PROGRAMME: BCA (Bachelor of Computer Applications)- ISMA
SEMESTER – V

Teaching Learning and Evaluation Plan

Course Information:

Course Code: **24BCAIS5C01** Course Title: **ETHICAL HACKING**

Credits Units: **03** Contact Hours: **45** L-T-P-E: **3-0-0-3**

IA: ESE Weightage - **50: 50** Pass Marks (IA & ESE) **0:40(MIN ESE 18)** Aggregate Pass Marks: **40**

ESE Question Paper Marks: **50** Special Examination Fees: **NA** Pre-requisite (if any): **NA**

Course Facilitator (s): **Dr. Mahesh V, Associate Professor, School of CS and IT**

Programme Outcomes (POs)	
At the end of the programme, students will be able to	
PO 1	**Computational Knowledge:** Understand and apply mathematical foundation, computing, and domain knowledge for the conceptualization of computing models from defined problems.
PO 2	**Problem Analysis:** Ability to identify, critically analyze and formulate complex computing problems using fundamentals of computer science and application domains.
PO 3	**Design / Development of Solutions:** Ability to transform complex business scenarios and contemporary issues into problems, investigate, understand, and propose integrated solutions using emerging technologies.
PO 4	**Conduct Investigations of Complex Computing Problems:** Ability to devise and conduct experiments, interpret data and provide well informed conclusions.
PO 5	**Modern Tool Usage:** Ability to select modern computing tools, skills and techniques necessary for innovative software solutions.
PO 6	**Professional Ethics:** Ability to apply and commit professional ethics and cyber regulations in a global economic environment.
PO 7	**Life-long Learning:** Recognize the need for and develop the ability to engage in continuous learning as a Computing professional.
PO 8	**Project Management:** Ability to understand management and computing principles with computing knowledge to manage projects in multidisciplinary environments.
PO 9	**Communication Efficacy:** Communicate effectively with the computing community as well as society by being able to comprehend effective documentations and presentations.
PO 10	**Societal & Environmental Concern:** Ability to recognize economic, environmental, social, health, legal, ethical issues involved in the use of computer technology and other consequential responsibilities relevant to professional practice.
PO11	**Individual & Teamwork:** Ability to work as a member or leader in diverse teams in multidisciplinary environment.
PO12	**Innovation and Entrepreneurship**: Identify opportunities, entrepreneurship vision and use of innovative ideas to create value and wealth for the betterment of the individual and society.
Program Specific Outcomes (PSO's)	
PSO 1	**Demonstrate** a deep understanding of the fundamental concepts of information security, including cryptography, network security, and application security.
PSO 2	**Apply** information security principles and practices to the design, development, and testing of mobile applications.
PSO 3	Conduct security **assessments** to identify and prioritize vulnerabilities.
PSO 4	**Implement** and manage security measures to protect from cyber threats.

Course Objectives (COB's)

COB1	**Demonstrate** an understanding of ethical hacking principles and the role of an ethical hacker
COB2	**Identify** and analyze different types of malware and implement appropriate countermeasures
COB3	**Perform** footprinting, scanning, and enumeration to gather information and assess network vulnerabilities
COB4	**Apply** network intrusion techniques, execute system hacking, and maintain access to compromised systems

Course Outcomes (CO's)

Sl No	Course Outcome	Description	Bloom's Taxonomy Level
1	**CO 1**	To Describe ethical hacking and its significance in information security	**L2**
2	**CO 2**	To examine various types of malware, including viruses, trojans, and worms, along with their analysis techniques.	**L4**
3	**CO 3**	To Use skills in footprinting, scanning, and enumeration techniques for information gathering and vulnerability assessment.	**L3**
4	**CO 4**	To understand network intrusion methods, system hacking techniques, and methods for maintaining remote system access	**L2**
5	**CO 5**	To assess and mitigate web application security risks, including social engineering attacks and session hijacking	**L5**

CO-PO/PSO Mapping:

