COURSE TITLE: Machine Learning									
Course Code:			MCSEDAE124			Examination Scheme			
Total number of Lecture Hours: 56						External	72		
						Internal	28		
Lecture (L):	4	Practicals(P):	-	Tutorial (T):	-	Total Credits	4		

Course Objectives

- To learn the concept of how to learn patterns and concepts from data without being explicitly programmed in various nodes.
- To design and analyse various machine learning algorithms and techniques with a modern outlook focusing on recent advances.
- Explore supervised and unsupervised learning paradigms of machine learning.
- To explore Deep learning technique and various feature extraction strategies.

Course Content	TEACHING HOURS
UNIT 1: Supervised Learning (Regression/Classification)	14-Hrs
• K Nearest-Neighbor Classifier • Decision Trees (ID3, SAFARI). • Linear Regression, Logistic Regression • Support Vector Machines, Nonlinearity and Kernel Methods • Beyond Binary Classification: Multi-class Outputs.	
UNIT 2: Unsupervised Learning	14-Hrs
• Distance-based methods • Clustering: K-means • Dimensionality Reduction: PCA • Generative Models	
UNIT 3:	14-Hrs
• Ensemble Methods • Boosting • Bagging • Random Forests	
UNIT 4:	14-Hrs
• Semi-supervised Learning, • Active Learning, • Reinforcement Learning, • Introduction to Bayesian Learning	
Textbooks	

1. Christopher Bishop, Pattern Recognition and Machine Learning, Springer, 2007.

Reference Books

1. Kevin Murphy, Machine Learning: A Probabilistic Perspective, MIT Press, 2012
2. Trevor Hastie, Robert Tibshirani, Jerome Friedman, The Elements of Statistical Learning, Springer 2009 (freely available online)
3. Christopher Bishop, Pattern Recognition and Machine Learning, Springer, 2007

COURSE OUTCOMES (CO):

After completion of course, students would be able to:

CO1: Extract features that can be used for a particular machine learning approach in various applications.

CO2: To compare and contrast pros and cons of various machine learning techniques and to get an insight of when to apply a particular machine learning approach.

CO3: To mathematically analyze various machine learning approaches and paradigms.

CO4: To discover Deep learning method and different feature extraction approaches.

LEVEL OF CO-PO MAPPING TABLE

	PO's											
CO's	1	2	3	4	5	6	7	8	9	10	11	12
1	3	2	3	3	2	1	1	-	1	2	1	2
2	2	-	3	-	2	2	1	-	1	2	2	3
3	3	3	2	3	2	1	1	-	1	3	2	3
4	2	2	3	3	2	1	1	3	3	2	1	2

Course Title: Data Storage Technologies & Networks							
Course Code: MCSEDAF124						Examination Scheme	
Total Number of Lecture Hours: 50						External	72
						Internal	28
Lecture (L)	4	Practical (P)	0	Tutorial (T)	0	Total Credits	4

Course Objectives

1. *To provide in-depth knowledge of various data storage architectures, systems, and technologies.*
2. *To understand the structure and operation of modern storage area networks (SAN, NAS, DAS).*
3. *To analyze performance, scalability, and security in enterprise storage environments.*
4. *To examine the role of storage networking protocols, virtualization, and cloud storage technologies.*

Course Content	No. of Teaching Hours
UNIT 1	10 Hrs

Introduction to Data Storage

Data explosion and storage challenges, Storage system environment: components and technologies, Data center infrastructure: physical and logical components, RAID: levels, techniques, and performance analysis

UNIT 2	12 Hrs

Storage Architectures and Interfaces

Direct-Attached Storage (DAS), Network-Attached Storage (NAS) – architecture, protocols (NFS, CIFS), Storage Area Networks (SAN) – Fibre Channel, iSCSI, Content-Addressed Storage (CAS), Object Storage basics

UNIT 3	12 Hrs

Storage Networking and Management

Storage virtualization – block and file level, Storage tiering, thin provisioning, deduplication, Backup and recovery techniques, Business continuity and disaster recovery strategies

UNIT 4	14 Hrs

Cloud and Modern Storage Systems

Cloud storage architectures: public, private, hybrid, Storage as a service (STaaS), APIs for cloud storage (e.g., S3), Storage security: threats, encryption, access control, Case studies: enterprise storage solutions and trends

Recommended Books:

1. ***EMC Education Services***, Information Storage and Management, *Wiley, 2nd Edition*
2. ***Robert Spalding***, Storage Networks: The Complete Reference, *Tata McGraw Hill*
3. ***Marc Farley***, Building Storage Networks, *Tata McGraw-Hill*
4. ***Ulf Troppens et al.***, Storage Networks Explained, *Wiley*
5. ***Tom Clark***, Designing Storage Area Networks, *Pearson Education*

Course Outcomes: *Upon successful completion of the course, the students will be able to:*

1. *Understand the fundamental concepts of storage technologies and architectures.*
2. *Analyze the design and implementation of various storage systems such as SAN, NAS, and DAS.*
3. *Evaluate performance, reliability, and security issues in storage networking systems.*
4. *Apply storage virtualization and cloud-based storage models to solve enterprise data management problems.*

Level of CO-PO Mapping

COs	POs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	2	0	0	1	0	0	0	0	0	0	0
2	3	3	2	1	2	0	0	0	0	0	0	0
3	2	3	3	2	2	0	0	1	0	0	0	0
4	2	2	3	2	3	1	1	1	1	1	0	2

Course Title: Digital Image Processing							
Course Code: MCSEDAG124						**Examination Scheme**	
Total Number of Lecture Hours: 48						**External**	**72**
						Internal	**28**
Lecture (L)	**4**	**Practical (P)**	**0**	**Tutorial (T)**	**0**	**Total Credits**	**4**

Course Objectives: *To introduce the concepts of image processing and basic analytical methods to be used in image processing. To familiarize students with image enhancement and restoration techniques, To explain different image compression techniques. To introduce segmentation and morphological processing techniques.*

