NOIDA INSTITUTE OF ENGINEERING & TECHNOLOGY, GREATER NOIDA, GAUTAM BUDDH NAGAR
(AN AUTONOMOUS INSTITUTE)

Affiliated to

DR. A.P.J. ABDUL KALAM TECHNICAL UNIVERSITY, LUCKNOW

Evaluation Scheme & Syllabus

For

Bachelor of Technology

Computer Science and Engineering (Cyber Security)

Fourth Year

(Effective from the Session: 2025-26)

NOIDA INSTITUTE OF ENGINEERING & TECHNOLOGY, GREATER NOIDA, GAUTAM BUDDH NAGAR
(AN AUTONOMOUS INSTITUTE)

Bachelor of Technology

Computer Science and Engineering (Cyber Security)

Evaluation Scheme

SEMESTER-VII

Sl. No.	Subject Codes	Subject	Types of Subjects	Periods			Evaluation Schemes				End Semester		Total	Credit
				L	T	P	CT	TA	TOTAL	PS	TE	PE		
1	ACSCY0701	Penetration Testing	Mandatory	3	0	0	30	20	50		100		150	3
2		Departmental Elective-V	Departmental-Elective	3	0	0	30	20	50		100		150	3
3		Open Elective - II	Open Elective	3	0	0	30	20	50		100		150	3
4		Open Elective - III	Open Elective	3	0	0	30	20	50		100		150	3
5	ACSCY0751	Penetration Testing Lab	Mandatory	0	0	2				25		25	50	1
6	ACSE0759	Internship Assessment-III	Mandatory	0	0	2				50			50	1
7		MOOCs (For B.Tech. Hons. Degree)	*MOOCs											
8		Total		12	0	4	120	80	200	75	400	25	**700**	**14**

*** List of MOOCs Based Recommended Courses for 4th year (Semester-VII) B. Tech Students**

. No.	Subject Code	Course Name	University / Industry Partner Name	No of Hours	Credits
1	AMC0333	AWS Certified Security Specialty 2024 [NEW]	Infosys Wingspan (Infosys Springboard)	38h	3
2	AMC0292	Database Management System - Science Graduates	Infosys Wingspan (Infosys Springboard)	55h 23m	4

Abbreviation Used:

L: Lecture, T: Tutorial, P: Practical, CT: Class Test, TA: Teacher Assessment, PS: Practical Sessional, TE: Theory End Semester Exam., PE: Practical End Semester Exam, CE: Core Elective, OE: Open Elective, DE: Departmental Elective, CA: Compulsory Audit, MOOCs: Massive Open Online Courses.

DEPARTMENTAL ELECTIVES

Subject Code	Subject Name	Types of subjects	Bucket Name	Branch	Semester
ACSAI0712	Natural Language Processing	Departmental Elective- V	Data Analytics	CYS	7
ACSE0713	Web Development using MERN Stack with DevOps	Departmental Elective- V	Full Stack Development	CYS	7

NOIDA INSTITUTE OF ENGINEERING & TECHNOLOGY, GREATER NOIDA, GAUTAM BUDDH NAGAR
(AN AUTONOMOUS INSTITUTE)

Bachelor of Technology
Computer Science and Engineering (Cyber Security)
Evaluation Scheme
SEMESTER-VIII

Sl. No.	Subject Codes	Subject	Types of Subjects	Periods		Evaluation Schemes					End Semester		Total	Credit
				L	T	P	CT	TA	TOTAL	PS	TE	PE		
1		Open Elective-IV	Open Elective	2	0	0	30	20	50		100		150	2
2	ACSE0859/ ACSE0858	Capstone Project/Industrial Internship	Mandatory	0	0	20				200		300	500	10
3		MOOCs (For B.Tech. Hons. Degree)	*MOOCs											
4		**TOTAL**		**2**	**0**	**20**	**30**	**20**	**50**	**200**	**100**	**300**	**650**	**12**

