERAL / OVERALL EXPECTATIONS:

- Students will understand fintech security concepts
- Students will analyze digital transactions
- Students will identify fraud patterns
- Students will evaluate system security
- Students will develop reporting skills

CDS-381-OJT HANDS-ON TRAINING (ON-THE-JOB TRAINING / INTERNSHIP)

Programme Name :	**B.Sc. Cyber and Digital Science**
Class :	**T. Y. B.Sc Cyber and Digital Science**
Semester :	VI
Course Type :	On Job Training
Course Code :	CDS-381-OJT
Course Title :	On Job Training
No. of Credits :	04

A. Rationale:

This course provides students with real-world industry exposure through hands-on training or internship. It enables students to apply theoretical and practical knowledge gained during the program in real working environments. The course helps learners develop professional skills, understand industry practices, and gain experience in cybersecurity domains such as network security, digital forensics, web security, and data analysis.

B. INDUSTRY / EMPLOYER EXPECTED OUTCOME:

- Develops industry-ready skills and professional experience
- Prepares students for real-world cybersecurity roles
- Enhances problem-solving and practical implementation skills
- Builds communication, teamwork, and reporting abilities

C. COURSE OUTCOMES (COs):

CO No.	Course Outcome Statement
CO1	Understand workplace environment and job roles
CO2	Apply cybersecurity knowledge in real-world scenarios
CO3	Perform assigned tasks using industry tools and practices
CO4	Analyze problems and provide appropriate solutions
CO5	Evaluate work outcomes and improve performance

CO6	Prepare internship report and present work experience

D. COURSE STRUCTURE AND CONTENTS:

Phase 1: Orientation and Training Setup (6 hours)

- Introduction to organization
- Understanding roles and responsibilities
- Activity: Training plan preparation

Phase 2: Practical Work / Task Execution (12 hours)

- Perform assigned tasks
- Work on real projects or simulations
- Activity: Daily task execution

Phase 3: Monitoring and Evaluation (6 hours)

- Review work progress
- Feedback from mentor
- Activity: Improve based on feedback

Phase 4: Documentation and Reporting (6 hours)

- Maintain internship logbook
- Prepare detailed report
- Activity: Document learning and work
-

E. SUGGESTED ASSIGNMENT / PROJECT:

- Internship report submission
- Work logbook with daily activities
- Case study or project based on training

F. GENERAL / OVERALL EXPECTATIONS:

- Students will gain real-world industry experience
- Students will apply technical knowledge practically
- Students will develop professional and communication skills
- Students will understand workplace ethics and teamwork
- Students will prepare and present internship report

Machine Learning for Data Analysis

Programme Name :	B.Sc. Cyber and Digital Science
Class :	TY B.Sc. Cyber and Digital Science
Semester :	VI
Course Type :	Minor (Theory)
Course Code :	CDS-391-VSC
Course Title :	Machine Learning for Data Analysis
No. of Credits :	02
No. of Teaching Hours :	30

A. Rationale:

Machine Learning for Data Analysis introduces students to basic machine learning concepts and their application in analyzing data. This subject focuses on understanding patterns, making predictions, and supporting decision-making using data-driven approaches. It helps students learn how machine learning is used in cybersecurity, business analytics, and real-world problem solving.

B. INDUSTRY / EMPLOYER EXPECTED OUTCOME:

- Develops knowledge of machine learning concepts and data analysis
- Prepares students for roles such as data analyst and ML beginner
- Enhances ability to interpret and analyze data patterns
- Builds understanding of ML applications in cybersecurity

C. COURSE OUTCOMES (COs):

CO No.	Course Outcome Statement
CO1	Recall basic concepts of machine learning and data analysis.
CO2	Explain machine learning models and data processing techniques.
CO3	Apply basic ML techniques for data analysis.
CO4	Analyze datasets to identify patterns and insights.

CO5	Evaluate model performance and results.
CO6	Create basic ML-based analysis reports and visualizations.

D. Syllabus

Unit	Course Contents	Hours	CO
1	**Introduction to Machine Learning**	4	1
	1.1 What is Machine Learning 1.2 Types of Machine Learning 1.3 Applications in Cyber Security 1.4 ML Workflow 1.5 Data Types		
2	**Data Preparation**	4	2
	2.1 Data Collection 2.2 Data Cleaning 2.3 Data Preprocessing 2.4 Feature Selection 2.5 Data Splitting		
3	**Basic ML Algorithms**	6	3
	3.1 Linear Regression 3.2 Classification Basics 3.3 Decision Trees 3.4 Clustering Concepts 3.5 Tools Overview (Python, Scikit-learn)		
4	**Data Analysis and Visualization**	8	4
	4.1 Data Visualization Techniques 4.2 Graphs and Charts 4.3 Pattern Identification 4.4 Tools: Python, Matplotlib 4.5 Data Interpretation		
5	**Model Evaluation**	8	5
	5.1 Accuracy and Performance Metrics 5.2 Confusion Matrix 5.3 Model Validation 5.4 Overfitting and Underfitting 5.5 Improving Models		
6	**Case Study and Reporting**	6	6
	6.1 ML Case Study in Cyber Security 6.2 Data Analysis Reports 6.3 Visualization Reports 6.4 Decision Making using ML 6.5 Future Trends in ML		

Reference Books:

- Hands-On Machine Learning – Aurélien Géron
- Machine Learning – Tom Mitchell
- Python Data Science Handbook – Jake VanderPlas
- Introduction to Machine Learning with Python – Andreas Müller