Course File

Faculty	:	Applied Computing
Department	:	BCA
School	:	School of computer science & IT
Program	:	BCA
Program Level	:	UG
Course Title	:	ETHICAL HACKING
Course Code	:	23BCA5I01
Academic Year	:	2026-2027
Semester	:	V
Semester Start Date	:	21 July 2026
Course Coordinator	:	Ms Adlin jebakumari
Course Coordinator email ID	:	j.adlin@jainuniversity.ac.in
Faculty member Name	:	Dr Mahesh V
Faculty member designation	:	Associate professors
Faculty member email ID	:	v.mahesh@jainuniversity.ac.in

Teaching Learning and Evaluation Plan (TLEP)

I) Program Details

Department	:	Computer science & IT
School	:	Computer science & IT
Program	:	BCA

1. Program Educational Objectives:

PEO 1	**Technical Proficiency and Problem-Solving** Demonstrate expertise in solving complex problems using modern computing tools.
PEO 2	**Lifelong Learning and Adaptability** Engage in lifelong learning to adapt to technological advancements**.**
PEO 3	**Ethical and Responsible Leadership** Exhibit ethical behavior and contribute to sustainable development.
PEO 4	**Effective Communication and Teamwork** Demonstrate strong communication skills and teamwork.
PEO 5	**Research and Innovation** Pursue research and entrepreneurial ventures in computing technologies.

2. Program Outcomes (POs) and Program Specific Outcomes (PSOs):

PO01	**Foundation Knowledge** Apply mathematical concepts and programming fundamentals to develop solutions for IT systems and applications.
PO02	**Problem Analysis** Analyze and interpret IT requirements to identify, formulate, and solve computational problems using standard practices.
PO03	**Design Development of Solutions** Design and develop IT solutions, including software and applications, to address real-world challenges.
PO04	**Modern Tool Usage** Use modern Computing tools and techniques necessary for innovative technological solutions.
PO05	**Individual and Teamwork** Work effectively both as an individual and as part of a team in multidisciplinary IT projects.
PO06	**Project Management** Apply project management principles and agile methodologies to plan, schedule, and execute IT projects.
PO07	**Ethics and Social Responsibility** Demonstrate ethical practices in IT solutions, including data privacy, cyber security, and sustainable development.
PO08	**Life-long Learning** Engage in continuous learning through certifications, workshops, and industry-relevant training to adapt to emerging technologies.
PO09	**Entrepreneurship and Innovation**

	Demonstrate innovation and entrepreneurial skills by identifying opportunities to create IT solutions for business and societal needs.
PSO01	**Demonstrate** a deep understanding of the fundamental concepts of information security, including cryptography, network security, and application security.
PSO02	**Apply** information security principles and practices to the design, development, and testing of mobile applications.
PSO03	Conduct security **assessments** to identify and prioritize vulnerabilities.

II) Course Details

Course Title	:	ETHICAL HACKING
Course Code	:	23BCA5I01
Credits	:	3
L-T-P-E	:	3-0-0-3
Notional Learning Hours	:	0
Contact Hours	:	45
Semester	:	V
Course Category	:	Discipline Elective
Contribution to Major/Minor	:	NA
Course Type	:	Theory
CA:ESE	:	50:50
CA Pass Percentage	:	0
ESE Pass Percentage	:	40
Aggregate Pass Marks	:	40

1. Nature and Orientation of Course

a. Percentage of the course that is oriented towards:

Skills	:	75
Entrepreneurship	:	20
Employability	:	05

b. Percentage of the course that is relevant towards the development needs

Globally	:	45
Nationally	:	30
Regionally	:	25
Locally	:	10

c. Percentage of the course that is oriented towards

Indian Knowledge Systems	:	**05 %**

Sustainable Development Goals (SDGs) *(Please specify which SDG)*	**:**	DG 4 – Quality Education (Cybersecurity knowledge and skill development) SDG 8 – Decent Work and Economic Growth (Cybersecurity employment and workforce development) SDG 9 – Industry, Innovation and Infrastructure (Secure digital infrastructure and innovation) **SDG 16 – Peace, Justice and Strong Institutions (Cybersecurity, cybercrime prevention, digital trust, and secure institutions)**
Emerging Technologies *(E.g. AI)*	**:**	1. Artificial Intelligence (AI) for Cybersecurity 2. Machine Learning-based Threat Detection 3. Generative AI and LLM Security 4. Cloud Security and Cloud Penetration Testing 5. Internet of Things (IoT) Security 6. Edge Computing Security 7. Blockchain Security 8. Zero Trust Security Architecture 9. Extended Detection and Response (XDR) 10. Security Orchestration, Automation and Response (SOAR) 11. Threat Intelligence Platforms 12. Quantum-Safe Cryptography 13. Digital Forensics and Incident Response (DFIR) 14. DevSecOps and Secure Software Development 15. Container and Kubernetes Security

