SEMESTER V

Sr No	Course Category	Course Code	Course Title	Hours per Week			Credits	Maximum Marks		
				L	T	P		Continual Assessment	End Sem Examination	Total
1	PCC	23CS501T	Network Vulnerability Analysis and Penetration Testing	3	-	-	3	30	70	100
2	PCC	23CS501P	Network Vulnerability Analysis and Penetration Testing Lab	-	-	2	1	25	25	50
3	PCC	23CS502T	Operating System	4	-	-	4	30	70	100
4	PCC	23CS502P	Operating System Lab	-	-	2	1	25	25	50
5	PCC	23CS503P	Cyber Security Lab -I	-	-	2	1	25	25	50
6	PEC	23CS504T	Professional Elective -I	3	-	-	3	15	35	50
7	OE	23CS505T	Open Elective - II	3	-	-	3	30	70	100
8	VSC	23CS506T	Technical Skill Development - II	2	-	-	2	50	-	50
9	SEC	23CS507P	Career Development - V	-	-	2	1	50	-	50
			Total	**15**		**8**	**19**	**320**	**280**	**600**
10	MDM	23CS508T	MDM-III	3	-	-	3	30	70	100
			Total	**18**		**8**	**22**	**350**	**350**	**700**

	Professional Elective - I		**Open Elective - I**
23CS504T(i)	Introduction to Cloud Security	23CS505T(i)	Open Source and Open Standards
23CS504T(ii)	Security Strategies in Windows & Linux	23CS505T(ii)	Basics of Computer Architecture
23CS504T(iii)	IOT and Security	23CS505T(iii)	Security Policies and Implementation

		July 2023	1.0	Applicable for 2023-24
Chairman - BoS	Dean – Academics	Date of Release	Version	

ST. VINCENT PALLOTTI COLLEGE OF ENGINEERING & TECHNOLOGY,NAGPUR

(An autonomous institution affiliated to Rashtrasant Tukadoji Maharaj Nagpur University)

B. Tech. Scheme of Examination & Syllabus 2023-24

COMPUTER SCIENCE & ENGINEERING(CYBER SECURITY)

FIFTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
22CS501T	Network Vulnerability and Penetration Testing	3			3	30	70	100

Course Objectives	Course Outcomes
This course is intended to : • Explain the basic principles and techniques of how attackers can enter computer systems. • Put acquired knowledge into practice by performing ethical penetration tests and hiding the intrusion. • Evaluate the societal role of hacking from a social, ethical and economic standpoint.	**Students will be able to** • Perform analyses of data breaches and audits of information technology security. • Evaluate the strengths and weaknesses of various information technology solutions regarding data security. • Independently present and perform demonstrations of pen tests for educational purposes

Unit I **[10Hrs]**

Introduction Ethics of Ethical Hacking: Why you need to understand your enemy's tactics, recognizing the gray areas in security, Vulnerability Assessment and Penetration Testing. Penetration Testing and Tools: Social Engineering Attacks: How a social engineering attack works, conducting a social engineering attack, common attacks used in penetration testing, preparing yourself for face-to-face attacks, defending against social engineering attacks.

Unit II **[12 Hrs]**

Physical Penetration Attacks: Why a physical penetration is important, conducting a physical penetration, Common ways into a building, Defending against physical penetrations. Insider Attacks: Conducting an insider attack, Defending against insider attacks. Metasploit: The Big Picture, Getting Metasploit, Using the Metasploit Console to Launch Exploits, Exploiting Client-Side Vulnerabilities with Metasploit, Penetration Testing with Metasploit's Meterpreter, Automating and Scripting Metasploit, Going Further with Metasploit.

Unit III **[12Hrs]**

Managing a Penetration Test: planning a penetration test, structuring a penetration test, execution of a penetration test, information sharing during a penetration test, reporting the results of a Penetration Test. Basic Linux Exploits: Stack Operations, Buffer Overflows, Local Buffer Overflow Exploits, Exploit Development Process. Windows Exploits: Compiling and Debugging Windows Programs, Writing Windows Exploits, Understanding Structured Exception Handling (SEH), Understanding Windows Memory Protections (XPSP3, Vista, 7 and Server 2008), Bypassing Windows Memory Protections.