Course Outcome	Blooms Taxonomy Levels	Program Outcomes (PO's) Mapped												Program Specific Outcomes (PSO's)			
		PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1 L3	PSO2 L4	PSO3 L5	PSO4 L6
CO1	**L2**	2	1	-	1	-	2	3	-	1	2	-	1	**3**	**3**	**1**	**1**
CO2	**L3**	3	3	2	2	2	2	3	-	-	3	2	2	**2**	**1**	**3**	**2**
CO3	**L4**	3	3	3	2	2	3	3	2	-	3	3	3	**2**	**3**	**3**	**2**
CO4	**L5**	2	2	2	3	3	3	3	3	3	3	3	3	**1**	**3**	**3**	**3**
CO5	**L6**	3	3	3	2	3	3	3	2	-	3	3	3	**2**	**2**	**3**	**3**
CO Avg.		2.6	2.4	2.5	2	2.5	2.6	3	2.3	2	2.8	2.7	2.4	**2**	**2.4**	**2.6**	**2.2**

Course Contents:

Module	Details	Contact Hours
I	**Introduction to Ethical Hacking** Overview of Information Security Threat and Attack vectors. Introduction to Hacking: Types, phases & scope for Hacking. IS controls, Role of Ethical Hacker: Types of Hackers, Roles and Responsibilities Scope & limitations of hacking. Case-based practical learning.	9
II	**Viruses, Trojans, Malwares, and OS Level Attacks and Counter Measures. Malware Analysis.** Malware Overviews: Introduction to Malware, different Ways a Malware can Get into a System, Common Techniques Attackers Use to Distribute Malware on the Web, Components of Malware Virus Worm & Trojan Concepts Introduction to Viruses, Worms & Trojan: Types of Virus, Worms &Trojan, Fake Antiviruses, How Did Antivirus Works. Malware Analysis. Case-based practical learning.	9
III	**Footprinting, Scanning & Enumeration** Footprinting through Search Engines, Web Services: Information Gathering Using Google. Overview of network scanning, techniques to check live systems, open ports. Understanding Scanning and IDS Evasion techniques. Tools for vulnerability scan, IP spoofing & detection. Understanding enumeration and different techniques and tools for enumeration, SNMP enumeration and LADP Enumeration.	9
IV	**Network Intrusion & System Hacking** Types of intrusion, Non-Technical Intrusion, Technical Intrusion: Dos, types of DOS, DDOS, SQL Injection, Manual SQL Injection. Overview of CEH Hacking methodology, techniques to gain access to system, privilege escalation techniques. Creating and maintaining remote access to system. Case-based practical learning.	9
V	**Web Application Hacking:** Overview of OWASP Top 10 Application Security Risks, Sniffing and types, Understanding Social Engineering Attack, insider threats, impersonation. Session Hijacking-Application & Network level hijacking.. Case-based penetration testing report.	9

Text Books (TB):

TB-1	Learn Ethical Hacking: A Hands-on Introduction to Breaking in by Daniel Graham, No Starch Press (2nd November 2021).
TB-2	The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking, by RonaldL.Krutz, Russell Dean Vines, Wiley Publications, First Edition 2007.

Reference Books (RB):

RB-1	The Basics of Hacking and Penetration Testing Ethical Hacking and Penetration Testing Made Easy Book 2011
RB-2	The Fundamentals of Computer Security for Beginners by Guy Mckinnon, Twentygo Ltd (1 November 2020).
RB-3	Penetration Testing: A Hands-On Introduction to Hacking by Georgia Weidman, No Starch Press; 1st edition (14 June 2014).

Other Reading (OR):

OR-1	Introduction to Ethical Hacking - https://www.geeksforgeeks.org/introduction-to-ethical-hacking/?ref=lbp. [Access Timestamp: 21-12-2021: 12:15 PM].
OR-2	Hacking Methodologies - https://geek-university.com/ccna-security/hacking-methodology/. [Access Timestamp: 21-12-2021: 12:20 PM].
OR-3	Wireless Security - https://www.geeksforgeeks.org/wireless-security-set-1/. [Access Timestamp: 21-12-2021: 12:45 PM].
OR-4	IDS vs IPS vs Firewall - https://ipwithease.com/firewall-vs-ips-vs-ids/. [Access Timestamp: 21-12-2021: 12:50 PM]