Course Content	No. of Teaching Hours
UNIT 1	**12 Hrs**
Digital Image Fundamentals: Fundamental steps in Digital Image Processing, Components of an Image processing system, Digital Image Representation, Basic relationship between pixels, Color Modules, RGB and HSI color models. Image Enhancement: Image negatives, Histogram Equalization, Local Enhancement, Image Subtraction, Image Averaging, Smoothing and Sharpening Spatial Filters, Combining Spatial Enhancement methods.	
UNIT 2	**12 Hrs**
Image Transform: Fourier Transform, Discrete Fourier Transform, Fast Fourier Transform, Smoothing Frequency Domain filters, Sharpening Frequency Domain filters, Homomorphic filtering, Convolution and Correlation Theorems, Wavelet Transforms, The Fast Wavelet Transforms. Image Restoration: Noise Models, Restoration in the presence of Noise-Only Spatial filtering , Mean filters, Adaptive filters Periodic Noise Reduction by Frequency Domain filtering , Inverse Filtering , Minimum Mean Square Error (Wiener) Filtering, Geometric Mean Filter.	
UNIT 3	**12 Hrs**
Image Segmentation: Detection of Discontinuities, Point Detection, Line detection, Edge Detection, Thresholding, Optimal Global and Adaptive thresholding, Region-based Segmentation. Representation and Description: Chain codes, Signatures, Boundary Segments, Skeletons, Boundary Descriptors, Regional Descriptors, Relational Descriptors.	
UNIT 4	**12 Hrs**
Image Compression: Fundamentals, Redundancy, Image Compression Models, Fidelity Criteria, Compression ratio, Coding Theorems, Error free Compression techniques like Variable- length Coding and Lossless Predictive Coding, Lossy Compression techniques like Lossy Predictive Coding and Wavelet Coding, Image Compression standards.	

Recommended Books:

1. *Digital Image Processing By Rafael C. Gonzalez, Richard Eugene Woods.*
2. *Fundamentals of Image Processing by Anil K. Jain Prentice Hall.*
3. *Kenneth R. Castleman, Digital Image Processing ', Pearson, 2006.*
4. *William K. Pratt, Digital Image Processing ', John* Wiley, New York, 2002

Course Outcomes:

1. *Understand the fundamentals of digital images, pixel relationships, color models (RGB, HSI), and apply various spatial domain enhancement techniques.*
2. *Apply Fourier and Wavelet transforms, understand frequency domain filtering techniques, and implement image restoration algorithms to recover degraded images.*
3. *Analyze and implement image segmentation and feature extraction, detect edges, lines, and regions using segmentation techniques, and extract meaningful features using boundary and regional descriptors for image analysis.*
4. *Apply Image Compression Techniques and evaluate them using compression ratios etc*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	2	2	1	2	-	-	1	1	2	-	2
2	3	2	2	3	2	-	-	1	1	2	-	2
3	3	3	3	3	2	1	-	1	1	2	1	2
4	3	2	3	2	3	-	-	1	1	2	1	2

Course Title: Digital Forensics							
Course Code: MCSEDAH124					Examination Scheme		
Total Number of Lecture Hours: 48					External	72	
					Internal	28	
Lecture (L)	4	Practical (P)	0	Tutorial (T)	0	Total Credits	4

Course Objectives

- *Provides an in-depth study of the rapidly changing and fascinating field of computer forensics.*
- *Combines both the technical expertise and the knowledge required to investigate, detect and prevent digital crimes.*
- *Knowledge on digital forensics legislations, digital crime, forensics processes and procedures, data acquisition and validation, e-discovery tools.*
- *E-evidence collection and preservation, investigating operating systems and file systems, network forensics, art of steganography and mobile device forensics.*

Course Content	No. of Teaching Hours
UNIT 1	**12 Hrs**

Digital Forensics Science: Forensics science, computer forensics, and digital forensics.
Computer Crime: Criminalistics as it relates to the investigative process, analysis of cyber-criminalistics area, holistic approach to cyber-forensics.
Cyber Crime Scene Analysis: Discuss the various court orders etc., methods to search and seizure electronic evidence, retrieved and un-retrieved communications, Discuss the importance of understanding what court documents would be required for a criminal investigation.

UNIT 2	12 Hrs

Evidence Management & Presentation: Create and manage shared folders using operating system, importance of the forensic mindset, define the workload of law enforcement, explain what the normal case would look like, Define who should be notified of a crime, parts of gathering evidence, Define and apply probable cause.

UNIT 3	12 Hrs

Computer Forensics: Prepare a case, begin an investigation, Understand computer forensics workstations and software, Conduct an investigation, Complete a case, Critique a case, Network Forensics: open-source security tools for network forensic analysis, requirements for preservation of network data

UNIT 4	12 Hrs

Mobile Forensics: mobile forensics techniques, mobile forensics tools. Legal Aspects of Digital Forensics: IT Act 2000, amendment of IT Act 2008. Recent trends in mobile forensic technique and methods to search and seizure electronic evidence.

Recommended Books:

1. Guide to Computer Forensics and Investigations by Bill Nelson, Amelia Phillips, Christopher Steuart, 6th Edition, 2018, Cengage Learning
2. Mobile Forensics – Advanced Investigative Strategies by Oleg Skulkin, Vladimir Katalov, Igor Mikhaylov, 1st Edition, 2016
3. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet by Eoghan Casey, 3rd Edition, 2011
4. John Sammons, The Basics of Digital Forensics, Elsevier

Course Outcomes:

CLO1: Understand relevant legislation and codes of ethics
CLO2: Computer forensics and digital detective and various processes, policies and procedures.
CLO3: E-discovery, guidelines and standards, E-evidence, tools and environment.
CLO4: Email and web forensics and network forensics

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	-	-	-	1	-	3	2	3	-	-	-	2
2	3	3	2	3	3	2	-	-	2	1	-	2
3	3	2	3	3	3	-	-	1	-	2	2	3
4	2	3	2	2	3	-	-	1	2	3	1	3

Course Title: Ethical Hacking							
Course Code: MCSEDAI124						Examination Scheme	
Total Number of Lecture Hours: 50						External	72
						Internal	28
Lecture (L)	4	Practical (P)	0	Tutorial (T)	0	Total Credits	4

Course Objectives

- *Introduce ethical considerations and legal frameworks in ethical hacking and disclosure.*
- *Equip students with hands-on experience in penetration testing and security tools.*
- *Develop skills in vulnerability analysis and reverse engineering techniques.*
- *Understand browser exploits, malware analysis, and exploitation techniques for security testing*