*** List of MOOCs Based Recommended Courses for 4th year (Semester-VIII) B. Tech Students**

Sr. No.	Subject Code	Course Name	University / Industry Partner Name	No of Hours	Credits
1	AMC0336	Comprehensive Training on Unix and Linux OS Fundamentals	Infosys Wingspan (Infosys Springboard)	29h 53m	2
2	AMC0338	Information Security A-Z: Cyber Security Bootcamp	Infosys Wingspan (Infosys Springboard)	12h 25m	0.5

Abbreviation Used:

L: Lecture, T: Tutorial, P: Practical, CT: Class Test, TA: Teacher Assessment, PS: Practical Sessional, TE: Theory End Semester Exam., PE: Practical End Semester Exam, CE: Core Elective, OE: Open Elective, DE: Departmental Elective, CA: Compulsory Audit, MOOCs: Massive Open Online Courses.

Course Title: Penetration Testing

Subject Name: Penetration Testing

Subject Code: ACSCY0701

Applicable in Department: CSE (Cyber Security)

Industry Requirement:

Technology/Application	Companies	Job Role	Package	Skills
Network Penetration Testing	IBM, Deloitte, Accenture	Penetration Tester	INR 6-10 LPA	Networking, Ethical Hacking, Vulnerability Assessment
Web Application Penetration Testing	Trustwave, Rapid7, NCC Group	Web Security Analyst	INR 5-9 LPA	Web Development, OWASP Top 10, Web Application Security
Mobile Application Penetration Testing	Synopsys, Checkmarx, AppSec Labs	Mobile Security Engineer	INR 7-12 LPA	Mobile Development, Reverse Engineering, Secure Coding Practices
Wireless Penetration Testing	Secureworks, McAfee, NetSPI	Wireless Security Specialist	INR 8-15 LPA	Wireless Protocols, Radio Frequency Analysis, Cryptography
Social Engineering Penetration Testing	Social-Engineer, PhishLabs, KnowBe4	Social Engineering Specialist	INR 6-11 LPA	Psychology, Social Engineering Tactics, Communication Skills

Content of the Subject:

Course Objective:

The course aims to provide students with a comprehensive understanding of penetration testing in cybersecurity. Through theoretical learning and hands-on practical exercises, students will grasp the fundamental concepts, methodologies, and ethical considerations associated with penetration testing. They will develop the skills to identify, assess, and exploit vulnerabilities in networks, web applications, mobile apps, and wireless systems. The course aims to equip students with the knowledge and tools necessary to conduct effective penetration tests and strengthen the security posture of organizations. Overall, it seeks to prepare students for roles in cybersecurity by fostering critical thinking, problem-solving, and ethical decision-making skills.

Course Outcome:

CO1: Students will understand the importance and ethical considerations of penetration testing in cybersecurity.

CO2: Students will demonstrate proficiency in conducting network reconnaissance, vulnerability assessment, and exploitation.

CO3: Students will be able to identify, assess, and exploit vulnerabilities in web applications, recommending appropriate mitigation strategies.

CO4: Students will acquire the skills to perform mobile application reconnaissance, vulnerability analysis, and exploitation, ensuring secure mobile development practices.

CO5: Students will learn advanced penetration testing methodologies, including wireless penetration testing and social engineering tactics, and will be able to prepare comprehensive penetration testing reports.