Relevant Website (RW):

RW-1	Ethical Hacking Tutorial - https://www.javatpoint.com/ethical-hacking-tutorial.
RW-2	Penetration Testing Tutorial - https://www.tutorialspoint.com/penetration_testing/index.htm.
RW-3	A Step-by-Step Guide to Vulnerability Assessment - https://securityintelligence.com/a-step-by-step-guide-to-vulnerability-assessment/.
RW-4	How to Crack a Password - https://www.guru99.com/how-to-crack-password-of-an-application.html.
RW-5	SQL Injection Tutorial - https://portswigger.net/web-security/sql-injection.
RW-6	Pentesting WPA/WPA2 Encrypted WLAN - https://www.tutorialspoint.com/wireless_security/wireless_security_pentesting_wpa_wpa2_encrypted_wlan.htm.
RW-7	Physical Security Countermeasures - https://www.vskills.in/certification/tutorial/physical-security-countermeasures/.

RW-8	Penetration Testing – Report Writing - https://www.tutorialspoint.com/penetration_testing/penetration_testing_report_writing.htm.

Video Links (VL):

VL-1	Ethical Hacking in 8 Minutes - https://www.youtube.com/watch?v=XLvPpirlmEs
VL-2	Basics of Hacking -Enumeration - https://www.youtube.com/watch?v=9UFU6Y3c1qM
VL-3	What is Network Sniffing? - https://www.youtube.com/watch?v=gXTuTfOoFjg
VL-4	Dos vs DDoS Attacks - https://www.youtube.com/watch?v=c9EjuOQRUdg
VL-5	Web Application Penetration Testing with Nmap - https://www.youtube.com/watch?v=BBKPr76TSLI
VL-6	Powerful Hacking Tools Hackers use - that https://www.youtube.com/watch?v=4EKKi9Trfg4
VL-7	WiFi (Wireless) Password Security - WEP, WPA, WPA2, WPA3, WPS Explained - https://www.youtube.com/watch?v=WZaIfyvERcA
VL-8	Life Cycle of Virus- https://www.youtube.com/watch?v=gkgMyzyH75w
VL-9	Physical Attacks and Countermeasures - https://www.youtube.com/watch?v=iM0asy-5T74.
VL-10	The COMPLETE Linux Hardening, & Guide - Privacy Security ! https://www.youtube.com/watch?v=Sa0KqbpLye4.
VL-11	What is a Firewall? - https://www.youtube.com/watch?v=kDEX1HXybrU
VL-12	Pentest Reporting and Best Practices - https://www.youtube.com/watch?v=6QIrXgPGJhM
VL-13	What is Risk Mitigation? - https://www.youtube.com/watch?v=LaQFrpc5Xo8

MOOC Courses (MC):

Sr.No.	Platform	Topic	CO	Link	Duration
MC-1	LinkedIn Learning	Introduction to Ethical Hacking	C01	https://www.linkedin.com/learning/ethical-hacking-introduction-to-ethical-hacking	1 hour 31 min

MC-2	LinkedIn Learning	Ethical Hacking: Footprinting & Reconnaissance	CO1 CO2	https://www.linkedin.com/learning/ethical-hacking-footprinting-and-reconnaissance	1 hour 42 min
MC-3	LinkedIn Learning	Ethical Hacking: Denial of Service	CO2 CO3	https://www.linkedin.com/learning/ethical-hacking-denial-of-service-2	1 hour 39 min
MC-4	LinkedIn Learning	Ethical Hacking: Scanning Networks	CO2 CO3	https://www.linkedin.com/learning/ethical-hacking-scanning-networks	2 hours 2 min
MC-5	LinkedIn Learning	Hacking Web Servers and Web Applications	CO1 CO2 CO3	https://www.linkedin.com/learning/ethical-hacking-hacking-web-servers-and-web-applications/	1 hour 26 min
MC-6	LinkedIn Learning	Ethical Hacking: SQL Injection	CO2 CO3	https://www.linkedin.com/learning/ethical-hacking-sql-injection/	1 hour 39 min
MC-7	LinkedIn Learning	Ethical Hacking: Evading IDS, Firewalls, and Honeypots	CO2 CO3	https://www.linkedin.com/learning/ethical-hacking-evading-ids-firewalls-and- honeypots/	2 hours 12 min
Total MOOC Course integration with Certification					**12 hours 11 minutes**

