

**SES's L.S. RAHEJA COLLEGE OF ARTS AND COMMERCE
(AUTONOMOUS)**



BOARD OF STUDIES: Information Technology and Data Science
PROGRAMME: Bachelor of Commerce (Banking and Insurance)
SEMESTER: IV
NOMENCLATURE OF THE COURSE: ETHICAL HACKING
NEP Vertical: OE
Credit: 02

(As Per Choice Based Credit System (under NEP 2020) with effect from the academic year 2025-26)



Programme:	Bachelor of Commerce (Banking and Insurance)
Nomenclature of the Course	Ethical Hacking
Total Marks	50
Semester:	IV
Academic year	2025-26

LEARNING OBJECTIVES:

1. To understand the ethics, legality, methodologies and techniques of hacking.
2. To describe various approaches and steps of ethical hacking.
3. To implement enterprise security techniques to prevent systems from hacking.

COURSE OUTCOMES:

1. Identify and describe various ethical hacking methodologies
2. Demonstrate a clear understanding of the ethical, legal, and professional frameworks that govern hacking
3. Distinguish between ethical and unethical hacking practices.
4. Design and implement security protocols and solutions to protect systems from potential cyber threats and vulnerabilities.

Unit	Course Content	Andragogy	No of Lectures
I	<p>1.1 Introduction: Black Hat vs. Gray Hat vs. White Hat (Ethical) hacking, Why is Ethical hacking needed?, How is Ethical hacking different from security auditing and digital forensics?, Signing NDA, Compliance and Regulatory concerns, Black box vs. White box vs. Black box, Vulnerability assessment and Penetration Testing.</p> <p>1.2 Approach: Planning - Threat Modeling, set up security verification standards, Set up security testing plan – When, which systems/apps, understanding functionality, black/gray/white, authenticated vs. unauthenticated, internal vs. external PT, Information gathering, Perform Manual and automated (Tools: WebInspect/Qualys, Nessus, Proxies, Metasploit) VA and PT, How WebInspect/Qualys tools work: Crawling/Spidering, requests forging, pattern. Enumeration techniques, Scanning, Sniffing matching to known vulnerability database and Analyzing results, Preparing report, Fixing security gaps following the report</p>	<ul style="list-style-type: none"> • Task or problem centred • Give students problems: Provide problems for students to solve independently or in groups. • Encourage self-directed learning: Allow students to choose their learning methods and materials. • Use real-life examples: Incorporate real-life examples into lessons. 	15
II	<p>2.1 Enterprise Security Phases : Gaining and Maintaining Access : Systems hacking – Windows and Linux – Metasploit and Kali Linux, Keylogging, Buffer Overflows, Privilege Escalation, Network hacking - ARP Poisoning, Password Cracking, WEP Vulnerabilities, MAC Spoofing, MAC Flooding, IPspoofing, SYN</p>	<ul style="list-style-type: none"> • Task or problem centred • Give students problems: Provide problems for 	15

	<p>Flooding, Smurf attack 2.2 Applications hacking : SMTP/Email-based attacks, VOIP vulnerabilities, Directory traversal, Input Manipulation, Brute force attack, Unsecured login mechanisms, SQL injection Case Study : Google Hacking (GHDB) and Doxing</p>	<p>students to solve independently or in groups.</p> <ul style="list-style-type: none"> • Encourage self-directed learning: Allow students to choose their learning methods and materials. • Use real-life examples: Incorporate real-life examples into lessons. 	
--	---	---	--

SUGGESTED READINGS

1. Certified Ethical Hacker Study Guide v9, Sean-Philip Oriyano, Sybex; Study Guide Edition, 2016
2. CEH official Certified Ethical Hacking Review Guide, Wiley India Edition, 2007
3. Certified Ethical Hacker: Michael Gregg, Pearson Education, 1st Edition, 2013

QUESTION PAPER PATTERN

(A) FOR CONTINUOUS EVALUATION

Particulars	Marks
Presentation/Viva Voce/Quiz	10
Assignment/Project	10
Total	20

(B) QUESTION PAPER PATTERN FOR SEMESTER END EXAMINATION

Question No.	Description	Total Marks
Q. 1	Attempt the following Unit I	15
A	Remembering	
B	Analysing	
C	Applying	
	OR	
P	Remembering	
Q	Analysing	
R	Applying	
Q. 2	Attempt the following Unit II	
A	Understand	
B	Applying	
C	Evaluating	
	OR	
P	Understand	
Q	Applying	
R	Evaluating	