GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Bachelor of Engineering
Level: UG
Subject Code : 3174802
Course / Subject Name : Ethical Hacking

w. e. f. Academic Year:	A.Y. 2025-26
Semester:	VII
Category of the Course:	**PCC**

Prerequisite :	**Basic knowledge of Networking, Operating Systems, and Security Principles.**
Rationale:	This course introduces students to the methodologies and tools used in ethical hacking and penetration testing. Students will explore real-world scenarios to understand attacker behavior and learn defensive strategies to protect IT infrastructure. The curriculum provides a balanced perspective on ethical responsibilities and the legal landscape in cybersecurity.

Course Outcome:
After Completion of the Course, Student will able to:

No	Course Outcomes	RBT Level
1	Understand ethical hacking concepts, roles, and legal aspects.	U
2	Apply footprinting, scanning, and enumeration techniques.	Ap
3	Identify vulnerabilities and perform basic penetration tests.	An
4	Analyze malware behavior, web/mobile threats, and develop countermeasures.	E
5	Understand the use of IDS, firewalls, and honeypots in system defense.	U

**Revised Bloom's Taxonomy (RBT)*

Teaching and Examination Scheme:

Teaching Scheme (in Hours)			Total Credits L+T+ (PR/2)	Assessment Pattern and Marks				Total Marks
				Theory		Tutorial / Practical		
L	T	PR	C	ESE (E)	PA / CA (M)	PA/CA (I)	ESE (V)	

4	0	2	5	70	30	20	30	150

Course Content:

Unit No.	Content	No. of Hours
1.	**Introduction to Ethical Hacking**: Security fundamentals, security testing, differences between hackers and crackers, legal considerations, and ethical guidelines in hacking	05
2.	**The Technical Foundations of Hacking**: The attacker's process, the ethical hacker's methodology, system security layers and the stack.	05
3	**Footprinting and Scanning**: Techniques for information gathering, identifying network ranges, detecting active machines, open ports, and OS fingerprinting	08
4	**Vulnerability Assessment and Penetration Testing**: Importance of vulnerability assessment, risk mitigation, and regulatory compliance.	05
5.	**Enumeration and System Hacking**: Techniques of enumeration, system hacking methodologies, DoS and DDoS attacks, and sniffers.	06
6.	**Malware Threats:** Types of malware including viruses, worms, Trojans; covert communications; keystroke logging and spyware; countermeasures.	06
7.	**Sniffers, Session Hijacking and Denial of Service:** Network sniffing, session hijacking strategies, and denial of service threats.	06
8.	**Web Server, Application, and Database Hacking:** Exploiting web servers and applications, attacking databases, and web session hijacking.	06
9.	**Wireless Technologies and Mobile Security:** Wireless protocols, vulnerabilities in WLANs, mobile device security, and pentesting for mobile systems.	06
10.	**IDS, Firewalls and Honeypots:** Overview of Intrusion Detection Systems, firewall types and configurations, and the role of honeypots.	06

Suggested Specification Table with Marks (Theory):

Distribution of Theory Marks (in %)					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
–	**18**	**28**	**22**	**17**	**15**

Where U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create (as per Revised Bloom's Taxonomy)

References/Suggested Learning Resources:

(a) Books:

Text Books

1. James S. Tiller, “The Ethical Hack: A Framework for Business Value Penetration Testing”, Auerbach Publications, CRC Press
2. EC-Council, “Ethical Hacking and Countermeasures Attack Phases”, Cengage Learning
3. Michael Simpson, Kent Backman, James Corley, “Hands-On Ethical Hacking and Network Defense”, Cengage Learning.
4. Hacking For Dummies, 6ed by Kevin Beaver - John Wiley Publication
5. Digital Forensic by Dr. Nilakshi Jain - John Wiley Publication

References:

1. Certified Ethical Hacker, Version 9, Second Edition, Michael Gregg, Pearson IT Certification.
2. Hacking the Hacker, Roger Grimes, Wiley.
3. The Unofficial Guide to Ethical Hacking, AnkitFadia, Premier Press.

Sample List of Experiments:

1. Perform footprinting using tools like Whois, NSLookup, and Maltego.
2. Scan for open ports using Nmap and identify services.
3. Conduct OS fingerprinting using Xprobe or Nmap.
4. Simulate a simple DoS attack in a lab environment.
5. Perform enumeration using SNMP, NetBIOS tools.
6. Explore and analyze malware using a sandbox environment.
7. Capture and analyze network packets using Wireshark.
8. Simulate session hijacking using tools like Ettercap.
9. Pen test a web application for SQL injection and XSS.
10. Configure a basic firewall and IDS using open-source tools.
11. Analyze mobile app traffic for security loopholes.
12. Deploy and test a honeypot using Honeyd or Kippo.

****