Hardware/Software/Equipment (HSE):

HSE-1	Virtual Machine for virtual experimental lab setup - Virtual Box - https://download.virtualbox.org/virtualbox/6.1.22/VirtualBox-6.1.22-144080-Win.exe - VMWare- https://my.vmware.com/en/web/vmware/downloads/info/slug/desktop_end_user_computing/vmware_workstation_player/16_0.
HSE-2	Maltego Tool – https://maltego-downloads.s3.us-east-2.amazonaws.com/windows/MaltegoSetup.JRE64.v4.3.0.exe.

HSE-3	Recon-NG Framework - https://github.com/lanmaster53/recon-ng.
HSE-4	OSINT Framework - https://github.com/lockfale/OSINT-Framework.
HSE-5	NMAP Network Scanner - https://nmap.org/dist/nmap-7.92-setup.exe.
HSE-6	Metasploitable Framework - https://sourceforge.net/projects/metasploitable/files/latest/download.
HSE-7	Wireshark – Network Forensics - https://2.na.dl.wireshark.org/win64/Wireshark-win64-3.4.6.exe
HSE-8	Nessus Vulnerability Scanner - https://www.tenable.com/products/nessus/nessus-essentials.

Session-wise Planning:

Module	Session	Topic	TB/RB / OR/RW /VL/	Pedagogy/ Activity planned	CO	Mode of delivery
Bride Course	**Zero Lecture**	**Ethical Hacking Fundamentals**	**VL-1 to VL-5**	Blended Learning Approach		Synchronous-PPT Asynchronous- Video
I	1	Introduction to Ethical Hacking	TB-1 OR1 VL1	Open Discussion Session MCQ		Synchronous-PPT Ethical_Hacking_S1.pptx Asynchronous- Video
	2	Types,Role of Ethical Hacker: Types of Hackers	TB-1 OR1	Blended Learning		Interactive Lecture Ethical_Hacking_S2.pptx Synchronous-Video
	3	phases & scope for Hacking	TB-1 OR2 VL1	PPT with MCQ		Synchronous-PPT Ethical_Hacking_S3.pptx Asynchronous- Video
	4-5	Roles and Responsibilities Scope & limitations of hacking	TB-1 OR2	Comparative Graphic Chart	**CO1**	Synchronous-PPT Ethical_Hacking_S4.pptx Asynchronous- Video
	6-7	**Case Study-** Discovery of blue box by John Drapers	OR-2 RB-3 RW-	Real Case Analysis with assessment		Open Theory\Module1\EH-5.pptx Discussion/Debate
	8	**Activity-1-**	MC-1	Interactive &		Synchronous-Video

		MOOC Course on Introduction to Ethical Hacking		Assessment with Report		& Assessment Certification with Report
	9	**Activity-1**- MOOC Course on Ethical Hacking: Denial of Service	MC-2	Interactive & Assessment with Report	CO1 CO3	Synchronous-Video & Assessment Certification with Report
II	10	Introduction to Malware	TB-2, RB-1, OR-1, VL-2	Flipped Class with MCQ at the start of the class		Synchronous - Interactive https://docs.google.com/presentation/d/1VPrLYRGpxAGQrX92LkuzstRyqG7EdNFy/edit?usp=drive_link&ouid=107962573861317139245&rtpof=true&sd=true Video Lecture with Quiz
	11	Different Ways a Malware can Get into a System	TB-2 RB-1 OR-1 VL-2 VL3	Flipped Class with MCQ at the start of the class	CO2	Synchronous-Interactive https://docs.google.com/presentation/d/16zfnq0dhjPUOeWd4_Emx0Y87LhewyqYy/edit?usp=drive_link&ouid=107962573861317139245&rtpof=true&sd=true Video Lecture with Quiz
	12	Common Techniques Attackers Use to Distribute Malware on the Web,	TB-1	Blended Mode with Interactive Assessment		Synchronous – PPT https://docs.google.com/presentation/d/1Jn2mexErh3QEdgZGGF3JFk5m7GfYrzaf/edit?usp=drive_link&ouid=107962573861317139245&rtpof=true&sd=true

