SAVITRIBAI PHULE PUNE UNIVERSITY

PUNE

CHOICE BASED CREDIT SYSTEM

For

B.Sc. (Cyber Security)

(Implemented from June 2024)

Savitribai Phule Pune University

B. Sc. (Cyber Security)

(To be implemented from Academic year 2024-2025)

1. **Name of Program: Cyber Security**

2. **Introduction:**

In today's interconnected world, the proliferation of digital technologies has brought about unprecedented convenience and efficiency. However, this digital transformation has also led to an increase in cyber threats, making cyber security an essential field. Cyber-attacks can cause significant harm to individuals, businesses, and national security. As a result, there is a growing demand for skilled cyber security professionals who can protect sensitive information and critical infrastructure.

The B.Sc. in Cyber Security program is designed to address this demand by providing students with a comprehensive education in the field. Aligned with the National Education Policy (NEP) 2020, this program emphasizes a holistic, flexible, and multidisciplinary approach to education, preparing students for the complexities of the cyber security landscape.

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.

3. **Objectives:**

- To Develop Proficiency in Cyber Security: Equip students with the skills to protect Information systems against cyber threats and vulnerabilities.
- To provide hands-on experience with current security technologies and tools.
- To an understanding of the ethical, legal, and societal implications of cyber security practices.
- To encourage innovative problem-solving and critical analysis of security issues.
- To develop an understanding of the global context and cultural dimensions of cyber security

4. 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 avocational subject of +2 level (MCVC)

PO No.	PO Outcomes
PO1	Become proficient in Linux administration, as it is essential in today's IT environment.
PO2	Address and take action to meet the cyber security needs of the modern IT world.
PO3	Cultivate creative abilities, critical thinking, analytical skills, and research capabilities to tackle real-world problems using cyber security expertise.
PO4	Understand the Concepts of cyber security, Networking and vulnerability testing and statistical methods.
PO5	Applying the Concepts of Digital Communication and IOT.
PO6	Identify and evaluate software vulnerabilities and security solutions to mitigate the risk of exploitation.
PO7	Acquire essential programming languages such as C and Python
PO8	Integrate ethics and cyber laws to understand the rules and regulations of the current IT environment.
PO9	To developing regulations and tactics for cyber security
PO10	Cloud security protects applications, data, and cloud-based infrastructure.
PO11	Comprehend security concepts such as cyber threat intelligence, block chain in cyber security, communication systems security, malware analysis, vulnerability assessment and penetration testing (VAPT), intrusion detection and prevention systems (IDS & IPS), and cybercrime reporting.

Savitribai Phule Pune University
Structure of UG Program as per NEP-2020
Name of Program: - B.Sc.(Cyber Security) Major Course: - Cyber Security

Level:-4.5(First Year) Sem:-I									
Course Type	**Course Code**	**Course Code**	**Course Title**		**Teaching Scheme Hr/Week**		**Evaluation Scheme & Max Marks**		
			TH	**PR**	**TH**	**PR**	**CE**	**EE**	**Total**
Subject 1	**CYS101MJ**	Fundamentals of Linux Administration	**2**		**2**		**15**	**35**	**50**
Subject 2	**CYS102MJ**	Foundations of C programming	**2**		**2**		**15**	**35**	**50**
Subject 3	**CYS103MJ**	Information Technology	**2**		**2**		**15**	**35**	**50**
Subject1 Practical	**CYS104MJP**	Practical based on CYS101MJ		**2**		**4**	**15**	**35**	**50**
Subject 2 Practical	**CYS105MJP**	Practical based on CYS102MJ		**2**		**4**	**15**	**35**	**50**
Subject3 Practical	**CYS106MJP**	Practical based on CYS103MJ		**2**		**4**	**15**	**35**	**50**
IKS	**CYS101IKS**	Computing in ancient India	**2**		**2**		**15**	**35**	**50**
GE/OE	**OE101CYS**	Office Automation/ Introduction to Google Tools	**2**		**2**		**15**	**35**	**50**
SEC	**SEC101CYS**	Basics of Digital Communication (Practical)		**2**		**4**	**15**	**35**	**50**
AEC	**AEC101MAR/ HIN/ENG**	MIL-I(Hindi) / MIL-I(Marathi)/ MIL-I(ENGLISH)	**2**		**2**		**15**	**35**	**50**
VEC	**VEC101ENV**	EVS-I	**2**		**2**		**15**	**35**	**50**
TOTAL			**14**	**8**	**14**	**16**			

Level:-4.5(First Year) Sem:-II									
Course Type	**Course Code**	**Course Code**	**Course Title**		**Teaching Scheme Hr/Week**		**Evaluation Scheme & Max Marks**		
			TH	**PR**	**TH**	**PR**	**CE**	**EE**	**Total**
Subject 1	**CYS151MJ**	Cyber Security Fundamentals	**2**		**2**		**15**	**35**	**50**
Subject 2	**CYS152MJ**	Computer Networks	**2**		**2**		**15**	**35**	**50**
Subject 3	**CYS153MJ**	Python Programming	**2**		**2**		**15**	**35**	**50**
Subject1 Practical	**CYS154MJP**	Practical based on CYS151MJ		**2**		**4**	**15**	**35**	**50**
Subject 2 Practical	**CYS155MJP**	Practical based on CYS152MJ		**2**		**4**	**15**	**35**	**50**
Subject3 Practical	**CYS156MJP**	Practical based on CYS153MJ		**2**		**4**	**15**	**35**	**50**
GE/OE	**OE152CYSP**	Office Automation/ Introduction to Google Tools		**2**		**4**	**15**	**35**	**50**
SEC	**SEC151CYS**	Statistical Methods-I		**2**		**4**	**15**	**35**	**50**
AEC	**AEC151MAR / HIN/ENG**	MIL-I(Hindi) / MIL-I(Marathi)/ MIL-I(ENGLISH)	**2**		**2**		**15**	**35**	**50**
VEC	**VEC151ENV**	EVS-II	**2**		**2**		**15**	**35**	**50**
CC	**CC151PE/ NSS/ NCC**	University Basket	**2**		**2**		**15**	**35**	**50**
TOTAL			**12**	**10**	**12**	**20**			

Semester-I

Savitribai Phule Pune University
F.Y.B.Sc.(Cyber Security)
Subject Code : CYS101MJ
Subject :Fundamentals of Linux Administration

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / Week	**2**	**CE: 15 marks** **EE: 35 marks**

Prerequisites :- Awareness with the Text-Based Console, Command Prompt, Shell Environment And Networking

Course Objectives: -

- To make the students understand the Linux OS
- To acquaint them with the rich set of utilities that are essential for system management, file manipulation.
- To help they manage a network interface to managing connections and troubleshooting network issues.

Course Outcomes: - Student will be able to: -

1. Illustrate Adeptness using the Linux command line and constructing shell scripts.
2. Execute maintenance tasks, including user and system management.
3. Install and configure system services.
4. Deploy and Configure Linux Operating Systems Network-wide
5. To Administer and Operate file permissions and network security aspects.

Course Contents

Chapter 1	**Introduction to Linux System Administration**	**6 hours**
Linux Operating System Summary. Linux Infrastructure Management Role. Navigating the Linux File System Basic Command-Line Navigation and Operations		
Chapter 2	**Application Deployment and Configuration**	**7 hours**
Linux Installation Techniques Partitioning and Storage Setup. User and Group Configuration Network Implementation and Problem Solving		
Chapter 3	**Control Statements and Functions**	**6 hours**
Package Handling with APT and YUM. Kernel Software Upgrades and Rebooting Log File Monitoring and Troubleshooting. System Performance Analysis.		
Chapter 4	**System Security and Access Management**	**6 hours**
PAM-Based User Authentication Network Firewalling and IP Address Control SSH Access Controls and Configuration Implementing Mandatory Access Controls with SE Linux/App- Armor.		
Chapter 5	**Specialized Linux Administration**	**5 hours**
Cron-Based Task Automation Virtualization and Docker- Based Containers. File and Directory Privileges Data Protection and Recovery Techniques		

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/

Linux Programming and Scripting: https://archive.nptel.ac.in/courses/117/106/117106113/

Savitribai Phule Pune University
F.Y.B.Sc.(Cyber Security)
Subject Code : CYS102MJ
Subject : Foundations of C programming

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / Week	**2**	**CE: 15 marks** **EE: 35 marks**

Prerequisites None

Course Objectives: -

- To develop the foundation and terminology of programming in general.
- To understand structured programming approach
- To implements the algorithms and Programing method in problem-solving techniques C language
- To develop programming skills to a level such that problems of reasonable complexity can be tackled successfully.

Course Outcomes: - Student will be able to :-

1. Understand flow of Control sequence as well as logical outputs of the program
2. Implements computational strategies for developing applications
3. Design applications from Simple to Complex using C programming language

Course Contents

Unit 1	**Basics of C Programming**	**6 hours**

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 associatively. Input output functions: printf, scanf functions, getchar, putchar, getch functions, gets, puts functions, Escape sequence characters, Format specifiers.

Unit 2	**Control and Iterative structures**	**4 hours**

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 3	**Functions**	**5 hours**

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. Scope of variables and Storage classes.

Unit 4	**Arrays and String**	**8 hours**

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, Introductions to Strings: Definition, Declaration, Initialization, String operations. Introduction to pointer : Indirection operator and address of operator, Pointer arithmetic, Dynamic memory allocation Functions and pointers, Dynamic memory allocation

Unit 5	**Structure and Union**	**4 hours**

Introduction to structure, Accessing members structure operation, nested structure and Introduction to Union: Accessing members structure operation, nested structure

Unit 6	**File Handling**	**3 hours**

Introduction to File, file handling concepts, Basic file operations: Reading from and writing to files, Searching ,Updating contents of file

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, Tata McGraw Hill.
6. Programming in ANSI C, E. Balagurusamy, 7th Edition, McGraw Hill.

Savitribai Phule Pune University
F.Y.B.Sc.(Cyber Security)
Subject Code : CYS103MJ
Subject : Information Technology

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / Week	**2**	**CE: 15 marks** **EE: 35 marks**

Prerequisites None

Course Objectives: -

- To Introduce Students to the Basic Concepts and terminology of computer science.
- To Learn Basic Commands of Operating system and application software
- To Understand the Basics of data Transmission and Network Security.

Course Outcomes: - Student will be able to :-

1. Learn the fundamental concepts of computer science.
2. Operating Systems Proficiency
3. Differentiate between hardware and software, including understanding operating systems and applications.

Course Contents

Chapter 1	**Introduction to Information Technology**	**8 hours**

Definition and Scope of Information Technology, History and evolution of computing (Block Diagram of computer and types of computer), Role of IT in modern society. Types of Programming Languages- Machine Languages, Assembly Languages, High-Level Languages, Translators- Assembler, Compiler, Interpreter Data Organization- Drives, Files, Directories

Chapter 2	**Computer Accessories and Peripherals**	**7 hours**

Primary and Secondary Memory Systems ,Primary storage devices – RAM, ROM, PROM, Cache Memory, and EPROM.Secondary Storage Devices - CD, HD, and Pen drive, Cloud Storage. 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**

Evolution of DOS (Disk Operating System),Introduction to Files and directories, Internal and External Commands Batch Files, Types of O.S.

Chapter 4	**Essentials of Internet Networking**	**4 hours**

Introduction to Networking ,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, Client Server

Chapter 5	**Foundations of Problem Solving**	**6 hours**

Concept: problem-solving, Algorithms and Flowcharts (Definitions, Symbols), Characteristics of an Algorithm Simple Arithmetic Problems, Basic Concepts of Viruses and Threats (Definition, Types and Prevention).

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 Tanenbaum Tata McGraw Hill Publication
4. How to solve it by Computer – R. G. Dromey
5. Introduction to algorithms – Cormen, Leiserson, Rivest, Stein

Savitribai Phule Pune University
F.Y.B.Sc.(Cyber Security)
Subject Code : CYS104MJP
Subject : Practical Based on CYS101MJ

Teaching Scheme	No. of Credits	Examination Scheme
4 hours / Week	**2**	**CE: 15 marks** **EE: 35 marks**

Prerequisites :- Problem solving with Python

Course Objectives: -

- Study the core principles of Linux OS
- Investigate a problem and design an algorithm

Course Outcomes: - Student will be able to :-

1. Deploy and manage a Linux server.
2. Create and administer policies.
3. Configure file services.

Practical:-Fundamentals of Linux System Administration

Assignment 1: Introduction to Linux System Administration

1. Set up a Linux distribution of your choice.
2. Review and illustrate the file system organization through basic shell commands.
3. Add a new user and group, showing user and group management

Assignment 2: Application Deployment and Configuration

1. Select an alternative Linux installation method compared to the previous question
2. Execute manual disk partitioning and file system configuration during installation
3. Configure network parameters and troubleshoot network connectivity

Assignment 3: System Maintenance and Updates

1. Utilize APT or YUM to install, upgrade, and uninstall packages on your system
2. Examine system logs to diagnose a particular problem (e.g., networking, package installation).
3. Track system performance with tools such as top or htop

Assignment 4: Security and Access Control

1. Set up user authentication with PAM. Apply firewall rules with IP tables
2. Protect SSH by changing its configuration settings
3. Use SE Linux or AppArmor to enforce Mandatory Access Control

Assignment 5: Advanced Topics in Linux Administration

1. Configure file and directory permissions for a particular use case
2. Operate a Docker container and give a summary of containerization concepts.
3. Configure file and directory access rights for a particular situation

Assignment 6: Installation and Configuration

1. Select an alternative Linux distribution from the one previously mentioned
2. Execute a complex partitioning layout with distinct partitions for /, /home, and swap, And apply user and group quotas to manage disk space

Assignment 7: System Maintenance and Updates

1. Examine and illustrate the steps for upgrading the Linux kernel.
2. Review system logs to diagnose and fix issues related to kernel updates
3. Apply performance monitoring utilities to find and fix performance slowdowns.

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

Savitribai Phule Pune University
F.Y.B.Sc.(Cyber Security)
Subject Code : CYS105MJP
Subject : Practical Based on CYS102MJ

Teaching Scheme	No. of Credits	Examination Scheme
4 hours / Week	**2**	**CE: 15 marks** **EE: 35 marks**

Prerequisites :- None

Course Objectives: -

- To Learn and apply the basic syntax and structure, different data types, control structures, etc. in C programs.
- To Implement user-defined functions and use standard library functions.
- To develop programming skills to a level such that problems of reasonable complexity can be tackled successfully.

Course Outcomes: - Student will be able to :-

1. Build Proficiency in Basic C Syntax and Structure
2. Develop effective Use of Data Types and Variables
3. Develop ability to work with arrays (single and multi-dimensional) and strings, performing operations
4. Demonstrate the ability to perform file input and output operations, reading from and writing to files using appropriate functions.

List of Practical:- Foundations of C Programming

1. Write a C program to find a maximum of two numbers using a conditional operator.
2. Write a C Program to find a maximum of three numbers using logical operators.
3. Write a C Program which illustrate increment and decrement operators (Use of Pre and Post increment is expected)
4. Accept dimensions of a cylinder and print the surface area and volume.
5. Write a program to accept an integer and check if it is even or odd.
6. Accept any year as input through the keyboard. Write a program to check whether the year is a leap year or not. (Hint leap year is divisible by 4 and not by 100 or divisible by 400)
7. Accept radius from the user and write a program having menu with the following options and corresponding actions Options Actions
   a. Area of Circle Compute area of circle and print
   b. Circumference of Circle Compute Circumference of circle and print
   c. Volume of Sphere Compute Volume of Sphere and print
8. Write a program to calculate the sum of digits of a given input number.
9. Write a program to check whether an input number is an Armstrong number or not.
10. Write a program to check whether an input number is palindrome or not.
11. Write a program to generate the following pattern.

```
5
4 5
3 4 5
2 3 4 5
1 2 3 4 5
```

12. Write a program to calculate the sum of digits of an input number using a function.
13. Write a program to find the factorial of an input number using a user defined function.
14. Write a program to calculate the sum of all odd elements of a 1-D array.
15. Write a program to sort 1D array elements in ascending order.
16. Write a program to find maximum and minimum elements of a matrix.
17. Write a program to count the occurrences of vowels from an input string.
18. Write a program to display the elements of an array containing n integers in the reverse order using a pointer to the array.
19. Create a structure employee (id, name, salary). Accept details of n employees and write a menu driven
20. Program to perform the following operations. Write separate functions for the different options
Search by name
Search by id
Display all
21. Create a structure Book (Bno, Bname, Price). Accept details of n Books and write a menu driven program to perform the following operations options.
   i. Display all Books having price > 500

ii. Display Book having maximum price

22. Write a C program to create a file and write contents, save and close the file.

23. Write a C program to read file contents and display on console.

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, 3rd edition, Schaum's outline Series, Tata McGraw Hill

Savitribai Phule Pune University

F.Y.B.Sc.(Cyber Security)

Subject Code : CYS106MJP

Subject : Practical Based on CYS103MJ

Teaching Scheme	No. of Credits	Examination Scheme
4 hours / Week	**2**	**CE: 15 marks** **EE: 35 marks**

Prerequisites :- Problem solving with Python

Course Objectives:-

- To Know the Basics of Information Technology.
- To Understand the Basics of Operating systems & Operating Systems Proficiency

Course Outcomes: - Student will be able to :-

1. Learn the fundamental concepts of Information Technology.
2. Develop the logic of problem-solving

List of Practical:- Information Technology

1. What is the installation process for Windows OS?
2. What is the installation process for the Linux Operating System?
3. Write down the steps for creating a new file in the Windows operating system.
4. Write down the steps of creating a new file in the Linux Operating System
5. What steps are involved in user and group management in Linux?
6. What steps are involved in user and group management in the Windows Operating System.?
7. How do you hide and unhide files in Windows OS?
8. File and folder management in Linux.
9. File and folder management in Windows.
10. Working with any five commands in the 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. What is the method for assigning an IP address to a PC and connecting it to a network?
16. Write the steps to connect the computer to the Local Area Network.
17. Write the steps How to connect Network Printer in Windows.
18. Write the steps To setting Local Area Network Proxy Server.

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 Tanenbaum Tata McGraw Hill Publication
4. How to solve it by Computer – R. G. Dromey
5. Introduction to algorithms – Cormen, Leiserson, Rivest, Stein

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

Savitribai Phule Pune University
F.Y.B.Sc.(Cyber Security)
Subject Code : SEC 101 CYS
Subject : Basics of Digital Communication System (Practical)

Teaching Scheme	No. of Credits	Examination Scheme
4 hours / Week	**2**	**CE: 15 marks** **EE: 35 marks**

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

1. Analog and Digital Communication
2. Electronics Devices and circuits
3. Mobile communication & Networking

Course Objectives: -

- To make the student familiar with electronic components
- To learn number systems and their representation.
- To understand basic logic gates, Boolean algebra and K-maps
- To learn about various wireless & cellular communication networks.
- To study arithmetic circuits, combinational circuits and sequential circuits
- To impart knowledge regarding concepts of AM, FM modulation and detection

Course Outcomes: - Student will be able to :-

1. 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.
2. To solve problems on Number systems and their representation
3. To familiarize with logic gates and applications in combinational and sequential circuits.
4. To identify the importance of different blocks in electronic communication systems.
5. Understand the working principles of mobile networks and Contrast different types of telecommunication networks.

List of Practical:-SEC101CYS:- Basics of Digital Communication System

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.

Assignment: 4 Realization of basic gates using universal logic gates. (Verification of Truth tables)
1. AND,NOT,OR using NAND/NOR

Assignments: 5 Study of Half Adder and Full Adder using Logic Gates.
1. Combinational Circuits :Implementation of half adder, full adder

Assignment: 6 Study of Decimal to BCD/ (Binary) Converter.
1. Number Systems: Decimal, Binary, Octal, Hexadecimal, Binary Coded Decimal number, inter- conversions.

Assignment :7 Flip-flops
1. Flip-flops SR , D and JK-FF

Assignment :8 Study of read and write action of RAM
1. Introduction to memory, types Volatile , non-volatile , RAM, ROM, Implementation of RAM

Assignment: 9 Study of Communication.
1. Elements of Communication system, Types of communication: simplex, half duplex, full duplex, baseband and broadband, Serial communication: asynchronous and synchronous

Assignment:10 Study of Pulse code Modulation
1. Need of modulation and demodulation, Digital Modulation technique-PCM.

Assignment :11 Error detection and correction using Hamming Code
1. Error detection, Error correction methods, hamming code, limitation

Assignment :12 Study of Mobile hardware (Study Experiment)
1. Basic block diagram of mobile hardware, applications of each block

Assignment :13 Mobile communication(GSM)(Study Experiment)
1. Basic cellular systems, cells, Concept of frequency reuse channels, Handoff GSM system architecture

Assignment :14 Computer Network Component(Study Experiment)
1. Computer network components : Cables, Connectors, Routers, Switches, Ethernet and related interfacing cards

Assignment :15 Configuration of IP & MAC(Study Experiment)

1. To study Configuration of IP and MAC address and to study Local Area Network setup

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 Sara, 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.
4. Digital Principles and Applications - Malvino and Leach, TMG Hill Edition.