Unit IV **[12Hrs]**

Web Application Security Vulnerabilities: Overview of top web application security vulnerabilities, Injection vulnerabilities, cross-Site scripting vulnerabilities, the rest of the OWASP Top Ten SQL Injection vulnerabilities, Cross-site scripting vulnerabilities. Vulnerability Analysis: Passive Analysis, Source Code Analysis, Binary Analysis..

Unit V **[12Hrs]**

Client-Side Browser Exploits: Why client-side vulnerabilities are interesting, Internet explorer security concepts, history of client- side exploits and latest trends, finding new browser-based vulnerabilities heap spray to exploit, protecting yourself from client-side exploit. Malware Analysis: Collecting Malware and Initial Analysis: Malware, Latest Trends in Honeynet Technology, Catching Malware: Setting the Trap, Initial Analysis of Malware.

Text Books

S.N	Title	Authors	Edition	Publisher
1	Gray Hat Hacking - The Ethical Hackers Handbook,	Allen Harper, Stephen Sims, Michael Baucom	III Edition	Tata Mc Graw-Hill.
2	The Web Application Hacker's Handbook-Discovering and Exploiting Security flaws	Dafydd Suttard, Marcus pinto	I Edition	Wiley Publishing

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Penetration Testing: Hands-on Introduction to Hacking"	Georgia Weidman	I Edition	Pearson edition
2	The Pen Tester Blueprint-Starting a Career as an Ethical Hacker	", L. Wylie, Kim Crawly	I Edition	Wiley Publications

		August 2024	NEP 2.0	Applicable for 2023-24
Chairman - BoS	Dean – Academics	Date of Release	Version	

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
23CS501P	Network Vulnerability and Penetration Testing Lab			2	1	CA	ESE	Total
						25	25	50

Course Objectives	Course Outcomes
This course is intended ★ **Understand Security Concepts**: Gain foundational knowledge of network security principles, protocols, and architectures. ★ **Threat Identification**: Develop skills to identify, analyze, and mitigate various network vulnerabilities and threats. ★ **Security Mechanisms**: Learn to implement and manage security tools, techniques, and policies to protect network infrastructure. ★ **Incident Response**: Equip learners with the ability to detect, respond to, and recover from network security breaches.	Students will be able to ★ **Comprehend Security Fundamentals**: Demonstrate a solid understanding of network security concepts, threats, and defense mechanisms. ★ **Implement Security Measures**: Apply appropriate tools and techniques to secure network infrastructures and ensure data integrity. ★ **Analyze and Mitigate Threats**: Identify and address potential network vulnerabilities and actively mitigate security risks. ★ **Respond to Security Incidents**: Develop strategies for effective incident detection, response, and recovery in real-world scenarios.

Expt. No.	Title of the experiment
1	1. Installation of KALI & WINDOWS with bridge Connection.
2	2.Social Engineering Attacks : - Setoolkit , Web Templet , Harvesting.
3	3.Penetration Testing and Tools :- WireShark, Nmap.
4	4.Physical Penetration Attacks :-Tailgating , Lock Picking, Dumpster Diving
5	5.Insider Attacks :- Data Theft, Sabotage.
6	6.Metasploit :- Exploiting a Vulnerable Service, Creating a Reverse Shell.
7	7. Managing a Penetration Test :- Planning and Scoping, Reconnaissance and Information Gathering.
8	8.Basic Linux Exploits :- Sudo Privilege Escalation, Kernel Exploits.
9	9.Windows Exploits :- Privilege Escalation with UAC Bypass, Identify Bypass Techniques.
10	10.Web Application Security Vulnerabilities :- Cross-Site Scripting (XSS) .

Text Books

S.N	Title	Authors	Edition	Publisher
1	Programming with Java	Primer, E.Balaguruswamy	6th Edition	TMH
2	The Complete Reference Java	Herbert Schildt	7th Edition	Tata McGraw Hill

		August 2024	NEP 2.0	Applicable for 2023-24
Chairman - BoS	Dean – Academics	Date of Release	Version	

FIFTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
23CS502T	Operating System	4			4	30	70	100

Course Objectives	Course Outcomes
This course is intended **1.** To provide foundational knowledge of operating system structures, types, services, and system calls. **2.** To develop an understanding of process management, CPU scheduling, synchronization, and deadlock handling techniques. **3.** To explore memory management strategies, including paging, segmentation, and virtual memory concepts.	**Students will be able to** 1. Describe OS structures, types, services, and system calls. 2. Analyze process management, scheduling, threading, and IPC. 3. Apply CPU scheduling and synchronization techniques. 4. Demonstrate deadlock handling using prevention, avoidance, and recovery methods. 5. Implement and compare memory management techniques including paging and segmentation.

