VULNERABILITY ASSESSMENT AND PENETRATION TESTING		Semester	VII
Course Code	**BCY701**	CIE Marks	50
Teaching Hours/Week (L:T:P: S)	3:0:2:0	SEE Marks	50
Total Hours of Pedagogy	40 hours Theory + 8-10 Lab slots	Total Marks	100
Credits	04	Exam Hours	03
Examination nature (SEE)	Theory/Practical		

Course objectives:

This course will enable students to,

- Introduce Vulnerability Assessment and Penetration Testing
- To be familiar with the Penetration Testing and Tools
- To get an exposure to Metasploit exploitation tool, Linux exploit and Windows exploit
- To gain knowledge on Web Application Security Vulnerabilities, Vulnerability analysis and Malware analysis

Teaching-Learning Process (General Instructions)

These are sample Strategies that teachers can use to accelerate the attainment of the various course outcomes.

1. Lecturer method (L) need not to be only traditional lecture methods, but alternative effective teaching methods could be adopted to attain the outcomes.
2. Use of Video/Animation to explain functioning of various concepts.
3. Encourage collaborative (Group Learning) Learning in the class.
4. Ask at least three HOT (Higher order Thinking) questions in the class, which promotes critical thinking.
5. Adopt Problem Based Learning (PBL), which fosters student's Analytical skills, develop design thinking skills such as the ability to design, evaluate, generalize, and analyze information rather than simply recall it.

MODULE-1

Introduction to 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.

Textbook: Ch. 1, Ch. 4.

MODULE-2

Physical Penetration Attacks: Need of Physical Penetration, 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.

Textbook: Ch. 5, Ch. 6, Ch. 8,

MODULE-3

Managing a Penetration Test: Planning a Penetration Test, Structuring a Penetration Testing Agreement, 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 (XP SP3, Vista 7 And Server 2008), Bypassing Windows Memory Protections.

Textbook: Ch. 9, Ch. 11, Ch. 15.

MODULE-4

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.

Textbook: Ch. 17, Ch. 20.

MODULE-5

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.

Textbook: Ch. 23, Ch. 28.

PRACTICAL COMPONENT OF IPCC

Sl.NO	Experiments
1	**Monitoring Network Traffic** Objective: To analyze and capture network traffic to identify patterns, detect anomalies and assess overall network performance and security.
2	**Host & Services Discovery using Nmap** Objective: To identify active hosts and the services they are running within a network using Nmap, enabling a comprehensive understanding of the network environment.
3	**Vulnerability Scanning using OpenVAS** Objective: To perform a systematic assessment of networked systems using OpenVAS to identify potential vulnerabilities that could be exploited by attackers.
4	**Internal Penetration Testing** a. Mapping b. Scanning c. Gaining Access through CVEs d. Sniffing POP3/FTP/Telnet Passwords e. ARP Poisoning f. DNS Poisoning Objective: To perform a thorough internal penetration test that systematically assesses the security of the organization's network infrastructure by mapping network resources, scanning for vulnerabilities, exploiting known weaknesses and demonstrating attack techniques, including credential sniffing and poisoning attacks, in order to identify and mitigate potential

	security risks effectively.
5	**External Penetration Testing** a. Evaluating External Infrastructure b. Creating Topological Map & Identifying IP Address of Target c. Lookup Domain Registry for IP Information d. Examining Use of IPv6 at Remote Location Objective: To conduct a comprehensive external penetration test aimed at evaluating the security of the organization's external infrastructure by assessing vulnerabilities, mapping the network topology, gathering IP and domain registry information, and examining the implementation of IPv6, ultimately identifying potential entry points and recommending measures to strengthen defenses against external threats.
6	**Different Types of Vulnerability Scanning** Objective: To explore and compare various vulnerability scanning techniques and tools, assessing their effectiveness in identifying and prioritizing security risks.
7	**Vulnerability Scanning with Nessus** Objective: To utilize Nessus for comprehensive vulnerability scanning, identifying security weaknesses in systems and providing recommendations for remediation.
8	**Web Application Assessment with Nikto & Burp Suite** Objective: To evaluate web applications for security vulnerabilities using Nikto and Burp Suite, identifying issues such as misconfigurations and common vulnerabilities in web applications.