			OR-1			
	13	Components of Malware Virus Worm & Trojan Concepts	TB-1 OR-1	Comparative Chart		Synchronous – PPT https://docs.google.com/presentation/d/1SHtVKGzsN_HV8AKm1JFyyGSVtGAFOLoz/edit?usp=drive_link&ouid=107962573861317139245&rtpof=true&sd=true
	14	Fake Antiviruses, How Did Antivirus Works.	TB-1 OR-1	Comparative Chart		Synchronous – PPT https://docs.google.com/presentation/d/1zp0EPXDHH_-6KWLgcccfIfAZlFzH-cFn/edit?usp=drive_link&ouid=107962573861317139245&rtpof=true&sd=true
	15	How Did Antivirus Works.	TB-2 RB-1 OR-1 VL3	Blended Mode with Interactive Assessment		Synchronous- https://docs.google.com/presentation/d/1ra2nRaGilwkwfbwDLRqosIEKXquC4lDa/edit?usp=drive_link&ouid=107962573861317139245&rtpof=true&sd=true Interactive Video Lecture with Quiz

	16	Malware Analysis	TB-1 RB-3 OR-1 VL-2 MC5	Animation Demonstration , Explanation	CO 2	Synchronous-PPT https://docs.google.com/presentation/d/1f4oU97fzpgCMYFBX91isflcA0D7tOzME/edit?usp=drive_link&ouid=107962573861317139245&rtpof=true&sd=true Asynchronous- Video
	17	**Activity-1-** MOOC Course Certificate Footprinting & Reconnaissance	TB-1 RB-3 OR-1 VL-2 MC5	PPT Presentation & Classroom interaction		Synchronous-PPT Asynchronous- Video
	18	**Mini Project with MOOC** -Abstract Submission- **Ethical Hacking Topic**	RW-4 RW-5 RW-6 MC-5	Open & Close Discussion, Query Resolution, Monitoring	CO 1 CO 3 CO 4	Asynchronous- Video, PPT Assessment Certification on Completion

III	19	Footprinting through Search Engines, Web Services	TB-1, RB-2, OR-1, VL-2	Interactive Lecture, Demonstration		Synchronous - PPT, https://docs.google.com/presentation/d/1hfDVooyLWTqAhOygi2ovXSFo7V9sRIvS/edit?usp=drive_link&ouid=107962573861317139245&rtpof=true&sd=true Live Demo
	20	Information Gathering Using Google	TB-1, RB-2, OR-1	Practical Exercise, Case Studies		https://docs.google.com/presentation/d/1UvOKRyUJk3cIdJfXfBe4yt1pFogqiCO6/edit?usp=drive_link&ouid=107962573861317139245&rtpof=true&sd=true Synchronous - Lab