Course Content	No. of Teaching Hours
UNIT 1	**12 Hrs**
Ethics of Ethical Hacking Ethical Hacking and the legal system Proper and Ethical Disclosure	
UNIT 2	**12 Hrs**
Penetration Testing and Tools: Using Metasploit, Using BackTrackLiveCD Linux Distribution	
UNIT 3	**12 Hrs**
Passive Analysis Advanced Static Analysis with IDA Pro Advanced Reverse Engineering	
UNIT 4	**14 Hrs**
Client-side browser exploits, Exploiting Windows Access Control Model for Local Elevation Privilege, Intelligent Fuzzing with Sulley, From Vulnerability to Exploit, Malware Analysis: Collecting Malware and Initial Analysis, Hacking Malware	

Recommended Books:

1. *Shon Harris, Allen Harper, Chris Eagle and Jonathan Ness, Gray Hat Hacking: The Ethical Hackers' Handbook, TMH Edition*

Course Outcomes

CLO1: Explain the ethical, legal, and procedural aspects of ethical hacking and disclosure.
CLO2: Apply penetration testing tools like Metasploit and BackTrack for identifying vulnerabilities.
CLO3: Perform vulnerability analysis and advanced reverse engineering using tools like IDA Pro.
CLO4: Analyze and assess browser and malware exploits, performing initial malware collection and analysis.

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	2	1	1	1	3	2	3	1	2	1	2
2	3	3	3	3	2	1	1	1	2	2	1	2
3	3	3	3	3	3	2	1	1	1	1	1	2
4	3	3	3	2	3	2	1	2	1	1	1	2

Course Title: Malware Analysis & Reverse Engineering							
Course Code: MCSEDAJ124					Examination Scheme		
Total Number of Lecture Hours: 48					External	72	
					Internal	28	
Lecture (L)	4	Practical (P)	0	Tutorial (T)	0	Total Credits	4

Course Objectives

The objective of this course is to provide an insight to fundamentals of malware analysis which includes analysis of JIT compilers for malware detection in legitimate code. DNS filtering and reverse engineering is included.

Course Content	No. of Teaching Hours
UNIT 1	**10 Hrs**
Fundamentals of Malware Analysis (MA), Reverse Engineering Malware (REM) Methodology, Brief Overview of Malware analysis lab setup and configuration, Introduction to key MA tools and techniques, Behavioral Analysis vs. Code Analysis, Resources for Reverse-Engineering Malware (REM) Understanding Malware Threats, Malware indicators, Malware Classification, Examining ClamAVSignatures, Creating Custom ClamAV Databases, Using YARA to Detect Malware Capabilities, Creating a Controlled and Isolated Laboratory, Introduction to MA Sandboxes, Ubuntu, Zeltser's REMnux, SANS SIFT, Sandbox Setup and Configuration New Course Form, Routing TCP/IP Connections, Capturing and Analyzing Network Traffic, Internet simulation using INetSim, Using Deep Freeze to Preserve Physical Systems, Using FOG for Cloning and Imaging Disks, Using MySQL Database to Automate FOG Tasks, Introduction to Python ,Introduction to x86 Intel assembly language, Scanners: Virus Total, Jotti, and NoVirus Thanks, Analyzers: Threat Expert, CWSandbox, Anubis, Joebox, Dynamic Analysis Tools: Process Monitor, Regshot, HandleDiff, Analysis Automation Tools: Virtual Box, VMWare, Python , Other Analysis Tools	
UNIT 2	**12 Hrs**
Using TSK for Network and Host Discoveries, Using Microsoft Offline API to Registry Discoveries , Identifying Packers using PEiD, Registry Forensics with Reg Ripper Plu-gins:, Bypassing Poison Ivy's Locked Files, Bypassing Conficker's File System ACL Restrictions, Detecting Rogue PKI Certificates. Opening and Attaching to Processes, Configuration of JIT Debugger for Shellcode Analysis, Controlling Program Execution, Setting and Catching Breakpoints, Debugging with Python Scripts and Py Commands, DLL Export Enumeration, Execution, and Debugging, Debugging a VMware Workstation Guest (on Windows), Debugging a Parallels Guest (on Mac OS X). Introduction to WinDbg Commands and Controls, Detecting Rootkits with WinDbgScripts, Kernel Debugging with IDA Pro.	
UNIT 3	**12 Hrs**
Memory Dumping with MoonSols Windows Memory Toolkit, Accessing VM Memory Files Overview of Volatility, Investigating Processes in Memory Dumps, Code Injection and Extraction, Detecting and Capturing Suspicious Loaded DLLs, Finding Artifacts in Process Memory, Identifying Injected Code with Malfind and YARA.	
UNIT 4	**14 Hrs**
Memory Dumping with MoonSols Windows Memory Toolkit, Accessing VM Memory Files Overview of Volatility, Investigating Processes in Memory Dumps, Code Injection and Extraction, Detecting and Capturing Suspicious Loaded DLLs, Finding Artifacts in Process Memory, Identifying Injected Code with Malfind and YARA. Using WHOIS to Research Domains, DNS Hostname Resolution, Querying Passive DNS, Checking DNS Records, Reverse IP Search New Course Form, Creating Static Maps, Creating Interactive Maps.	
Recommended Books: Michael Sikorski, Andrew Honig "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software" publisher Williampollock, Ist Edition, 2012. C. C. Elisan, "Malware Analysis and Detection Engineering", publisher Elsevier, Ist Ed, 2018.	
Course Learning Outcomes CLO1: Understand the concept of malware and reverse engineering CLO2: Implement tools and techniques of malware analysis	

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	2	2	3	2	1	1	2	1	1	1	3
2	3	3	3	3	3	1	1	2	2	2	1	3

Course Title: Secure Software Design and Enterprise Computing							
Course Code: MCSEDAK124					Examination Scheme		
Total Number of Lecture Hours: 40					External	72	
					Internal	28	
Lecture (L)	4	Practical (P)	0	Tutorial (T)	0	Total Credits	4

Course Objectives

- *To fix software flaws and bugs in various software.*
- *To make students aware of various issues like weak random number generation, information leakage, poor usability, and weak or no encryption on data traffic*
- *Techniques for successfully implementing and supporting network services on an enterprise scale and heterogeneous systems environment.*
- *Methodologies and tools to design and develop secure software containing minimum vulnerabilities and flaws.*

Course Content	No. of Teaching Hours
UNIT 1	**12 Hrs**
Identify software vulnerabilities and perform software security analysis, Master security programming practices, Master fundamental software security design concepts, Perform security testing and quality assurance.	
UNIT 2	**12 Hrs**
Describe the nature and scope of enterprise software applications, Design distributed N-tier software application, Research technologies available for the presentation, business and data tiers of an enterprise software application, Design and build a database using an enterprise database system, Develop components at the different tiers in an enterprise system, Design and develop a multi-tier solution to a problem using technologies used in enterprise system, Present software solution.	
UNIT 3	**12 Hrs**
Design, implement and maintain a directory-based server infrastructure in a heterogeneous systems environment, Monitor server resource utilization for system reliability and availability, Install and administer network services (DNS/DHCP/Terminal Services/Clustering/Web/Email).	
UNIT 4	**12 Hrs**
Obtain the ability to manage and troubleshoot a network running multiple services, Understand the requirements of an enterprise network and how to go about managing them. Handle insecure exceptions and command/SQL injection, Defend web and mobile applications against attackers, software containing minimum vulnerabilities and flaws.	