Unit No.	Module	Topics Covered	Pedagogy	Lecture Require (Total = Lecture + Practical)	Practical/Assignment/Lab	Co-Mapping	Aligned with University/Industry/Certifications (Format in Details)
Unit 1	Introduction to Penetration Testing	Overview of Penetration Testing, Importance and Scope, Legal and Ethical Considerations	Lecture, Case Studies, Discussions	4 (2 + 2)	Research on Ethical Guidelines for Penetration Testing, Case Studies	CO1	Aligned with CEH (Certified Ethical Hacker), CompTIA Security+
Unit 2	Network Penetration Testing	Network Reconnaissance, Scanning and Enumeration, Exploitation Techniques	Lecture, Hands-on Labs, Demonstrations	5 (3 + 2)	Network Scanning and Exploitation Lab	CO2	Aligned with OSCP (Offensive Security Certified Professional)
Unit 3	Web Application Penetration Testing	OWASP Top 10, Web Application Scanning, SQL Injection, XSS, CSRF	Lecture, Live Demonstrations, Practice Exercises	6 (4 + 2)	Web Application Vulnerability Assessment Lab	CO3	Aligned with eWPT (eLearnSecurity Web Application Penetration Tester)
Unit 4	Mobile Application Penetration Testing	Android and iOS Security Fundamentals, Reverse Engineering, Secure Coding Practices	Lecture, Practical Workshops, Hands-on Exercises	7 (5 + 2)	Mobile App Penetration Testing Lab	CO4	Aligned with eMAPT (eLearnSecurity Mobile Application Penetration Tester)
Unit 5	Advanced Techniques and Reporting	Advanced Exploitation Techniques, Reporting and Documentation, Post-Exploitation Techniques	Lecture, Case Studies, Mock Assessments	8 (4 + 4)	Penetration Testing Report Preparation	CO5	Aligned with GPEN (GIAC Penetration Tester)

List of Practical's:

Course Objective:

The practical component of the "Penetration Testing" syllabus aims to equip students with hands-on experience and proficiency in ethical hacking principles, network and web application penetration testing, mobile application security assessments, and advanced exploitation techniques. Students will learn to utilize industry-standard tools and methodologies to identify vulnerabilities, exploit security weaknesses, and generate comprehensive penetration testing reports. Emphasis is placed on adhering to legal and ethical guidelines, developing critical thinking skills, and preparing for industry certification examinations such as CEH, OSCP, and eWPT.

Lab No.	Unit No.	Topic	Program Logic Building	CO Mapping	Aligned with University/Industry/Certifications
1	Unit 1	Ethical Hacking Principles	Create a simulated network environment, identify vulnerabilities, and devise ethical hacking strategies.	CO1	Aligned with CEH (Certified Ethical Hacker)
2	Unit 1	Network Reconnaissance	Use tools like Nmap and Wireshark to conduct network reconnaissance and analyze captured network traffic.	CO1	Aligned with OSCP (Offensive Security Certified Professional)
3	Unit 1	Legal and Ethical Considerations	Research and present case studies highlighting legal and ethical implications of penetration testing.	CO1	Aligned with CEH (Certified Ethical Hacker)
4	Unit 1	Penetration Testing Methodologies	Develop a penetration testing methodology document outlining various phases and techniques.	CO1	Aligned with GPEN (GIAC Penetration Tester)
5	Unit 2	Network Scanning and Enumeration	Perform network scans using tools like Nessus and identify active hosts, open ports, and services.	CO1	Aligned with OSCP (Offensive Security Certified Professional)
6	Unit 2	Exploitation Techniques	Exploit vulnerabilities identified during scanning, gaining unauthorized access to target systems.	CO2	Aligned with eMAPT (eLearnSecurity Mobile Application Penetration Tester)
7	Unit 2	Firewall Evasion Techniques	Design and execute firewall evasion techniques to bypass network defenses and gain access to internal systems.	CO2	Aligned with CEH (Certified Ethical Hacker)
8	Unit 2	Network Traffic Analysis	Analyze packet captures to detect and mitigate network-based attacks, such as DoS and DDoS attacks.	CO2	Aligned with OSCP (Offensive Security Certified Professional)
9	Unit 3	OWASP Top 10 Vulnerabilities	Identify and exploit common web application vulnerabilities outlined in the OWASP Top 10 list.	CO3	Aligned with eWPT (eLearnSecurity Web Application Penetration Tester)
10	Unit 3	Web Application Scanning	Utilize tools like Burp Suite to perform web application scans and identify security vulnerabilities.	CO3	Aligned with eWPT (eLearnSecurity Web Application Penetration Tester)