Course outcomes (Course Skill Set):

At the end of the course, the student will be able to:

- Explain the ethical considerations and legal implications in conducting ethical hacking activities using appropriate tools.
- Analyze social engineering, physical penetration and insider attacks using automating penetration testing processes.
- Identify report penetration tests effectively to develop and execute Linux and Windows exploits, bypassing memory protections.
- Illustrate web application security vulnerabilities to conduct vulnerability analysis.
- Inspect protection against client-side browser exploits.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

CIE for the theory component of the IPCC (maximum marks 50)

- IPCC means practical portion integrated with the theory of the course.
- CIE marks for the theory component are **25 marks** and that for the practical component is **25 marks**.
- 25 marks for the theory component are split into **15 marks** for two Internal Assessment Tests (Two

Tests, each of 15 Marks with 01-hour duration, are to be conducted) and **10 marks** for other assessment methods mentioned in 22OB4.2. The first test at the end of 40-50% coverage of the syllabus and the second test after covering 85-90% of the syllabus.

- Scaled-down marks of the sum of two tests and other assessment methods will be CIE marks for the theory component of IPCC (that is for **25 marks)**.
- The student has to secure 40% of 25 marks to qualify in the CIE of the theory component of IPCC.

CIE for the practical component of the IPCC

- **15 marks** for the conduction of the experiment and preparation of laboratory record, and **10 marks** for the test to be conducted after the completion of all the laboratory sessions.
- On completion of every experiment/program in the laboratory, the students shall be evaluated including viva-voce and marks shall be awarded on the same day.
- The CIE marks awarded in the case of the Practical component shall be based on the continuous evaluation of the laboratory report. Each experiment report can be evaluated for 10 marks. Marks of all experiments' write-ups are added and scaled down to **15 marks**.
- The laboratory test **(duration 02/03 hours)** after completion of all the experiments shall be conducted for 50 marks and scaled down to **10 marks.**
- Scaled-down marks of write-up evaluations and tests added will be CIE marks for the laboratory component of IPCC for **25 marks**.
- The student has to secure 40% of 25 marks to qualify in the CIE of the practical component of the IPCC.

SEE for IPCC

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (**duration 03 hours**)

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.
3. The students have to answer 5 full questions, selecting one full question from each module.
4. Marks scored by the student shall be proportionally scaled down to 50 Marks

The theory portion of the IPCC shall be for both CIE and SEE, whereas the practical portion will have a CIE component only. Questions mentioned in the SEE paper may include questions from the practical component.

Suggested Learning Resources:

Textbook:

1. Gray Hat Hacking - The Ethical Hackers Handbook, Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, and Terron Williams, 3rd Edition, Tata McGraw-Hill.

Reference Books:

1. The Web Application Hacker's Hand Book - Discovering and Exploiting Security flaws, Dafydd Suttard, Marcuspinto,1st Edition, Wiley Publishing.
2. Penetration Testing: Hands-on Introduction to Hacking, Georgia Weidman, 1st Edition, No

Starch Press.

3. The Pen Tester Blueprint - Starting a Career as an Ethical Hacker, L. Wylie, Kim Crawly,1st Edition, Wiley Publications.

Web links and Video Lectures (e-Resources):

1. https://www.youtube.com/watch?v=fgdcE4kfQBc
2. https://www.youtube.com/watch?v=bQh-nhhYcS4
3. https://www.youtube.com/watch?v=i5GLg9XWJg4
4. https://ieeexplore.ieee.org/document/8463920
5. https://qualysec.com/penetration-testing-and-vulnerability-assessment/

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning

- Group Activity: Identify Vulnerabilities (**5 marks**)
  - Scenario Setup: Provide groups with a simulated web application or network diagram.
  - Task: Each group identifies potential vulnerabilities based on provided documentation and visual cues.
  - Tools: Use a checklist or framework (e.g., OWASP Top Ten) to guide their assessment.
- Presentation: Tools for Vulnerability Assessment (**5 Marks**)
  - Overview of Tools: Nessus, OpenVAS, Burp Suite, Nmap
  - Demo: Show how to use one of these tools (e.g., running a scan with Nmap)