Recommended Books:

1. Theodor Richardson, Charles N Thies, Secure Software Design, Jones & Bartlett
2. Kenneth R. van Wyk, Mark G. Graff, Dan S. Peters, Diana L. Burley, Enterprise Software Security, Addison Wesley.

Course Outcomes:

1. *Differentiate between various software vulnerabilities.*
2. *Software process vulnerabilities for an organization.*
3. *Monitor resources consumption in a software.*
4. *Interrelate security and software development process.*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	2	3	3	2	2	3	2	3	2
2			2	2	3	2	2	2	3	2	3	2
3			2	1	1	3	3	3	2	2	3	2
4	1		1	2	3	1	2	2	2	2	3	1

Course Title: Biometrics									
Course Code: MCSEDAL124							Examination Scheme		
Total Number of Lecture Hours: 50							External	72	
							Internal	28	
Lecture (L)	4	Practical (P)	0	Tutorial (T)		0	Total Credits		4

Course Objectives: *The aim of this course is to understand biometric technologies, their components, modalities, and applications across sectors like security, healthcare, and finance. Explore the fundamental principles behind biometric systems, covering sensor design, feature extraction, matching algorithms, and system evaluation metrics, design and implement biometric solutions in real-world applications.*

Course Content	No. of Teaching Hours
UNIT 1	**12 Hrs**
Introduction to biometric technologies and their applications in security, healthcare, finance, etc. Components of a biometric system (sensor, feature extractor, matcher, database, decision-making module). Enrolment, feature extraction, matching, and decision-making.	
UNIT 2	**12 Hrs**
Bio-metric modalities: Fingerprint, Face, Iris, Hand Geometry, Gait Recognition, Ear, Voice, Palm print, On-Line Signature Verification, 3D Face Recognition, Dental Identification and DNA	
UNIT 3	**12 Hrs**
Components of a biometric system: sensor devices, feature extraction, database storage, matching algorithms. Design considerations in biometric system implementation (e.g., trade-offs between speed, accuracy, and cost). Common performance metrics in biometrics, including False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER).	
UNIT 4	**14 Hrs**
The Law and the use of multi bio-metrics systems. Statistical measurement of Biometric. Bio-metrics in Government Sector and Commercial Sector. Real-world Applications in security (access control, identity management), healthcare (patient identification), mobile (phone unlocking). Recent trends in Bio-metric technologies and applications in various domains.	

Books:

1. *Jain, Anil K., Arun Ross, and Karthik Nandakumar. Handbook of Biometrics. Springer, 2004.*
2. *D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer Verlag, 2003.*
3. *Guide to Biometrics: Ruud M.Bolle, Sharath Pankanti, Nalini K. Ratha,Andrew W. Senior, Jonathan H. Connell, Springer 2009.*
4. *J. Wayman, A.K. Jain, D. Maltoni, and D. Maio (Eds.), Biometric Systems: Technology, Design and Performance Evaluation, Springer, 2004.*

Course Outcomes

1. *Perform R&D on bio-metrics methods and systems, understand the working of a biometric system, and identify its applications in fields like security and healthcare.*
2. *Analyze various biometric modalities and their characteristics gain knowledge of different biometric traits such as fingerprint, iris, face, voice, palm print, DNA, etc., and compare their usability, distinctiveness, permanence, and user acceptability.*
3. *Evaluate biometric system components and performance metrics, matching algorithms, and assess performance by FAR, FRR, and EER, considering accuracy, cost, and speed trade-offs.*
4. *Investigate legal, ethical, and real-world applications of biometrics, explore the legal aspects, government and commercial applications, and recent trends in biometric technology across domains such as security, healthcare, and mobile systems.*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	2	1	1	2	2	1	2	2	2	1	2
2	3	3	2	-	2	1	1	1	1	1	1	2
3	3	3	2	2	3	1	1	1	1	1	1	2
4	2	2	2	2	2	3	2	3	2	2	-	2

Course Title: Next Generation Networks							
Course Code: MCSEDAM124						Examination Scheme	
Total Number of Lecture Hours: 50						External	72
						Internal	28
Lecture (L)	4	Practical (P)	0	Tutorial (T)	0	Total Credits	4

Course Objectives:

The aim of this course is to provide background, comprehensive and deep knowledge of state-of-the-art networking concepts with focus on high speed LANs and WANs. It also highlights the challenges existing in the conventional networks and introduces the novel SDN architecture.

Course Content	No. of Teaching Hours
UNIT 1	**12 Hrs**

Introduction: Overview of computer networks, seven-layer architecture, TCP/IP protocol suite.
MAC Protocols: Overview of MAC protocols for high-speed LANS, MANs, and wireless LANs. (For example, FDDI, Gigabit Ethernet, Wireless ethernet, etc.)
ATM: Comparative study of Frame relay and ATM, ATM Protocol Architecture, ATM Logical Connection, ATM Cell, ATM Service Categories, AAL.

UNIT 2	12 Hrs

MPLS: Benefits of MPLS, MPLS architecture, forwarding labelled packets, LDP overview.
Network Layer: Overview of Routing Algorithms, features and classification.
IPv6: Why IPv6, basic IPv4 protocol, IPv6 extensions and options, support for QoS, etc.

UNIT 3	12 Hrs

IP Multicasting: Multicast routing protocols, address assignments, session discovery, etc.
Mobility: Mobile IP.
Flow and Congestion Control: Flow identification, packet classifiers, filters, Window and Rate based schemes, etc.

UNIT 4	14 Hrs

QoS and QoE: IETF integrated services model, differentiated services model.
Network Management: SNMP, issues in management of large networks.
SDN: SDN multi-layered architecture, Comparison of SDN and Conventional Networks, Overview of OpenFlow, SDN Controllers.

