NIRMA UNIVERSITY

Institute:	Institute of Technology
Name of Programme:	BTech CSE, Integrated BTech (CSE)-MBA, BTech CSE (Artificial Intelligence & Machine Learning)
Course Code:	XXXX
Course Title:	Ethical Hacking and Vulnerability Assessment
Course Type:	Department Elective–I
Year of Introduction:	2024-25

L	T	Practical Component				C
		LPW	PW	W	S	
3	0	2	-	-	-	4

Course Learning Outcomes (CLO):

At the end of the course, students will be able to –

1. summarise the core concepts related to malware, hardware, and software vulnerabilities and their causes (BL2) (BL3)
2. choose state-of-the-art tools to exploit the vulnerabilities related to the computer system and networks (BL4)
3. survey various tools to exploit web applications (BL6)
4. solve the security issues in web applications.

Unit	Contents	Teaching Hours (Total 45)
Unit-I	**Introduction to Ethical Hacking:** Information Security Overview, Hacking Methodologies and Frameworks, Hacking Concepts	05
Unit-II	**Footprinting and Reconnaissance:** Footprinting Concepts, types of Footprinting, scanning the networks, Enumeration	10
Unit-III	**Wi-Fi security dangers and protections:** Wireless Concepts, Wireless Encryption, Wireless Threats, Wireless Hacking Methodology, Wireless Hacking Tools, Wireless Attack Countermeasures	10
Unit-IV	**Hacking Web Applications:** System Hacking, Malware Threats, Sniffing, Web Server Attack Countermeasures, Web Application Security, Cloud Security	10
Unit-V	**Vulnerability Analysis:** Vulnerability Assessment Concepts, Vulnerability Classification and Assessment Types, Vulnerability Assessment Tools, Vulnerability Assessment Reports, Mitigation Techniques	10

Self-Study:

The self-study contents will be declared at the commencement of the semester. Around 10% of the questions will be asked from self-study content

Suggested Readings/ References:

1. David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni, Metasploit: The Penetration Tester's Guide, No Starch Press
2. Harpreet Singh, Himanshu Sharma, Hands-On Web Penetration Testing with Metasploit: The subtle art of using Metasploit 5.0 for web application exploitation, Packt Publishing

3. John Slavio Hacking: A Beginners' Guide to Computer Hacking, Basic Security, And Penetration Testing, independently published
4. Samir Kumar Rakshit, Ethical Hacker's Penetration Testing Guide, BPB Publications

Laboratory Work:
Laboratory work will be based on the above syllabus with a minimum of 10 experiments to be incorporated. The students in a suitable group size will design and perform one experiment as a part of Laboratory work.

Sr. No.	List of Experiments/Exercises	Hours
1	Setting Lab Environment -Virtual machine of Kali linux, Vulnerable OS	02
2	To gather information about a target organization or domain using various reconnaissance techniques and tools- write the python code	04
3	To perform network scanning using Nmap to identify open ports, services, and potential vulnerabilities in a target network.	04
4	Write a python code to enumerate network services and find useful information.	02
5	Implementing the Buffer Overflow Attacks on web server	04
6	Implement the Metasploit Exploit on network resources or web servers	02
7	Developing a simple application and performing various OWASP attacks on the application	04
8	Implementing the Windows Privilege Escalation	02
9	Impalement Wi-Fi hacking with tools or own script.	02
10	Use Vulnerability Assessment Tool/s and prepare and study the report	04