11	Unit 3	SQL Injection	Execute SQL injection attacks against vulnerable web applications to extract sensitive information.	CO3	Aligned with eWPT (eLearnSecurity Web Application Penetration Tester)
12	Unit 3	Cross-Site Scripting (XSS)	Inject malicious scripts into web applications to exploit XSS vulnerabilities and perform client-side attacks.	CO3	Aligned with eWPT (eLearnSecurity Web Application Penetration Tester)
13	Unit 4	Android Security Fundamentals	Analyze Android security architecture, identify security controls, and develop secure coding practices.	CO4	Aligned with eMAPT (eLearnSecurity Mobile Application Penetration Tester)
14	Unit 4	iOS Security Fundamentals	Explore iOS security mechanisms, analyze secure coding guidelines, and mitigate common security threats.	CO4	Aligned with eMAPT (eLearnSecurity Mobile Application Penetration Tester)
15	Unit 4	Mobile Application Reverse Engineering	Reverse engineer Android and iOS applications to identify vulnerabilities and analyze application logic.	CO4	Aligned with eMAPT (eLearnSecurity Mobile Application Penetration Tester)
16	Unit 4	Mobile App Penetration Testing	Perform comprehensive security assessments of mobile applications, identifying and exploiting vulnerabilities.	CO4	Aligned with eMAPT (eLearnSecurity Mobile Application Penetration Tester)
17	Unit 5	Advanced Exploitation Techniques	Employ advanced exploitation techniques like buffer overflows and privilege escalation to gain system access.	CO5	Aligned with GPEN (GIAC Penetration Tester)
18	Unit 5	Post-Exploitation Techniques	Explore post-exploitation techniques such as lateral movement and persistence to maintain access to compromised systems.	CO5	Aligned with GPEN (GIAC Penetration Tester)
19	Unit 5	Penetration Testing Report Preparation	Compile penetration testing findings into a comprehensive report, including vulnerabilities, exploits, and recommendations.	CO5	Aligned with GPEN (GIAC Penetration Tester)
20	Unit 5	Mock Penetration Testing Assessment	Simulate a real-world penetration testing engagement, demonstrating proficiency in all aspects of the penetration testing process.	CO5	Aligned with GPEN (GIAC Penetration Tester)

Required software and tools for the labs mentioned above:

Tool	Description	Availability
Kali Linux	Penetration testing Linux distribution	Free
Metasploit Framework	Penetration testing framework	Free/Paid
Wireshark	Network protocol analyzer	Free
Nmap	Network scanner and mapper	Free
Burp Suite	Web application security testing tool	Free/Paid
Nessus	Vulnerability scanner	Paid
Nikto	Web server scanner	Free
SQLMap	SQL injection and database takeover tool	Free
Aircrack-ng	Wireless network security assessment tool	Free
John the Ripper	Password cracking tool	Free
Hydra	Password cracking tool	Free
OWASP ZAP	Web application security testing tool	Free
OSINT Framework	Open-Source Intelligence gathering tool	Free
GDB	GNU Debugger	Free
IDA Pro	Interactive Disassembler	Paid
Ghidra	Software reverse engineering tool	Free
Hashcat	Password recovery tool	Free
Maltego	Forensic and intelligence tool	Paid
BloodHound	Active Directory reconnaissance tool	Free
CrackMapExec	Post-exploitation tool for Windows networks	Free
Responder	LLMNR, NBT-NS, and MDNS poisoner	Free

Current Requirement of the tools mentioned above/ software in industry:

S. No.	Tool Name	Current Industry Requirement
1	Kali Linux	Primary operating system for penetration testing and ethical hacking tasks.
2	Metasploit Framework	Comprehensive framework for exploit development, vulnerability assessment, and penetration testing automation.
3	Wireshark	Essential for network protocol analysis, troubleshooting, and security assessments, providing deep packet inspection.
4	Burp Suite	Widely used for web application security testing, including scanning, crawling, and exploitation of web vulnerabilities.
5	Nmap	Essential for network discovery and vulnerability scanning, offering robust port scanning and host enumeration features.

