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.