Unit I	**[8 Hrs]**
Introduction and System Structures - OS overview, objectives, types (batch, time-sharing, real-time, distributed, parallel), OS services, system calls , Computer system operation, I/O structure, OS structure models: simple, layered, microkernel, virtual machine	
Unit II	**[13 Hrs]**
Process and Thread Management - Process concept, states, PCB, Process scheduling algorithms: FCFS, SJF, Priority, Round Robin, Threads: Definition, need for threads, Differences, advantages, limitations, user vs. kernel threads, multithreading models : Many-to-One, One-to-One , Many-to-Many, Thread Libraries (POSIX Threads, Java Threads), Inter-process communication (IPC)	
Unit III	**[10 Hrs]**
CPU Scheduling: Introduction to Scheduling, Scheduling criteria, Scheduling Algorithms, Algorithm Evaluation and Scheduling in different Systems Process Synchronization Synchronization Hardware, Semaphores, and Classical Problem of Synchronization,	
Unit IV	**[8 Hrs]**
Introduction to Deadlocks: Deadlocks: Definition, Necessary and sufficient conditions for Deadlock, Deadlock Prevention, Deadlock Avoidance: Banker's algorithm, Deadlock detection and Recovery. Memory Management: Single Contiguous Memory Management, Fixed Partition	
Unit V	**[8 Hrs]**
Memory Management: Introduction, Allocation Algorithm, swapping ,relocation and address translation Variable Partition: Introduction ,Allocation Algorithm, swapping ,relocation and address traslation,Non-contigious Allocation -general concepts , Paging ,Segmentation Virtual Memory Management system :general concepts ,Page replacement algorithm: First in First Out (FIFO), Least Recently used (LRU), and Optimal.	

Text Books

S.N	Title	Authors	Edition	Publisher
1	Operating System	A.Godbole	3rd Edition	The McGraw-Hill.
2	Operating systems: Internals & design principles	William Stallings,	7th Edition	Pearson

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Operating System Concepts	Silberschatz, Galvin	8 or 10th edition	Wiley

		March 2025	1	Applicable for 2023-24
Chairman - BoS	Dean – Academics	Date of Release	Version	

FIFTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
23CS502P	Operating System Lab	-	-	2	1	25	25	50

Course Objectives	Course Outcomes
This course is intended • Hands-on experience with OS concepts: process, synchronization, memory, file management. • Develop skills in system call programming and debugging. • Understand OS security through practical tasks.	Students will be able to CO1: Implement and analyze process creation, states, and CPU scheduling techniques. CO2: Apply synchronization mechanisms such as semaphores to solve classic concurrency problems. CO3: Simulate and handle deadlocks and memory management using paging and replacement algorithms. CO4: Demonstrate file and directory operations using system calls. CO5: Develop shell programs and simulate user-level authentication mechanisms.

Expt. No.	Title of the experiment
1	Process Creation and States: Create multiple processes using fork () and demonstrate process states.
2	CPU Scheduling Algorithms: Implement FCFS, SJF, Round Robin, and Priority scheduling
3	Producer-Consumer Problem: Solve using semaphores
4	Readers-Writers Problem: Implement synchronization for readers and writers.
5	Deadlock Detection and Recovery: Simulate resource allocation and deadlock handling
6	Paging and Page Replacement: Implement paging and simulate FIFO and LRU algorithms
7	File Operations: Use system calls to create, read, write, and delete files.
8	Directory and Permission Handling: Implement directory operations and modify file permissions
9	User Authentication: Simulate user authentication with password verification
10	Simple Shell: Develop a simple shell program to execute user commands

Text Books

S.N	Title	Authors	Edition	Publisher
1	Operating System Concepts – 10th Edition	Abraham Silberschatz, Peter B. Galvin, Greg Gagne	10 th	Wiley
2	Operating Systems – 4th Edition	William Stallings	4th	Pearson