Reference Books:

Textbooks:

S. No.	Tool Name	Book Title	Author
1	Kali Linux	"Kali Linux Revealed: Mastering the Penetration Testing Distribution"	Raphael Hertzog
2	Metasploit Framework	"Metasploit: The Penetration Tester's Guide"	David Kennedy et al.
3	Wireshark	"Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide"	Laura Chappell
4	Burp Suite	"The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws"	Dafydd Stuttard et al.
5	Nmap	"Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning"	Gordon Fyodor Lyon

Links:

S. No.	Tool Name	Recommended Link
1	Kali Linux	Kali Linux Official Website
2	Metasploit Framework	Metasploit Framework GitHub Repository
3	Wireshark	Wireshark Official Website
4	Burp Suite	Burp Suite Official Website
5	Nmap	Nmap Official Website

Sample Projects:

S. No.	Tool	Project 1	Project 2
1	Kali Linux	Setting up a Virtual Lab Environment for Penetration Testing	Performing Network Sniffing and Analysis using Wireshark
2	Metasploit Framework	Exploiting a Vulnerable Virtual Machine using Metasploit Exploits	Creating Custom Payloads and Exploiting Target Systems using Metasploit
3	Wireshark	Analyzing Network Traffic to Identify Suspicious Activity	Decrypting and Analyzing Secure HTTPS Traffic using Wireshark
4	Burp Suite	Intercepting and Modifying HTTP Requests and Responses	Identifying and Exploiting Web Application Vulnerabilities using Burp Suite Scanner
5	Nmap	Performing Host Discovery and Port Scanning on a Local Network	Conducting a Comprehensive Vulnerability Scan using Nmap and Analyzing Results

Any Industry Aligned Certification/Courses for this subject:

Name of Certification:

S. No.	Certification/Course	Justification	Industry Requirement
1	CEH (Certified Ethical Hacker)	Covers comprehensive ethical hacking techniques, tools, and methodologies.	Widely recognized and required for penetration testing roles in various industries.
2	OSCP (Offensive Security Certified Professional)	Focuses on hands-on penetration testing skills, including exploit development and network security.	Highly respected in the industry for its rigorous practical examination and skill assessment.
3	eWPT (eLearnSecurity Web Application Penetration Tester)	Specialized in web application penetration testing techniques and methodologies.	Essential for professionals focusing on web application security assessments and testing.
4	eMAPT (eLearnSecurity Mobile Application Penetration Tester)	Covers mobile application security testing and exploitation techniques.	Addresses the growing demand for professionals skilled in mobile application security assessments.
5	GPEN (GIAC Penetration Tester)	Demonstrates proficiency in penetration testing methodologies and tools.	Recognized by employers seeking skilled penetration testers and ethical hackers.

Requirement/Value of Certification in the Industry:

S. No.	Certification Name	Value
1	CEH (Certified Ethical Hacker)	Widely recognized and respected certification demonstrating proficiency in ethical hacking techniques.
2	OSCP (Offensive Security Certified Professional)	Highly valued for its hands-on approach and real-world scenarios, indicating practical penetration testing skills.
3	eWPT (eLearnSecurity Web Application Penetration Tester)	Recognized for its focus on web application security testing and practical skill assessment.
4	eMAPT (eLearnSecurity Mobile Application Penetration Tester)	Valuable for professionals specializing in mobile application security assessments and exploitation.
5	GPEN (GIAC Penetration Tester)	Esteemed certification demonstrating expertise in penetration testing methodologies and tools.