2. Course Objectives

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

3. Course Outcomes and Bloom's Taxonomy

CO	Course Outcome	BT Level	Attainment Threshold
CO01	Describe ethical hacking and its significance in information security	**L2**	60
CO02	Examine various types of malwares, including viruses, trojans, and worms, along with their analysis techniques.	**L4**	60
CO03	Use skills in footprinting, scanning, and enumeration techniques for information gathering and vulnerability assessment.	**L3**	60
CO04	Demonstrate network intrusion methods, system hacking techniques, and methods for maintaining remote system access	**L3**	60
CO05	Assess and mitigate web application security risks, including social engineering attacks and session hijacking	**L5**	60

4. CO: PO Mapping

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PSO1	PSO2	PSO3
CO1	2	1	-	1	-	2	3	-	1	**3**	**3**	**1**
CO2	3	3	2	2	2	2	3	-	-	**2**	**1**	**3**
CO3	3	3	3	2	2	3	3	2	-	**2**	**3**	**3**
CO4	2	2	2	3	3	3	3	3	3	**1**	**3**	**3**
CO5	3	3	3	2	3	3	3	2	-	**2**	**2**	**3**
Articulation	2.6	2.4	2.5	2	2.5	2.6	3	2.3	2	**2**	**2.4**	**2.6**

5. Syllabus

Module	Topics	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

Reference Books:

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

III) **Session Plan**

Cohort/Section	CTIS/ISMA-V Sem
Faculty Member	Mahesh V

Innovative Pedagogies Planned – if Any

1. **Case-Based Learning (CBL)** – Analysis of real-world cyber attacks, malware incidents, data breaches, and penetration testing reports.
2. **Problem-Based Learning (PBL)** – Solving cybersecurity challenges involving vulnerability assessment, malware detection, and network security.
3. **Project-Based Learning** – Mini-projects on vulnerability scanning, web application security testing, and security auditing.
4. **Experiential Learning** – Hands-on ethical hacking exercises in controlled lab environments using industry-standard tools.
5. **Simulation-Based Learning** – Cyber attack and defense simulations, capture-the-flag (CTF) exercises, and virtual cyber ranges.
6. **Gamification** – Cybersecurity challenges, quizzes, and ethical hacking competitions to enhance engagement.

Session no.	Module No.	Topic	L-T-P-E Component	Mode of Delivery	Pedagogical Tool / Engagement	Reading Material	CO
1	I	Introduction to Ethical Hacking	L	PPT	Open Discussion	TB-1, OR-1, VL-1	CO1
2	I	Types of Hackers and Ethical Hacker Roles	L	Interactive Lecture	Blended Learning	TB-1, OR-1	CO1
3	I	Phases and Scope of Hacking	L	PPT	PPT with MCQ	TB-1, OR-2, VL-1	CO1
4	I	Roles of Ethical Hackers	L	PPT	Comparative Chart	TB-1, OR-2	CO1
5	I	Responsibilities and Limitations of Hacking	L	PPT	Comparative Chart	TB-1, OR-2	CO1
6	I	Case Study: John Draper and Blue Box	T	Discussion	Case Analysis	OR-2, RB-3	CO1
7	I	Ethical Hacking Case Assessment	T	Discussion	Debate & Assessment	OR-2, RB-3	CO1
8	I	MOOC Activity: Ethical Hacking Fundamentals	E	Video	Interactive Learning	MC-1	CO1
9	I	MOOC Activity: DoS Attack Concepts	E	Assessment	Certification Activity	MC-2	CO1, CO3
10	II	Introduction to Malware	L	Interactive Lecture	Flipped Classroom	TB-2, RB-1, OR-1, VL-2	CO2
11	II	Malware Entry Mechanisms	L	Interactive Lecture	Quiz-Based Learning	TB-2, RB-1, OR-1	CO2
12	II	Malware Distribution Techniques	L	PPT	Interactive Assessment	TB-1, OR-1	CO2
13	II	Virus, Worm and Trojan Concepts	L	PPT	Comparative Chart	TB-1, OR-1	CO2
14	II	Fake Antivirus and Malware Trends	L	PPT	Comparative Chart	TB-1, OR-1	CO2