ETHICAL HACKING		Semester	VII
Course Code	**BCY702**	CIE Marks	50
Teaching Hours/Week (L:T:P: S)	3:0:2:0	SEE Marks	50
Total Hours of Pedagogy	40 hours Theory + 8-10 Lab slots	Total Marks	100
Credits	04	Exam Hours	03
Examination nature (SEE)	Theory/Practical		

Course objectives:

This course will enable students to,

- Grasp the ethical implications, legal considerations and best practices associated with ethical hacking
- Learn various methodologies for conducting penetration tests, including reconnaissance, enumeration and exploitation
- Gain hands-on experience with industry-standard tools (e.g., Nmap, Metasploit, Burp Suite) and techniques for vulnerability assessment, network scanning and exploitation
- Learn how to effectively document and present penetration testing results, including creating detailed reports and presentations that outline vulnerabilities, potential impacts etc.

Teaching-Learning Process (General Instructions)

These are sample Strategies that teachers can use to accelerate the attainment of the various course outcomes.

1. Lecturer method (L) need not to be only traditional lecture methods, but alternative effective teaching methods could be adopted to attain the outcomes.
2. Use of Video/Animation to explain functioning of various concepts.
3. Encourage collaborative (Group Learning) Learning in the class.
4. Ask at least three HOT (Higher order Thinking) questions in the class, which promotes critical thinking.
5. Adopt Problem Based Learning (PBL), which fosters student's Analytical skills, develop design thinking skills such as the ability to design, evaluate, generalize, and analyze information rather than simply recall it.

MODULE-1

Introduction: Hacking Impacts, The Hacker

The Framework: Planning the test, Sound Operations, Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Final Analysis, Deliverable, Integration.

Security Program: The Process of Information Security, Component Parts of Information Security Program, Risk Analysis and Ethical Hacking.

Textbook: Ch. 2, Ch. 3, Ch. 5.

MODULE-2

The Business Perspective: Business Objectives, Security Policy, Previous Test Results, Business Challenges.

Planning for a Controlled Attack: Inherent Limitations, Imposed Limitations, timing is Everything, Attack Type, Source Point, Required Knowledge, Multi-Phased Attacks, Teaming and Attack Structure, Engagement Planner, The Right Security Consultant, The Tester, Logistics, Intermediates, Law Enforcement.

Textbook: Ch. 6, Ch. 7.

MODULE-3

Preparing for a Hack: Technical Preparation, Managing the Engagement. **Reconnaissance:** Social Engineering, Physical Security, Internet Reconnaissance. **Textbook:** Ch. 8, Ch. 9.
MODULE-4
Enumeration: Enumeration Techniques, Soft Objective, Looking Around or Attack, Elements of Enumeration, Preparing for the Next Phase. **Exploitation:** Intuitive Testing, Evasion, Threads and Groups, Operating Systems, Password Crackers, Rootkits, Applications, Wardialing, Network, Services and Areas of Concern. **Textbook:** Ch. 10, Ch. 12.
MODULE-5
The Deliverable: The Deliverable, The Document, Overall Structure, Aligning Findings, Presentation. **The Integration:** Integrating the Results, Integration Summary, Mitigation, Defense Planning, Incident Management, Security Policy. **Textbook:** Ch. 13, Ch.14.

PRACTICAL COMPONENT OF IPCC

Sl.NO	Experiments
1	**Risk Analysis and Ethical Hacking Simulation** Objective: Evaluate the components of an information security program through a simulated risk analysis and ethical hacking scenario. Tools: Risk management software (like FAIR or OCTAVE), Ethical hacking documentation templates (OWASP).
2	**Controlled Attack Planning Simulation** Objective: Plan a controlled attack scenario, considering all factors that affect the engagement and outcomes. Tools: Engagement planning templates (e.g., from OWASP), Threat modeling tools (e.g., STRIDE).
3	**Technical Preparation and Engagement Management** Objective: Understand the technical preparations necessary for conducting a penetration test and how to manage the engagement effectively. Tools: Kali Linux (or similar penetration testing OS), Metasploit, Burp Suite, Project management tools (e.g., Asana, Trello).
4	**Reconnaissance Techniques** Objective: Explore various reconnaissance techniques, including social engineering, physical security assessments, and internet reconnaissance. Tools: Social engineering tools (e.g., phishing simulation software), Online reconnaissance tools (e.g., Maltego, Shodan), Physical security assessment checklist.
5	**Enumeration Techniques** Objective: Gain hands-on experience with various enumeration techniques to gather detailed