Company: IBM

- Explain the difference between black-box and white-box testing in penetration testing.
- How do you approach a penetration test for a web application?
- Describe a time when you discovered a critical vulnerability during a penetration test and how you remediated it.
- What tools do you use for network reconnaissance during a penetration test?
- How do you prioritize vulnerabilities discovered during a penetration test?

Company: Deloitte

- Describe the steps involved in conducting a penetration test on a corporate network.
- How do you handle sensitive data discovered during a penetration test?
- Explain the concept of social engineering and its role in penetration testing.
- Describe a time when you encountered a particularly challenging vulnerability during a penetration test and how you approached it.
- How do you stay updated with the latest security threats and vulnerabilities?

Company: Accenture

- What methodologies do you follow for penetration testing?
- Explain the importance of reporting and documentation in penetration testing.
- Describe a time when you successfully exploited a vulnerability to gain unauthorized access during a penetration test.
- How do you assess the security posture of a mobile application during a penetration test?
- What are the limitations of automated vulnerability scanners in penetration testing?

Company: Microsoft

- How do you ensure compliance with relevant laws and regulations during a penetration test?
- Describe a time when you collaborated with other team members during a penetration test project.
- How do you handle disagreements with clients regarding vulnerability severity ratings?
- What are the key differences between a vulnerability assessment and a penetration test?
- How do you approach testing for security misconfigurations during a penetration test?

Company: Google

- Describe a recent security vulnerability that made headlines and its potential impact.
- How do you prioritize security vulnerabilities for remediation?
- Explain the concept of zero-day vulnerabilities and their significance in penetration testing.
- Describe a time when you had to explain technical concepts related to penetration testing to non-technical stakeholders.
- How do you ensure the confidentiality and integrity of sensitive information discovered during a penetration test?

B. TECH FOURTH YEAR		
Subject Code: ACSAI0712		**L T P** **3 0 0**
Course Title: Natural Language Processing		**Credits** **3**
Course objective: The course aims to provide an understanding of the foundational concepts and techniques in NLP. The focus is on providing application-based knowledge.		
Pre-requisites: Programming Skills, Data Structures, Algorithms, Probability and Statistics, Machine Learning.		
Course Contents / Syllabus		
Unit-1	**Overview of Natural Language Processing** Definition, Applications and emerging trends in NLP, Challenges. Ambiguity. NLP tasks using NLTK: Tokenization, stemming, lemmatization, stop-word removal, POS tagging, Parsing, Named Entity Recognition, coreference resolution.	**8 Hours**
Unit-2	**Regular Expressions** Data Preprocessing: Convert to lower case, handle email-id, HTML tags, URLs, emojis, repeat characters, normalization of data (contractions, standardize) etc. Vocabulary, corpora, and linguistic resources, Linguistic foundations: Morphology, syntax, semantics and pragmatics, Language models: Unigram, Bigram, N-grams.	**8 Hours**
Unit-3	**Text Analysis and Similarity** Text Vectorization: Bag-of-Words model and vector space models, Term Presence, Term Frequency, TF-IDF Textual Similarity: Cosine similarity, Word Mover's distance, Word embeddings: Word2Vec, GloVe.	**8 Hours**
Unit-4	**Text Classification & NLP Applications** Text classification: Implement of applications of NLP using text classification-Sentiment Analysis, Topic modelling, Spam detection. High Level NLP applications: Machine translation: Rule-based and statistical approaches, Text summarization Dialog systems, conversational agents and chatbots.	**8 Hours**
Unit-5	**Advanced NLP Techniques** Sequential data, Introduction to sequence models - RNN and LSTM, Attention Mechanism, Transformer, Transformer-based models: BERT, GPT, T5, Introduction to Hugging Face Transformers, Case studies.	**8 Hours**
Course outcome: After completion of this course students will be able to:		
CO 1	Discuss the emerging trends and challenges in NLP and perform the basic NLP tasks using some NLP library.	K2
CO 2	Apply regular expressions for data cleaning and understand the fundamental concepts and theories underlying NLP.	K3
CO 3	Extract features and find similarity in text data.	K3

CO4	Implement NLP techniques to design real-world NLP applications	K3
CO 5	Apply advanced techniques like sequential modelling and attention mechanism to develop NLP applications	K4

Textbooks:

1. Daniel Jurafsky, James H. Martin, "Speech and Language Processing", Second Edition, Pearson Education, 2009 ISBN 0131873210.