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Modern Operating Systems – 4th Edition	Andrew S. Tanenbaum, Herbert Bos	4th	Pearson
2	Operating Systems: A Concept-Based Approach – 2nd Edition	D. M. Dhamdhere	2nd	McGraw-Hill Education
3				

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
23CS503P	**Cyber Security Lab - I**			**2**	**1**	**CA**	**ESE**	**Total**
						25	**25**	**50**

Course Objectives	Course Outcomes
This course is intended ★ **Understand Security Concepts**: Gain foundational knowledge of network security principles, protocols, and architectures. ★ **Threat Identification**: Develop skills to identify, analyze, and mitigate various network vulnerabilities and threats. ★ **Security Mechanisms**: Learn to implement and manage security tools, techniques, and policies to protect network infrastructure. ★ **Incident Response**: Equip learners with the ability to detect, respond to, and recover from network security breaches.	**Students will be able to** ★ **Comprehend Security Fundamentals**: Demonstrate a solid understanding of network security concepts, threats, and defense mechanisms. ★ **Implement Security Measures**: Apply appropriate tools and techniques to secure network infrastructures and ensure data integrity. ★ **Analyze and Mitigate Threats**: Identify and address potential network vulnerabilities and actively mitigate security risks. ★ **Respond to Security Incidents**: Develop strategies for effective incident detection, response, and recovery in real-world scenarios.

Expt. No.	Title of the experiment
1	VLAN - Inter Vlan
2	Configuring Standard and Extended ACLs
3	Routing Protocol, RIP, EIGRP, OSPF
4	IPSec VPN with Advanced Configuration
5	Wireless Security Simulation
6	Multilayer Switch Configuration
7	IPv6 Network Setup
8	IPv6 Routing Configuration
9	AAA Configuration
10	Bridge connection between routing protocols.
11	Advance network designing.

Text Books

S.N	Title	Authors	Edition	Publisher
1	Programming with Java	Primer, E.Balaguruswamy	6th Edition	TMH
2	The Complete Reference Java	Herbert Schildt	7th Edition	Tata McGraw Hill

ST. VINCENT PALLOTTI COLLEGE OF ENGINEERING & TECHNOLOGY,NAGPUR

(An autonomous institution affiliated to Rashtrasant Tukadoji Maharaj Nagpur University)

B. Tech. Scheme of Examination & Syllabus 2023-24

Computer Science & Engineering (CYBER SECURITY)

SIXTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
23CS504T	Introduction to Cloud Security	3	-	-	3	15	35	50

Course Objectives	Course Outcomes
This course is intended 1. Learning basics of cloud and challenges in its implementation. 2. Understanding the cloud environment and its security issues. 3. Understanding the various ways to secure cloud programming environments.	**Students will be able to** • Articulate the concepts of cloud computing, its various deployment and service models and vulnerabilities. • Develop solutions based on the concept of virtualization, resource management and migration. • Design measures for cloud data security and identity management. • Provide recommendations for Cloud Infrastructure Security based on cloud compliance and policies.

Unit I	**[9Hrs]**
Introduction: Evolution of Cloud Computing, Cloud Fundamentals: Cloud Definition, Evolution, Architecture, Cloud Characteristics – Elasticity in Cloud – On-demand Provisioning, Applications, deployment models - Public, Private and Hybrid Clouds, and service models - Infrastructure as a Service (IaaS) - Resource Virtualization: Server, Storage, Network. Platform as a Service (PaaS) - Cloud platform & Management: Computation, Storage. Software as a Service (SaaS) - Anything as a service (XaaS), Security as a service. Vulnerability Issues and Security Threats, Security Challenges	
Unit II	**[9Hrs]**
Definition, Understanding and Benefits of Virtualization. Implementation Level of Virtualization, Virtualization Structure/Tools and Mechanisms, Issues with virtualization, virtualization technologies and architectures, introduction to Various Hypervisors, virtualization of data centers, and Virtual Machine level Security, Virtualization security Issues	
Unit III	**[9Hrs]**
Resource Management and Load Balancing : Distributed Management of Virtual Infrastructures, Resource management, Load Balancing. Interoperability, Migration and Fault Tolerance: Issues with interoperability, Cloud Migration, Migration of virtual Machines and techniques. Fault Tolerance Mechanisms. Risk Assessment on Cloud Migration	
Unit IV	**[9Hrs]**
Cloud Data Security and Storage : Cloud storage: Introduction to Storage Systems, Cloud Storage Concepts, Data in the cloud- Cloud file systems. Data level Security, Data Protection (rest, at transit, in use), Data Information lifecycle, Cloud Data Audit, Multi-tenancy Issues.	
Unit V	**[9Hrs]**
Identity and Access Management : Introduction to Identity and Access Management, IAM Challenges, IAM Architecture, IAM Standards and Protocols for Cloud Services, Cloud Authorization Management.	