	information about a target system or network. Tools: Kali Linux (or other penetration testing distribution), Nmap, Enum4linux, Metasploit, Wireshark, Netcat.
6	**Exploitation Techniques** Objective: Practice various exploitation techniques to gain unauthorized access to systems while understanding different attack vectors. Tools: Kali Linux, Metasploit, Burp Suite, Hashcat (for password cracking), DVWA (Damn Vulnerable Web Application) or OWASP Juice Shop.
7	**Creating a Penetration Test Deliverable** Objective: Learn how to compile findings from a penetration test into a structured and professional deliverable. Tools: Word processing software (e.g., Microsoft Word, Google Docs), Presentation software (e.g., PowerPoint, Google Slides), Templates for security reports and presentations.
8	**Integrating Results into a Security Strategy** Objective: Learn how to integrate findings from a penetration test into a broader security framework, focusing on mitigation and incident management. Tools: Risk management software (e.g., FAIR, OCTAVE), Security policy templates, Incident response plan templates.

Course outcomes (Course Skill Set):

At the end of the course, the student will be able to:

- Explain a comprehensive ethical hacking framework, integrating planning, reconnaissance, exploitation and risk analysis to identify vulnerabilities within information security systems.
- Develop a strategic plan for a controlled ethical hacking engagement that aligns with business objectives and security policies, effectively navigating inherent and imposed limitations.
- Model an ethical hacking engagement by effectively conducting reconnaissance through social engineering, physical security assessments and internet reconnaissance techniques.
- Develop proficiency in employing enumeration techniques to gather critical information and prepare for exploitation, utilizing intuitive testing methods, evasion strategies and a variety of tools and applications.
- Develop a comprehensive deliverable that effectively communicates the findings of an ethical hacking engagement, including documentation and structured reporting, while integrating results into actionable mitigation strategies.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

CIE for the theory component of the IPCC (maximum marks 50)

- IPCC means practical portion integrated with the theory of the course.
- CIE marks for the theory component are **25 marks** and that for the practical component is **25 marks**.

- 25 marks for the theory component are split into **15 marks** for two Internal Assessment Tests (Two Tests, each of 15 Marks with 01-hour duration, are to be conducted) and **10 marks** for other assessment methods mentioned in 22OB4.2. The first test at the end of 40-50% coverage of the syllabus and the second test after covering 85-90% of the syllabus.
- Scaled-down marks of the sum of two tests and other assessment methods will be CIE marks for the theory component of IPCC (that is for **25 marks)**.
- The student has to secure 40% of 25 marks to qualify in the CIE of the theory component of IPCC.

CIE for the practical component of the IPCC

- **15 marks** for the conduction of the experiment and preparation of laboratory record, and **10 marks** for the test to be conducted after the completion of all the laboratory sessions.
- On completion of every experiment/program in the laboratory, the students shall be evaluated including viva-voce and marks shall be awarded on the same day.
- The CIE marks awarded in the case of the Practical component shall be based on the continuous evaluation of the laboratory report. Each experiment report can be evaluated for 10 marks. Marks of all experiments' write-ups are added and scaled down to **15 marks**.
- The laboratory test **(duration 02/03 hours)** after completion of all the experiments shall be conducted for 50 marks and scaled down to **10 marks.**
- Scaled-down marks of write-up evaluations and tests added will be CIE marks for the laboratory component of IPCC for **25 marks**.
- The student has to secure 40% of 25 marks to qualify in the CIE of the practical component of the IPCC.