Recommended Books:

1. J. F. Kurose "Computer Networking", Addison-Wesley.
2. D. E. Comer, "Internetworking with TCP/IP", Volume 1, 2 and 3, PHI.
3. L. D. Ghein, "MPLS Fundamentals", Cisco.
4. T. D. Nadeau and K. Gray, "Software Defined Networking", O'Reilly.

Course Outcomes:

1. *Understand the basic working of LAN and WAN Protocols*
2. *Apply concept of hierarchical routing and sub-netting to design networks and optimize routing in Internet.*
3. *Apply the concept of multicasting, mobility and congestion control to manage network traffic in dynamic environments.*
4. *Issues in conventional networks and how SDN addresses such challenges.*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	2	3	1	1	1	-	2	-	1	2	1	2
2	2	3	3	3	2	-	2	-	1	2	1	2
3	2	3	3	3	1	-	2	-	1	2	-	2
4	2	3	3	3	3	-	3	-	2	2	2	3

Course Title: Graph Theory							
Course Code: MCSEDAN124					Examination Scheme		
Total Number of Lecture Hours: 50					External	72	
					Internal	28	
Lecture (L)	4	Practical (P)	0	Tutorial (T)	0	Total Credits	4

Course Objectives

1. *To understand the fundamental concepts of graphs and their applications in computer science.*
2. *To analyze various types of graphs, their properties, and standard problems.*
3. *To study algorithms on graphs for traversal, optimization, and network analysis.*
4. *To apply graph theory in real-world problems such as computer networks, data mining, and AI.*

Course Content	No. of Teaching Hours
UNIT 1	**12 Hrs**
Fundamentals and Representations Introduction to graph theory: definitions, degree, types of graphs, Graph representations: adjacency list, adjacency matrix, Subgraphs, complements, isomorphism, Special graphs: bipartite, regular, complete, planar graphs	
UNIT 2	**12 Hrs**
Connectivity and Traversal Paths, walks, cycles, connectedness, Eulerian and Hamiltonian paths and circuits, Graph traversal algorithms: BFS, DFS, Applications in web crawling, social networks	
UNIT 3	**12 Hrs**
Trees and Optimization Trees and their properties, Spanning trees, minimal spanning trees (Prim's and Kruskal's algorithms), Dijkstra's and Bellman-Ford algorithms, Applications in network design, routing, and infrastructure	
UNIT 4	**14 Hrs**
Matching, Coloring, and Advanced Topics Matchings in bipartite graphs, Hall's theorem, Vertex and edge coloring, chromatic number, Planarity, Kuratowski's theorem, Network flows: Ford-Fulkerson algorithm, Applications in scheduling, register allocation, compiler design	

Recommended Books

1. **Douglas B. West**, *Introduction to Graph Theory*, Prentice Hall
2. **Narsingh Deo**, *Graph Theory with Applications to Engineering and Computer Science*, PHI
3. **Reinhard Diestel**, *Graph Theory*, Springer
4. **Jonathan L. Gross and Jay Yellen**, *Graph Theory and Its Applications*, CRC Press
5. Online resources and lecture notes from MIT, Stanford, and IITs

Course Outcomes

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

1. *Understand basic definitions and representations of graphs and types.*
2. *Analyze and solve problems related to connectivity, matchings, and graph coloring.*
3. *Apply graph algorithms for shortest paths, spanning trees, and network flows.*
4. *Use graph theory models to solve practical problems in computing and related areas.*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	2	1	2	1	0	0	0	0	0	0	1
2	3	3	2	2	2	0	0	0	0	0	0	2
3	3	3	3	3	3	0	0	1	0	1	0	2
4	3	2	3	3	3	1	1	1	1	2	1	3

Course Title: Data Science Lab							
Course Code: MCSELAA124					**Examination Scheme**		
Total Number of Lecture Hours: 30					**External**	**36**	
					Internal	**14**	
Lecture (L)	**0**	**Practical (P)**	**4**	**Tutorial (T)**	**0**	**Total Credits**	**2**

Course Objectives

1. *To implement core concepts in Data Science through Python programming.*
2. *To apply data analytics, visualization, and machine learning tools for solving real-world problems.*
3. *To perform statistical, NLP, and unsupervised learning tasks using Python libraries such as NumPy, Pandas, Matplotlib, SciPy, Scikit-learn, and Seaborn.*
4. *To practice hands-on experiments that reflect topics from theoretical units, enhancing understanding through projects and exercises.*

List of Experiments

1. Introduction to SciPy and Linear Algebra with SciPy
2. Integration, Optimization, CDF & PDF using SciPy
3. Visualization with Matplotlib
4. Pair Plot with Seaborn
5. Data Mugging and Wrangling with Pandas
6. Linear & Logistic Regression using Scikit-learn
7. Decision Trees and Random Forests, Support Vector Machines and K-Nearest Neighbours
8. K-Means Clustering and PCA
9. Statistical Analysis using Python
10. NLP – Text Preprocessing and Sentiment Analysis

Note: *This is only a suggested list of experiments/simulations. The instructor is encouraged to familiarize students with additional relevant exercises.

Course Learning Outcomes:

CLO1: **Implement data manipulation techniques using Python libraries such as NumPy and Pandas.**
CLO2: **Apply scientific computing methods using SciPy for solving mathematical/statistical problems.**
CLO3: **Visualize data effectively using Matplotlib and Seaborn to interpret and communicate insights.**
CLO4: **Perform exploratory data analysis (EDA) and preprocessing tasks to prepare data for modeling.**
CLO5: **Build and evaluate supervised and unsupervised machine learning models using Scikit-learn.**
CLO6: **Apply** Natural Language Processing techniques for sentiment analysis & text classification tasks.