2. James Allen, Natural Language Understanding, 2nd edition, 1995 Pearson Education ISBN 13: 9780805303346.

3. Akshar Bharti, Vineet Chaitanya and Rajeev Sangal, NLP: A Paninian Perspective,1st edition1995, Prentice ISSBN 9788120309210

Reference Books:

1. Christopher D. Manning and Hinrich Schutze, "Foundations of Statistical Natural Language Processing" , MIT Press, 1999 Second Edition, ISBN No. 0-262-13360-l.

2. T. Winograd, Language as a Cognitive Process, 1st edition, 1983 Addison- Wesley ISBN 020108-571-2

3. L.M. Ivansca, S. C. Shapiro, Natural Language Processing and Knowledge Representation, 2nd edition, 2000 AAAI Press ISBN-13: 978-0262590211

Links:

https://realpython.com/nltk-nlp-python/

https://www.coursera.org/lecture/python-text-mining/basic-nlp-tasks-with-nltk-KD8uN

https://www.coursera.org/lecture/nlp-sequence-models/learning-word-embeddings-APM5s

https://www.coursera.org/projects/regular-expressions-in-python

https://www.coursera.org/learn/python-text-mining/lecture/sVe8B/regular-expressions

B. TECH.- B. TECH FOURTH YEAR		
Subject Code: ACSE0713		**L T P 3 0 0**
Subject Name: Web Development using MERN Stack with DevOps		**Credits 3**
Course Objective: This course focuses on how to design and build static as well as dynamic web pages and interactive web applications. Students can understand how to put them together to create a MERN stack application.		
Pre- requisites: Student should have the knowledge of HTML, CSS and ES6		
Course Contents/Syllabus		
Unit-1	**Introduction to React JS:** Overview of frameworks, NPM commands, React App, Project Directory Structure, React Component Basic, Understanding JSX, Props and State, Stateless and Stateful Components, Component life cycle, Hooks, react-router vs react-router-dom,	**8 Hours**
Unit-2	**Connecting React with mongodB:** Google Material UI, AppBar, Material UI's Toolbar, NavBar, Material UI Buttons, SQL and Complex Transactions, Dynamic Schema, create Index (), get Indexes () & drop Index (), Replication, Statement-based vs. Binary Replication, Auto-Sharding and Integrated Caching, Load balancing, Aggregation, scalability.	**8 Hours**
Unit-3	**Node js & Express Framework:** Introduction, Environment Setup, serving static resources, template engine with vash and jade, Connecting Node.js to Database, Mongoose Module, Creating Rest APIs, Express Framework, MVC Pattern, Routing, Cookies and Sessions, HTTP Interaction, User Authentication	**8 Hours**
Unit-4	**Evolution of DevOps:** DevOps Principles, DevOps Lifecycle, DevOps Tools, and Benefits of DevOps, SDLC (Software Development Life Cycle) models, Lean, ITIL and Agile Methodology, Agile vs DevOps, Process flow of Scrum Methodologies, Project planning, scrum testing, sprint Planning and Release management, Continuous Integration and Delivery pipeline.	**8 Hours**
Unit-5	**CI/CD concepts (GitHub, Jenkins, Sonar):** GitHub, Introduction to Git, Version control system, Jenkins Introduction, Creating Job in Jenkins, adding plugin in Jenkins, Creating Job with Maven & Git, Integration of Sonar, Dockers, Containers Image: Run, pull, push containers, Container lifecycle, Introduction to Kubernetes.	**8 Hours**
Course Outcomes –		
CO1	Apply the knowledge of ES6 that are vital to implement react application over the web.	K3