SEE for IPCC

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (**duration 03 hours**)

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.
3. The students have to answer 5 full questions, selecting one full question from each module.
4. Marks scored by the student shall be proportionally scaled down to 50 Marks

The theory portion of the IPCC shall be for both CIE and SEE, whereas the practical portion will have a CIE component only. Questions mentioned in the SEE paper may include questions from the practical component.

Suggested Learning Resources:

Textbook:

1. James S. Tiller, "The Ethical Hack: A Framework for Business Value Penetration Testing", Auerbach Publications, CRC Press.

Reference Books:

1. EC-Council, "Ethical Hacking and Countermeasures Attack Phases", Cengage Learning.
2. Michael Simpson, Kent Backman, James Corley, "Hands-On Ethical Hacking and Network

Defense", Cengage Learning.

Web links and Video Lectures (e-Resources):

1. https://www.youtube.com/watch?v=fNzpcB7ODxQ
2. https://www.youtube.com/watch?v=uHU2uajL1EE
3. https://www.youtube.com/watch?v=K6V7fc5Hj2s
4. https://archive.nptel.ac.in/courses/106/105/106105217/

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning

Students can choose one of the following activities: Capture the Flag (CTF) Competition, SQL Injection Challenge, Phishing Simulation, Social Engineering Role-Play, Security Policy Creation, Incident Response Simulation, Cryptography Challenge, Ethics Debate etc. (**10 Marks**)

	MACHINE LEARNING		Semester	7
	Course Code	**BIC703**	CIE Marks	50
	Teaching Hours/Week (L: T:P: S)	4:0:0:0	SEE Marks	50
	Total Hours of Pedagogy	50	Total Marks	100
	Credits	04	Exam Hours	03
	Examination type (SEE)	Theory		

Course objectives:

- To introduce the fundamental concepts and techniques of machine learning.
- To understanding of various types of machine learning and the challenges faced in real-world applications.
- To familiarize the machine learning algorithms such as regression, decision trees, Bayesian models, clustering, and neural networks.
- To explore advanced concept like reinforcement learning and provide practical insight into its applications.
- To enable students to model and evaluate machine learning solutions for different types of problems.

Teaching-Learning Process (General Instructions)
These are sample Strategies, which teachers can use to accelerate the attainment of the various course outcomes.

1. Lecturer method (L) needs not to be only a traditional lecture method, but alternative effective teaching methods could be adopted to attain the outcomes.
2. Use of Video/Animation/Demonstration to explain functioning of various concepts.
3. Encourage collaborative (Group Learning) Learning in the class.
4. Ask at least three HOT (Higher order Thinking) questions in the class, which promotes critical thinking.
5. Adopt Problem/Practical Based Learning (PBL), which fosters students' Analytical skills, develop design thinking skills, and practical skill such as the ability to design, evaluate, generalize, and analyze information rather than simply recall it.
6. Use animations/videos to help the students to understand the concepts.
7. Demonstrate the concepts using PYTHON and its libraries wherever possible

Module-1

Introduction: Need for Machine Learning, Machine Learning Explained, Machine Learning in Relation to other Fields, Types of Machine Learning, Challenges of Machine Learning, Machine Learning Process, Machine Learning Applications

Understanding Data – 1: Introduction, Big Data Analysis Framework, Descriptive Statistics, Univariate Data Analysis and Visualization.

Chapter-1, 2 (2.1-2.5)