15	II	Antivirus Working Principles	L	Interactive Video	Blended Learning	TB-2, RB-1, OR-1	CO2
16	II	Malware Analysis Fundamentals	P	PPT & Demo	Animation Demonstration	TB-1, RB-3, OR-1	CO2
17	II	Footprinting & Reconnaissance MOOC	P	PPT & Video	Classroom Interaction	TB-1, RB-3, OR-1	CO2
18	II	Mini Project: Ethical Hacking Topic	E	Assessment	Project-Based Learning	RW-4, RW-5, RW-6	CO1, CO3, CO4
19	III	Footprinting through Search Engines	L	PPT	Interactive Lecture	TB-1, RB-2, OR-1	CO3
20	III	Information Gathering Using Google	P	Lab	Practical Exercise	TB-1, RB-2, OR-1	CO3
21	III	Overview of Network Scanning	L	PPT	Interactive Quiz	TB-1, RB-2, OR-2	CO3
22	III	Techniques to Check Live Systems	P	Lab	Hands-On Practice	TB-1, RB-2, OR-2	CO3
23	III	Open Port Detection	P	Lab	Practical Exercise	TB-1, RB-2, OR-2	CO3
24	III	IDS Evasion Techniques	L	PPT	Interactive Lecture	TB-1, RB-2, OR-3	CO3
25	III	Vulnerability Scanning Tools	P	Lab	Hands-On Lab	TB-1, RB-2, OR-3	CO3
26	III	Network Scanning Techniques	L	PPT	Interactive Quiz	TB-1, RB-2, OR-3	CO3
27	III	Enumeration Techniques and Tools	P	Lab	Case Study	TB-1, RB-2, OR-3	CO3
28	IV	Types of Intrusion	L	PPT	Interactive Lecture	TB-1, RB-2, OR-1	CO4
29	IV	DoS and DDoS Attacks	P	Lab	Practical Exercise	TB-1, RB-2, OR-1	CO4
30	IV	SQL Injection Fundamentals	L	PPT	Quiz-Based Learning	TB-1, RB-2, OR-2	CO4

31	IV	Manual SQL Injection	P	Lab	Hands-On Exercise	TB-1, RB-2, OR-2	CO4
32	IV	CEH Hacking Methodology	P	Lab	Practical Demonstration	TB-1, RB-2, OR-2	CO4
33	IV	Techniques to Gain System Access	L	PPT	Interactive Lecture	TB-1, RB-2, OR-3	CO4
34	IV	Privilege Escalation Techniques	P	Lab	Case Study	TB-1, RB-2, OR-3	CO4
35	IV	Creating and Maintaining Remote Access	L	PPT	Interactive Quiz	TB-1, RB-2, OR-3	CO4
36	IV	Network Intrusion Case Study	P	Lab	Case-Based Learning	TB-1, RB-2, OR-3	CO4
37	V	Attacks on Web Servers	L	PPT	Interactive Lecture	TB-1, RB-3, OR-2	CO5
38	V	Web Server Vulnerability Exploits	P	Lab	Practical Exercise	TB-1, RB-3, OR-2	CO5
39	V	OWASP Top 10 Security Risks	L	PPT	Interactive Lecture	TB-1, RB-3, OR-3	CO5
40	V	Sniffing and Types of Sniffing	P	Lab	Practical Demonstration	TB-1, RB-3, OR-3	CO5
41	V	Social Engineering Attacks	L	PPT	Case-Based Discussion	TB-1, RB-3, OR-3	CO5
42	V	Insider Threats and Impersonation	L	PPT	Scenario Analysis	TB-1, RB-3, OR-3	CO5
43	V	Session Hijacking Concepts	P	Lab	Hands-On Exercise	TB-1, RB-3, OR-3	CO5
44	V	Application and Network-Level Hijacking	P	Lab	Case Study	TB-1, RB-3, OR-3	CO5
45	V	Penetration Testing Report Preparation & Case Study	E	Presentation & Assessment	Project-Based Learning	TB-1, RB-3, OR-3	CO5

IV) Evaluation Plan

Innovative Assessments Planned (If any)

1. MOOC-Based Assessment -25%
2. Quiz and MCQ-Based Evaluation- 25%
3. Capture the Flag (CTF) Challenges- 50%

Component	Assessment Type	Formative/Summative	Weightage	CO1	CO2	CO3	CO4	CO5	Total
CA1	**MCQ Test**	**F**	**10**	5	7	-	-	-	12
CA2	**Mid – Term**	**F**	**10**	-	5	2.5	2.5	-	10
CA3	**Class Participation**	**F**	**03**	0.6	0.6	0.6	0.6	0.6	3
CA4	**Preparatory exam**	**F**	**10**	2	2	2	2	2	10
CA5	**Class Activity**	**S**	**15**	-	5	2.5	2.5	5	15
Total CA			**50**	**7.6**	**19.6**	**7.6**	**7.6**	**7.6**	**50**

ESE		**S**	**50**						

CA: Instructions and Rubrics

CA1:

Instructions to students / Description of Assessment Component

1. MOOC-Based Assessment – 25%
Evaluation based on the successful completion of relevant MOOCs (e.g., SWAYAM, NPTEL, Coursera, edX, Udemy, FutureLearn) aligned with the course outcomes. Assessment may include course completion certificates, assignment scores, discussion participation, reflective reports, and application-based activities demonstrating knowledge gained through the online course.