Semester -II

Savitribai Phule Pune University
F.Y.B.Sc.(Cyber Security)
Subject Code : CYS151MJ
Subject :Cyber Security Fundamentals

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / Week	**2**	**CE: 15 marks** **EE: 35 marks**

Prerequisites :-

1. Fundamentals of Computers
2. Fundamentals of networking

Course Objectives: -

- The purpose of this course is to arm students with the technical know-how and abilities required to safeguard and defend computer networks and systems.
- In order to grow, pupils must be able to recognize contemporary computer security flaws.

Course Outcomes: - Student will be able to: -

1. Course Outcomes: - Students will be able to measure performance and troubleshoot Cyber Security Systems: - Analyze and evaluate an organization's needs for cyber security.
2. To outline the latest activities pertaining to cyberspace.

Course Contents

Chapter 1	**Introduction to Cyber security**	**5 hours**

Overview of Cyber security: 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, ransom ware, etc.
Defense-in-depth and layered security Risk Management in Cyber security 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 Cyber security.

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

Essentials Fundamentals:-Overview of networking principles Fundamentals of network protocols and TCP/IP.Types of Network Attacks, Eaves dropping, man-in-the-middle, and real-world instances and case studies are some examples of network attack types.
Common Network Attacks: Technologies for Network Security Security of Wireless Networks.
Wireless Network Security: Wireless network risks Protecting wireless networks against unwanted access Protecting Network Equipment,
Securing Network Devices: Best practices for securing routers, switches, and other devices Implementing access controls and monitoring. Key Principles of Cyber security Confidentiality, integrity, Availability (CIA Triad)

Chapter 3	**System Security for Operating Systems**	**8 hours**

Fundamentals of Security for Operating Systems: Important operating system security features, Access controls and user account management Patch Administration.
Antivirus and Malware: The significance of software upgrades techniques for handling patches in an efficient manner Antivirus and Malware Protection Defense Antivirus software's function in cyber security Assessing and choosing antiviral medicines. Secure Boot and Encryption Using encryption to secure data establishing a safe boot procedure Security of Endpoints

Chapter 4	Web Application Security	5 hours

Web Application Security Basics: online application vulnerabilities, The best methods for safe coding. **Secure Web Browsing:** safeguards and safe browsing practices, Identifying and preventing phishing attempts, **HTTPS and SSL/TLS:** Importance of encrypted communication on the web, Configuring and implementing SSL/TLS for websites.

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

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

Chapter 5	Security Best Practices and Emerging Trends	4 hours

Training and Awareness of Security: The importance of cyber security education in creating security-conscious organizational culture. Response to and Management of Incidents, Formulating a plan for responding to incidents carrying out simulations and drills for incident response.

Basics of Cloud Security: Understanding the security implications in cloud environments The shared responsibility concept and best practices.

Information Exchange and Threat Intelligence: The role of threat intelligence in cyber security Participating in information-sharing communities.

Cyber security's Future Trends: Examining new technology and issues Learning new things constantly and changing to counter threats.

Reference Books:

1. Computer Security Basics by by Rick Lehtinen , Publisher : O'Reilly Media; 2nd edition
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),
3. Cryptography and Network Security,Publisher:Mc Graw Hill.
4. Computer Networking And the Internet ,Publisher:Harshall Kulkarni.
5. Data Communication and Computer Networks Publisher:Rajnesh Agrawal,Bharat Bhushan Tiwari
6. Cyber Cops, Cyber Criminal & Internet. Publisher:Deepti Chopra & Keith Merrill

E-Books and Online Learning Material

2. https://www.w3schools.com/linux/

Linux Programming and Scripting: https://archive.nptel.ac.in/courses/117/106/117106113/

Savitribai Phule Pune University
F.Y.B.Sc.(Cyber Security)
Subject Code : CYS152MJ
Subject :Computer Networks

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / Week	**2**	**CE: 15 marks** **EE: 35 marks**

Course Objectives: -

- To understand basic terms of computer networks and the internet environment.
- Become familiar with layered communication architectures (OSI and TCP/IP).

Course Outcomes: - Student will be able to: -

1. To familiarize the student with the basic taxonomy and terminology of computer networks.
2. To prepare the student for advanced courses in computer networking.
3. To understand data transmission across the network.
4. Gather knowledge of various types of networks and topologies.
5. Get an overview of the Internet, its applications and various browsers available to access theInternet.
6. Connect to the Internet using various modes of connections/devices available.

Course Contents

Chapter 1	**Networking Fundamentals**	**9 Hours**

1.1 Beginnings of Networking and data communication, ARPnet
1.2 Understanding Network Basics (N/W Components, N/W Device Roles)
1.3 Network Topologies : Bus, Ring, Star and Mesh Topologies
1.4 Transmission Modes (Simplex, Half Duplex, Full Duplex)
1.5 Types of Computer Networks (PAN, LAN, MAN, WAN)
1.6 Network Architectures (Centralized, Decentralized and Distributed)
1.7 Difference between Internet, Intranet and Extranet

Chapter 2	**Physical Layer Principles**	**7 Hours**

2.1 **Network Models:** TCP/IP protocol suite, OSI Model
2.2 **Switching:** Packet , Message and Circuit Switching
2.3 **Physical Layer:** Guided Transmission media: twisted pairs, coaxial cable, fiber optics,Wireless transmission.
2.4 Analog and Digital signal, Analog to Digital transmission
2.5 Bandwidth utilization: Multiplexing and Spectrum Spreading

Chapter 3	**Basics of Data Link Layer**	**7 Hours**

3.1 Function of data link layer,
3.2 Data framing techniques: Character Count, Character stuffing, Bit stuffing
3.3 Link layer addressing, Data Link layer design Issue
3.4 Error detection and correction : Parity, Checksum
3.5 Elementary data link protocol: Stop and wait, Sliding window protocol-Go back N:ARQ,Selective repeat ARQ
3.6 MAC Sub layer
3.7 Random Access Protocol: ALOHA,CSMA, CSMA/CD, CSMA/CA
3.8 Data link layer devices: Bridges, Switches

Chapter 4	**Core Network Layer**	**7 Hours**
4.1 Function of network layer 4.2 Network service type: virtual circuit and datagram 4.3 Routing algorithm: shortest path routing, Flooding , Distance vector routing, Link state routing, hierarchical routing 4.4 Congestion control: algorithm and congestion prevention policies 4.5 Internet protocols: Ip frame format, IP addressing, subnets 4.6 Internet control protocols: ICMP, ARP, DHCP 4.7 Internetworking: network layer device-router		
Reference Books:		
1. Computer Networks and Internets, 5th Edition, Douglas E. Comer, Pearson 2. Networking Basics, 2nd Edition, Patrick Ciccarelli, Christina Faulkner, Jerry Fitzgerald, Alan Dennis, David Groth and Toby Skandier with Frank Miller, Wiley 3. Internetworking with TCP/IP, Volume I, 5th Edition, Douglas E. Comer, PHI. 4. Internetworking with TCP/IP, Volume II, 3rd Edition, Douglas E. Comer, D.L. Stevens, PHI 5. TCP/IP Illustrated, Eastern Economy Edition, N.P. Gopalan, B. Siva Selvan, PHI 6. Computer Networking by Ed Tittel, McGRaw Hills Companies		

Savitribai Phule Pune University
F.Y.B.Sc.(Cyber Security)
Subject Code : CYS153MJ
Subject : Python Programming

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / Week	**2**	**CE: 15 marks** **EE: 35 marks**

Prerequisites: - Knowledge of procedure oriented programming language.

Course Objectives: -

- To define the structure and components of a Python program. Also, Gain a solid understanding of Python syntax and semantics.
- To acquaint with data types, input/output statements, decision making, looping and functions in Python.
- Learn and implement various data structures such as lists, tuples, dictionaries, and sets in Python programs.
- Develop proficiency in writing reusable and modular code using functions in Python.
- Gain a solid understanding of OOP principles and concepts.
- Understand the importance of modules and packages in Python.

Course Outcomes: - 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	**Foundational of Python Programming**	**7 hours**

Python Basics: History, Introduction to Features and Applications of Python; Python Versions; Installation of Python; Python Command Line mode and Python IDEs; Structure of python program, Simple Python Program, Identifiers; Keywords; Statements and Expressions; Variables; Operators; Precedence and Association; Data Types; Indentation; Comments; Built-in Functions- Console Input and Console Output, Type Conversions; **Conditional statements-**If, If-Else, nested if-else, Examples.
Looping-For, While, Nested loops, Examples
Control Statements-Break, Continue, Pass.

Chapter 2	**Python Data Structures**	**7 hours**

String Manipulation-Concept, Declaration, Accessing String, Basic Operations, String Slices, Function and Methods, Examples.
Lists-Introduction, accessing list, operations, working with lists, function & methods.
Tuple-Introduction, Accessing tuples, operations working, function & methods, Examples.
Set - concept, declaration, inserting, updating, deleting and accessing elements, Set operations
Dictionaries-Introduction, Accessing values in dictionaries, working with dictionaries, properties, function, Examples. Python data structure conversion
Functions-Defining a function, calling a function, types of function, function arguments, anonymous function, global & local variable, Examples.

Chapter 3	Modules and Packages	5 hours
Built in Modules: Importing modules in python program, Working with Random Modules. E.g. - built-ins module like time, date time, calendar, random, math, sys, statistics, collections, OS etc **Packages:-** Predefined Packages, User defined Packages		
Chapter 4	**Object Oriented Concepts**	**6 hours**
Object oriented programming concept: Classes and Objects-Classes as User Defined Data Type, Objects as Instances of Classes, Creating Class and Objects, Creating Objects By Passing Values, Variables, class variables, instance variables, class methods and static methods, Python Constructor, Data hiding. **Inheritance:–** Create a parent class and child class, add the __init__() function, use super() function, adding variables and functions **Types of Inheritance: -** Single inheritance, multilevel inheritance, multiple inheritance, hybrid inheritance, hierarchical inheritance **Polymorphism: –** function polymorphism and class polymorphism		
Chapter 5	**Arrays and Libraries**	**5 hours**
Concept of Array: Creating and accessing Array elements, Slicing python array, changing and adding array, element, removing python element **Array Operations -** Traverse, Insertion, Deletion, Search and Update Built-in Array methods Introduction to Python libraries: Statistical Analysis - NumPy, SciPy, Pandas, StatsModels **Data Visualization**-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/ 4. https://www.w3schools.com/python/default.asp		

Savitribai Phule Pune University
F.Y.B.Sc.(Cyber Security)
Cyber Security Fundamentals : (CYS154MJP)
Practical Based on CYS151MJ

Teaching Scheme	No. of Credits	Examination Scheme
4 hours / Week	**2**	**CE: 15 marks EE: 35 marks**

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: -

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.

Practical Assignment 1: Introduction to cyber Security

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: Web application security and networking

1. Identify and fix common vulnerabilities in a web application (e.g., SQL injection, cross-site scripting).
2. Configure SSL/TLS for a website to ensure secure communication.
3. Use web security tools like OWASP ZAP to perform security assessments.
4. Secure a Wi-Fi network by implementing WPA2/WPA3 encryption.
5. Configure a wireless intrusion detection system (WIDS) to monitor wireless traffic.
6. Investigate and respond to a simulated wireless security incident.

Practical Assignment 3:System Security for OS

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 4: Strengthening Endpoint Security, Incident response and Management.

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.
4. Develop an incident response plan for a simulated security incident.
5. Simulate a security incident and follow the incident response plan.
6. Conduct a post-incident analysis and propose improvements to the plan.

Practical Assignment 5: Best Practices and Trends in Cyber security

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 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 userawareness.
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 cyber security.

Reference Books:

1. Computer Security Basics by by Rick Lehtinen , Publisher : O'Reilly Media; 2nd edition (23June 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 Security)
Computer Networks : (CYS155MJP)
Practical Based on CYS152MJ

Teaching Scheme	No. of Credits	Examination Scheme
4 hours / Week	**2**	**CE: 15 marks EE: 35 marks**

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: -

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.

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()

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 4 Router Basic Commands and Security Configuration

1.CISCO IOS Configuration Router Basic Commands

2.Security Configuration, Operation and Verification in IOS, Running and Start-up Configuration

Assignment No 5 Static Routing

1. Configure Static Routing Configuration in Sample Network

Assignment No 6 Dynamic Routing using Protocols

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

Assignment No 7 Remote Management using Network Protocols

1. Configuring and Verifying TELNET and SSH

Assignment No 8 Switch Configuration

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

Assignment No 9 Data Encryption

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

Assignment No 10 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 StallingsPublisher: Addison-Wesley 2015
5. William Stallings, Cryptography and Network Security: Principles and Standards, PrenticeHallIndia, 3rd Edition, 2003

Savitribai Phule Pune University
F.Y. B.Sc.(Cyber Security)
Practical course based on CYS153MJ
Python Programming (CYS156 MJP)

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

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.
4. How to download libraries and its use in the programs.

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.
4. Develop an application using packages
5. Apply python libraries in the program for statistical operation, scientific operation.

Assignment 1: Write a Python program to:

1. Function to find the sum of digits of a number.
2. A function that generates all the factors of a number.

Assignment 2: Write a Python program to:

1. Function to find GCD/LCM of 2 numbers.
2. To find the largest among 3 numbers

Assignment 3: Write a Python program to:

1. To find factorial of a given number.
2. To check prime number

Assignment 4: Write a Python program to:

1. To count repeated characters in a string. Sample string: the quick brown fox jumps over the lazy dog. Expected output: o-4, e-3, u-2, h-2, r-2, t-2
2. Get a string from a given string where all occurrences of its first character have been changed to '$', except the first character itself.

Assignment 5: Write a Python program to:

1. Change a given string to a new string where the first and last characters have been exchanged.
2. Remove the nth index character from a non-empty string

Assignment 6: Write a Python program to:

1. Shuffle and print a specified list.
2. Merge two python dictionaries.

Assignment 7: Write a Python program to:

1. Sort(ascending and descending) dictionary by value.
2. Accept a string and calculate the number of digits, letters and other characters.

Assignment 8: Write a Python program to:

1. Function to concatenate two strings.
2. 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.
2. Convert decimal to binary using recursion.

Assignment 10: 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.
2. 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 11: Write a Python program to:

1. Program to display Fibonacci series using recursion.
2. To display power of 2 using anonymous function

Assignment 12: Write a Python program to:

1. To generate Fibonacci terms using generator function.
2. Define a class Employee having members id, name, department, salary. Create a subclass called manager with member bonus. Define methods accept and display in both the classes. Create n objects of the manager class and display the details of the manager having the maximum total salary (salary+bonus).

Assignment 13: Write a Python program to:

1.Using class, which has two methods get_String and print_String. get_String accept a string from the user and print_String print the string in upper case.
2. Using package to calculate area and volume of cube and sphere

Assignment 14: Write a Python program to: 1.To find the repeated items of a tuple
2.To compute element-wise sum of given tuples. Original lists: (1, 2, 3, 4) (3, 5, 2, 1) (2, 2, 3, 1)
Element-wise sum of the said tuples: (6, 9, 8, 6)

Assignment 15: Write a Python program to:1.To accept string and remove the characters which have odd index values of given string using user defined function.
2. To create a class Rectangle with data member's length, width and methods area, perimeter which can compute the area and perimeter of rectangle.

Assignment 16: Write a Python program to:

1. Create a list a = [1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89] and write a python program that prints out all the elements of the list that are greater than 10
2. To define the class person having members name, address. Create a subclass called Employee with members staffed salary. Create 'n' objects of the Employee class and display all the details of the employee.

Assignment 17: Write a Python program to:

1.Define a class named Shape and its subclass(Square/ Circle). The subclass has an init function which takes an argument (Length /radius). Both classes should have methods to calculate area and volume of a given shape.
2.To create a class Circle and Compute the Area and the circumferences of the circle.(use parameterized constructor)

Assignment 18: Write a Python program to:

1. To generate and print a dictionary which contains a number (between 1 and n) in the form(x,x*x). Sample Dictionary (n=5) Expected Output: {1:1, 2:4, 3:9, 4:16, 5:25}
2. Write a Python script to Create a Class which Performs Basic Calculator Operations.

Assignment 19: Write a Python program to:

1.To find the sum of all elements of an array 2. To find largest element in the array.

Assignment 20: Write a Python program to:

1.To find the occurrence of a particular number in array
2. Merge two sorted array as a new array.

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 Security)
SEC151CYS- Statistical Methods-I

Teaching Scheme	No. of Credits	Examination Scheme
4 hours / week	**2**	**CE: 15 Marks EE: 35 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. Set up and Install the system services.
4. Predict the values in correlation & regression and interpret to make decisions.

Course Contents

Chapter 1 Data Condensation and Graphical methods 7 hours

- Types of data, Types of variable constant, attribute.
- 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), Median, 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- 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 8 hours

- Concept of Correlation, Types of correlation.
- Scatter Diagram, Karl- Pearson correlation coefficient
- Numerical Problems on Correlation ,Concept 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. Fundamental of Mathematical Statistics, S.C.Gupta and V.K.Kapoor, Sultan Chand & Sons, New Delhi.
2. Statistical Methods, George W. Snedecor, William G, Cochran, John Wiley & sons
3. Fundamentals of Applied Statistics (3rd Edition), Gupta and Kapoor, S.Chand and Sons, New

Delhi, 1987.
4. 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

(Formerly University of Pune)

Four Year Degree Program

B.Sc. (Cyber Security)

With

Major: Cyber Security

(Faculty of Science and Technology)

Syllabi for

S.Y.B.Sc. (Cyber Security)

(For Colleges Affiliated to Savitribai Phule Pune University)

Choice Based Credit System (CBCS)

Syllabus under National Education Policy

(NEP)

To be implemented from Academic Year 2025-2026

Level:-5.0(Second Year) Sem:-III									
CourseType	Course Code	Course Code	Course Title		Teaching Scheme Hr Week		Evaluation /Scheme and Max Marks		
			TH	PR	TH	PR	CE	EE	Total
Major Core (6+2)	CYS201MJ	Ethical Cyber Hacking-I	2		2		15	35	50
	CYS202MJ	Ethics and Cyber Law	2		2		15	35	50
	CYS203MJ	Advance Network Security	2		2		15	35	50
	CYS204MJP	Practical based on CYS201MJ		2		4	15	35	50
VSC(2)	CYS221VSC	Data Structure in Python	2		2		15	35	50
FP/OJT/CEP(2)	CYS231FP	Mini Projects based on CYS201MJ		2		4	15	35	50
Minor (2+2)	CYS241MN	Web Development Technologies	2		2		15	35	50
	CYS242MNP	Practical based on CYS241MN		2		4	15	35	50
GE/OE(2)	OE201CYS	From University Basket	2		2		15	35	50
AEC(2)	AEC201	From University Basket	2		2		15	35	50
CC(2)	CC201PE/ NSS/NCC	From University Basket	2		2		15	35	50
TOTAL			16	06	16	12			

Level:-5.0 (Second Year) Sem:-IV									
CourseType	Course Code	Course Code	Course Title		Teaching Scheme Hr Week		Evaluation /Scheme and Max Marks		
			TH	PR	TH	PR	CE	EE	Total
MajorCore (6+2)	CYS251MJ	Ethical Cyber Hacking-II	2		2		15	35	50
	CYS252MJ	Cloud Cyber Security	2		2		15	35	50
	CYS253MJ	Database Management System	2		2		15	35	50
	CYS254MJP	Practical based on CYS251MJ		2		4	15	35	50
FP/OJT/CEP(2)	CYS281FP	Mini Projects based on CYS251MJ		2		4	15	35	50
Minor (2+2)	CYS291MN	Modern Web Development	2		2		15	35	50
	CYS292MNP	Practical based on CYS291MN		2		4	15	35	50
GE/OE (2)	OE251CYS	From University Basket		2		4	15	35	50
SEC(2)	SEC251CYSP	Business Communication		2		4			
AEC(2)	AEC251	From University Basket	2		2		15	35	50
CC(2)	CC251PE /NSS/NCC	From University Basket	2		2		15	35	50
TOTAL			12	10	12	20			

Semester-III

Savitribai Phule Pune University
S.Y.B.Sc. (Cyber Security) - Sem – III
Course Type: Subject Code :CYS-201MJ
Course Title : Ethical Cyber Hacking-I

Teaching Scheme 02 Hrs / week	No. of Credits: 2	Examination Scheme IE : 15 marks UE: 35 marks

Prerequisites

- Fundamentals of Cyber Security
- Fundamentals of OSI Model and TCP/IP Suite
- Fundamentals of GNU/Linux Operating System

Course Objectives

- To introduce students to the fundamentals of ethical hacking and cyber security threats.
- To familiarize students with various hacking methodologies and techniques.
- To develop practical skills in penetration testing and vulnerability assessment.
- To educate students on legal and ethical responsibilities in cyber security.
- To enhance students' ability to recognize and mitigate cyber threats effectively.

Course Outcomes (COs):

Upon successful completion of this course, students will be able to:

CO1: Explain the fundamentals of ethical hacking, cyber security threats, and the importance of ethical responsibilities in hacking practices

CO2: Perform reconnaissance techniques using various foot printing and information-gathering tools to identify vulnerabilities in a target system.

CO3: Conduct network scanning operations to detect live hosts, open ports, and potential security flaws using advanced scanning techniques.