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
1	3	2	2	2	3	-	-	1	-	-	-	1
2	3	3	2	3	3	-	-	-	-	-	-	1
3	3	2	2	2	3	-	-	-	-	-	-	1
4	3	3	3	3	3	-	-	1	1	1	-	2
5	3	3	3	3	3	-	-	-	-	-	1	2
6	3	3	3	3	3	-	-	-	-	-	1	2

14

36

Course Title: Distributed Systems Lab												
Course Code: MCSELAB124								**Examination Scheme**				
Total Number of Lecture Hours: 30								**External**			**36**	
								Internal			**14**	
Lecture (L)	**0**	**Practical (P)**	**4**	**Tutorial (T)**		**0**	**Total Credits**					**2**

Course Objectives

1. *To provide hands-on experience in simulating distributed database design and operations across multiple environments.*
2. *To develop skills in query processing, optimization, and transaction management in distributed systems.*
3. *To understand and implement distributed concurrency control, failure handling, and recovery protocols.*
4. *To analyze the performance implications of distributed query processing, load balancing, and system integration techniques.*

List of Experiments

1. Set up a simulated distributed database environment using multiple database instances or virtual machines.
2. Perform horizontal, vertical, and hybrid fragmentation on a relational schema and distribute fragments.
3. Simulate data allocation strategies across multiple sites and validate distributed design.
4. Create distributed views and implement user-level access control with SQL privileges.
5. Simulate query decomposition and localization in a distributed system using sample queries.
6. Analyze and simulate execution plans to compare centralized vs. distributed query processing.
7. Implement and simulate the two-phase commit protocol using SQL scripts or procedural code.
8. Simulate concurrency control scenarios with locking, isolation levels, and deadlock handling.
9. Simulate various system failures (site, link, transaction) and apply recovery protocols.
10. Demonstrate parallel query processing, load balancing, and simulate integration of mobile or heterogeneous databases.

Note: *This is only a suggested list of experiments/simulations. The instructor is encouraged to familiarize students with additional relevant exercises.

Course Learning Outcomes:

CLO1: Design and simulate distributed database architectures with data fragmentation, allocation, and replication.

CLO2: Implement query decomposition, localization, and analyze performance trade-offs in distributed query processing.

CLO3: Apply and simulate distributed transaction management techniques such as two-phase commit and concurrency control.

CLO4: Demonstrate fault tolerance mechanisms including recovery protocols and simulate integration with mobile or heterogeneous systems.

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	3	3	3	2	2	2	1	1	1	1	2
2	3	3	3	3	3	2	1	1	2	1	2	2
3	3	3	3	3	3	2	2	1	2	2	2	3
4	3	3	3	2	3	3	2	2	2	2	2	3

Course Title: Data Preparation and Analysis Lab							
Course Code: MCSELAC124						**Examination Scheme**	
Total Number of Lecture Hours: 30						**External**	**36**
						Internal	**14**
Lecture (L)	**0**	**Practical (P)**	**4**	**Tutorial (T)**	**0**	**Total Credits**	**2**

Course Objectives

1. *To gain hands-on experience in data wrangling and preprocessing.*
2. *To work with real-world datasets for cleaning, transformation, and reduction.*
3. *To implement feature engineering and automation in data preparation pipelines.*

List of Experiments

1. Exploring data using Pandas (loading, summarizing, visualization)
2. Handling missing data using imputation techniques
3. Detecting and treating outliers using statistical methods and visualizations
4. Normalization and Standardization of data
5. Encoding categorical variables (Label encoding, One-hot encoding)
6. Data integration from multiple files/sources
7. Data reduction using PCA and Feature Selection methods
8. Feature engineering: creation of new features from existing data
9. Using Scikit-learn pipelines for data preprocessing

Note: *This is only a suggested list of experiments/simulations. The instructor is encouraged to familiarize students with additional relevant exercises.

Course Learning Outcomes:

After completing this course, the students will be able to:

1. *Understand and apply data preprocessing techniques such as handling missing values, outliers, and normalization.*
2. *Perform feature engineering and selection methods using Python libraries like Pandas and Scikit-learn.*
3. *Implement end-to-end data preparation pipelines for real-world datasets using Python and relevant tools.*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
1	3	2	2	1	2	-	-	-	-	1	-	1
2	2	3	3	2	3	-	-	-	1	2	1	2
3	3	3	3	3	3	2	-	-	1	2	2	3

Course Title: Recommender System Lab									
Course Code: MCSELAD124							Examination Scheme		
Total Number of Lecture Hours: 30							External	36	
							Internal	14	
Lecture (L)	0	Practical (P)	4	Tutorial (T)		0	Total Credits		2

Course Objectives

- *To enable students to gain practical insights into Information Retrieval and Recommender Systems. Students will explore the creation of user profiles and the core functions of recommender systems, including content-based filtering and similarity-based retrieval.*
- *Students will explore collaborative filtering approaches (both user-based and item-based), matrix factorization techniques, and hybrid recommendation models.*
- *Students will develop the skills needed to design, implement, and assess various types of recommender systems effectively.*

List of Experiments

1. Introduction to Information Retrieval
2. Retrieval Models
3. Search Techniques and Relevance Feedback
4. User Profiles and Recommender System Functions
5. Content-Based Filtering Techniques
6. Similarity-Based Retrieval
7. Collaborative Filtering: User-Based and Item-Based
8. Matrix Factorization Techniques
9. Hybrid Recommender Systems
10. Evaluating Recommender Systems
11. Advanced Evaluation Techniques
12. Types of Recommender Systems

Note: *This is only a suggested list of experiments/simulations. The instructor is encouraged to familiarize students with additional relevant exercises.

Course Learning Outcomes:

1. *Understand and implement foundational retrieval models and search techniques. Students will gain hands-on experience with various retrieval models, relevance feedback, and search algorithms, enabling them to build and evaluate basic information retrieval systems.*
2. *Design and analyze content-based and similarity-based filtering techniques. Students will be able to apply user profiling, content analysis, and similarity metrics to develop personalized recommendation solutions.*
3. *Develop and compare collaborative filtering and matrix factorization methods. Through practical implementation, students will learn the differences between user-based, item-based, and latent factor-based techniques, and understand their strengths and limitations.*
4. *Evaluate and optimize recommender systems using standard and advanced metrics. Students will be able to apply evaluation metrics and performance analysis tools to assess recommender systems and suggest improvements using hybrid approaches.*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	3	2	2	3	1	-	-	1	1	-	2
2	3	3	3	2	3	1	-	1	2	1	1	2
3	3	3	3	2	3	1	-	1	2	2	1	2
4	3	3	2	3	3	1	-	1	2	2	1	2

Course Title: Machine Learning Lab							
Course Code: MCSELAE124					Examination Scheme		
Total Number of Lecture Hours: 30					External	36	
					Internal	14	
Lecture (L)	0	Practical (P)	4	Tutorial (T)	0	Total Credits	2

Course Objectives

To enable students to design and implement machine learning solutions to classification, regression and clustering problems and be able to evaluate and interpret the results of the algorithms using python and other development environments.