Module-2

	Understanding Data – 2: Bivariate Data and Multivariate Data, Multivariate Statistics, Essential Mathematics for Multivariate Data, Feature Engineering and Dimensionality Reduction Techniques. **Basic Learning Theory:** Design of Learning System, Introduction to Concept of Learning, Modelling in Machine Learning. **Chapter-2 (2.6-2.8, 2.10), Chapter-3 (3.3, 3.4, 3.6)**
	Module-3
	Similarity-based Learning: Nearest-Neighbor Learning, Weighted K-Nearest-Neighbor Algorithm, Nearest Centroid Classifier, Locally Weighted Regression (LWR). **Regression Analysis:** Introduction to Regression, Introduction to Linear Regression, Multiple Linear Regression, Polynomial Regression, Logistic Regression. **Decision Tree Learning:** Introduction to Decision Tree Learning Model, Decision Tree Induction Algorithms. **Chapter-4 (4.2-4.5), Chapter-5 (5.1-5.3, 5.5-5.7), Chapter-6 (6.1, 6.2)**
	Module-4
	Bayesian Learning: Introduction to Probability-based Learning, Fundamentals of Bayes Theorem, Classification Using Bayes Model, Naïve Bayes Algorithm for Continuous Attributes. **Artificial Neural Networks:** Introduction, Biological Neurons, Artificial Neurons, Perceptron and Learning Theory, Types of Artificial Neural Networks, Popular Applications of Artificial Neural Networks, Advantages and Disadvantages of ANN, Challenges of ANN. **Chapter-8 (8.1-8.4), Chapter-10 (10.1-10.5, 10.9-10.11)**
	Module-5
	Clustering Algorithms: Introduction to Clustering Approaches, Proximity Measures, Hierarchical Clustering Algorithms, Partitional Clustering Algorithm, Density-based Methods, Grid-based Approach. **Reinforcement Learning:** Overview of Reinforcement Learning, Scope of Reinforcement Learning, Reinforcement Learning as Machine Learning, Components of Reinforcement Learning, Markov Decision Process, Multi-Arm Bandit Problem and Reinforcement Problem Types, Model-based Learning, Model Free Methods, Q-Learning, SARSA Learning. **Chapter -13 (13.1-13.6), Chapter-14 (14-1-14.10)**

Course outcome (Course Skill Set)

At the end of the course, the student will be able to :

1. Describe the machine learning techniques, their types and data analysis framework.
2. Apply mathematical concepts for feature engineering and perform dimensionality reduction to enhance model performance.
3. Develop similarity-based learning models and regression models for solving classification and prediction tasks.
4. Build probabilistic learning models and design neural network models using perceptrons and multilayer architectures
5. Utilize clustering algorithms to identify patterns in data and implement reinforcement learning techniques

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

- For the Assignment component of the CIE, there are 25 marks and for the Internal Assessment Test component, there are 25 marks.
- The first test will be administered after 40-50% of the syllabus has been covered, and the second test will be administered after 85-90% of the syllabus has been covered
- Any two assignment methods mentioned in the 22OB2.4, if an assignment is project-based then only one assignment for the course shall be planned. The teacher should not conduct two assignments at the end of the semester if two assignments are planned.
- For the course, CIE marks will be based on a scaled-down sum of two tests and other methods of assessment.

Internal Assessment Test question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester-End Examination:

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (**duration 03 hours).**

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.
3. The students have to answer 5 full questions, selecting one full question from each module.
4. Marks scored shall be proportionally reduced to 50 marks

Suggested Learning Resources:

Books

1. S Sridhar, M Vijayalakshmi, "Machine Learning", OXFORD University Press 2021, First Edition.

Reference Books

1. Murty, M. N., and V. S. Ananthanarayana. Machine Learning: Theory and Practice, Universities Press, 2024.
2. T. M. Mitchell, "Machine Learning", McGraw Hill, 1997.
3. Burkov, Andriy. *The hundred-page machine learning book*. Vol. 1. Quebec City, QC, Canada: Andriy Burkov, 2019.

Web links and Video Lectures (e-Resources):

- Machine Learning Tutorials: https://www.geeksforgeeks.org/machine-learning/
- Machine Learning Tutorials: https://www.tutorialspoint.com/machine_learning/index.htm
- Python for Machine Learning: https://www.w3schools.com/python/python_ml_getting_started.asp
- Introduction to Machine Learning: https://onlinecourses.nptel.ac.in/noc22_cs29/preview

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning

- Programming Assignment-1: Implementation of important concepts of Feature Engineering, Data Representation, Regression models, Nearest Neighbor-Based Models, and Decision Tree Models - 10 Marks.
- Programming Assignment-2: Implementation of simple Machine Learning models using various supervised and unsupervised ML algorithms - 15 Marks.

Note: Refer the ***Reference book 1*** for programming assignments
https://www.universitiespress.com/resources?id=9789393330697