NIRMA UNIVERSITY

Institute:	Institute of Technology
Name of Programme:	MTech CSE (Cyber Security)
Course Code:	6CS461
Course Title:	Hacking and Counter Hacking
Course Type:	(☐ Core/ ☐ Value Added Course / √ **Department Elective** / ☐ Institute Elective/ ☐ University Elective/ ☐ Open Elective / ☐ Any other)
Year of Introduction:	2022-23

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

Course Learning Outcomes (CLOs):
At the end of the course, the student will be able to –
1. summarize the core concepts related to system security and software vulnerabilities and their causes (BL2)
2. examine security and trust in hardware (BL4)
3. choose state-of-the-art tools to exploit the vulnerabilities related to computer system and networks (BL5)
4. solve the security issues in computer systems (BL6)

Syllabus: **Total Teaching hours: 45**

Unit	Syllabus	Teaching hours
Unit-I	**Introduction to Practical Security** Introduction to Practical Computer Security, The Computer Security Environment Today, Security Frameworks, CIA, PKI, Cryptocurrency	10
Unit-II	**Cyber Threats and Hacking** Threats and Attacks, Network based attacks, Client and Server-side attacks, OWASP Top 10 attacks, Penetration testing using Kali Linux	10
Unit-III	**Detecting and Mitigating Cyber Threats and Attacks** Introduction to Intrusion Detection and Prevention, Firewalls, Vulnerability assessment, Vulnerability Scanning, Attack graphs	10
Unit-IV	**Proactive Computer Security** Defence in Depth, Securing and hardening systems: Bastille, CIS, MS Baseline, GDPR	10
Unit-V	**Hardware Security and Protection** Hardware implementation of Hash and RSA, Hardware Metering, Side channel attacks and counter measures, Hardware Trojan detection	05

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

Suggested Readings/ References:	1. William Stallings Network Security Essentials: Applications and Standards, Prentice Hall
	2. Gus Khwaja, Practical Web Penetration Testing, O'Reilly
	3. Open Web Application Security Project, OWASP Top 10: The Top 10 most critical web application security threats
	4. An Adams, T Thompson and A Khan, Ethical Hacking: Beginner to Advance Bundle, Code Academy
	5. Ebook: Modern Defense In-Depth, A Briefing on Cyber Security in the Era of Cloud (oracle.com)
	6. Stephen Gates, Modern Defense in Depth: An integrated approach to better web application security, O'Reilly
	7. Debdeep Mukhopadhyay, Rajat Subhra Chakraborty, Hardware Security: Design, Threats and Safeguards, CRC Press

Suggested List of Experiments:	Sr. No.	Title	Hours
	1	Setting up the Virtual Environment with Kali Linux, Windows and Metasploitable	02
	2	Implementing the Buffer Overflow Attacks	04
	3	Implementation of various OWASP Top 10 attacks on DVWA application	04
	4	Demonstrating the BurpSuite Tool	02
	5	Implementing the Metasploit Exploit	02
	6	Developing a simple application and performing various OWASP attacks on the application	04
	7	Implementing User Profile based application	04
	8	Implementing the Windows Privilege Escalation	04
	9	Developing a secured application	04