CO2	Implement and understand the impact of web designing by database connectivity with Mongodb.	K3
CO3	Explain, analyze and apply the role of server-side scripting language like Nodejs and Express js framework.	K4
CO4	Identify the benefits of DevOps over other software development processes to Gain insights into the DevOps environment.	K2
CO5	Demonstrate popular open-source tools with features and associated terminology used to perform Continuous Integration and Continuous Delivery.	K3

Textbooks:

1. Kirupa Chinnathambi, "Learning React", 2nd Edition 2016, Addison Wesley Publication.
2. Mohan Mehul, "Advanced Web Development with React", 2nd Edition 2020, BPB Publications.
3. Dhruti Shah, "Comprehensive guide to learn Node.js", 1st Edition, 2018 BPB Publications.
4. Jennifer Davis, Ryn Daniels, "Effective DevOps: Building, Collaboration, Affinity, and Tooling at Scale",1st Edition, 2016, O'Reilly Media Publication.
5. John Edward Cooper Berg, "DevOps. Building CI/CD Pipelines with Jenkins, Docker Container, AWS (Amazon Web Services) ECS, JDK 11, Git and Maven 3, Sonar, Nexus", Kindle Edition,2019, O'Reilly Media Edition.

Reference Books:

1. Anthony Accomazzo, Ari Lerner, and Nate Murray, "Fullstack React: The Complete Guide to ReactJS and Friends", 4th edition, 2020 International Publishing. □
2. David Cho, "Full-Stack React, Type Script, and Node: Build cloud-ready web applications using React 17 with Hooks and GraphQL", 2nd edition, 2017 Packt Publishing Limited.
3. Richard Haltman & Shubham Vernekar, "Complete node.js: The fast guide: Learn complete backend development with node.js"5th edition, 2017 SMV publication.
4. Glenn Geenen, Sandro Pasquali, Kevin Faaborg, "Mastering Node.js: Build robust and scalable real-time server-side web applications efficiently" 2nd edition Packt,2017 Publishing Limited.
5. Greg Lim," Beginning Node.js, Express & MongoDB Development, kindle edition,2019 international publishing.
6. Daniel Perkins, "ReactJS Master React.js with simple steps, guide and instructions" 3rd edition, 2015 SMV publication.
7. Peter Membrey, David Hows, Eelco Plugge, "MongoDB Basics", 2nd edition ,2018 International Publication.

Links: NPTEL/You Tube/Web Link:

https://youtu.be/QFaFIcGhPoM?list=PLC3y8-rFHvwgg3vaYJgHGnModB54rxOk3 https://youtu.be/pKd0Rpw7O48
https://youtu.be/TlB_eWDSMt4,
https://youtu.be/QFaFIcGhPoM

https://youtu.be/Kvb0cHWFkdc
https://youtu.be/pQcV5CMara8 https://youtu.be/c3Hz1qUUlyQ

https://youtu.be/Mfp94RjugWQ https://youtu.be/SyEQLbbSTWg
https://youtu.be/BLl32FvcdVM https://youtu.be/fCACk9ziarQ https://youtu.be/YSyFSnisip0 https://youtu.be/7H_QH9nipNs https://youtu.be/AX1AP83CuK4
https://youtu.be/2N-59wUIPVI https://youtu.be/hQcFE0RD0cQ https://youtu.be/UV16BbPcMQk https://youtu.be/fqMOX6JJhGo
https://youtu.be/m0a2CzgLNsc https://youtu.be/1ji_9scA2C4 https://youtu.be/tuIZok81iLk https://youtu.be/IluhOk86prA https://youtu.be/13FpCxCClLY