Text Books

S.N	Title	Authors	Edition	Publisher
1	Distributed and cloud computing from Parallel Processing to the Internet of Things	Kai Hwang, Geoffrey C. Fox and Jack J. Dongarra		Morgan Kaufmann, Elsevier – 2012
2	Cloud Security and Privacy An Enterprise Perspective on Risks and Compliance	Tim Mather, SubraKumaraswamy, and Shahed Latif		O'Reilly 09

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Cloud Computing Bible	Barrie Sosinsky		john Wiley & Sons
2	Cloud Computing Principles and Paradigms	Ronald L. Krutz,Russell Dean Vines,		Wiley Publishers.

		May 2024	1.3	Applicable for 2023-24
Chairman - BoS	Dean – Academics	Date of Release	Version	

ST. VINCENT PALLOTTI COLLEGE OF ENGINEERING & TECHNOLOGY,NAGPUR

(An autonomous institution affiliated to Rashtrasant Tukadoji Maharaj Nagpur University)

B. Tech. Scheme of Examination & Syllabus 2023-24

COMPUTER SCIENCE & ENGINEERING(CYBER SECURITY)

FIFTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
23CS505T(iii)	OE-II Security Policies and Implementation	3				30	70	100

Course Objectives	Course Outcomes
This course is intended 1. To analyze the need for security policies, procedures and security awareness. 2. To understand the types & approaches of policy designing. 3. To identify security policies considerations & implement them. 4. To critique existing security policy for its effectiveness and completeness.	**Students will be able to** 1. Explain the fundamentals of IT security policies and their business drivers. 2. Identify national and international compliance laws and governance challenges. 3. Apply standard frameworks to design and implement IT security policies. 4. Differentiate types of security policies across various IT domains. 5. Analyze and recommend cyber security policies through real-world case studies.

Unit I : The Need for IT Security Policy Frameworks **[8Hrs]**

Introduction to Security Policies, Information Systems Security, Information Assurance Information systems Security Policies, Business Drivers for Information Security Policies.

Unit II: : Role of Governance and Business **[8Hrs]**

Compliance Laws – India, Compliance Laws – International, Seven Domains of IT Infrastructure, Business Challenges & Policies to Mitigate the Risks, Information Security Policy Implementation Issues

Unit III: Policy Framework & Designing **[8Hrs]**

Program Framework Policy, Business Considerations for Framework, Information Assurance Considerations, IT Security Standards & Frameworks, How to Design, Organize, Implement & Maintain IT Security Policies, IT Security Policy Framework Approaches

Unit IV: Types of Policies **[8Hrs]**

User Domain Policies, IT Infrastructure Security Policies, Data Classification and Handling Policies, Risk Management Policies, Incident Response Team (IRT) Policies, Special Access Policies, Physical Security Policy, DLP Policies,

Unit V **[8Hrs]**

Project 1 – Research on Existing and/or Lack of Cybersecurity Polices in Local IT Companies, Analyse the Results and Generate a Comprehensive & Customised List of Cybersecurity Policies for the Companies

Text Books

S.N	Title	Authors	Edition	Publisher
1	Security Policies and implementation Issues	Robert Johnson & Chick Easttom. Jones & Bartlett Learning	Third Edition	. Wiley Publishing.
2	Computer Security Handbook	y Seymour Bosworth, M.E. Kabay & Eric Whyne	Fifth Edition	Wiley Publishing

Reference Books

S.N	Title	Authors	Edition	Publisher
1	The Cyber Crime Law and Practices	CS Mamta Binani	1st	The Institute of Company Secretaries of India

		April 2023	1	Applicable for 2023-24
Chairman - BoS	Dean – Academics	Date of Release	Version	