List of Experiments

1. Implementation of Distance-Based Methods (e.g., K-Nearest Neighbours).
2. Building Decision Trees for Classification and Regression (ID3).
3. Linear Regression and Logistic Regression using Python/Scikit-learn.
4. Training Support Vector Machines with Linear and Nonlinear Kernels.
5. Implementing Multi-class Classification Techniques.
6. K-means Clustering on real-world datasets (e.g., customer segmentation).
7. Dimensionality Reduction using PCA and visualizing results in 2D/3D.
8. Implementing Generative Models for unsupervised learning.
9. Implementing Bagging and Random Forests for robust classification.
10. Experimenting with Boosting Techniques (e.g., AdaBoost, Gradient Boosting).
11. Hyperparameter tuning and model evaluation using Cross-Validation.

This is only a suggested list of experiments/simulations. The instructor is encouraged to familiarize students with additional relevant exercises.

Course Learning Outcomes:

1. *Apply distance-based and tree-based classification algorithms such as K-Nearest Neighbours and ID3 to solve real-world classification and regression problems.*
2. *Implement and analyze linear models including Linear and Logistic Regression, and advanced classifiers like Support Vector Machines, for both binary and multi-class problems using Python libraries.*
3. *Develop unsupervised learning solutions through clustering (K-Means), dimensionality reduction (PCA), and generative models, and visualize results effectively in 2D/3D.*
4. *Evaluate and enhance model performance using ensemble techniques (Bagging, Random Forests, Boosting), along with hyperparameter tuning and cross-validation strategies.*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	3	2	2	2	-	-	-	1	1	0	1
2	3	3	3	2	3	-	-	-	1	1	1	2
3	3	3	3	3	3	1	-	1	1	2	1	2
4	3	3	3	3	3	1	-	1	2	2	2	2

Course Title: Data Storage Technologies and Networks Lab							
Course Code: MCSELAF124						Examination Scheme	
Total Number of Lecture Hours: 50						External	36
						Internal	14
Lecture (L)	0	Practical (P)	4	Tutorial (T)	0	Total Credits	2

Course Objectives

1. *To provide hands-on experience with various types of storage systems and protocols.*
2. *To configure and manage DAS, NAS, and SAN environments.*
3. *To implement and test storage virtualization and backup mechanisms.*
4. *To explore cloud storage platforms and simulate data access/security models.*

List of Experiments

1. **RAID Configuration:** Create and analyze RAID 0, 1, and 5 using Linux or simulation tools.
2. **DAS Setup:** Configure and benchmark performance of DAS on a local system.
3. **NAS Configuration:** Setup NAS using FreeNAS/TrueNAS and access via NFS/CIFS.
4. **SAN Configuration:** Setup a basic SAN environment using open-source SAN tools (Openfiler/iSCSI targets).
5. **Backup & Recovery:** Simulate backup and restoration using tools like Bacula, Amanda, or rsync.
6. **Storage Virtualization:** Implement block/file level virtualization using LVM or ZFS.
7. **Cloud Storage Access:** Access AWS S3/Azure Blob/Google Cloud Storage via SDK or API.
8. **Disaster Recovery Simulation:** Implement a simple DR mechanism using replication or snapshots.
9. **Storage Security:** Demonstrate encryption of data at rest and in transit using SSL/TLS.
10. **Performance Analysis:** Use benchmarking tools (FIO, IOzone) to measure storage throughput and latency.

****This is only a suggested list of experiments/simulations. The instructor is encouraged to familiarize students with additional relevant exercises.***

Recommended Books:

Course Outcomes: By the end of this lab, students will be able to:

1. *Configure and compare different RAID levels for performance and fault tolerance.*
2. *Set up and manage DAS, NAS, and SAN environments for enterprise storage.*
3. *Implement storage virtualization and backup/recovery solutions.*
4. *Apply cloud storage services and enforce basic security and DR mechanisms*

Level of CO-PO Mapping

COs	POs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	2	2	2	2	3	0	0	0	0	0	0	0
2	3	2	3	2	3	1	0	0	1	0	0	1
3	2	3	3	2	3	0	0	1	1	1	0	1
4	2	2	2	2	2	1	1	1	1	1	0	2

Course Title: Digital Image Processing Lab							
Course Code: MCSELAG124					Examination Scheme		
Total Number of Lecture Hours: 50					External	36	
					Internal	14	
Lecture (L)	0	Practical (P)	4	Tutorial (T)	0	Total Credits	2

Course Objectives: *The aim of the course is to provide hands-on experience in implementing fundamental and advanced image processing techniques, including image enhancement, filtering, transformation, restoration, segmentation, feature extraction, and compression.*

List of Experiments

1. Implement the basic image operations reading, displaying, resizing, converting color spaces.
2. Apply image negative, gamma law and log transform to grayscale images.
3. Implement histogram equalization and histogram matching.
4. Demonstrate and implement image filtering in spatial domain.
5. Implement Fourier and Wavelet Transforms and visualize magnitude and phase.
6. Demonstrate and implement image filtering in frequency domain.
7. Add noise (Gaussian, salt & pepper) and restore using Mean, Median, Wiener, and Adaptive filters.
8. Apply Sobel, Prewitt, Canny, and Laplacian edge detectors.
12. Implement thresholding and region-based segmentation.
13. Extract textural features using Gray-Level Co-occurrence Matrix (GLCM).
14. Implement Image compression techniques e.g Huffman coding or Run-Length Encoding (RLE) etc.

This is only a suggested list of experiments/simulations. The instructor is encouraged to familiarize students with additional relevant exercises.

Recommended Books:

Course Outcomes:

1. *Apply some basic and advanced intensity transformation techniques to enhance image such as negative transformation, logarithmic and gamma correction, histogram equalization, and histogram matching.*
2. *Analyze and apply spatial and frequency domain filtering methods (e.g., smoothing, sharpening, Fourier and Wavelet transforms) and visualize the corresponding effects on image data.*
3. *Apply noise models and restoration filters and implement segmentation techniques such as thresholding, edge detection, and region-based methods for accurate object detection.*
4. *Extract features using GLCM and implement basic image compression techniques such as Huffman Coding and Run-Length Encoding (RLE), evaluating efficiency based on fidelity and compression ratio.*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	3	2	2	1	2	-	-	1	1	1	1	2
2	3	3	2	2	3	-	-	1	1	1	-	2
3	3	3	2	3	3	-	-	1	1	1	-	2
4	3	2	2	2	2	1	-	1	1	1	1	2

Course Title: Digital Forensics Lab							
Course Code: MCSELAH124					Examination Scheme		
Total Number of Lecture Hours: 30					External	36	
					Internal	14	
Lecture (L)	0	Practical (P)	4	Tutorial (T)	0	Total Credits	2

Course Objectives

This course aims to provide students with a comprehensive understanding of forensic science, computer forensics, and digital forensics, emphasizing their importance in investigating cybercrimes. It focuses on developing practical skills for identifying, collecting, preserving, and presenting electronic evidence while adhering to legal standards and forensic methodologies. Students will gain hands-on experience with forensic tools for computer, network, and mobile investigations, while also learning about the legal and ethical frameworks, including compliance with the IT Act 2000/2008 and its amendments.