CO4: Demonstrate system hacking techniques such as password cracking, privilege escalation, and malware attacks while understanding countermeasures.

CO5: Analyze and exploit common web application vulnerabilities, including SQL Injection, Cross-Site Scripting (XSS), and CSRF, using ethical hacking tools.

CO6: Evaluate wireless network security by performing attacks on WEP, WPA, and WPA2 encryption and implementing security best practices.

Course Contents

Chapter 1	Introduction to Ethical Hacking	(6 Hours)

- Overview of Cyber security and Ethical Hacking
- Understanding Hacking: Types and Phases
- Ethical Hacking vs. Malicious Hacking
- Cyber Laws and Ethical Responsibilities
- Setting up a Lab Environment for Ethical Hacking

Chapter 2	Foot printing and Reconnaissance	(5 Hours)

- Basics of Foot printing
- Active vs. Passive Reconnaissance
- Information Gathering Techniques
- WHOIS Lookup, DNS Enumeration, Google Dorking
- Tools: Maltego, Shodan, Nmap, Recon-ng

Chapter 3	Scanning Networks	(5 Hours)

- Network Scanning Fundamentals
- Types of Scanning (Port, Vulnerability, Service)
- Identifying Live Systems and Open Ports
- Scanning Techniques: TCP/UDP Scans, SYN Scans
- Tools: Nmap, Netcat, Angry IP Scanner

Chapter 4	System Hacking and Gaining Access	(6 Hours)

- Exploiting System Vulnerabilities
- Password Cracking Techniques (Brute Force, Dictionary Attack)
- Privilege Escalation and Maintaining Access
- Malware: Keyloggers, Trojans, Rootkits
- Tools: Metasploit, John the Ripper, Hydra

Chapter 5	Web Application Hacking Basics	(4 Hours)

- Common Web Vulnerabilities (SQL Injection, XSS, CSRF)
- OWASP Top 10 Overview
- Basics of Website Enumeration
- Tools: Burp Suite, SQLmap, ZAP Proxy

Chapter 6	Wireless Hacking Basics	(4 Hours)

- Fundamentals of Wireless Networks and Security
- Cracking WEP/WPA/WPA2 Encryption
- MITM (Man-in-the-Middle) Attacks in Wireless Networks
- Tools: Aircrack-ng, Wireshark, Kismet

Reference Books:

- **Certified Ethical Hacker (CEH) v12 Study Guide** – Matt Walker
- **Hacking: The Art of Exploitation** – Jon Erickson
- **The Web Application Hacker's Handbook** – Dafydd Stuttard & Marcus Pinto
- Online Labs: TryHackMe, Hack The Box, PentesterLab

Savitribai Phule Pune University
S.Y.B.Sc. (Cyber Security) - Sem – III
Course Type: Subject Code :CYS-202MJ
Course Title : Ethics and Cyber Law

Teaching Scheme 02Hrs / week	No. of Credits: 2	Examination Scheme IE : 15 marks UE: 35 marks

Prerequisites

- Basic knowledge of computer systems and networking.
- Awareness of cyber security concepts.
- Interest in digital security laws and ethics

Course Objectives

- To understand the ethical and legal issues in cyber security.
- To familiarize students with national and international cyber laws.
- To examine ethical frameworks for digital security.
- To analyze case studies on cybercrime and legal consequences.

Course Outcomes (COs):

Upon successful completion of this course, students will be able to:

- **CO 1**: Recognize ethical concerns in cyber security.
- **CO 2**: Understand key cyber laws in India and globally
- **CO 3**: Apply legal frameworks to cybercrime cases.
- **CO 4**: Develop ethical decision-making skills.
- **CO 5**: Analyze cyber forensic techniques in legal contexts.
- **CO 6**: Evaluate international cyber laws and their impact on digital security.

Course Contents

Chapter 1	**Introduction to Cyber Ethics**	**(6 Hours)**

- Ethics in Cyber security
- Ethical Theories (Utilitarianism, Deontology, Virtue Ethics)
- Ethical Hacking , Malicious Hacking
- Digital Rights and Responsibilities
- Intellectual Property Rights (IPR) in Cyberspace

Chapter 2	**Cybercrime and Cyber Law**	**(6 Hours)**

- Cybercrimes and Their Types
- Social Engineering and Cyberbullying
- Basics of Cyber Forensics
- Role of Law Enforcement
- Overview of IT Act, 2000

Chapter 3	Indian Cyber Law Framework	(6 Hours)

- IT Act, 2000: Objectives, Scope, and Amendments
- Cyber Law and E-Governance
- Digital Signatures and Electronic Authentication
- Cybercrime Cases in India: Analysis and Legal Consequences
- Right to Privacy and Data Protection Laws

Chapter 4	International Cyber Law and Policies	(6 Hours)

- Global Perspectives on Cyber Law: GDPR, HIPAA, COPPA
- Role of Organizations like ICANN, CERT-In, and UN
- Cyber Warfare and International Treaties
- Ethical Challenges in AI and IoT Security
- Case Studies on Cross-Border Cybercrime

Chapter 5	Emerging Trends in Cyber security and Legal Challenges	(6 Hours)

- AI and Machine Learning in Cyber security
- Block chain and Crypto currency Laws
- Cloud Security and Data Regulations
- Cyber security Threats in the Metaverse
- Future Trends in Cyber Law

Reference Books:

- Cyber Law & Cyber Crimes – Pankaj Agarwal
- Cyber security Ethics – Mary Manjikian
- Information Technology Law and Practice – Vakul Sharma
- Cyber Crime and Legal Framework – Anirudh Rastogi
- The Ethics of Cyber security – Markus Christen et al.

Savitribai Phule Pune University
S.Y.B.Sc. (Cyber Security)
Subject Code: CYS203MJ
Subject: Advance Network Security

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

Prerequisites:

- To understand process of data communication using protocols and standards
- To learn various topologies and applications of network.

Course Objectives:

- To prepare students with basic networking concept.
- To understand process of data communication using protocols and standards
- To understand the concept of network security, networking attacks, cryptography.

Course Outcomes:

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

- Understand Network Security Concepts
- Identify Security Threats and Vulnerabilities
- Implement Cryptographic Technique
- Monitor and Analyze Network Traffic:

Course Contents

Chapter 1	**Introduction**	**5 hours**

- Communication models- OSI Overview, TCP/IP Overview
- Communication protocol overview
- Bridging and Switching Overview
- Virtual Private Networks Overview
- Introduction Attacks on Computers and Computer Security

Chapter 2	**TCP/IP Protocol Overview**	**5 hours**

- Over of IP Addressing-Architecture
- Class of Address- Example of Addressing, Special Addresses
- Addressing and Networks
- Introduction to Subnetting - Simple Subnets, Complex subnets , Variable Length Subnets
- IP Addressing Design

Chapter 3	Network Fundamental and Security	8 hours

- Need for Security
- Security Attacks (Active and Passive attacks)
- Services and Mechanisms
- Network Security
- Network Security Mode
- Internet Standards and RFCs
- Symmetric Key Cryptography

Chapter 4	User Authentication and security at Application and Transport Layer	12 hours

- Pretty Good Privacy (PGP) and S/MIME.
- User Authentication 1. Remote User-Authentication Principles
- Remote User-Authentication Using Symmetric 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 Layer Security, HTTPS, Secure Shell (SSH)

Reference Books:

- Certified Ethical Hacker (CEH) v12 Study Guide – Matt Walker
- Cryptography & Network Security – William Stallings
- TCP / IP Protocol Suite Fourth Edition – Behrouz A. Forouzan

E-Books and Online Learning Material

- http://www.w3schools.com/html/html5_intro.asp
- Network Security Essentials by William Stallings
- Network Security: Private Communication in a Public World by Charlie Kaufman, Radia Perlman, and Mike Speciner

Savitribai Phule Pune University
S.Y.B.Sc. (Cyber Security) - Sem – III
Course Type: Subject Code :CYS-204MJP
Course Title : Ethical Cyber Hacking-I (Practical)

Teaching Scheme 04 Hrs / week	No. of Credits: 2	Examination Scheme IE : 15 marks UE: 35 marks

Course Objectives:

- To provide hands-on experience in ethical hacking techniques and tools.
- To develop skills in reconnaissance, scanning, and exploitation of system vulnerabilities.
- To familiarize students with penetration testing methodologies.
- To analyze and secure web applications and wireless networks against cyber threats.
- To enhance understanding of cyber security best practices and ethical considerations.

Course Outcomes (COs):

Upon successful completion of this course, students will be able to:
CO1: Set up and configure an ethical hacking lab environment using virtualization tools.
CO2: Perform reconnaissance techniques and information gathering using open-source intelligence (OSINT) tools.
CO3: Conduct network scanning and identify vulnerabilities in target systems.
CO4: Execute system hacking techniques including password cracking, privilege escalation, and malware deployment.
CO5: Identify and exploit common web application vulnerabilities like SQL Injection and XSS.
CO6: Assess wireless network security and conduct attacks on WEP, WPA, and WPA2 encryption.

Practical List

Lab 1: Introduction to Ethical Hacking Environment

Objective: Set up an ethical hacking lab using a virtualized environment.

Tasks:

- Install Virtual Box/VMware on the system.
- Set up Kali Linux and Metasploitable VM.
- Configure network settings for penetration testing.
- Verify installation of essential hacking tools (Nmap, Metasploit, Wireshark).

Lab 2: Information Gathering & Foot printing

Objective: Perform reconnaissance and gather information about a target system.

Tasks:

- Perform WHOIS lookup and analyze results.
- Conduct DNS enumeration using nslookup and dig.
- Use Google Dorking techniques to find sensitive information.
- Use tools like Maltego and Shodan to gather intelligence.

Lab 3: Network Scanning Techniques

Objective: Identify live hosts, open ports, and running services on a target network.

Tasks:

- Perform a basic Nmap scan on a target machine.
- Conduct SYN, TCP Connect, and UDP scans.
- Detect operating system and version details.
- Analyze scan results using Wireshark.

Lab 4: System Hacking and Password Cracking

Objective: Exploit system vulnerabilities and crack passwords.

Tasks:

- Use John the Ripper to crack hashed passwords.
- Perform a brute-force attack using Hydra on SSH.
- Demonstrate privilege escalation techniques.
- Deploy Keyloggers and analyze logs.

Lab 5: Web Application Hacking Basics

Objective: Exploit common web vulnerabilities like SQL Injection and XSS.

Tasks:

- Perform SQL Injection attacks using SQLmap.
- Demonstrate XSS attacks using Burp Suite.
- Analyze OWASP Top 10 vulnerabilities.
- Use ZAP Proxy to intercept and modify HTTP requests.

Lab 6: Wireless Network Security & Attacks

Objective: Analyze and exploit weaknesses in wireless networks.

Tasks:

- Capture Wi-Fi packets using Wireshark.
- Perform WEP/WPA2 cracking using Aircrack-ng.
- Conduct a deauthentication attack.
- Simulate a MITM attack in a controlled lab environment.

Savitribai Phule Pune University
S.Y.B.Sc. (Cyber Security) - Sem – III
Course Type: Subject Code:CYS221VSC
Course Title : Data Structure in Python

Teaching Scheme **02Hrs / week**	**No. of Credits: 2**	**Examination Scheme** **IE : 15 marks** **UE: 35 marks**

Prerequisites

- Introductory Programming (in Python)
- Basic Discrete Mathematics (helpful, but not strictly required)

Course Objectives

- Understand and implement fundamental data structures such as arrays, linked lists, stacks, queues, and hash tables.
- Analyze the time and space complexity of basic algorithms.
- Apply appropriate data structures to solve security-related problems.
- Develop proficiency in Python programming for secure coding practices.
- Understand the importance of efficient data handling in cyber security contexts.

Course Outcomes (COs):

Upon successful completion of this course, students will be able to:
CO1 : Implement efficient algorithms using appropriate data structures.
CO2 : Analyze the performance of algorithms and select suitable data structures for specific problems.
CO3 : Apply data structures to solve practical cyber security challenges.
CO4 : Write well-structured and documented Python code.
CO5 : Demonstrate an understanding of the trade-offs between different data structures in terms of performance.
CO6 : Evaluate and implement secure data handling practices to protect sensitive information in data structures

Course Contents

Chapter 1	**Introduction to Data Structures and Python Review**	**(7 Hours)**

- Introduction to Data Structures: Definition, Classification, and Applications
- Python Review: Basic syntax, data types, control structures, functions, and modules.
- Object-Oriented Programming in Python: Classes, objects, inheritance, and polymorphism.
- Basic Security Considerations in Python.

Chapter 2	Arrays and Strings	(7 Hours)

- Arrays: Static and dynamic arrays, multi-dimensional arrays.
- Array Operations: Insertion, deletion, searching, and sorting.
- Strings: String manipulation, pattern matching.
- Applications: Implementing simple ciphers, storing cryptographic keys.

Chapter 3	Linked Lists	(7 Hours)

- Linked Lists: Singly linked lists, doubly linked lists, circular linked lists.
- Linked List Operations: Insertion, deletion, traversal, and searching.
- Applications: Implementing dynamic data structures, memory management.

Chapter 4	Stacks and Queues	(6 Hours)

- Stacks: LIFO principle, stack operations.
- Queues: FIFO principle, queue operations.
- Applications: Expression evaluation, backtracking algorithms, network packet queuing

Chapter 5	Security Considerations and Data Structures	(3 Hours)

- Secure Coding Practices with Data Structures
- Common Vulnerabilities: Buffer overflows, injection attacks.

Reference Books:

- Data Structures and Algorithms in Python by Michael T. Goodrich, Roberto Tamassia, and Michael H. Goldwasser
- Algorithms and Data Structures in Python by Day Nicholas
- Data Structures and Algorithms Using Python by Rance D. Necaise
- Algorithms for Sorting and Searching by Thomas H. Cormen

Savitribai Phule Pune University

S.Y.B.Sc. (Cyber Security) - Sem – III

Course Type: Subject Code :CYS-231FP

Course Title : Mini Project based on CYS201MJ

Teaching Scheme 04 Hrs / week	No. of Credits: 2	Examination Scheme IE : 15 marks UE: 35 marks

Course Objectives:

- To provide hands-on experience in ethical hacking projects.
- To enhance problem-solving skills in identifying and mitigating cyber threats.
- To enable students to apply ethical hacking tools and techniques in real-world scenarios.
- To develop analytical skills in vulnerability assessment, penetration testing, and system security.
- To promote ethical considerations and responsible hacking practices.

Course Outcomes (COs):

Upon successful completion of the mini-projects, students will be able to:

CO1: Identify and define cyber security challenges and propose ethical hacking solutions.
CO2: Apply ethical hacking methodologies to conduct security assessments.
CO3: Demonstrate the ability to analyze vulnerabilities in networks, web applications, and systems.
CO4: Develop and document a structured approach to penetration testing and risk mitigation.
CO5: Implement security measures to counteract identified threats.
CO6: Present findings and recommendations in a professional security report format.

Project Guidelines:

- Projects should be performed in a controlled lab environment using ethical hacking tools.
- Each project should include **problem definition, objectives, methodology, tools used, results, and conclusions**.
- The final project report should include **screenshots, observations, and security recommendations**.
- Group size: **Maximum of 2 students per project**.

Suggested Mini Projects List:

- **Vulnerability Assessment of a Web Application** – Perform penetration testing on a dummy website using OWASP tools like Burp Suite and SQLmap.
- **Network Scanning and Exploitation** – Conduct an in-depth analysis of a local network, identify vulnerabilities, and demonstrate controlled exploitation.
- **Wireless Security Testing** – Analyze security flaws in Wi-Fi networks and perform WEP/WPA cracking in a test environment.
- **Phishing Attack Simulation** – Create an awareness-based phishing simulation and analyze user response rates.

- **Reverse Engineering Malware** – Analyze a harmless malware sample, detect its functionality, and implement countermeasures.
- **Social Engineering Attack Simulation** – Design and test social engineering attacks like email spoofing and USB baiting to demonstrate awareness.
- **Developing a Keylogger** – Create a simple keylogger for educational purposes and analyze security measures to counteract it.
- **Security Audit of a Linux System** – Perform a security audit of a Linux system and recommend hardening measures.

Submission Guidelines:

- Each lab should be documented with **objective, tools used, procedure, observations, and conclusion**.
- Screenshots must be included for each step of the practical.
- The completed lab book must be submitted before the deadline.

Savitribai Phule Pune University
S.Y.B.Sc. (Cyber Security) - Sem – III
Course Type: Subject Code : CYS241MN
Course Title : Web Development Technology

Teaching Scheme 02Hrs / week	No. of Credits: 2	Examination Scheme IE : 15 marks UE: 35 marks

Prerequisites

- Fundamentals of Web development
- Fundamentals of developing web site using HTML,CSS and JavaScript

Course Objectives

- To learn about the Internet, World Wide Web (WWW), and web technologies.
- To know and understand the concept of web designing.
- To understand how to develop web-based applications using HTML and CSS
- To implement Interactivity with JavaScript
- To develop Real-World Web Applications

Course Outcomes (COs):

Upon successful completion of this course, students will be able to:

CO1: Explain the concepts of the Internet, World Wide Web (WWW), web browsers, and web servers and understand client-server architecture and HTTP/HTTPS protocols.

CO2: Create Basic Web Pages Using HTML and Develop structured web pages using HTML5 elements, forms, and multimedia tags.

CO3: Apply CSS for Web Page Styling and use CSS to design visually appealing and responsive web pages, implement layouts, colors, fonts, and animations using CSS.

CO4: Implement Basic Interactivity with JavaScript, Use JavaScript for simple form validation, user interaction, and DOM manipulation.

CO5: Understand Web Hosting and Deployment, learn the basics of web hosting, domain names, and deploying static websites.

CO6: Work on a Basic Web Project, develop a small project applying HTML, CSS, and JavaScript concepts.

Course Contents

Chapter 1	Introduction to HTML	(6 Hours)

- Introduction to HTML, Basic HTML Structure ,Common HTML Tags
- Physical and Logical HTML ,Types of Images, client side and server-side Image mapping,
- List, Table, Frames, Embedding Audio, Video, HTML form and form elements.

Chapter 2	Basics of Style sheets	(6 Hours)

- Need for CSS, Introduction to CSS, What is CSS? ,Importance of CSS in Web Development
- Types of CSS: Inline CSS, Internal CSS ,External CSS
- Basic CSS Syntax and Structure

Chapter 3	Advanced Styling and Layouts in CSS	(8 Hours)

- **CSS Selectors:** Element Selector Class Selector ,ID Selector ,Group Selector Universal Selector
- **CSS Properties:** Colors (color, background-color),Fonts (font-family, font-size, font-style) ,Text Formatting (text-align, text-decoration, text-transform)
- **Box Model and Layouts:** Understanding the Box Model (Margin, Border, Padding, Content) Width, Height, and Overflow, Display Property (block, inline, inline-block, none),Positioning Elements (static, relative, absolute, fixed, sticky)
- Styling Lists, Links, and Tables: Customizing Lists (ordered, unordered, nested lists), Styling Links (hover, active, visited, focus),Table Styling (borders, spacing, background)

Chapter 4	Introduction to JavaScript	(6 Hours)

- Introduction to Java Script, What is JavaScript?
- Importance of JavaScript in Web Development
- How JavaScript Works (Client-Side vs. Server-Side)
- Writing and Running JavaScript (Inline, Internal, and External JS)
- Comments in JavaScript, Alert, Prompt, and Console.log(),
- Identifier & operator,
- Control Structure, Conditional Statements (if, if-else, switch-case),Loops (for, while, do-while),Break and Continue Statements,
- Functions ,Predefined functions, math & string functions ,Array in Java scripts
- Introduction to Arrays ,Creating, Accessing, Modifying ,Array Methods (push, pop, shift, unshift, for Each, map) ,Introduction to Objects (Properties and Methods) ,Accessing Object Data (Dot Notation vs. Bracket Notation)

Chapter 5	DOM Manipulation (Document Object Model)	(4 Hours)

- What is the DOM?, Selecting Elements (getElementById, querySelector)
- Changing HTML and CSS with JavaScript ,Handling Events (onclick, onmouseover, onkeyup) , Event Listeners (add Event Listener) ,Keyboard and Mouse Events
- Form Validation Basics

Reference Books:

- HTML and CSS: Design and Build Websites – Jon Duckett
- CSS: The Missing Manual – David Sawyer McFarland
- Mastering CSS: A Beginner's Guide – Rich Finelli
- JavaScript and JQuery: Interactive Front-End Web Development – Jon Duckett
- JavaScript: The Definitive Guide – David Flanagan

Savitribai Phule Pune University
S.Y.B.Sc. (Cyber Security) - Sem – III
Course Type: Subject Code :CYS-242MNP
Course Title : Practical based on CYS241MJ

Teaching Scheme **04 Hrs / week**	**No. of Credits: 2**	**Examination Scheme** **IE : 15 marks** **UE: 35 marks**

Course Objectives:

- Learn about the fundamental components of web development (HTML, CSS, JavaScript).
- Understand the difference between front-end and back-end development.
- Develop structured web pages using HTML.
- Apply CSS for styling and layout designs.
- Implement interactive features using JavaScript

1) Creating a JavaScript code block, which checks the contents entered in a form's Text element. If the text entered is in the lower case, convert to upper case.
2) Design a login form with fields username, password and login button.
3) Write a JavaScript to accept username and password, validate login details and display a message accordingly.
4) Creating a web page using two image files, which switch between one another as the mouse pointer moves over the images.
5) Creating a web page, which accepts user information and user comments on the web site to check if all the Text fields have being entered with data else display an alert.
6) Write a program in JavaScript and DOM to update the backgroundColor dynamically.
7) Write a java script function that reverse a input number.
8) Write a JavaScript code to accept a string from the user and display the occurrences of every vowel character from the string
9) Write a JavaScript to read a number from user, store its factors into the array and display that array. (Handle onClick event).
10) Write a JavaScript function that retrieves the first and last name values, concatenates them, and displays the full name in an alert.
11) Write a JavaScript function that prevents the default form submission and displays the form values in a designated div element.
12) Write a JavaScript program to set paragraph background color.
13) Write a JavaScript program to remove items from a drop-down list.
14) Write a JavaScript program to display a random image (clicking on a button)
15) Write a JavaScript program to find all HTML elements that match a specified CSS selector (id, class names, types, attributes, values of attributes, etc), use the querySelectorAll() method.