2. Quiz and MCQ-Based Evaluation – 25%
Continuous assessment through periodic quizzes and multiple-choice question (MCQ) tests designed to evaluate conceptual understanding, analytical thinking, problem-solving ability, and application of course concepts. Assessments may be conducted online or offline and include module-wise quizzes, surprise tests, and comprehensive MCQ examinations.

Rubrics:

1. MOOC-Based Assessment – 25%

Criteria	85–100% (Excellent)	65–85% (Very Good)	50–65% (Satisfactory)	40–50% (Limited)	<40% (Poor)
Course Completion	Successfully completes the MOOC with distinction/high score and submits all required evidence.	Completes the MOOC with good performance and submits required evidence.	Completes most course requirements with acceptable performance.	Partial completion with several missing requirements.	Fails to complete the MOOC or provide evidence.
Assignment Performance	Achieves excellent scores in MOOC assignments and activities.	Achieves above-average scores in assignments.	Meets minimum assignment requirements.	Low assignment performance with frequent errors.	Poor or no assignment submission.
Reflection and	Demonstrates deep	Demonstrates good	Shows basic understandi	Minimal understandi	No meaningful

Learning Application	understanding and excellent application of learned concepts to real-world scenarios.	understanding and application of concepts.	ng with limited application.	ng and weak application.	reflection or application demonstrated.
Participation and Engagement	Actively participates in discussions, forums, and learning activities.	Regular participation in learning activities.	Occasional participation.	Limited participation.	

3. **Quiz and MCQ-Based Evaluation – 25%**

Criteria	**85–100% (Excellent)**	**65–85% (Very Good)**	**50–65% (Satisfactory)**	**40–50% (Limited)**	**<40% (Poor)**
Quiz Performance	Scores consistently above 85% in quizzes and MCQ assessments.	Scores between 65%–85% in most assessments.	Scores between 50%–65% in assessments.	Scores between 40%–50% in assessments.	Scores below 40% in assessments.
Consistency and Preparation	Demonstrates excellent preparation and consistent performance throughout the course.	Demonstrates good preparation and regular performance.	Demonstrates moderate preparation and performance.	Inconsistent preparation and performance.	Poor preparation and inconsistent participation.

CA2:

Instructions to students / Description of Assessment Component

3. Capture the Flag (CTF) Challenges – 50%
Assessment based on participation and performance in cybersecurity-oriented Capture the Flag (CTF) challenges. Students will solve practical security problems involving areas such as cryptography, web security, network security, digital forensics, reverse engineering, vulnerability analysis, and ethical hacking. Evaluation will consider challenge completion, problem-solving approach, technical accuracy, innovation, teamwork (where applicable), and submission of detailed solution reports demonstrating the methodologies used to identify and exploit or mitigate security vulnerabilities.

Rubrics:

Criteria	**85–100% (Excellent)**	**65–85% (Very Good)**	**50–65% (Satisfactory)**	**40–50% (Limited)**	**<40% (Poor)**
Challenge Completion	Successfully solves most or all assigned CTF challenges across multiple domains with high accuracy.	Solves a majority of challenges with good accuracy.	Solves a moderate number of challenges with acceptable accuracy.	Solves only a few challenges with limited success.	Unable to solve challenges or demonstrates minimal progress.
Technical Skills and Accuracy	Demonstrates excellent technical proficiency in identifying, analyzing, and exploiting or mitigating vulnerabilities.	Demonstrates strong technical skills with minor inaccuracies.	Demonstrates adequate technical skills and understanding.	Demonstrates limited technical competency with frequent errors.	Demonstrates poor technical understanding and execution.
Problem-Solving and Analytical Approach	Employs innovative, systematic, and efficient approaches to solve complex security challenges.	Uses effective problem-solving techniques for most challenges.	Demonstrates basic analytical and problem-solving abilities.	Shows limited analytical thinking and problem-solving capability.	Unable to apply appropriate problem-solving methods.
Documentation and Solution Reporting	Provides comprehensive, well-structured reports with detailed methodologies, screenshots, and clear explanations.	Provides clear and organized reports with sufficient technical details.	Provides basic documentation covering key steps and findings.	Documentation is incomplete or lacks clarity and detail.	Documentation is missing or inadequate.
Time Management and	Demonstrates exceptional self-learning ability,	Shows strong independent learning	Demonstrates adequate self-learning and meets	Requires significant guidance and	Shows little initiative and fails to complete

Independent Learning	initiative, and timely completion of challenges.	and completes tasks on time.	most deadlines.	misses some deadlines.	tasks within the stipulated time.