List of Experiments

1. Introduction to Digital Forensics Tools
- Install and familiarize with tools like Autopsy, FTK Imager, and EnCase.

2. Recover Deleted Files from a Hard Drive
- Practice recovering deleted documents and images using forensic recovery tools.

3. Simulate and Analyze a Computer Crime Scene

4. Search and Seizure Simulation for Electronic Evidence

5. Creating and Managing Shared Folders with OS Permissions
- Use Windows/Linux to create shared folders, assign permissions, and simulate evidence storage protocols.

6. Evidence Collection and Preservation Workshop
- Demonstrate correct methods to image a hard disk and maintain the integrity of digital evidence.

7. Preparing and Managing a Forensic Case Report

8. Setting up a Computer Forensics Workstation
- Configure a dedicated forensic workstation (write blockers, analysis tools, hashing utilities).

9. Network Traffic Capture and Analysis
- Use open-source tools like Wireshark and TCP dump to capture and analyze network traffic for suspicious activity.

10. Mobile Device Forensics Investigation
- Perform logical extraction of data from Android/iOS devices using mobile forensic tools like Cellebrite or MOBILedit.

Course Outcomes:

1. *Explain the fundamental concepts of digital forensics and distinguish between forensic science, computer forensics, and cyber forensics.*
2. *Apply appropriate methods and tools to identify, collect, and preserve digital evidence from computers, networks, and mobile devices.*
3. *Demonstrate the ability to manage forensic investigations, document findings, and present digital evidence in a legally admissible manner.*
4. *Analyze legal, ethical, and regulatory issues related to digital forensics, with particular emphasis on the IT Act 2000 and its 2008 amendment.*

Level of CLO-PLO Mapping

CLOs	PLOs											
	1	2	3	4	5	6	7	8	9	10	11	12
1	2	2	2	-	-	2	-	3	-	-	-	-
2	2	1	2	-	3	2	-	2	-	-	-	-
3	-	1	-	3	-	2	-	2	1	-	-	-
4	-	2	-	1	-	3	-	3	-	-	-	-

Course Title: Ethical Hacking Lab								
Course Code: MCSELAI124					Examination Scheme			
Total Number of Lecture Hours: 50					External		36	
					Internal		14	
Lecture (L)	0	Practical (P)	4	Tutorial (T)	0	Total Credits		2

List of Experiments

1. **Study of Ethical Hacking Principles and Legal Considerations**
   - Research and present case studies on ethical vs. unethical hacking, legal frameworks (like the IT Act), and responsible disclosure.
2. **Foot printing and Passive Information Gathering**
   - Use tools like Whois, nslookup, to gather passive intelligence about a target system.
3. **Network Scanning and Enumeration**
   - Perform network scanning using tools like Nmap, Netdiscover, and identify open ports, services, and operating systems.
4. **Vulnerability Assessment and Exploitation using Metasploit Framework**
   - Conduct a basic penetration test using Metasploit to exploit known vulnerabilities on a test virtual machine.
5. **Hands-on Penetration Testing using Kali Linux (BackTrack successor)**
   - Perform full-cycle penetration testing including scanning, enumeration, exploitation, and post-exploitation using Kali Linux.
6. **Password Cracking and Authentication Attacks**
   - Use tools like Hydra, or Hashcat to crack passwords through dictionary and brute-force attacks.
7. **Sniffing and Network Traffic Analysis**
   - Use Wireshark and tcpdump to capture and analyze packets, demonstrating man-in-the-middle and session hijacking techniques.

This is only a suggested list of experiments/simulations. The instructor is encouraged to familiarize students with additional relevant exercises.

Course Title: Malware Analysis & Reverse Engineering Lab							
Course Code: MCSELAJ124					Examination Scheme		
Total Number of Lecture Hours: 30					External	36	
					Internal	14	
Lecture (L)	0	Practical (P)	4	Tutorial (T)	0	Total Credits	2

List of Experiments

1. **Setting Up a Malware Analysis Lab** – Configuring an isolated and controlled environment using VirtualBox, VMware, and REMnux.
2. **Capturing and Analyzing Network Traffic** – Using Wireshark and INetSim to inspect malicious network activity.
3. **Scanning Malware with ClamAV and YARA** – Detecting malware signatures and creating custom ClamAV databases.
4. **Behavioral Analysis of Malware** – Monitoring system changes using Process Monitor and Regshot.
5. **Static Analysis of Malware** – Extracting metadata and examining file headers using PEiD and VirusTotal.
6. **Dynamic Malware Analysis** – Using CWSandbox, Anubis, and Joebox for real-time malware behavior monitoring.
7. **Debugging Malware with WinDbg** – Attaching processes, setting breakpoints, and controlling execution flow.
8. **Reverse Engineering with IDA Pro** – Analyzing disassembled malware code to understand its functionality.
9. **Registry Forensics with RegRipper** – Identifying malware persistence techniques via Windows registry analysis.
10. **Memory Forensics with Volatility** – Extracting and analyzing memory dumps to identify injected code and artifacts.
11. **Using Python for Malware Analysis** – Automating malware analysis with Python scripting.
12. **Identifying Packed Malware with PEiD** – Detecting and unpacking obfuscated malware samples.

This is only a suggested list of experiments/simulations. The instructor is encouraged to familiarize students with additional relevant exercises.

Lab Setup Notes:

- **Operating System**: Windows, Linux (Ubuntu, REMnux, SANS SIFT)
- **Programming Language**: Python, Assembly (x86)
- **Tools/Software**: Wireshark, Volatility, IDA Pro, ClamAV, YARA, PEiD, VirtualBox, VMware, Process Monitor, WinDbg, Regshot, Anubis, Joebox, INetSim