	21	Overview of Network Scanning	TB-1, RB-2, OR-2, VL-2	Interactive Lecture, Quiz		Synchronous - PPT, https://docs.google.com/presentation/d/1HNah72HaxNMptUE6yB-4FF3HQBAQhaBP/edit?usp=drive_link&ouid=107962573861317139245&rtpof=true&sd=true Quiz
	22	Techniques to Check Live Systems	TB-1, RB-2, OR-2	Practical Exercise		Synchronous - Lab
	23	Open Ports Detection	TB-1, RB-2, OR-2	Practical Exercise, Quiz		Synchronous - Lab
	24	Scanning and IDS Evasion Techniques	TB-1, RB-2, OR-3	Interactive Lecture, Quiz		Synchronous - PPT, https://docs.google.com/presentation/d/1Rr1aD-fdKUX1pxv43YvLGNMDQmuampnK/edit?usp=drive_link&ouid=107962573861317139245&rtpof=true&sd=true Quiz
	25	Tools for Vulnerability Scan, IP Spoofing & Detection	TB-1, RB-2, OR-3, VL-3	Hands-On Lab, Case Study		Synchronous - Lab, Case Study
	26	Scanning Networks	TB-1, RB-2, OR-3, VL-3	Interactive Lecture, Quiz		Synchronous - PPT, https://docs.google.com/presentation/d/1POGLQbV3Nb2ldNgK5B01CjVxzNsXID9s/edit?usp=drive_link&ouid=107962573861317139245&rtpof=true&sd=true Quiz
	27	Enumeration and Different Techniques	TB-1, RB-2, OR-3, VL-3	Hands-On Lab, Case Study		Synchronous - Lab, https://docs.google.com/presentation/d/1d8qwjmWcMP36lkumgGvzysXR8g9B5iZl/edit?usp=drive_link&ouid=107962573861317139245&rtpof=true&sd=true Case Study
IV	28	Types of Intrusion: Non-Technical, Technical	TB-1, RB-2, OR-1, VL-4	Interactive Lecture, Demonstration	CO4	Synchronous - PPT, https://docs.google.com/presentation/d/1rCDxwa7kmHqQQP6IEqF092c_LCfwwDne

						/edit?usp=drive_link&ouid=107962573861317139245&rtpof=true&sd=true Live Demo
	29	DoS and DDoS Attacks	TB-1, RB-2, OR-1, VL-4	Practical Exercise, Case Studies		Synchronous - Lab
	30	SQL Injection	TB-1, RB-2, OR-2, VL-5	Interactive Lecture, Quiz		Synchronous - PPT, https://drive.google.com/file/d/1pQLnlLeBiAyX_fqZMF2HQ489bJCFRfgM/view?usp=drive_link Quiz
	31	Manual SQL Injection	TB-1, RB-2, OR-2	Practical Exercise		Synchronous - Lab
	32	CEH Hacking Methodology	TB-1, RB-2, OR-2	Practical Exercise, Quiz		Synchronous - Lab
	33	Techniques to Gain Access to System	TB-1, RB-2, OR-3	Interactive Lecture, Quiz		Synchronous - PPT, https://www.javatpoint.com/gaining-access Quiz
	34	Privilege Escalation Techniques	TB-1, RB-2, OR-3, VL-3	Hands-On Lab, Case Study		Synchronous - Lab, Case Study
	35	Creating and Maintaining Remote Access	TB-1, RB-2, OR-3, VL-3	Interactive Lecture, Quiz		Synchronous - PPT, https://phoenixnap.com/blog/secure-remote-access Quiz
	36	Case-Based Practical Learning	TB-1, RB-2, OR-3, VL-3	Hands-On Lab, Case Study		Synchronous - Lab, Case Study
	37	Attacks on Web Servers	TB-1, RB-3, OR-2, VL-5	Interactive Lecture, Demonstration		Synchronous - PPT, Live Demo
	38	Web Server Vulnerability Exploits	TB-1, RB-3, OR-2	Practical Exercise, Case Studies		Synchronous - Lab
	39	Wireless Network Security	TB-2, RB-3, OR-3, VL-6	Interactive Lecture, Quiz		Synchronous - PPT, Quiz
	40	Wireless Encryption Techniques	TB-2, RB-3, OR-3	Practical Exercise		Synchronous - Lab
	41	Attacks on Wireless Networks	TB-2, RB-3, OR-3	Practical Exercise, Quiz		Synchronous - Lab
	42	WEP, WPA, WPA2 Cracking	TB-2, RB-3, OR-3	Interactive Lecture, Quiz		Synchronous - PPT, Quiz
	43	Tools for Wireless Network Hacking	TB-2, RB-3, OR-3, VL-6	Hands-On Lab, Case Study		Synchronous - Lab, Case Study
	44	Wireless Intrusion Detection Systems	TB-2, RB-3, OR-3, VL-6	Interactive Lecture, Quiz		Synchronous - PPT, Quiz
V	45	Case-Based Practical Learning	TB-2, RB-3, OR-3, VL-6	Hands-On Lab, Case Study	CO5	Synchronous - Lab, Case Study