Semester-IV

Savitribai Phule Pune University
S.Y.B.Sc. (Cyber Security) - Sem – IV
Course Type: Subject Code:CYS-251MJ
Course Title : Ethical Cyber Hacking-II

Teaching Scheme 02Hrs /Week	No. of Credits: 2	Examination Scheme IE : 15 marks UE: 35 marks

Prerequisites

- Basic Knowledge of Ethical Hacking
- Networking Fundamentals
- Web Application Security Basics

Course Objectives

- To provide advanced knowledge of ethical hacking techniques.
- To explore complex attack vectors and countermeasures.
- To enhance practical skills in penetration testing and red teaming.
- To introduce forensic analysis in cyber investigations.
- To ensure ethical compliance and best security practices.

Course Outcomes (COs):

Upon successful completion of this course, students will be able to:

CO1: Explain advanced network penetration testing techniques, including bypassing firewalls, IDS/IPS evasion, and exploiting network vulnerabilities.

CO2: Perform advanced web application exploitation using techniques such as SQL injection, XML External Entity (XXE) attacks, and Server-Side Request Forgery (SSRF

CO3: Analyze and exploit vulnerabilities in wireless networks and IoT devices, including WPA3 attacks, RFID exploitation, and Bluetooth security flaws

CO4: Evaluate security risks in cloud environments by identifying and exploiting misconfigurations in AWS, Azure, and GCP.

CO5: Apply digital forensic techniques to perform memory and disk analysis, log investigation, and malware analysis for cyber security incident response.

CO6: Demonstrate red teaming methodologies, privilege escalation, lateral movement, and social engineering tactics used in advanced penetration testing.

Course Contents

Chapter 1	**Advanced Network Penetration Testing**	**(6 Hours)**

- Advanced Scanning Techniques and Bypassing Firewalls
- Exploiting Network Vulnerabilities (SMB, SNMP, FTP, SSH)
- Man-in-the-Middle (MITM) Attacks & DNS Spoofing
- IDS/IPS Evasion Techniques
- Tools: Wireshark, Scapy, Bettercap

Chapter 2	Web Application Exploitation	(5 Hours)
• Advanced SQL Injection Techniques • Exploiting XML External Entity (XXE) and Server-Side Request Forgery (SSRF) • Advanced Cross-Site Scripting (XSS) & Cross-Site Request Forgery (CSRF) • Server-Side Template Injection (SSTI) • Tools: Burp Suite Pro, OWASP ZAP, SQLmap		
Chapter 3	**Wireless and IoT Hacking**	**(5 Hours)**
• WPA3 & Advanced Wireless Attacks • Exploiting IoT Devices: Smart Home Security Risks • Bluetooth and RFID Hacking Techniques • Drone and Embedded System Security • Tools: Aircrack-ng, Kismet, Bettercap, HackRF		
Chapter 4	**Cloud Security and Hacking**	**(6 Hours)**
• Cloud Security Architecture (AWS, Azure, GCP) • Exploiting Cloud Misconfigurations (S3 Bucket, IAM Policies) • Server less & Container Security (Docker, Kubernetes) • Cloud Forensics & Incident Response • Tools: Pacu, Scout Suite, Cloud Sploit		
Chapter 5	**Cyber Forensics and Incident Response**	**(4 Hours)**
• Memory and Disk Forensics • Log Analysis and Malware Reverse Engineering • Threat Hunting and SOC Operations • Digital Evidence Handling and Chain of Custody • Tools: Autopsy, Volatility, FTK, Splunk		
Chapter 6	**Red Teaming and Advanced Exploitation**	**(4 Hours)**
• Red Team vs. Blue Team Methodologies • Exploiting Privilege Escalation and Lateral Movement • Social Engineering Tactics and Physical Security Bypass • Post-Exploitation and Data Exfiltration • Tools: Cobalt Strike, Empire, Blood Hound		
Reference Books:		
• **The Hacker Playbook 3** – Peter Kim • **Black Hat Python: Python Programming for Hackers and Pentesters** – Justin Seitz • **The Web Application Hacker's Handbook** – Dafydd Stuttard & Marcus Pinto • Online Platforms: Hack The Box, TryHackMe, PentesterLab		

Savitribai Phule Pune University
S.Y.B.Sc. (Cyber Security) - Sem – IV
Course Type: Subject Code:CYS-252MJ
Course Title : Cloud Cyber Security

Teaching Scheme 02Hrs /Week	**No. of Credits: 2**	**Examination Scheme IE : 15 marks UE: 35 marks**

Prerequisites : Understanding of operating systems (Windows/Linux)

- Basic understanding of TCP/IP, HTTP/HTTPS
- Knowledge of cloud service models (IaaS, PaaS, SaaS)
- Awareness of cyber threats (phishing, malware, ransomware

Course Objectives

- To introduce students to Provide foundational knowledge of cloud security.
- To equip learners with skills to identify and mitigate cloud security threat.
- To develop an understanding of network and data security principles in the cloud.
- To Offer hands-on experience with cloud security tools.
- To Train learners in incident response and disaster recovery planning.

Course Outcomes (COs):

Upon successful completion of this course, students will be able to:

CO1: Demonstrate an understanding of cloud computing models and security principles, including IaaS, PaaS, SaaS, and various cloud deployment strategies.

CO2: Identify and analyze cloud security threats and vulnerabilities, such as data breaches, insecure APIs, and misconfigurations.

CO3: Implement cloud security measures, including encryption, access control, identity and access management (IAM), and secure authentication methods..

CO4: Evaluate compliance and regulatory frameworks (GDPR, IT Act 2000, ISO 27001, NIST) and apply best practices for cloud security governance.

CO5: Utilize cloud security tools and technologies, such as AWS Security Hub, Azure Security Center, and Google Cloud Security Command Center, to monitor and mitigate risks..

CO6: Design and apply incident response and disaster recovery strategies for handling security breaches and ensuring business continuity in cloud environments..

Course Contents

Chapter 1	**Fundamentals of Cloud Security**	**(4 Hours)**

- Introduction to Cloud Computing
- Cloud Service Models (IaaS, PaaS, SaaS)
- Cloud Deployment Models (Public, Private, Hybrid, Multi-Cloud)
- Shared Responsibility Model in Cloud Security
- Key Cloud Security Challenges and Risks

Chapter 2	Cloud Security Threats and Risk Management	(6 Hours)
• Common Cloud Threats: Data Breaches, Insecure APIs, Account Hijacking • Risk Management Strategies in Cloud Environments • Identity and Access Management (IAM) Best Practices • Data Protection, Encryption, and Secure Data Storage in the Cloud • Security Compliance and Regulatory Frameworks (GDPR, IT Act 2000, ISO 27001)		
Chapter 3	**Network Security in Cloud Environments**	**(6 Hours)**
• Cloud Network Architecture and Security • Virtual Private Cloud (VPC) and Network Segmentation • Firewalls, Intrusion Detection and Prevention Systems (IDS/IPS) • Secure Communication Protocols (HTTPS, TLS, VPNs • Denial-of-Service (DoS/DDoS) Attack Prevention in Cloud		
Chapter 4	**Introduction to AWS Security**	**(7 Hours)**
• Overview of **Amazon Web Services (AWS)** and Cloud Security Features • AWS Identity and Access Management (IAM) • AWS Security Tools: AWS Shield, AWS WAF, AWS CloudTrail • Securing AWS Storage (S3) and Databases (RDS, DynamoDB) • AWS Compliance and Best Practices for Cloud Security		
Chapter 5	**Incident Response and Disaster Recovery in Cloud Security**	**(7 Hours)**
• Understanding Security Incidents in Cloud Environments • Cloud-Based Security Monitoring and Logging • Incident Response Planning and Execution • Disaster Recovery Strategies for Cloud-Based Systems • Case Studies on Cloud Security Breaches and Mitigation		
Reference Books:		
• Practical Cloud Security: A Guide for Secure Design and Deployment" - by Chris Dotson **Publisher:** O'Reilly Media • Cloud Security Handbook: A Hands-on Guide to Securing Your Cloud Environment" - by Eyal Estrin **Publisher:** Packt Publishing • "Security in Computing (6th Edition) - by Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies **Publisher:** Pearson • Cloud Computing Security: Foundations and Challenges" - John R. Vacca **Publisher:** CRC Press		

Savitribai Phule Pune University
S.Y.B.Sc. (Cyber Security) - Sem – IV
Course Type: Subject Code:CYS-253MJ
Course Title : Database Management System

Teaching Scheme 02Hrs /Week	No. of Credits: 2	Examination Scheme IE : 15 marks UE: 35 marks

Prerequisites

- Knowledge of fundamental concepts and principles of organizing, storing, and retrieving data.

Course Objectives

- To understand Database Management System conceptually.
- To understand how user requirements can be mapped to schemas.
- To introduce core principles and techniques required in the design and implementation of database systems.
- To become skilled at organizing, maintaining, and retrieving - efficiently and effectively information from a DBMS.

Course Outcomes (COs):

Upon successful completion of this course, students will be able to:

1. Take the most important responsibility as a Database Administrator.
2. Design an Entity-Relationship model from a realistic problem specification.
3. Improve the database design by applying normalization techniques to normalize the database.
4. Convert the ER model to relational tables and formulate SQL queries on data to manage the designed database.

Course Contents

Chapter 1	Fundamentals of Database Management Systems	(4 Hours)

- Introduction to Data, Database, and Database Management System(DBMS)
- File System Vs. DBMS
- Structure of DBMS
- DBMS users and their roles
- Levels of Abstraction and Data Independence
- Advantages and Disadvantages of DBMS

Chapter 2	Relational Database Structuring and Normalization	(8 Hours)

- Overview of DB design
- Introduction to Data models (Hierarchical, Network, Relational)
- E-R data model (Types of entities, attributes, relations, entity sets, relationship sets)
- Extended features (Generalization, Specialization, Aggregation)
- Structure of Relational Databases (table, row, column, attribute, key)
- Concept of Normalization - Normal forms 1NF, 2NF, 3NF with Example, BCNF only definition
- Case Studies

Chapter 3	SQL for Data Management	(14Hours)

- Introduction to SQL, Features, Advantages, Data Types
- Introduction to Database Languages (DDL, DML, DCL, TCL)
- DDL and DML commands with examples, DCL and TCL commands introduction
- Constraints (Not Null, Unique, Check, Primary Key, Referential, Key)
- The basic structure of SQL query, Nested Sub-queries
- Set operations, Aggregate functions, Logical operators, Range Searching, Pattern Matching, clause (distinct, order by, group by, having)
- SQL mechanisms for joining relations (inner joins, outer joins and their types)
- Views
- Case Studies

Chapter 4	Fundamentals of Database Technologies	(4 Hours)

- NoSQL databases. (Introduction, Advantages and Disadvantages, Applications)
- Cloud databases. (Introduction, Advantages and Disadvantages, Applications)
- Mongo DB (Introduction, Advantages and Disadvantages, Applications)

Reference Books:

- Henry F. Korth, Abraham Silberschatz, S. Sudarshan, "Database System Concepts", Tata McGraw-Hill Education
- Raghu Ramakrishnan and Johannes Gehrke, "Database Management Systems", McGraw- Hill
- Beginning Databases with PostgreSQL: From Novice to Professional, Richard Stones, Neil Matthew, ISBN:9781590594780, Apress

E-Books and Online Learning Material

http://www.w3schools.com/html/html5_intro.asp
https://www.matillion.com/blog/the-types-of-databases-with-examples https://www.geeksforgeeks.org/dbms

Savitribai Phule Pune University
S.Y.B.Sc. (Cyber Security) - Sem – IV
Course Type: Subject Code:CYS-254MJP
Course Title : Practical based on CYS251MJ

Teaching Scheme 02Hrs /Week	No. of Credits: 2	Examination Scheme IE : 15 marks UE: 35 marks

Course Objectives

- To provide hands-on experience in advanced ethical hacking techniques.
- To develop expertise in penetration testing, digital forensics, and cloud security.
- To analyze and exploit security vulnerabilities in networks, web applications, wireless systems, and IoT devices.
- To understand red teaming methodologies and security countermeasures.
- To ensure compliance with ethical and legal considerations in cyber security testing.

Course Outcomes (COs):

Upon successful completion of this course, students will be able to:

CO1: Perform advanced network penetration testing, including firewall evasion and exploitation of vulnerabilities.

CO2: Conduct in-depth web application security assessments using advanced exploitation techniques.

CO3: Analyze and exploit security flaws in wireless networks and IoT devices.

CO4: Assess security risks in cloud platforms and identify misconfigurations.

CO5: Apply cyber forensic techniques for malware analysis and incident response.

CO6: Implement red teaming methodologies, privilege escalation, and social engineering tactics.

Practical Assignments:

Lab 1: Advanced Network Penetration Testing

Objective: Conduct network vulnerability assessment and bypass security defenses.

Tasks:

- Perform Nmap scans with IDS/IPS evasion techniques.
- Exploit SMB, SNMP, and FTP vulnerabilities using Metasploit.
- Conduct MITM attacks using Bettercap.
- Perform DNS spoofing and analyze traffic manipulation.

Lab 2: Web Application Exploitation

Objective: Exploit web vulnerabilities and perform security assessments.

Tasks:

- Conduct SQL Injection using SQLmap.
- Exploit XXE and SSRF vulnerabilities using Burp Suite.
- Perform advanced XSS and CSRF attacks.
- Exploit Server-Side Template Injection (SSTI).

Lab 3: Wireless and IoT Hacking

Objective: Assess security weaknesses in wireless and IoT networks.

Tasks:

- Capture Wi-Fi traffic and analyze WPA3 vulnerabilities using Aircrack-ng.
- Exploit smart home IoT devices and analyze security flaws.
- Perform Bluetooth and RFID hacking techniques.
- Simulate drone security testing and embedded system vulnerabilities.

Lab 4: Cloud Security Assessment

Objective: Identify security misconfigurations in cloud environments.

Tasks:

- Perform AWS S3 bucket enumeration and access control testing.
- Identify and exploit IAM policy misconfigurations.
- Analyze container security in Docker and Kubernetes.
- Conduct forensic analysis on cloud logs and threat events.

Lab 5: Cyber Forensics and Incident Response

Objective: Perform forensic analysis for cyber security incidents.

Tasks:

- Conduct memory and disk forensics using Autopsy and Volatility.
- Perform log analysis and identify malware behaviors.
- Apply threat-hunting techniques in a simulated Security Operations Center (SOC).
- Handle digital evidence and maintain chain of custody.

Lab 6: Red Teaming and Advanced Exploitation

Objective: Simulate real-world cyber-attacks using red teaming methodologies.

Tasks:

- Implement privilege escalation and lateral movement techniques.
- Perform social engineering attacks such as phishing and physical security bypass.
- Deploy post-exploitation tactics for data exfiltration.
- Utilize Cobalt Strike and Bloodhound for attack simulations.

Savitribai Phule Pune University

S.Y.B.Sc. (Cyber Security) - Sem – IV

Course Type: Subject Code :CYS-281FP

Course Title : Mini Project based on CYS251MJ

Teaching Scheme 04 Hrs / week	No. of Credits: 2	Examination Scheme IE : 15 marks UE: 35 marks

Course Objectives:

- To provide hands-on experience in ethical hacking projects.
- To enhance problem-solving skills in identifying and mitigating cyber threats.
- To enable students to apply ethical hacking tools and techniques in real-world scenarios.
- To develop analytical skills in vulnerability assessment, penetration testing, and system security.
- To promote ethical considerations and responsible hacking practices.

Course Outcomes (COs):

Upon successful completion of the mini-projects, students will be able to:

CO1: Identify and define cyber security challenges and propose ethical hacking solutions.
CO2: Apply ethical hacking methodologies to conduct security assessments.
CO3: Demonstrate the ability to analyze vulnerabilities in networks, web applications, and systems.
CO4: Develop and document a structured approach to penetration testing and risk mitigation.
CO5: Implement security measures to counteract identified threats.
CO6: Present findings and recommendations in a professional security report format.

Project Guidelines:

- Projects should be performed in a controlled lab environment using ethical hacking tools.
- Each project should include **problem definition, objectives, methodology, tools used, results, and conclusions**.
- The final project report should include **screenshots, observations, and security recommendations**.
- Group size: **Maximum of 2 students per project**.

Suggested Mini Projects List:

- **Advanced Web Application Penetration Testing** – Conduct security assessments using automated and manual techniques on a dummy web application.
- **Cloud Security Audit** – Identify misconfigurations in AWS, Azure, or GCP and provide remediation strategies.
- **IoT Security Analysis** – Test and exploit vulnerabilities in smart home devices.
- **Red Teaming Simulation** – Execute a controlled red team engagement, including reconnaissance, exploitation, and privilege escalation.
- **Wireless Security Assessment** – Perform advanced attacks on WPA3-protected networks and analyze security flaws.

- **Malware Analysis and Reverse Engineering** – Analyze a sample malware to identify attack vectors and propose mitigation measures.

Submission Guidelines:

- Each lab should be documented with **objective, tools used, procedure, observations, and conclusion**.
- Screenshots must be included for each step of the practical.
- The completed lab book must be submitted before the deadline.

Savitribai Phule Pune University
S.Y.B.Sc. (Cyber Security) - Sem – IV
Subject Code : CYS291MN
Course Title : Modern Web Development

Teaching Scheme **02Hrs /Week**	**No. of Credits: 2**	**Examination Scheme** **IE : 15 marks** **UE: 35 marks**

Prerequisites : Fundamentals of HTML

- Basic knowledge of Java Script.
- Basics of web application development.
- Basic Knowledge of what is Client and Server side programming.

Course Objectives : To introduce students for modern web technologies.

- To learn and use server side programming using Node.js
- To introduce structure a Node application in modules
- To build a Web Server in Node and understand how it really works
- To learn how to a SQL or Mongo database in Node

Course Outcomes (COs):

Upon successful completion of this course :

CO1 : Define Node.js and its key features like event loop and non-blocking I/O.
CO2 : Explain how Node.js handles asynchronous operations and manages HTTP requests.
CO3 : Develop a basic server and implement RESTful APIs using Node.js and Express.
CO4 : Analyzing: Break down middleware, routing, and error handling to optimize server performance.
CO5 : Compare Node.js with other backend technologies to determine the best use cases.
CO6 : Build and deploy a secure, full-stack web application using Node.js and databases.

Course Contents

Chapter 1	**Introduction to Node**	**(4 Hours)**

- Introduction
- What is Node JS and its advantages
- Traditional Web Server Model
- Node JS Process model
- Installation of Node JS
- Node JS event loop

Chapter 2	**Node JS Modules**	**(4 Hours)**

- Functions
- Buffer
- Module
- Module Types
- Module. Exports

Chapter 3	Node Package Manager	(4 Hours)

- What is NPM?
- Installing package locally
- Adding dependencies in package. Son
- Installing packages globally
- Updating packages
- Managing Dependencies

Chapter 4	Web Server	(3 Hours)

- Creating web server
- Handling http requests
- Sending requests

Chapter 5	File System	(5 Hours)

- FS Model
- Files and Directories
- Streams
- Reading and Writing Files
- Reading and Writing Directories
- Other File Operations

Chapter 6	Working with Databases	(5 Hours)

- Working with Databases
- Connection String
- Configuring
- Working with Select command
- Various database operations

Chapter 7	Express JS	(5 Hours)

- Introduction to Express JS
- The MVC pattern
- Routing
- HTTP requests and responses
- Middleware
- Error handling

Reference Books:

- Node.js complete reference guid , velentin Bojinov, David Herron, Dioge Resende,
- packt Publishing Ltd
- Mastering Nod.js By Sandro Pasquali , packt Publishing
- Smashing Node.js, Java Script Everywhere , Guillermo Rauch, John wiley & Sons
- Web Development with Node and Express by Ethen brown
- Beginning Node.js, Express & MongoDB Development by Greg Lim

Savitribai Phule Pune University
S.Y.B.Sc. (Cyber Security) - Sem – IV
Subject Code : CYS292MNP
Course Title : Practical based on CYS291MN

Teaching Scheme 04Hrs /Week	No. of Credits: 2	Examination Scheme IE : 15 marks UE: 35 marks

Course Objectives :

- Set up Node.js, run scripts, and understand basic syntax.
- Use built-in and custom modules to structure code efficiently.
- Build an HTTP server to handle basic requests and responses.
- Connect Node.js with databases like MySQL/Mongo DB for data storage.
- Create a web server using express with routes and middleware.

