GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Master of Engineering

Level: PG

Branch: Cyber Security

Subject Code : ME02059031

Subject Name : Ethical Hacking

w. e. f. Academic Year:	2024-25
Semester:	2
Category of the Course:	Professional Elective Course

Prerequisite:	**Computer Network, Internetworking concepts.**
Rationale:	• The course will explore the knowledge of attacks and Indicator of Compromises for the system. • The course will focus on gathering information at a different level through which a system can be compromised and countermeasures to make it secure. • The course will also cover advanced attacks based on AI

Course Outcome:

After Completion of the Course, Student will able to:

No	Course Outcomes	RBT Level
01	To outline the Indicator of Compromise for the system.	UN
02	To apply the attack plan which covers Plan, organize and perform penetration testing on a simple network.	AN
03	To analyze different models & techniques for securing the systems.	AP
04	To differentiate the tools to conduct ethical hacking as per the CEH modules.	AP
05	Critiquing how the red team and blue team process in terms to compromise the system and to defend the system as per IOC	EL

**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)	
03	00	02	04	70	30	20	30	150

GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Master of Engineering

Level: PG

Branch: Cyber Security

Subject Code : ME02059031

Subject Name : Ethical Hacking

Course Content:

Unit No.	Content	No. of Hours	% of Weightage
1	Unit-I: An Introduction to Ethical Hacking: Security Fundamental, Security testing, Hacker and Cracker, Descriptions, Test Plans-keeping It legal, MITRE ATT&CK framework, Threat Intelligence and Tools like CTM360, Trend Micro, Prisma etc.	04	10
2	Unit-II: The Technical Foundations of Hacking: The Attacker's Process, The Ethical Hacker's Process, Security and the Stack.	04	10
3	Unit-III: Footprinting and scanning: Information Gathering, Determining the Network Range, Identifying Active Machines, Finding Open Ports and Access Points, OS Fingerprinting Services, Mapping the Network Attack Surface	06	15
4	Unit-IV: Enumeration, System Hacking and Malware Threats: Enumeration, System Hacking, Viruses and Worms, Trojans, Covert Communication, Keystroke Logging and Spyware, Malware Countermeasures.	06	15
5	Unit-V: Web Server attacks and its Security Sniffers, Session Hijacking, Denial of Service, Distributed Denial of Service, Web Server Hacking, Web Application Hacking, Database Hacking, Web Server Countermeasures, Google Dorking.	08	20
6	Unit-IV: Network Security, Wireless Technologies, Mobile Security and Attacks Intrusion Detection Systems, Firewalls, Honeypots, Wireless Technologies, Mobile Device Operation and Security, Wireless LANs, Physical Security, Social Engineering, Metasploit.	09	20
7	Unit-VII: Current Trends The latest technology attacks with AI and its countermeasures	06	10
	TOTAL	**45**	**100**

Suggested Specification Table with Marks (Theory):

Distribution of Theory Marks (in %)					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
10	**20**	**20**	**20**	**20**	**10**

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

References/Suggested Learning Resources:

(a) Books:

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, Ankit Fadia, Premier Press

(b) Open source software and website:

1. Course-related online MOOC on SWAYAM NPTEL/Coursera Platform.
2. Recently published papers/articles of reputed journals/conferences.s

Suggested Course Practical List:

- List of Laboratory/Learning Resources Required: The practical work will be carried out based on the content covered during the academic sessions.

List of Laboratory/Learning Resources Required: SANS, NIST, DFIR websites etc.

Suggested Project List: Creation of local network and its security projects.

* * * * * * *