Assessment Scheme: IA: UE – 50:50

Sl. No.	Assessment Instrument	Formative/ Summative	Frequency	Weightage (%)	CO
1.	Activity-1 -MOOC Courses	Formative	1	15	CO1, CO2, CO3, CO4, CO5
2.	Activity-2 -Mini Project-Case base study		1	15	CO3, CO4, CO5
3.	Class participation		-	5	-
4.	Internal Exam- 1		1	7.5	CO1, CO2
5.	Internal Exam- 2		1	7.5	CO3, CO4, CO5
6.	University Exam	Summative	1	50	CO1, CO2, CO3, CO4, CO5
	100				

Activity-1 structured plan to assess a 15-mark activity divided into:

1. **Coursera Certification (Part A – 7 Marks)**
2. **100 Days of Code (Part B – 8 Marks)**

Rubrics (Total: 15 Marks)
Part A: Coursera Certification (7 Marks)

Criteria	Excellent (7)	Good (5–6)	Average (3–4)	Poor (0–2)
Completion of course	Verified Certificate	No certificate		
Relevance to subject/domain	Highly relevant	Moderately relevant	Slightly relevant	Not relevant
Quality of course (rating, hours)	>4.5★, >10 hrs	3.5–4.5★, 5–10 hrs	<3.5★ or <5 hrs	Very low quality

2 Marks – Course Relevance
3 Marks – Completion Status with certificate
2 Marks – Quality (rating + duration)

Part B: 100 Days of Code (8 Marks)

Criteria	Excellent (7–8)	Good (5–6)	Average (3–4)	Poor (0–2)
Regularity (GitHub or Log Proof)	90–100 days	70–89 days	40–69 days	<40 days
Project/Code quality (optional check)	Documented + Functional	Basic implementation	Irregular/Low quality	Incomplete
Daily log or GitHub commits	Consistent commits/logs	Moderate consistency	Gaps	No proof

3 Marks – Proof of Consistency (GitHub, screenshots, logs)
3 Marks – Code Quality / Project Outcome
2 Marks – Reflection / Learning Outcome

Marks Distribution sheet

Roll No	Name	Course Name	Certificate Submitted	Course Duration	Part A Marks (7)	Days Logged	GitHub/Proof	Part B Marks (8)	Total (15)	Remarks
				(hrs)		(out of 100)	Link/Screenshot			

Activity-2 structured plan to assess a 15-mark activity divided into:

Case study and Research paper

Rubric: Case Study (5 Marks)

Criteria	Excellent (5)	Good (3–4)	Average (2)	Poor (0–1)
Relevance to Subject	Highly relevant and insightful	Relevant with minor gaps	Partially relevant	Not relevant
Depth of Analysis	Thorough and well-reasoned analysis	Good analysis with some limitations	Basic analysis with weak justification	Very weak or no analysis
Presentation & Clarity	Clear structure, well-written	Adequate structure and clarity	Some clarity issues	Poorly presented

Rubric: Research Paper (10 Marks)

Criteria	Excellent (9–10)	Good (7–8)	Average (4–6)	Poor (0–3)
Originality & Innovation	Very original with new insights	Some originality, mostly derivative	Low originality	Copied or no originality
Technical Depth / Literature Review	Strong technical depth with rich literature	Good depth and adequate literature	Superficial technical content	Lacks technical merit
Formatting & Citations	Follows all academic formats (APA/IEEE)	Minor formatting issues	Formatting inconsistencies	No proper format or citations
Language & Presentation	Highly professional language and structure	Well written with minor flaws	Average language and presentation	Weak writing and presentation

Marks Distribution sheet

Roll No	Name	Case Study Title	Case Study Submitted (Yes/ No)	Case Study Relevance (Excellent/ Good/Average/Poor)	Case Study Marks (out of 5)	Research Paper Title	Paper Submitted (Yes/ No)	Paper Quality (Excellent/Good/ Average/ Poor)	Originality / Plagiarism Check (Yes/No)	References Used (APA/IEEE/None)	Research Paper Marks (out of 10)	Total Marks (out of 15)	Remarks