Practical Assignments

1) Create a Node.js application that will convert the output "Hello World!" into upper-case letters.

2) Create a Node.js application that uses user defined Module to return the factorial of given number.

3) Create a Node.js application that uses user defined module circle.js which exports functions area () and circumference () and display the details on console.

4) Create Node.js application that uses user defined module Rectangle.js to find area of rectangle and display the details on console.

5) Create a Simple Web Server using node js.

6) Create a Simple Web Server using Node.js that shows the college information.

7) Create a Node.js application that demonstrate create database Student and student table (rno, name, percentage) in MySQL.

8) Create a Node.js file that Insert Multiple Records in "Student" table, and display the result object on console.

9) Create a Node.js file that Select all records from the "Student" table, and delete the specified record.

10) Create a Node.js Application that Update Marks of given student rno in "student" table and display the result.

11) Using Node.js create Application that contains Voters details and check proper validation for (name, age, and nationality), as Name should be in upper case letters only, Age should not be less than 18 yrs and Nationality should be Indian and store the data in database.

12) Using Node.js create a web page to read two file names from user and append contents of first file into second file

13) Using Node.js create a web page to read two file names from user and combine in third file with all content in Upper case.

14) Create a Node.js file that opens the requested file and returns the content to the client. If anything goes wrong, throw a 404 error

15) Create a Node.js Application to count number of lines in a file and display the count on console.

16) Create a Node.js Application to count occurrence of given word in a file and display the count on console.

17) Create a Node.js Application for validating student registration form.

18) Create an Node.js Application that contain the Student Registration details and validate Student first and last name should not contains any special symbols / digits and also age should be between 6 to 25.

19) Create a User Login System using Node.js.

20) Crate an Electricity bill calculation System using Node.js.

Savitribai Phule Pune University

(Formerly University of Pune)

Bachelors Degree in Cyber Security

(Faculty of Science and Technology)

Syllabi for
B.Sc. (Cyber Security)-Third Year
Sem-V and VI

(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 2026-27

Savitribai Phule Pune University

Syllabus Structure as per NEP Guidelines

B.Sc. (Cyber Security) from 2026-27

TY (Level 5.5) SEMESTER V

Course Type	Course code	Course Name	Credits		Teaching Scheme Hrs/Week		Examination Scheme and Marks		
			TH	PR	TH	PR	CE	EE	Total
Major Core	CYS-301-MJ-T	Web Application Security	2		2		15	35	50
	CYS-302-MJ-T	Vulnerability Assessment	2		2		15	35	50
	CYS-303-MJ-T	Basics of API security testing	2		2		15	35	50
	CYS-304-MJ-T	Automation in Python for Cyber Security	2		2		15	35	50
	CYS-305-MJ-P	Lab Course based on CYS-301-MJ-T & CYS-302-MJ-T		2		4	15	35	50
	CYS-306-MJ-P	Lab Course based on CYS-303-MJ-T & CYS-304-MJ-T		2		4	15	35	50
Major Elective	CYS-310-MJ-T	Basics of Digital Forensic	2				15	35	50
	CYS-311-MJ-P	Lab Course based on CYS-310-MJ-T		2		4	15	35	50
		OR							
	CYS-312-MJ-T	DevOps Fundamentals	2		2		15	35	50
	CYS-313-MJ-P	Lab Course based on CYS-312-MJ-T		2		4	15	35	50
VSC	CYS-321-VSC-T	Embedded Systems	2		2		15	35	50
FP/CEP	CYS-331-FP	Project on Cyber Security		2		4	15	35	50
Minor	CYS-341-MN-T	Internet of Things for Cyber Security	2		2		15	35	50
		Total	**14**	**8**	**14**	**16**			**550**

Savitribai Phule Pune University

Syllabus Structure as per NEP Guidelines

B.Sc. (Cyber Security) from 2026-27

TY (Level 5.5) SEMESTER VI

Course Type	Course code	Course Name	Credits		Teaching Scheme Hrs/Week		Examination Scheme and Marks		
			TH	PR	TH	PR	CE	EE	Total
Major Core	CYS-351-MJ-T	Windows Terminal for Cyber Security	2		2		15	35	50
	CYS-352-MJ-T	PowerShell basics	2		2		15	35	50
	CYS-353-MJ-T	Fundamentals of Active Directory	2		2		15	35	50
	CYS-354-MJ-T	Penetration Testing	2		2		15	35	50
	CYS-355-MJ-P	Lab Course based on CYS-351-MJ-T & CYS-352-MJ-T		2		4	15	35	50
	CYS-356-MJ-P	Lab Course based on CYS-353-MJ-T & CYS-354-MJ-T		2		4	15	35	50
Major Elective	CYS-360-MJ-T	Advanced Digital Forensic	2		2		15	35	50
	CYS-361-MJ-P	Lab Course based on CYS-360-MJ-T		2		4	15	35	50
		OR							
	CYS-362-MJ-T	DevSecOps Fundamentals	2		2		15	35	50
	CYS-363-MJ-P	Lab Course based on CYS-362-MJ-T		2		4	15	35	50
VSC	CYS-371-VSC	Embedded Systems Programming		2		4	15	35	50
OJT	CYS-381-OJT	On Job Training		4		8	30	70	100
		Total	**10**	**12**	**10**	**24**			**550**

Detail Syllabus
B.Sc. (Cyber Security)
Semester-V

Savitribai Phule Pune University
B.Sc. Cyber Security
Sem-V

CYS-301-MJ-T: Web Application security

No. of Credits:	Teaching Scheme	Examination Scheme
2	Theory: 2 Hrs/Week	Continuous Evaluation: 15 Marks End Semester : 35 Marks

Prerequisites

- Basic knowledge of networking
- Web technologies (HTML, HTTP)
- Cybersecurity fundamentals

Objectives

- To understand the architecture and working of web applications.
- To know common web vulnerabilities.
- To study secure coding principles to prevent attacks.
- To study web penetration testing using security tools.
- To apply modern practices for enhanced protection.

Course Outcomes

On Completion of this course, student will be able to –
CO1: Understand the architecture and working of web applications.
CO2: Identify and analyze common web vulnerabilities.
CO3: Apply secure coding principles to prevent attacks.
CO4: Perform web penetration testing using security tools.
CO5: Implement modern practices such as DevSecOps and WAF for enhanced protection.

Unit No.	Name of Unit	Teaching Hours	CO Targeted
1	**Introduction to Web Application Security**	**5**	**CO1**

- Understanding Web Application Architecture (Client, Server, Database)
- HTTP/HTTPS Basics and Communication Flow
- Common Attack Surface in Web Applications
- Importance of Secure Coding Practices
- OWASP and its Role in Web Security
- Overview of OWASP Top 10 Vulnerabilities (2021 edition)
- Web Application Security Testing Life Cycle (WSTLC)
- Learning Outcome: Students understand web app components, vulnerabilities, and security frameworks like OWASP.

2	**Authentication and Session Management**	**5**	**CO1**

- Authentication vs Authorization
- Secure Password Storage (Hashing, Salting, PBKDF2, bcrypt)

- Multi-Factor Authentication (MFA)
- Session Management: Cookies, Tokens, and JWT
- Common Attacks: Session Hijacking, Session Fixation, Cookie Poisoning
- Secure Implementation of Login/Logout Mechanisms
- Best Practices for Identity and Access Management (IAM)
- Learning Outcome: Students learn secure methods of managing users and protecting sessions.

3	**Web Application Vulnerabilities and Exploits**	6	CO2

- Cross-Site Scripting (XSS): Types and Prevention
- SQL Injection and Database Security
- Cross-Site Request Forgery (CSRF)
- Command Injection and Path Traversal
- Insecure Direct Object Reference (IDOR)
- XML External Entities (XXE)
- Case Studies: Famous Web Security Breaches
- Practical Component: Hands-on demonstration using DVWA / OWASP Juice Shop.
- Learning Outcome: Students identify, exploit (ethically), and patch vulnerabilities in web applications.

4	**Secure Coding and Defensive Mechanisms**	5	CO3

- Secure Development Life Cycle (SDLC)
- Input Validation and Output Encoding
- Error and Exception Handling
- Use of Security Libraries and Frameworks
- Content Security Policy (CSP)
- Secure File Upload and Data Storage
- Logging and Monitoring of Web Applications
- Learning Outcome: Students understand secure programming practices and how to integrate them in development.

5	**Web Application Penetration Testing**	5	CO4

- Penetration Testing Methodology (Information Gathering to Reporting)
- Reconnaissance and Vulnerability Scanning Tools
- Manual vs Automated Testing
- Tools: Burp Suite, OWASP ZAP, Nikto, Nmap
- Report Writing and Risk Assessment
- Ethical and Legal Aspects of Web Testing
- Learning Outcome: Students can perform and document a basic penetration test ethically and professionally.

6	**Modern Web Security Practices**	4	CO5

- Secure APIs and RESTful Security
- Web Application Firewalls (WAFs)

- Cloud-based Web Security Solutions
- HTTPS, TLS/SSL Certificates and HSTS
- Secure DevOps (DevSecOps) Concepts
- Zero Trust Architecture for Web Security
- Security in Single Page Applications (SPA) and Mobile Web
- Learning Outcome: Students explore advanced and modern techniques for securing web apps in cloud and DevOps environments

Reference Books

- Web Application Hacker's Handbook, by Dafydd Stuttard and Marcus Pinto, Released September 2011,
  Publisher(s): Wiley Publishing, ISBN: 9781118026472.
- OWASP Testing Guide, by OWASP, Released 2021,
  Publisher(s): OWASP Foundation.
- The Tangled Web: A Guide to Securing Modern Web Applications, by Michal Zalewski, Released November 2011,
  Publisher(s): No Starch Press, ISBN: 9781593273880
- Web Security for Developers, by Malcolm McDonald, Released June 2009,
  Publisher(s): O'Reilly Media, ISBN: 9780596802769.
- SQL Injection Attacks and Defense, by Justin Clarke, Released April 2012,
  Publisher(s): Syngress, ISBN: 9781597499637.

E-Books and Online Learning Material

- **https://owasp.org/www-project-top-ten/?utm_source=chatgpt.com**
- **https://owasp.org/www-project-top-ten/?utm_source=chatgpt.com**

Savitribai Phule Pune University

CYS-302-MJ-T : Vulnerability Assessment

No. of Credits: 2	Teaching Scheme Theory: 2 Hrs/Week	Examination Scheme Continuous Evaluation: 15 Marks End Semester : 35 Marks

Prerequisites: Basic knowledge of HTTP, REST architecture, and web security fundamentals.

Objectives

- To study VA methodology, tools, and legal/ethical constraints.
- To discover and enumerate assets using passive and active techniques.
- To study automated vulnerability scans for reducing false positives.
- To study critical vulnerabilities and impact safely.
- To create prioritized remediation plans and reports.
- To integrate VA practices into ongoing security workflows.

Course Outcomes

On Completion of this course, student will be able to –

CO1: Explain VA methodology, tools, and legal/ethical constraints.

CO2: Discover and enumerate assets using passive and active techniques.

CO3: Run and interpret automated vulnerability scans and reduce false positives.

CO4: Manually validate critical vulnerabilities and demonstrate impact safely.

CO5: Create prioritized remediation plans and professional VA reports.

CO6: Integrate VA practices into ongoing security/DevOps workflows.

Unit No.	Name of Unit	Teaching Hours	CO Targeted
1	**Fundamentals of Vulnerability Assessment**	4	CO1

- Definitions: vulnerability, threat, risk, exploit, exposure
- VA vs Penetration Testing vs Risk Assessment
- Vulnerability lifecycle and CVE/CVSS basics
- Types of assets and attack surfaces (network, host, application, cloud, IoT)
- Legal, ethical, and compliance considerations
- Outcome: Understand core concepts and scope of VA.

2	**Reconnaissance & Information Gathering**	5	CO2

- Passive vs active reconnaissance
- Open Source Intelligence (OSINT) techniques and tools
- Network discovery: host discovery, service enumeration
- Fingerprinting: OS, services, application versions
- Asset inventory and prioritization
- Practical component: Use Nmap, Netdiscover, and basic OSINT tools.
- Outcome: Collect and prioritize accurate information for assessment.

3	**Vulnerability Scanning**	6	CO3

- Types of scanners: network, host, web, database, cloud
- Scanning methodologies: authenticated vs unauthenticated scans
- Popular scanners and their architectures (Nessus, OpenVAS, Qualys, Nexpose)

- Scan tuning, false positives/negatives, credentialed scans
- Interpreting scanner output and vulnerability databases (NVD)
- Practical component: Configure and run scans with OpenVAS / Nessus; analyze results.
- Outcome: Run effective automated scans and interpret results.

4	**Manual Verification & Exploitation Basics**	6	CO4

- Why manual verification is needed; triaging scan results
- Exploitation vs proof-of-concept vs validation
- Safe exploit testing in lab environments (VMs, containers, CTF images)
- Tools: Metasploit for validation, Burp Suite for web verification, SQLmap basics
- Privilege escalation basics and impact analysis
- Practical component: Validate selected vulnerabilities using Metasploit and Burp.
- Outcome: Verify, validate and safely demonstrate real vulnerabilities.

5	**Vulnerability Management & Remediation**	5	CO5

- Risk rating using CVSS and business context
- Prioritization frameworks (likelihood × impact)
- Patch management basics and change control interactions
- Mitigation strategies (configuration, compensating controls, WAFs)
- Re-scan cycles and verifying remediation
- Outcome: Convert findings into prioritized, actionable remediation plans.

6	**Reporting, Metrics & Automation**	4	CO6

- Writing effective vulnerability assessment reports (executive summary, technical details, remediation steps)
- Remediation tracking and SLAs
- Key performance metrics (time-to-remediate, re-open rates, vulnerability backlog)
- Integrating VA into CI/CD & DevSecOps pipelines (automated scans, gating)
- Continuous monitoring and trending
- Outcome: Produce professional reports and integrate VA into organizational processes

Reference Books

1. OWASP Testing Guide (latest).
2. The Web Application Hacker’s Handbook — Dafydd Stuttard & Marcus Pinto.
3. Nmap Network Scanning — Gordon 'Fyodor' Lyon.
4. Vendor docs: Nessus/OpenVAS user guides.
5. NVD (National Vulnerability Database) and CVE resources.
6. Recent industry whitepapers and research on VA trends.
7. The Basics of Hacking and Penetration Testing, by Patrick Engebretson, Released 2013, Publisher(s): Elsevier, ISBN: 9780124116443.
8. Metasploit: The Penetration Tester’s Guide, by David Kennedy, Jim O’Gorman, Devon Kearns, Mati Aharoni, Released July 2011, Publisher(s): No Starch Press, ISBN: 9781593272883.

9. Web Application Hacker's Handbook, by Dafydd Stuttard and Marcus Pinto, Released September 2011,
Publisher(s): Wiley Publishing, ISBN: 9781118026472.
10. Nmap Network Scanning, by Gordon Fyodor Lyon, Released January 2009,
Publisher(s): Insecure.Com LLC, ISBN: 9780979958717.

E-Books and Online Learning Material

1. **https://www.nist.gov/cyberframework?utm_source=chatgpt.com**
2. **https://www.nist.gov/cyberframework?utm_source=chatgpt.com**
3. **https://greenbone.github.io/docs/latest/?utm_source=chatgpt.com**

Savitribai Phule Pune University
B.Sc. Cyber Security
Sem-V

CYS-303-MJ-T: Basics of API Security Testing

No. of Credits: 2	Teaching Scheme Theory: 2 Hrs/Week	Examination Scheme Continuous Evaluation: 15 Marks End Semester : 35 Marks

Prerequisites

- Basics of networking, operating systems, and cybersecurity fundamentals

Objectives

- To understand the fundamentals of APIs, API architectures, and communication methods.
- To introduce students to REST, SOAP, and GraphQL APIs and their security challenges.
- To study common API vulnerabilities based on OWASP API Security Top 10.
- To develop practical skills in API security testing using industry-standard tools.
- To learn authentication and authorization testing techniques for APIs.
- To understand methods for identifying input validation, injection, and data exposure vulnerabilities.
- To perform basic vulnerability assessment and penetration testing of APIs.

Course Outcomes

On Completion of this course, student will be able to –

CO1: Know the architecture and working principles of modern APIs.

CO2: Understand authentication and authorization mechanisms in APIs.

CO3: Identify common vulnerabilities and their security implications.

CO4: Apply testing methodologies to assess API security posture.

CO5: Utilize tools to detect and interpret API vulnerabilities.

CO6: Recommend mitigation strategies and follow best practices for secure API development.

Unit No.	Name of Unit	Teaching Hours	CO Targeted
1	**Introduction to API Security**	**5**	**CO1,CO2**

- Overview of API concepts: REST, SOAP, GraphQL
- API architecture: client, server, endpoints, methods, and payloads
- Role of APIs in modern web and mobile applications
- Differences between Web App Security and API Security
- Common API authentication mechanisms: API Keys, OAuth 2.0, JWT
- API vulnerabilities vs traditional web vulnerabilities
- OWASP API Security Top 10 overview

2	API Authentication and Authorization	5	CO2

- Authentication vs Authorization
- API Keys, Basic Auth, and Token-based Auth
- OAuth 2.0: Flow, Access Tokens, Refresh Tokens
- JSON Web Tokens (JWT): Structure, Signature, and Validation
- Common authentication flaws: Weak tokens, token reuse, session hijacking
- Broken Object Level Authorization (BOLA)
- Secure implementation of authorization at endpoint level

3	Common API Vulnerabilities	5	CO3

- Injection flaws: SQL, NoSQL, Command injection
- Broken Authentication and Session Management
- Excessive Data Exposure
- Lack of Rate Limiting
- Mass Assignment and Insecure Deserialization
- Improper Assets Management
- Misconfigured Security Headers (CORS, CSP, TLS)
- Real-world case studies of API breaches

4	API Security Testing Methodology	5	CO4

- API Testing Lifecycle: Discovery → Mapping → Testing → Reporting
- Reconnaissance: identifying endpoints and data flow
- Endpoint mapping and parameter analysis
- Testing inputs, headers, cookies, and authentication tokens
- Fuzzing and input validation testing concepts
- Handling responses and interpreting status codes
- Documentation analysis: Swagger/OpenAPI security checks
- Safe testing in non-production environments

5	API Security Tools and Techniques	5	CO5

- Manual testing tools: Postman, Insomnia
- Interception and proxy tools: Burp Suite, OWASP ZAP
- Automated testing tools: Nikto, Nmap, APIsec, RESTler
- Token analysis: jwt.io, JWT Tool
- Common payloads and fuzzing concepts
- Logging, monitoring, and security testing automation in pipelines
- Interpreting results and avoiding false positives

6	Reporting, Remediation, and Best Practices	5	CO6

- Structure of API Security Testing Report
- Risk rating using CVSS
- Writing vulnerability descriptions, impact analysis, and remediation guidance
- Secure coding guidelines for API developers
- Input validation and output encoding standards

- Importance of encryption (HTTPS, TLS, certificates)
- Secure DevOps (DevSecOps) integration for API lifecycle

Reference Books

1. OWASP API Security Top 10 – https://owasp.org/www-project-api-security/
2. API Security in Action – Neil Madden
3. The Web Application Hacker's Handbook – Dafydd Stuttard & Marcus Pinto
4. OWASP Testing Guide (latest edition)
5. NVD (National Vulnerability Database) – https://nvd.nist.gov/
6. RFC 6749: OAuth 2.0 Authorization Framework

E-Books and Online Learning Material

- **https://owasp.org/API-Security/?utm_source=chatgpt.com**

https://owasp.org/www-project-api-security/?utm_source=chatgpt.com

Savitribai Phule Pune University
B.Sc. Cyber Security
Sem-V

CYS-304-MJ-T：Automation in Python for Cyber Security

No. of Credits:	Teaching Scheme	Examination Scheme
2	Theory: 2 Hrs/Week	Continuous Evaluation: 15 Marks End Semester : 35 Marks

Prerequisites

- Basic knowledge of Python programming and computer networks

Objectives

- To understand the basics of Python programming for cybersecurity applications.
- To learn Python scripting for automating security and administrative tasks.
- To develop skills in file handling, log analysis, and network programming using Python.

Course Outcomes

CO1: Explain automation's role in cybersecurity operations.
CO2: Develop Python scripts for automating network and log analysis.
CO3: Perform automated web and API security testing using Python.
CO4: Use Python for malware detection and forensic analysis.
CO5: Create automated reports and alerts for cybersecurity workflows.

Unit No.	Name of Unit	Teaching Hours	CO Targeted
1	**Introduction to Automation and Python Basics**	5	CO1

- Need for automation in Cyber Security
- Overview of scripting vs manual processes
- Introduction to Python environment setup
- Python modules and libraries for security
- File handling and OS operations
- Exception handling and logging
- Understanding APIs and command-line automation

2	**Networking and Packet Analysis with Python**	5	CO2

- Networking modules: socket, ipaddress
- Creating simple port scanners using Python
- Packet capture and analysis using scapy
- Packet structure and headers
- Detecting suspicious traffic patterns
- Parsing pcap files for security events
- Simulating network testing (safe lab environment)

3	**Log Analysis and File Monitoring Automation**	6	CO3

- Role of logs in cyber security
- Automating system log collection and parsing
- Using Regular Expressions for pattern matching

- Detecting anomalies and failed login attempts
- Monitoring changes in system files and directories
- Log correlation using Python
- Integration with SIEM tools

4	**Web and API Automation for Security Testing**	**5**	**CO3**

- Automating web requests using requests and urllib
- HTTP methods and response handling
- Extracting data using BeautifulSoup
- Automating login testing and brute-force detection
- API testing using Python scripts
- Validating input/output for vulnerabilities
- Basic integration with Burp Suite or OWASP ZAP APIs

5	**Malware, Forensics, and Threat Automation**	**5**	**CO4**

- Basics of malware analysis and sandboxing
- Automating hash generation (MD5, SHA1, SHA256)
- File integrity monitoring scripts
- Threat intelligence feeds automation (VirusTotal, AbuseIPDB APIs)
- Parsing JSON threat data
- Detecting suspicious processes and registry keys
- Automated forensic reporting concepts

6	**Reporting, Scheduling, and Best Practices**	**5**	**CO5**

- Automating report generation (CSV, Excel, PDF formats)
- • Email and alert automation
- • Task scheduling using schedule and cron
- • Logging and error handling in automated scripts
- • Security and ethical scripting practices
- • Version control and script maintenance
- • Secure coding and deployment considerations

Reference Books

1. Violent Python – TJ O'Connor
2. Black Hat Python – Justin Seitz
3. Python for Cybersecurity – Packt Publishing
4. Automate the Boring Stuff with Python – Al Sweigart
5. Python for Offensive PenTest – Hussam Khrais
6. OWASP and MITRE ATT&CK documentation

E-Books and Online Learning Material

- **https://docs.python.org/3/?utm_source=chatgpt.com**
- https://www.w3schools.com/python/?utm_source=chatgpt.com

Savitribai Phule Pune University
B.Sc. Cyber Security
Sem-V

CYS-305-MJ-P: Lab Course based on CYS-301-MJ-T & CYS-302-MJ-T

No. of Credits: 2	**Teaching Scheme** Practical: 4 Hrs/Week	**Examination Scheme** Continuous Evaluation: 15 Marks End Semester : 35 Marks

Prerequisites

- Basic knowledge of Python programming and computer networks

Objectives

- To implement secure coding and defensive techniques.

Course Outcomes

CO1: To provide hands-on experience in web application security testing.
CO2: To understand common web vulnerabilities through practical demonstrations.
CO3: To implement secure coding and defensive techniques.
CO4: To develop professional web security testing and reporting skills.

Practical No.	Title of Experiment	Teaching Hours	
1	**Installation and Setup of Web Security Lab Environment**	5	
2	**HTTP/HTTPS Traffic Analysis using Browser Developer Tools and Wireshark**	10	
3	**Web Application Mapping using Burp Suite**	10	
4	**Cross-Site Scripting (XSS) Attack and Prevention & SQL Injection Testing using SQLmap and Manual Techniques**	15	
5	**Web Vulnerability Scanning using Nikto and OWASP ZAP**	10	
6	**Vulnerability Scanning using OpenVAS & Exploitation Basics using Metasploit Framework**	10	

Savitribai Phule Pune University
B.Sc. Cyber Security
Sem-V
CYS-306-MJ-P : Lab Course based on CYS-303-MJ-T & CYS-304-MJ-T

No. of Credits: 2	**Teaching Scheme** Practical: 4 Hrs/Week	**Examination Scheme** Continuous Evaluation: 15 Marks End Semester : 35 Marks

Prerequisites

- Basic knowledge of computer networks and web technologies.
- Understanding of HTTP/HTTPS protocols and client-server architecture.

Objective:

- To understand API testing methods and vulnerabilities.
- To implement secure API handling and testing practices.
- To use Python for automation in cybersecurity tasks.
- To analyze, report, and mitigate API security issues using scripts and tools.

Course Outcomes

CO1: Test REST and SOAP APIs for security vulnerabilities.
CO2: Automate cybersecurity tasks using Python scripting.
CO3: Analyze and interpret API responses and vulnerabilities.
CO4: Write Python scripts for scanning, data collection, and automation.
CO5: Generate and document testing reports effectively.

Practical No.	Name of Unit	Teaching Hours	CO Targeted
1	**API Security Testing**	**6**	**CO1**
Objective: Set up a testing environment for RESTful APIs and explore tools like Postman and Burp Suite. **Tools:** Postman, Burp Suite, OWASP Juice Shop API			
2	**Practical 2: Authentication and Authorization Testing in APIs**	**6**	**CO1**
Objective: Test API endpoints using Basic Auth, Token-based Auth, and OAuth. **Tools:** Postman, OWASP ZAP Learning Outcome: Students learn secure methods of managing users and protecting sessions.			
3	**Input Validation and Injection Testing**	**6**	**CO2**
• **Objective:** Identify input-based vulnerabilities such as SQL Injection and Command Injection in API endpoints. **Tools:** Burp Suite, SQLMap XML External Entities (XXE) • Case Studies: Famous Web Security Breaches • Practical Component: Hands-on demonstration using DVWA / OWASP Juice Shop.			
4	**API Rate Limiting, Error Handling, and Information Disclosure Testing**	**6**	**CO3**

- **Objective:** Test for improper rate limiting, verbose error messages, and sensitive data leaks.
  Tools: Postman, Burp Suite

5	**Secure API Development and Reporting**	6	CO3, CO4

- **Objective:** Develop a simple Flask API with secure coding and generate a test report.
  Tools: Python (Flask), Postman

B	**Section B — Automation in Python for Cyber Security**	30	CO4, CO5

Practical 6:
Title: Python Basics for Cyber Security
Objective: Write Python scripts for basic operations (file handling, data parsing, OS commands).
Tools: Python, Jupyter Notebook / VS Code

Practical 7:
Title: Network Scanning Automation using Python
Objective: Automate network scanning using Python scripts.
Tools: Python, socket, scapy libraries

Practical 8:
Title: Log Analysis and Threat Detection
Objective: Write Python scripts to read and analyze log files for suspicious activities.
Tools: Python, Regex

Practical 9:
Title: Web Scraping and Data Extraction for Threat Intelligence
Objective: Use Python to extract information from web sources for cybersecurity analysis.
Tools: Python, requests, BeautifulSoup

Practical 10:
Title: Vulnerability Scanner Automation (Mini Project)
Objective: Develop a simple Python-based vulnerability scanning script and generate a report.
Tools: Python, requests, nmap module

Reference Books and Tools

- Postman / Burp Suite Community Edition
- OWASP ZAP
- OWASP Juice Shop (for API testing)
- Python 3.x
- Libraries: requests, os, socket, nmap, scapy, BeautifulSoup, json
- Flask / FastAPI (for secure API design)
- OWASP API Security Top 10 Guidelines
- PTES and NIST SP 800-115 (for structured testing approach)
- **https://owasp.org/www-project-top-ten/?utm_source=chatgpt.com**

Savitribai Phule Pune University
B.Sc. Cyber Security
Sem-V

CYS-310-MJ-T: Basics of Digital Forensic

No. of Credits: 2	Teaching Scheme Theory: 2 Hrs/Week	Examination Scheme Continuous Evaluation: 15 Marks End Semester : 35 Marks

Prerequisites

- Basic knowledge of computer networks and web technologies.
- Understanding of HTTP/HTTPS protocols and client-server architecture.

Objective:

- To introduce the fundamentals of digital forensics and investigation processes.
- To identify and preserve digital evidence for legal proceedings.
- To understand forensic tools, techniques, and ethical considerations.
- To perform basic forensic analysis on systems, networks, and mobile devices.

Course Outcomes

CO1: Explain digital forensic principles, tools, and investigation processes.

CO2: Identify and preserve digital evidence from different sources.

CO3: Use forensic tools to analyze computer and mobile data.

CO4: Prepare forensic reports and maintain evidence integrity.

CO5: Apply forensic techniques to solve cybercrime case studies.

Unit No.	Name of Unit	Teaching Hours	CO Targeted
1	**Introduction to Digital Forensics**	**6**	**CO1**

- Definition, Need, and Importance of Digital Forensics
- History and Evolution of Digital Forensics
- Categories: Computer, Network, Mobile, Cloud, and Database Forensics
- Role of Forensic Experts and Investigators
- Legal and Ethical Issues

2	**Digital Evidence and Data Acquisition**	**6**	**CO2**

- Types of Digital Evidence
- Chain of Custody and Documentation
- Evidence Collection Procedures
- Bit Stream Imaging and Verification
- Preservation of Volatile and Non-Volatile Data

3	**File Systems and Data Recovery**	**6**	**CO3, CO4**

- Understanding FAT, NTFS, EXT, and HFS+ File Systems
- Deleted File Recovery and Unallocated Space Analysis
- Metadata and Timestamps
- File Carving Techniques

- Use of Tools like Autopsy and FTK Imager

4	**System and Network Forensics**	6	CO3, CO4

- Windows and Linux Forensics Basics
- Event Log and Registry Analysis
- Browser History and Cache Analysis
- Network Traffic Capturing and Analysis (Wireshark, TCPDump)
- Email Forensics

5	**Mobile and Cloud Forensics**	6	CO3, CO4, CO5

- Mobile Device Structure and Data Extraction Techniques
- SIM, SD Card, and Application Data Analysis
- Cloud Storage Investigation
- Forensic Challenges in Virtualization and Cloud Environments
- Reporting and Case Documentation

Reference Books

- Digital Forensics and Incident Response, by Gerard Johansen, Released June 2017, Publisher(s): Packt Publishing, ISBN: 9781783987467.
- Guide to Computer Forensics and Investigations, by Bill Nelson, Amelia Phillips, Christopher Steuart, Released January 2018, Publisher(s): Cengage Learning, ISBN: 9781337568944.
- Computer Forensics: Investigating Network Intrusions and Cyber Crime, by EC-Council, Released 2010, Publisher(s): Cengage Learning, ISBN: 9781435483521.
- File System Forensic Analysis, by Brian Carrier, Released March 2005, Publisher(s): Addison-Wesley Professional, ISBN: 9780321268174.
- Practical Mobile Forensics, by Satish Bommisetty, Heather Mahalik, and Rohit Tamma, Released December 2014, Publisher(s): Packt Publishing, ISBN: 9781783285198

Savitribai Phule Pune University
B.Sc. Cyber Security
Sem-V

CYS-311-MJ-P: Lab Course based on CYS-310-MJ-T

No. of Credits: 2	Teaching Scheme Practical: 4 Hrs/Week	Examination Scheme Continuous Evaluation: 15 Marks End Semester : 35 Marks

Prerequisites

- Basic knowledge of computer networks and web technologies.
- Understanding of HTTP/HTTPS protocols and client-server architecture.

Objective:

- To introduce the fundamentals of digital forensics and investigation processes.
- To identify and preserve digital evidence for legal proceedings.
- To understand forensic tools, techniques, and ethical considerations.
- To perform basic forensic analysis on systems, networks, and mobile devices.

Course Outcomes

1. CO1: Explain digital forensic principles, tools, and investigation processes.
2. CO2: Identify and preserve digital evidence from different sources.
3. CO3: Use forensic tools to analyze computer and mobile data.
4. CO4: Prepare forensic reports and maintain evidence integrity.
5. CO5: Apply forensic techniques to solve cybercrime case studies.

Practical No.	Name of Practicals	Teaching Hours	CO Targeted
1	**Introduction to Digital Forensic Tools**	**12**	**CO1**
• Explore and install basic forensic tools (Autopsy, FTK Imager, Wireshark).			
2	**Disk Imaging and Verification & Network Traffic Capture and Analysis**	**12**	**CO2, CO3**
• Create a forensic image of storage media using FTK Imager and verify integrity using hash functions. • Capture live network traffic using Wireshark and identify possible intrusions.			
3	**File Recovery and Deleted Data Analysis & Mobile Forensics Using Open-Source Tools**	**12**	**CO2, CO3**
• Recover deleted files and analyze recovered metadata.			
4	**Windows Log and Registry Analysis & Reporting and Documentation**	**12**	**CO4**
• Analyze event logs and registry entries for suspicious activities. • Investigate artifacts from cloud services (Google Drive, Dropbox).			

5	**Browser and Email Forensics & Mini Project on Digital Investigation**	12	CO5

- Extract and interpret browsing history and email artifacts.
- Conduct an end-to-end forensic analysis (case simulation).

Reference Books

- Digital Forensics and Incident Response, by Gerard Johansen, Released June 2017, Publisher(s): Packt Publishing, ISBN: 9781783987467.
- Guide to Computer Forensics and Investigations, by Bill Nelson, Amelia Phillips, Christopher Steuart, Released January 2018, Publisher(s): Cengage Learning, ISBN: 9781337568944.
- Computer Forensics: Investigating Network Intrusions and Cyber Crime, by EC-Council, Released 2010, Publisher(s): Cengage Learning, ISBN: 9781435483521.
- File System Forensic Analysis, by Brian Carrier, Released March 2005, Publisher(s): Addison-Wesley Professional, ISBN: 9780321268174.
- Practical Mobile Forensics, by Satish Bommisetty, Heather Mahalik, and Rohit Tamma, Released December 2014, Publisher(s): Packt Publishing, ISBN: 9781783285198

Savitribai Phule Pune University
B.Sc. Cyber Security
Sem-V

CYS-312-MJ-T: DevOps Fundamentals

No. of Credits:	Teaching Scheme	Examination Scheme
2	Theory: 2 Hrs/Week	Continuous Evaluation: 15 Marks End Semester : 35 Marks

Prerequisites

- To understand DevOps concepts, tools, and lifecycle for continuous development and deployment.
- To integrate DevOps principles into secure software development environments.
- To automate deployment, configuration, and monitoring using modern tools.
- To implement CI/CD pipelines and Infrastructure as Code (IaC).

Objective:

- To introduce the fundamentals of digital forensics and investigation processes.
- To identify and preserve digital evidence for legal proceedings.
- To understand forensic tools, techniques, and ethical considerations.
- To perform basic forensic analysis on systems, networks, and mobile devices.

Course Outcomes

CO1: Explain DevOps concepts, benefits, and lifecycle.

CO2: Use Git and GitHub for version control and collaboration.

CO3: Implement automation using Jenkins, Docker, and Ansible.

CO4: Deploy applications using containerization and orchestration tools.

CO5: Integrate security practices into the DevOps pipeline (DevSecOps).

Unit No.	Name of Unit	Teaching Hours	CO Targeted
1	**Introduction to DevOps**	**6**	**CO1**

- Evolution of Software Development and Operations
- What is DevOps?
- Key Concepts and Principles of DevOps
- DevOps Lifecycle: Continuous Integration, Continuous Deployment, Continuous Monitoring
- Benefits and Challenges of DevOps
- DevSecOps Overview

2	**Version Control Systems**	**6**	**CO2**

- Introduction to Git and GitHub
- Repository, Branching, Merging, and Forking
- Git Commands and Workflow
- Managing Source Code and Collaboration

- CI Integration with GitHub

3	**Continuous Integration and Continuous Deployment**	6	CO3

- Concept of CI/CD
- Jenkins Setup and Pipeline Configuration
- Automated Build, Test, and Deployment
- Integration with GitHub and Docker
- Role of CI/CD in Secure Development

4	**Containerization and Orchestration**	6	CO4

- Introduction to Virtualization and Containers
- Docker Installation, Images, Containers, and Dockerfile
- Docker Compose and Networking
- Kubernetes Basics – Pods, Services, Deployments
- Container Security Concepts

5	**Configuration Management and Monitoring**	6	CO5

- Infrastructure as Code (IaC)
- Ansible Basics – Playbooks, Inventory, Modules
- Monitoring Tools: Prometheus, Grafana
- Log Management and Alerts
- DevOps Security Best Practices

Reference Books

- Len Bass, Ingo Weber, Liming Zhu — *DevOps: A Software Architect's Perspective*
- Gene Kim — *The Phoenix Project*
- Kief Morris — *Infrastructure as Code*
- Docker & Kubernetes Documentation
- Jenkins and Ansible Official Guides

Savitribai Phule Pune University
B.Sc. Cyber Security
Sem-V

CYS-313-MJ-P: Lab Course based on CYS-312-MJ-T

No. of Credits: 2	Teaching Scheme Practical: 4 Hrs/Week	Examination Scheme Continuous Evaluation: 15 Marks End Semester : 35 Marks

Prerequisites

- Basic knowledge of computer networks and web technologies.
- Understanding of HTTP/HTTPS protocols and client-server architecture.

Objective:

- To introduce the fundamentals of digital forensics and investigation processes.
- To identify and preserve digital evidence for legal proceedings.
- To understand forensic tools, techniques, and ethical considerations.
- To perform basic forensic analysis on systems, networks, and mobile devices.

Course Outcomes

CO1: Explain digital forensic principles, tools, and investigation processes.

CO2: Identify and preserve digital evidence from different sources.

CO3: Use forensic tools to analyze computer and mobile data.

CO4: Prepare forensic reports and maintain evidence integrity.

CO5: Apply forensic techniques to solve cybercrime case studies.

Practical No.	Name of Practicals	Teaching Hours	CO Targeted
1	**Introduction to DevOps Tools and Setup & Version Control using Git and GitHub**	**12**	**CO1**
• Install and configure Git, Jenkins, Docker, and Ansible in a lab environment. • Create repositories, manage branches, and perform merge operations.			
2	**Automating Build Process using Jenkins & Kubernetes Basics – Deployment and Scaling**	**12**	**CO2**
• Configure Jenkins and create a simple CI job linked with GitHub. • Kubernetes Basics – Deployment and Scaling			
3	**Docker Basics – Containers and Images & Creating Dockerfiles and Using Docker Compose**	**12**	**CO3**
• Create, run, and manage Docker containers for sample applications. • Build custom Docker images and deploy multi-container applications.			

4	**Continuous Deployment using Jenkins and Docker & Configuration Management with Ansible**	**12**	**CO4**
• Write Ansible playbooks to automate system configuration. • Automate application deployment pipeline with Jenkins and Docker.			
5	**Monitoring and Logging in DevOps & Mini Project – End-to-End DevOps Pipeline**	**12**	**CO5**
• Build a secure CI/CD pipeline integrating Git, Jenkins, Docker, and Ansible. • Use Prometheus or Grafana for real-time application monitoring.			

Reference Books

- Len Bass, Ingo Weber, Liming Zhu — *DevOps: A Software Architect's Perspective*
- Gene Kim — *The Phoenix Project*
- Kief Morris — *Infrastructure as Code*
- Docker & Kubernetes Documentation
- Jenkins and Ansible Official Guides

Savitribai Phule Pune University
B.Sc. Cyber Security
Sem-V

CYS-321-VSC: Embedded Systems

No. of Credits: 2	Teaching Scheme Theory: 2 Hrs/Week	Examination Scheme Continuous Evaluation: 15 Marks End Semester : 35 Marks

Prerequisites

- Basic knowledge of computer organization and digital electronics.
- Understanding of programming concepts using C/C++ language.

Objective:

- To understand the fundamentals and architecture of embedded systems.
- To learn microcontroller design and functioning.
- To explore communication protocols and interfacing techniques.
- To understand applications of embedded systems in cybersecurity and IoT.

Course Outcomes

CO1: Explain the architecture and working of embedded systems.

CO2: Describe microcontrollers, sensors, and communication interfaces.

CO3: Analyze embedded applications used in IoT and cybersecurity.

CO4: Understand real-time operating systems and firmware basics.

CO5: Evaluate security aspects of embedded devices.

Unit No.	Name of Unit	Teaching Hours	CO Targeted
1	**Introduction to Embedded Systems**	**6**	**CO1**

- Definition and Characteristics of Embedded Systems
- Embedded vs General Purpose Systems
- Design Challenges and Real-Time Constraints
- Embedded System Lifecycle
- Applications in Cybersecurity, IoT, and Industrial Automation

2	**Architecture of Embedded Systems**	**6**	**CO2**

- Basic Components: Processor, Memory, Input/Output Devices
- Types of Processors: Microcontroller, Microprocessor, DSP
- Harvard vs Von Neumann Architectures
- Memory Organization and Buses
- Embedded System Hardware Blocks

3	**Microcontrollers and Programming Concepts**	**6**	**CO3**

- Overview of 8051, ARM, Arduino, and Raspberry Pi
- GPIO, Timers, Interrupts, and Peripheral Devices
- Embedded C and MicroPython Overview

- Compilation, Uploading, and Debugging Process
- Firmware Design and Real-Time Execution

4	**Interfacing and Communication Protocols**	6	CO4

- Sensor and Actuator Basics
- Data Conversion: ADC and DAC
- Communication Interfaces: UART, SPI, I2C
- Display Devices (LCD, LED, OLED)
- Wireless Modules: Wi-Fi, Bluetooth, ZigBee

5	**Embedded Systems in Cyber Security and IoT**	6	CO5

- Role of Embedded Systems in IoT
- Common Security Threats and Vulnerabilities in Embedded Devices
- Secure Boot, Encryption, and Firmware Protection
- Case Study: IoT-Based Smart Security System
- Future Directions in Embedded and Secure System Design

Reference Books

- Raj Kamal — *Embedded Systems: Architecture, Programming, and Design*
- Frank Vahid & Tony Givargis — *Embedded System Design: A Unified Hardware/Software Introduction*
- Mazidi — *The 8051 Microcontroller and Embedded Systems*
- Elecia White — *Making Embedded Systems*
- Arduino & Raspberry Pi Official Documentation

Savitribai Phule Pune University
B.Sc. Cyber Security
Sem-V

CYS-331-FP: Project on Cyber Security

No. of Credits:	Teaching Scheme	Examination Scheme
2	Practical: 4 Hrs/Week	Continuous Evaluation: 15 Marks End Semester : 35 Marks

Prerequisites

- Basic knowledge of computer organization and digital electronics.
- Understanding of programming concepts using C/C++ language.

Objective:

- To enable students to practically apply cybersecurity concepts and tools.
- To develop problem-solving and research-based project skills.
- To strengthen project documentation, teamwork, and presentation abilities.
- To create awareness about professional ethics and innovation in cybersecurity.

Course Outcomes

CO1: Identify a practical or research-oriented cybersecurity problem.

CO2: Design and implement a small-scale project or prototype.

CO3: Apply cybersecurity tools, languages, or frameworks for real-world solutions.

CO4: Prepare project documentation and present findings effectively.

1. **Type of Project:**
    - Mini or applied project related to cybersecurity, networking, IoT, or automation.
    - Can be **individual** or **group-based** (maximum 2–3 students).
2. **Duration:**
    - Total workload equivalent to **30 hours** per semester.
3. **Supervision:**
    - Each project should be guided by a faculty member.
4. **Project Stages:**
    - **Phase I:** Problem Identification & Synopsis Submission
    - **Phase II:** System Design & Implementation
    - **Phase III:** Final Presentation & Viva

Suggested Project Areas:

- Web or API Security Testing
- Network Scanning Automation
- IoT Device Security
- Log Analysis for Threat Detection
- Malware Simulation and Defense
- Cloud Security Implementation
- Python Automation for Cyber Tasks
- Vulnerability Assessment Tools
- Digital Forensics Evidence Analyzer
- Secure Communication Application

Project Synopsis / Proposal	10
Project Report & Documentation	15
Working Model / Implementation	15
Presentation & Viva	10
Total	**50 Marks**

Suggested Tools and Platforms:

- Programming Languages: Python, C/C++, Java
- Cyber Tools: Kali Linux, Burp Suite, OWASP ZAP, Wireshark
- IoT Tools: Arduino, Raspberry Pi
- Cloud Platforms: AWS / Azure / Google Cloud
- Report Tools: MS Word, LaTeX, Google Docs

Savitribai Phule Pune University
B.Sc. Cyber Security
Sem-V

CYS-341-MN-T: Internet of Things for Cyber Security

No. of Credits:	Teaching Scheme	Examination Scheme
2	Theory: 2 Hrs/Week	Continuous Evaluation: 15 Marks End Semester : 35 Marks

Prerequisites

- Basic knowledge of computer networks and web technologies.
- Understanding of HTTP/HTTPS protocols and client-server architecture.

Objective:

- To introduce the fundamentals of digital forensics and investigation processes.
- To identify and preserve digital evidence for legal proceedings.
- To understand forensic tools, techniques, and ethical considerations.
- To perform basic forensic analysis on systems, networks, and mobile devices.

Course Outcomes

CO1: Explain IoT architecture and its core building blocks.

CO2: Identify and analyze IoT communication protocols.

CO3: Understand and mitigate IoT-related cybersecurity threats.

CO4: Evaluate and apply IoT security frameworks and standards.

Unit No.	Name of Unit	Teaching Hours	CO Targeted
1	**Introduction to IoT**	6	CO1

- Definition and Characteristics of IoT
- IoT Components: Devices, Gateways, Cloud, and Applications
- Evolution and Importance of IoT in Modern Systems
- IoT Applications in Smart Homes, Healthcare, and Industry
- Role of IoT in Cyber Security

2	**IoT Architecture and Communication Models**	6	CO2

- 3-Layer and 5-Layer IoT Architectures
- IoT Functional Blocks and Sensors
- IoT Communication Models: Device-to-Device, Device-to-Cloud, Gateway-Based
- IoT Networking Technologies: RFID, NFC, Bluetooth, ZigBee, Wi-Fi, LoRaWAN
- Cloud and Edge Computing in IoT

3	**IoT Communication Protocols**	6	CO3

- Overview of IoT Protocol Stack
- Application Layer Protocols: MQTT, CoAP, HTTP, AMQP
- Transport and Network Layer: TCP, UDP, IPv6, 6LoWPAN

- Security Features of Common IoT Protocols
- Case Study: MQTT Security Implementation

4	**IoT Security Challenges and Threats**	6	CO4

- Vulnerabilities in IoT Devices and Networks
- Common IoT Attacks: DDoS, Botnets, Firmware Exploits, Side-Channel Attacks
- Authentication and Access Control in IoT
- Data Privacy, Integrity, and Encryption Techniques
- Risk Assessment and Mitigation Strategies

5	**Secure IoT Design and Future Trends**	6	CO3, CO4

- Secure IoT Development Life Cycle
- Security Standards: OWASP IoT Top 10, ISO/IEC 27030
- Secure Boot and Firmware Update Mechanisms
- Blockchain and AI Integration in IoT Security
- Future Trends: Smart Cities, Industrial IoT, and Edge AI

Reference Books

- Arshdeep Bahga & Vijay Madisetti — *Internet of Things: A Hands-On Approach*
- Raj Kamal — *Internet of Things: Architecture and Design Principles*
- Alan Bensky — *Short-Range Wireless Communication*
- Qusay F. Hassan — *Internet of Things: Challenges, Advances, and Applications*
- OWASP IoT Project Documentation

Detail Syllabus
B.Sc. (Cyber Security)
Semester-VI

Savitribai Phule Pune University
B.Sc. Cyber Security
Sem-VI

CYS-351-MJ-T: Windows Terminal for Cyber Security

No. of Credits: 2	Teaching Scheme Theory: 2 Hrs/Week	Examination Scheme Continuous Evaluation: 15 Marks End Semester : 35 Marks

Prerequisites

- Basic knowledge of Windows OS, command-line operations, and cybersecurity concepts.

Objective:

- To introduce the fundamentals of digital forensics and investigation processes.
- To identify and preserve digital evidence for legal proceedings.
- To understand forensic tools, techniques, and ethical considerations.
- To perform basic forensic analysis on systems, networks, and mobile devices.

Course Outcomes

CO1: Configure and securely use Windows Terminal with PowerShell and WSL for cybersecurity tasks.
CO2: Use PowerShell and CLI tools to inspect system, network, and process states.
CO3: Extract and analyze logs to build basic forensic timelines using terminal tools.
CO4: Write scripts to automate data collection, triage, and remediation tasks.
CO5: Harden terminal/shell configurations and detect malicious script activity.
CO6: Apply ethical and secure practices when using terminal tools for investigations

Unit No.	Name of Unit	Teaching Hours	CO Targeted
1	**Introduction to Windows Terminal and Shells**	5	CO1, CO2

- Overview of Windows Terminal: features, UI (tabs, panes, profiles, settings)
- Differences between Command Prompt, PowerShell, and WSL (bash)
- Installing and configuring Windows Terminal (profiles, keybindings, themes)
- Terminal security basics (secure profiles, execution policies)
- Common terminal workflows in security operations

2	**PowerShell Essentials for Security**	5	CO2

- PowerShell fundamentals: cmdlets, objects, and pipelines
- Execution policy, modules, and profiles
- Working with files, registry, processes, and services
- PowerShell remoting and WinRM basics (security considerations)
- Security features: Constrained Language Mode, AMSI, script signing

3	**CLI Tools & Windows Sysinternals**	5	CO2

- Using built-in CLI tools: netstat, tasklist, ipconfig, route, sc, wevtutil, wmic
- Introduction to Sysinternals Suite (Process Explorer, Autoruns, Procmon, PsExec, TCPView)
- Integrating Sysinternals tools via PowerShell/Terminal
- Reading and filtering Windows Event Logs (wevtutil & Get-WinEvent)
- Network and process forensics using CLI tools

4	**Log Analysis, Parsing & Forensics in Terminal**	**5**	**CO3, CO4**

- Understanding Windows Event Logs: authentication, application, system logs
- Querying and filtering logs using PowerShell (Get-WinEvent, Select-String)
- Parsing logs using regex and PowerShell pipelines
- Analyzing IIS and application logs in terminal
- Timeline building and forensic triage using terminal workflows

5	**Automation, Scripting & Incident Response Workflows**	**5**	**CO4, CO5**

- Writing PowerShell scripts for security automation
- Automating scans, alerts, and data collection (Task Scheduler)
- Using Terminal for IR workflows (collect, analyze, remediate)
- Safe remote collection with PSRemoting, SMB, WinRM, and SFTP
- Integrating with SIEM/APIs using PowerShell
- Hardening Terminal and shells: secure settings, profile separation
- Detecting malicious PowerShell activity (logging, AMSI, transcription)

6	**Advanced Topics, Hardening & Best Practices**	**5**	**CO5, CO6**

- Hardening Terminal and shells: secure settings, profile separation
- Detecting malicious PowerShell activity (logging, AMSI, transcription)
- WSL security considerations and Linux tooling on Windows
- Red-team vs blue-team terminal use (ethical aspects)
- Credential handling, secret management, and secure logging

Reference Books

- Microsoft Docs: PowerShell, Windows Terminal, Event Logs, and WinRM.
- Sysinternals Suite – Mark Russinovich (Microsoft).
- PowerShell for Sysadmins – Adam Bertram.
- Windows Forensics and Incident Recovery – select chapters on CLI workflows.
- OWASP and SANS whitepapers on PowerShell abuse and defenses.
- Microsoft Security Blog – Defender and AMSI integration updates.

Savitribai Phule Pune University
B.Sc. Cyber Security
Sem-VI

CYS-352-MJ-T: PowerShell basics

No. of Credits: 2	Teaching Scheme Theory: 2 Hrs/Week	Examination Scheme Continuous Evaluation: 15 Marks End Semester : 35 Marks

Prerequisites

- Basic knowledge of Windows Operating System and Command Line Interface.

Objective:

- To introduce the fundamentals of digital forensics and investigation processes.
- To identify and preserve digital evidence for legal proceedings.
- To understand forensic tools, techniques, and ethical considerations.
- To perform basic forensic analysis on systems, networks, and mobile devices.

Course Outcomes

CO1: Understand PowerShell architecture and command structure.
CO2: Execute and automate administrative tasks using cmdlets and scripts.
CO3: Write structured PowerShell scripts for automation.
CO4: Manage system configurations, network settings, and user accounts.
CO5: Use PowerShell in security monitoring and forensic analysis.
CO6: Apply PowerShell as a cyber defense tool to identify and respond to threats.

Unit No.	Name of Unit	Teaching Hours	CO Targeted
1	**Introduction to PowerShell**	**5**	**CO1**

- Overview of PowerShell and its evolution
- PowerShell vs Command Prompt
- PowerShell editions and versions (Windows PowerShell vs PowerShell Core)
- Understanding cmdlets, scripts, and pipelines
- PowerShell console and Integrated Scripting Environment (ISE)
- Basic commands for file and system navigation

2	**Working with Cmdlets and Objects**	**5**	**CO2**

- Structure and syntax of cmdlets
- Using Get-Command, Get-Help, and Get-Member
- Working with objects, properties, and methods
- Piping and chaining commands
- Formatting outputs (Format-Table, Format-List, Select-Object)

- Sorting, filtering, and exporting data (Sort-Object, Where-Object, Export-CSV)

3	**PowerShell Scripting Fundamentals**	5	CO3

- Writing and running PowerShell scripts (.ps1 files)
- Variables, data types, and operators
- Conditional statements (if, else, switch)
- Loops (for, foreach, while, do-while)
- Functions and parameters
- Script execution policy and digital signatures

4	**System Administration using PowerShell**	5	CO4

- Managing files, folders, and drives
- Process and service management (Get-Process, Stop-Service, etc.)
- Managing users and groups (local machine)
- Registry manipulation and system configuration
- Scheduling tasks and automating administrative actions
- Querying system information and performance data

5	**PowerShell for Networking and Security**	5	CO5

- PowerShell networking cmdlets (Test-Connection, Get-NetIPAddress, Get-NetTCPConnection)
- Retrieving and analyzing network configurations
- PowerShell Remoting (Enable-PSRemoting, Enter-PSSession)
- Managing firewall settings via PowerShell
- Introduction to security modules (Get-ExecutionPolicy, Set-ExecutionPolicy)
- Generating system and security audit reports

6	**PowerShell in Cyber Security Operations**	5	CO6

- PowerShell as a tool in Cyber Security
- Gathering forensic artifacts using PowerShell
- Monitoring event logs and user activity
- Detecting malicious processes and network activity
- PowerShell in incident response and digital forensics
- Defensive scripting and preventing misuse of PowerShell

Reference Books

- *Learn Windows PowerShell in a Month of Lunches* – Don Jones & Jeffrey Hicks.
- *Windows PowerShell Cookbook* – Lee Holmes.
- *PowerShell in Depth* – Don Jones, Jeffrey Hicks, and Richard Siddaway.
- *Microsoft Docs: PowerShell Overview and Command Reference.*
- *PowerShell for Cybersecurity* – SANS Institute Whitepapers.
- *PowerShell and Active Directory Administration Guide* – Microsoft Learn.

Savitribai Phule Pune University
B.Sc. Cyber Security
Sem-VI

CYS-353-MJ-T: Fundamentals of Active Directory

No. of Credits:	Teaching Scheme	Examination Scheme
2	Theory: 2 Hrs/Week	Continuous Evaluation: 15 Marks End Semester : 35 Marks

Prerequisites

- Basic knowledge of Computer Networks
- Understanding of Operating Systems (Windows/Linux)
- Fundamentals of Cyber Security
- Basic knowledge of Client-Server Architecture
- Familiarity with TCP/IP and DNS concepts

Objective:

- To introduce the concepts and architecture of Active Directory services.
- To understand domain structures, organizational units, users, groups, and policies in Active Directory.
- To learn authentication, authorization, and access control mechanisms in Windows environments.
- To understand Group Policy Management and security configurations in enterprise networks.
- To study Active Directory security threats, monitoring, and best practices for secure administration.

Course Outcomes

CO1: Understand the architecture and components of Active Directory services
CO2: Configure and manage domains, users, groups, and organizational units
CO3: Apply authentication and authorization mechanisms using Active Directory
CO4: Implement Group Policies and security configurations in enterprise environments.
CO5: Analyze Active Directory security risks and recommend protection mechanisms.

Unit No.	Name of Unit	Teaching Hours	CO Targeted
1	**Introduction to Active Directory**	6	

- Fundamentals of Active Directory
- Evolution of Directory Services
- Active Directory Architecture
- Domains, Trees, Forests, and Sites
- Domain Controllers and Roles
- Active Directory Services Overview

2	**Active Directory Objects and Management**	6	

- Users, Groups, and Computers
- Organizational Units (OUs)
- Creating and Managing User Accounts
- Group Types and Scopes
- Active Directory Administrative Tools
- Delegation of Administrative Control

3	**Authentication and Access Control**	**6**	

- Kerberos Authentication Protocol
- LDAP Fundamentals
- NTLM Authentication
- Access Control Lists (ACLs)
- User Authentication and Authorization
- Password Policies and Account Security

4	**Group Policy and Security Management**	**6**	

- Introduction to Group Policy Objects (GPOs)
- Group Policy Processing
- Managing Security Policies
- Software Deployment using GPO
- Auditing and Monitoring in Active Directory
- Backup and Recovery Concepts

5	**Active Directory Security and Best Practices**	**6**	

- Active Directory Security Threats
- Privilege Escalation and Misconfigurations
- Active Directory Attack Techniques Overview
- Security Hardening Techniques
- Best Practices for AD Administration
- Introduction to Hybrid Identity and Azure AD

Reference Books

- Mastering Active Directory – Packt Publishing.
- Active Directory Administration Cookbook – Packt Publishing.
- Windows Server Administration Fundamentals – Wiley Publications.
- Active Directory for Dummies – Wiley Publishing.
- Windows Server 2022 & PowerShell All-in-One For Dummies – Wiley Publishing.
- Identity with Windows Server 2016 – Microsoft Press.

Savitribai Phule Pune University
B.Sc. Cyber Security
Sem-VI

CYS-354-MJ-T: Penetration Testing

No. of Credits: 2	Teaching Scheme Theory: 2 Hrs/Week	Examination Scheme Continuous Evaluation: 15 Marks End Semester : 35 Marks

Prerequisites

- Fundamentals of networking, operating systems, basic web technologies, and cybersecurity concepts

Objective:

- Understand what PT is, different approaches, legal/ethical boundaries, and industry frameworks.
- Be able to plan and perform comprehensive, ethical information gathering and map attack surface.
- Know how to discover and prioritize vulnerabilities and enumerate services and accounts.
- Understand common exploitation vectors, their impact, and how to safely validate findings.

Course Outcomes

CO1: Describe PT methodologies, legal/ethical constraints, and testing scopes.
CO2: Collect and analyze reconnaissance data to map attack surfaces.
CO3: Use scanning and enumeration theory to identify and prioritize vulnerabilities.
CO4: Explain common exploitation techniques and their impact on systems and web apps.
CO5: Understand post-exploitation objectives and defensive countermeasures.
CO6: Prepare professional penetration test reports with prioritized remediation guidance.

Unit No.	Name of Unit	Teaching Hours	CO Targeted
1	**Introduction to Penetration Testing**	**5**	**CO1**

- Definition, scope and objectives of penetration testing
- Types: Black-box, White-box, Grey-box
- PT methodology & phases (Planning → Recon → Scanning → Exploitation → Post-exploitation → Reporting)
- Legal, ethical, and contractual considerations (scope, rules of engagement, permissions)
- Risk, vulnerability vs exploit, CVE/CVSS basics
- PT frameworks and standards (OSSTMM, PTES, NIST)

2	**Reconnaissance & Footprinting**	**5**	**CO2**

- Passive reconnaissance: OSINT sources, domain/IP discovery, WHOIS, Google dorking
- Active reconnaissance basics: ping, DNS enumeration, banner grabbing concepts
- Asset identification and attack surface mapping
- Profiling technologies (web server, CMS, frameworks)

- Social engineering overview (conceptual) and data gathering ethics

3	**Scanning, Enumeration & Vulnerability Discovery**	5	CO3

- Network scanning concepts: host discovery, port scanning, service detection
- Vulnerability scanning types and tuning (authenticated vs unauthenticated)
- Enumeration: SMB, LDAP, SNMP, web directories, user enumeration concepts
- Interpreting scan results and reducing false positives
- Vulnerability databases & exploit search (NVD, Exploit-DB basics)

4	**Exploitation Techniques & Web App Testing**	5	CO4

- Exploitation fundamentals and exploit development concepts (high-level)
- Common web application attacks: SQLi, XSS, CSRF, file upload, authentication bypasses
- Command injection, RCE, file inclusion, path traversal concepts
- Safe testing principles and use of exploit frameworks (conceptual: Metasploit)
- Demonstration-level theory of payloads and shells (no hands-on)

5	**Post-Exploitation, Privilege Escalation & Lateral Movement6**	5	CO5

- Post-exploitation goals: persistence, data access, pivoting, cleanup (ethics!)
- Windows and Linux privilege escalation strategies (theory): misconfigurations, SUID, weak permissions, unpatched services
- Credential harvesting, Kerberos basics, pass-the-hash/pass-the-ticket concepts (overview)
- Lateral movement techniques and segmentation importance
- Evidence handling, forensic implications of PT activities

6	**Reporting, Risk Management & Defence Recommendations**	5	CO6

- Structure of a professional PT report: executive summary, technical findings, PoC, remediation steps, risk rating
- Prioritization using CVSS and business context; communicating to technical and non-technical stakeholders
- Remediation advice: configuration, patches, controls, WAF, network segmentation
- Metrics for PT programs and retest cycles
- Integrating PT with secure SDLC and continuous security testing

Reference Books

- PTES (Penetration Testing Execution Standard) — ptes.org
- OWASP Testing Guide & OWASP Top 10 (for web testing) — owasp.org
- *The Web Application Hacker's Handbook* — Stuttard & Pinto (for theory)
- *Metasploit: The Penetration Tester's Guide* — conceptual reading (no lab required)
- NVD / CVE databases; Exploit-DB for exploit descriptions
- NIST SP 800-115: Technical Guide to Information Security Testing and Assessment

Savitribai Phule Pune University
B.Sc. Cyber Security
Sem-VI

CYS-355-MJ-P: Lab Course based on CYS-351-MJ-T & CYS-352-MJ-T

No. of Credits: 2	**Teaching Scheme** Practical: 4 Hrs/Week	**Examination Scheme** Continuous Evaluation: 15 Marks End Semester : 35 Marks

Prerequisites

- Fundamentals of networking, operating systems, basic web technologies, and cybersecurity concepts

Objective:

- To provide practical knowledge of Windows administration and management.
- To introduce automation through PowerShell scripting for system administration.
- To enhance cybersecurity awareness and defensive skills in Windows environments.
- To prepare students for professional tasks in system and security administration

Course Outcomes

CO1: Perform essential Windows administrative operations.
CO2: Configure, monitor, and secure Windows systems.
CO3: Automate administrative and cybersecurity tasks using PowerShell.
CO4: Develop simple PowerShell scripts for managing users, files, and processes.
CO5: Implement automation for monitoring and reporting system performance

Guidelines

- Students must perform **practical assignments** (Windows and PowerShell).
- Each practical must include **commands, screenshots, and result explanations**.
- Final evaluation includes **a mini project** and **viva** based on both sections.

Section A – Windows Practicals

No.	Practical Title
1	Explore Windows interface, Control Panel, Device Manager, and System Tools.
2	Configure and test Windows Firewall and Defender Security options
3	Create and manage disk partitions and perform backup & restore operations
4	Monitor system performance using Task Manager and Resource Monitor
5	Create and manage disk partitions and perform backup & restore operations
6	Optional: Configure local security policy and user access controls

Section B – PowerShell Practicals

No.	Practical Title
1	Introduction to PowerShell environment and basic cmdlets (Get-Help, Get-Command, etc.).
2	Write a PowerShell script to manage files, folders, and permissions.
3	Create and delete user accounts using PowerShell commands.
4	Automate system information collection (IP, CPU, RAM details).
5	Write a PowerShell script to monitor running services and export report to file.
6	Optional: Mini Project – Automate security audit tasks using PowerShell.

Tools and Environment

- **Operating System:** Windows 10 / 11
- **Utilities:** Control Panel, Task Manager, Computer Management
- **Scripting Tool:** PowerShell 5.1 or 7+
- **Optional:** Virtual Machine for testing, VS Code / PowerShell ISE

Recommended Resources

1. Don Jones & Jeffrey Hicks — *Learn Windows PowerShell in a Month of Lunches*
2. Microsoft Documentation — *Windows Administration & PowerShell Reference*
3. Ed Wilson — *Windows PowerShell Step by Step*
4. Microsoft Learn — *Windows System Management & Security Modules*
5. TutorialsPoint — *Windows and PowerShell for Beginners*

Savitribai Phule Pune University
B.Sc. Cyber Security
Sem-VI

CYS-356-MJ-P: Lab Course based on CYS-353-MJ-T & CYS-354-MJ-T

No. of Credits: 2	**Teaching Scheme** Practical: 4 Hrs/Week	**Examination Scheme** Continuous Evaluation: 15 Marks End Semester : 35 Marks

Prerequisites

- Fundamentals of networking, operating systems, basic web technologies, and cybersecurity concepts

Objective:

- To provide hands-on experience in setting up and managing Active Directory environments.
- To develop practical skills in penetration testing and ethical hacking tools.
- To understand security configurations, access control, and network exploitation.
- To apply cybersecurity principles in securing and testing real-world systems.

Course Outcomes

CO1: Configure and manage users, groups, and policies in Active Directory.

CO2: Implement authentication, authorization, and access control mechanisms.

CO3: Use penetration testing tools to identify vulnerabilities.

CO4: Perform reconnaissance, scanning, exploitation, and reporting.

CO5: Demonstrate ethical and responsible use of security testing tools

Guidelines

- Students must perform practical assignments (on Active Directory + on Penetration Testing).
- Each practical should include commands, configurations, screenshots, and result explanations.
- Mini-project or case-based test recommended at semester end

Section A – Active Directory Practicals

1. Install and configure Active Directory Domain Services on Windows Server
2. Create and manage users, groups, and organizational units (OUs).
3. Implement Group Policy Objects (GPOs) for system and user configurations
4. Configure authentication and password policies
5. Manage user permissions and shared resources using access control
6. Backup and restore Active Directory objects

Section B – Penetration Testing Practicals

1. Introduction to Kali Linux and ethical hacking lab setup.
2. Perform network scanning using Nmap and identify open ports.
3. Conduct vulnerability assessment using OpenVAS or Nessus.
4. Perform web application testing using OWASP ZAP or Burp Suite
5. Exploit a test system using Metasploit Framework and generate a report.
6. Wireless network security testing using Aircrack-ng suite

Tools and Environment

- Active Directory Tools: Windows Server 2016/2019, AD DS, Group Policy Editor
- Penetration Testing Tools: Kali Linux, Nmap, Burp Suite, Metasploit, OWASP ZAP, OpenVAS
- Virtualization: VirtualBox / VMware for Lab Setup
- Documentation Tools: Word / Markdown for Reports

Recommended Resources

1. Brian Svidergol — Active Directory Administration Cookbook
2. Microsoft Learn — Active Directory and Group Policy Management
3. Dafydd Stuttard & Marcus Pinto — The Web Application Hacker's Handbook
4. Georgia Weidman — Penetration Testing: A Hands-On Introduction to Hacking
5. OWASP Documentation and Kali Linux Official User Guide

Savitribai Phule Pune University
B.Sc. Cyber Security
Sem-VI

CYS-360-MJ-T: Advanced Digital Forensic

No. of Credits: 2	Teaching Scheme Theory: 2 Hrs/Week	Examination Scheme Continuous Evaluation: 15 Marks End Semester : 35 Marks

Prerequisites

- Fundamentals of networking, operating systems, basic web technologies, and cybersecurity concepts

Objective:

- To understand advanced techniques of digital evidence collection and analysis.
- To explore forensic tools and methods used in cybercrime investigations.
- To apply forensic techniques to real-world scenarios and case studies.
- To strengthen analytical and reporting skills in digital forensic processes.

Course Outcomes

CO1: Explain advanced concepts of digital evidence acquisition and preservation.

CO2: Use forensic tools for data recovery and system investigation.

CO3: Analyze forensic data from various devices and environments.

CO4: Prepare professional forensic reports with integrity and authenticity.

CO5: Demonstrate hands-on experience through practical forensic exercises.

Unit No.	Name of Unit	Teaching Hours	CO Targeted
1	**Introduction to Advanced Digital Forensics**	6	CO1

- Review of Digital Forensics Fundamentals
- Digital Evidence and Cybercrime Overview
- Chain of Custody and Legal Considerations
- Stages of Forensic Investigation
- Challenges in Modern Forensics

2	**Forensic Acquisition and Preservation**	6	CO2

- Forensic Imaging and Cloning Techniques
- Data Integrity and Hash Functions (MD5, SHA1, SHA256)
- Volatile and Non-Volatile Data Acquisition
- Evidence Handling Procedures
- Case Study: Disk Image Analysis

3	**File System and Data Analysis**	6	CO3

- File System Structures: FAT, NTFS, EXT, HFS+
- Recovering Deleted Files and Hidden Data
- Memory and Log File Analysis

- Metadata and Timestamp Analysis
- Tools: Autopsy, FTK Imager, X-Ways

4	**Network and Mobile Forensics**	6	CO4

- Basics of Network Forensics and Packet Capture
- Log Analysis and Traffic Reconstruction
- Mobile Device Data Extraction Techniques
- SIM, SD Card, and App-Level Analysis
- Tools: Wireshark, Cellebrite, Oxygen Forensic Suite

5	**Cloud and Advanced Forensic Techniques**	6	CO4, CO5

- Challenges in Cloud Forensics
- Remote Evidence Collection
- Anti-Forensic Techniques and Countermeasures
- Reporting, Documentation, and Expert Testimony
- Emerging Trends in AI-Based Forensics

Reference Books

- Eoghan Casey — *Digital Evidence and Computer Crime*
- Nelson, Phillips, Steuart — *Guide to Computer Forensics and Investigations*
- Maras — *Cybercrime and Digital Forensics*
- Kruse & Heiser — *Computer Forensics: Incident Response Essentials*
- Official Documentation of Autopsy, FTK, and Wireshark

Savitribai Phule Pune University
B.Sc. Cyber Security
Sem-VI

CYS-361-MJ-P: Lab Course based on CYS-360-MJ-T

No. of Credits: 2	**Teaching Scheme** Practical: 4 Hrs/Week	**Examination Scheme** Continuous Evaluation: 15 Marks End Semester : 35 Marks

Prerequisites

- Fundamentals of networking, operating systems, basic web technologies, and cybersecurity concepts

Objectives:

- To understand advanced techniques of digital evidence collection and analysis.
- To explore forensic tools and methods used in cybercrime investigations.
- To apply forensic techniques to real-world scenarios and case studies.
- To strengthen analytical and reporting skills in digital forensic processes.

Course Outcomes

CO1: Explain advanced concepts of digital evidence acquisition and preservation.

CO2: Use forensic tools for data recovery and system investigation.

CO3: Analyze forensic data from various devices and environments.

CO4: Prepare professional forensic reports with integrity and authenticity.

CO5: Demonstrate hands-on experience through practical forensic exercises.

Guidelines

- Students should perform **practical assignments** covering forensic tools and techniques.
- Each practical must include **screenshots, analysis reports, and findings**.
- One **mini project or case investigation** must be completed at the end of the semester.

Practical Assignments

1. Perform disk imaging using FTK Imager or Autopsy.
2. Recover deleted files from storage media.
3. Analyze Windows event logs and system registry for evidence
4. Perform memory dump and analyze using Volatility Framework
5. Conduct file system forensic analysis (FAT/NTFS).
6. Capture and analyze network packets using Wireshark
7. Perform email header and attachment analysis.
8. Mobile device data extraction using open-source tools
9. Cloud data investigation (Google Drive / AWS sample case).

10. Mini Project: Complete forensic case study with full report

Tools and Software Suggested

- **Forensic Tools:** Autopsy, FTK Imager, Volatility, Wireshark, EnCase (demo)
- **Mobile Tools:** Cellebrite UFED, MOBILedit, Oxygen Forensic Suite
- **Platforms:** Windows, Linux (Kali), Virtual Machines for testing

Recommended Books

1. Eoghan Casey — *Digital Evidence and Computer Crime*
2. Nelson, Phillips, Steuart — *Guide to Computer Forensics and Investigations*
3. Maras — *Cybercrime and Digital Forensics*
4. Kruse & Heiser — *Computer Forensics: Incident Response Essentials*
5. Official Documentation of Autopsy, FTK, and Wireshark

Savitribai Phule Pune University
B.Sc. Cyber Security
Sem-VI

CYS-362-MJ-T: DevSecOps Fundamentals

No. of Credits: 2	Teaching Scheme Theory: 2 Hrs/Week	Examination Scheme Continuous Evaluation: 15 Marks End Semester : 35 Marks

Prerequisites

- Basic knowledge of software development life cycle (SDLC).
- Understanding of operating systems and computer networks.

Objective:

- To understand the principles of DevOps and its security integration (DevSecOps).
- To explore tools and practices that automate and secure the software development lifecycle (SDLC).
- To apply continuous integration and deployment (CI/CD) pipelines with embedded security.
- To perform hands-on practicals for secure coding, automation, and vulnerability scanning.

Course Outcomes

CO1: Explain DevOps lifecycle and integration of security (DevSecOps).

CO2: Use automation tools to implement CI/CD pipelines.

CO3: Identify and mitigate vulnerabilities in code, containers, and cloud environments.

CO4: Apply security tools within CI/CD for compliance and monitoring.

CO5: Develop a mini secure pipeline for software deployment.

Unit No.	Name of Unit	Teaching Hours	CO Targeted
1	**Introduction to DevOps and DevSecOps**	**6**	**CO1**

- DevOps fundamentals and SDLC phases
- Key components: CI, CD, automation, and collaboration
- Need for integrating security (DevSecOps)
- DevSecOps principles: “Shift Left Security”
- Culture, people, process, and tools

2	**DevSecOps Lifecycle & Architecture**	**6**	**CO1**

- Secure Software Development Lifecycle (SSDLC)
- Stages: Plan → Code → Build → Test → Release → Deploy → Operate → Monitor
- Automation in security testing
- Integrating security in DevOps pipelines
- Case study: CI/CD pipeline with security gates

3	**Tools and Platforms**	**6**	**CO2, CO3**

- Git, GitHub, Jenkins, Docker, Kubernetes overview

- Security Tools: SonarQube, OWASP Dependency-Check, Trivy, Snyk
- Infrastructure as Code (IaC) with Ansible and Terraform
- Container Security and Image Scanning
- Cloud Security basics (AWS / Azure pipelines)

4	**Security Testing in CI/CD**	6	CO4

- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)
- Software Composition Analysis (SCA)
- Secrets management (Vault, environment variables)
- Security monitoring and incident response integration.

5	**Best Practices and Compliance**	6	CO5

- Secure coding practices and automation
- Logging and auditing DevOps activities
- Continuous compliance and governance
- DevSecOps metrics and KPIs
- Emerging trends: AI in DevSecOps, Zero Trust Pipelines

Reference Books

- Gene Kim et al. — *The DevOps Handbook*
- Jim Bird — *DevSecOps: Building Security into DevOps*
- AWS Whitepapers — *DevSecOps Implementation Guide*
- OWASP Foundation — *DevSecOps Best Practices*
- Official Documentation of Jenkins, Docker, SonarQube, and Trivy

Savitribai Phule Pune University
B.Sc. Cyber Security
Sem-VI

CYS-363-MJ-P: Lab Course based on CYS-362-MJ-T

No. of Credits: 2	**Teaching Scheme** Theory: 4 Hrs/Week	**Examination Scheme** Continuous Evaluation: 15 Marks End Semester: 35 Marks

Prerequisites

- Fundamentals of networking, operating systems, basic web technologies, and cybersecurity concepts

Objective:

- To understand the principles of DevOps and its security integration (DevSecOps).
- To explore tools and practices that automate and secure the software development lifecycle (SDLC).
- To apply continuous integration and deployment (CI/CD) pipelines with embedded security.
- To perform hands-on practicals for secure coding, automation, and vulnerability scanning.

Course Outcomes

CO1: Explain DevOps lifecycle and integration of security (DevSecOps).
CO2: Use automation tools to implement CI/CD pipelines.
CO3: Identify and mitigate vulnerabilities in code, containers, and cloud environments.
CO4: Apply security tools within CI/CD for compliance and monitoring.
CO5: Develop a mini secure pipeline for software deployment.

Guidelines

- Perform **practical assignments** focused on integrating security in DevOps tools.
- Maintain **screenshots, reports, and explanations** in a journal.
- Final **mini project** to create a secure CI/CD pipeline with security tools integrated.

Practical Assignments

1. Install and configure Git and Jenkins on local or cloud environment
2. Create a basic CI/CD pipeline in Jenkins for a sample web app
3. Integrate SonarQube for code quality and vulnerability scanning
4. Perform SAST and DAST testing using OWASP tools.
5. Implement containerization using Docker and image scanning with Trivy.
6. Deploy a secure container using Kubernetes (Minikube or Docker Desktop)

7. Automate deployment using Ansible or Terraform.
8. Integrate security testing tools (e.g., OWASP Dependency-Check) in CI/CD pipeline
9. Manage secrets securely using HashiCorp Vault or Jenkins credentials plugin
10. Mini Project: Build a secure CI/CD pipeline integrating Jenkins, Docker, and SonarQube

Tools & Software

- **Version Control:** Git, GitHub
- **CI/CD:** Jenkins, GitLab CI, GitHub Actions
- **Security Tools:** SonarQube, Trivy, OWASP ZAP, Dependency-Check
- **Container Tools:** Docker, Kubernetes
- **Automation Tools:** Ansible, Terraform
- **Cloud Platforms:** AWS, Azure (optional labs)

Recommended Books / Resources

1. Gene Kim et al. — *The DevOps Handbook*
2. Jim Bird — *DevSecOps: Building Security into DevOps*
3. AWS Whitepapers — *DevSecOps Implementation Guide*
4. OWASP Foundation — *DevSecOps Best Practices*
5. Official Documentation of Jenkins, Docker, SonarQube, and Trivy

Savitribai Phule Pune University
B.Sc. Cyber Security
Sem-VI

CYS-371-VSC: Embedded System Programming

No. of Credits: 2	Teaching Scheme Practical: 4 Hrs/Week	Examination Scheme Continuous Evaluation: 15 Marks End Semester : 35 Marks

Prerequisites

- Fundamentals of networking, operating systems, basic web technologies, and cybersecurity concepts

Objective:

- To provide hands-on experience in embedded system programming and interfacing.
- To understand microcontroller-based system development and IoT integration.
- To learn programming for sensors, actuators, and communication modules.
- To apply embedded system concepts for security and automation applications.

Course Outcomes

After successful completion of this course, students will be able to:

CO1: Write and execute embedded programs using microcontrollers.

CO2: Interface sensors, actuators, and displays with controllers.

CO3: Implement communication protocols such as UART, I2C, and SPI.

CO4: Develop mini-projects using Arduino or ESP32 boards.

CO5: Apply embedded programming concepts in cybersecurity or IoT domains.

Guidelines

- Perform **following practical assignments** (mandatory).
- Maintain **journal records** with circuit diagrams, code listings, output screenshots, and explanations.
- At the end, each student must complete a **mini-project or case study** based on embedded applications.

Tools and Hardware

- **Development Boards:** Arduino Uno / ESP32 / Raspberry Pi (optional)
- **Sensors:** DHT11, PIR, IR, LDR, Ultrasonic, etc.
- **Software:** Arduino IDE / MicroPython / Tinkercad (simulation)
- **Connectivity:** Wi-Fi, Serial Monitor, USB

List of Practical Assignments

No.	Title of Practical / Experiment
1	Introduction to Arduino IDE and programming basics.
2	Write a program to blink LED using Arduino/ESP32.
3	Interfacing push button and controlling output device.
4	Interfacing temperature or humidity sensor (e.g., DHT11).
5	Display sensor data on serial monitor or LCD.
6	Interfacing motion sensor (PIR) for detecting movement.
7	Implement serial communication between Arduino and computer.
8	Interfacing buzzer and controlling it using conditions.
9	Build a simple IoT-based security alert system (with Wi-Fi module).
10	Mini Project: Design an embedded application for home or network security.

Recommended Resources

1. Simon Monk — *Programming Arduino: Getting Started with Sketches*
2. Massimo Banzi — *Getting Started with Arduino*
3. Dr. Raj Kamal — *Embedded Systems: Architecture, Programming and Design*
4. Espressif Documentation — *ESP32 Developer Guide*
5. Arduino Official Tutorials — https://www.arduino.cc/en/Tutorial/HomePage

Savitribai Phule Pune University
B.Sc. Cyber Security
Sem-VI

CYS-381-OJT: On Job Training (Internship)

No. of Credits:	Teaching Scheme	Examination Scheme
4	Practical: 8 Hrs/Week	Continuous Evaluation: 30 Marks End Semester : 70 Marks

Prerequisites:

- Basic knowledge of Computer Networks and Cyber Security concepts
- Understanding of Operating Systems and Networking fundamentals
- Familiarity with programming/scripting basics
- Knowledge of cyber security tools and safe computing practices
- Completion of Second Year B.Sc. (Cyber Security) coursework

Objective:

- To provide students with practical exposure to cyber security tools, technologies, and industrial practices.
- To enable students to apply theoretical cyber security concepts in real-world environments.
- To develop analytical thinking, ethical hacking awareness, and security problem-solving abilities.
- To encourage teamwork, communication, and professional interaction within cyber security domains.
- To familiarize students with industry standards, cyber laws, and secure working practices.

Course Outcomes

CO1: Enhance knowledge related to cyber security tools, technologies, and industrial practices.
CO2: Analyze and solve security-related problems using appropriate techniques and methodologies.
CO3: Apply critical thinking and analytical skills to identify and mitigate cyber threats.
CO4: Demonstrate effective communication and teamwork skills while working with industry experts and mentors
CO5: Gain practical experience in cyber security projects, security auditing, or related industry work
CO6: Prepare professional documentation including design, implementation, testing, and security reports
CO7: Understand industry-specific cyber security standards, policies, and compliance requirements.
CO8: Complete assigned projects/tasks successfully within predefined objectives and timelines

Guidelines for On Job Training:

- Students are expected to complete cybersecurity-related work/projects within 120 hours assigned by the organization (company/industry/consultancy/institution).

- Students can start the OJT/Internship immediately after completion of Sem V (Fulltime in vacation period) or during Sem VI (Parttime after lecture/practical hours).
- The internship work may involve cybersecurity assignments such as vulnerability assessment, penetration testing, security monitoring, network security, incident response, digital forensics, security auditing, secure software development, cloud security, or equivalent work.
- The college should assign mentors/guides to students for monitoring progress throughout the OJT.
- Students must submit weekly progress reports duly signed by concerned authorities of the organization to the assigned mentor.
- At the end of OJT, students should prepare documentation and submit the internship report to the college in the prescribed format.
- After completion of OJT, final presentation and documentation shall be evaluated by the examination panel as per university norms
- Students must follow ethical practices, confidentiality policies, and cybersecurity guidelines of the organization during the internship period.