NIRMA UNIVERSITY

Institute:	Institute of Technology
Name of Programme:	Master of Computer Application (2-Years Programme)
Course Code:	3MCAD361
Course Title:	Cyber Security and Cyber Laws
Course Type:	Departmental Elective
Year of Introduction:	2021-22

Credit Scheme

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. understand the need for computer security
2. analyze the vulnerabilities in the computer system
3. design system to handle simple cyber attacks
4. understand the legal aspects to handle cyber-crimes and cyber frauds

Syllabus: **Total Teaching hours: 45**

Unit	Syllabus	Teaching hours
Unit-I	**Overview:** Computer Security concepts, Threats, Attacks and Assets, Security Functional Requirements, Scope of Computer Security, Cryptographic tools	06
Unit-II	**User Authentication:** Mechanisms of Authentication, Password - based Authentication, Token based Authentication, Biometric Authentication, Remote User Authentication **Access Control:** Access Control Principles, Subjects, Objects and Access Rights, DAC	07
Unit-III	**Database Security:** DBMS, RDBMS, Database Access Control, Inference, Statistical Databases, Database Encryption	04
Unit-IV	**Malware:** Types, Viruses, Virus attacks, Virus Countermeasures, Worms, Bots, Rootkits, Trojans **Denial of Service Attacks:** Introduction, Flooding Attacks, Distributed Denial of Service Attacks, Reflector and Amplifier Attacks, Defenses against Denial of Service Attacks and Responding	06
Unit-V	**Trusted Computing and Multilevel Security:** Bell-La Padula Model for Computer Security, Biba Model, Clark Wilson Integrity Model, Discretionary Access Control, Graham Denning Model, Mandatory Access Control, Concept of Trusted Systems, Application of multilevel security, Security Modes of Operation, Take Grant Protection Model, trusted computing and trusted platform module, common criteria for IT Security Evaluation	09

Unit-VI	**Buffer Overflow:** Stack Overflow, Defending against buffer overflows, and other forms of overflow attacks **Other Software Security Issues:** Software Security Issues, Handling Program Input, Writing safe program code, interacting with the operating system and other programs, handling program input	06
Unit-VII	**Developing Secure Web Applications:** Design Issues, Deployment Considerations, input validation, authentication, authorization, Configuration management, sensitive data, session management, Parameter Manipulation, Exception Management, Auditing and Logging **Secured Communication:** IPSec, Secured Socket Layer, Transport Layer Security, Secured Shell	04
Unit-VIII	**Cyber Crimes and Cyber Laws:** Introduction to IT laws & Cyber Crimes – Internet, Hacking, Cracking, Viruses, Virus Attacks, Pornography, Software Piracy, Intellectual property, Legal System of Information Technology, Social Engineering, Mail Bombs, Bug Exploits, and Cyber Security, IT Act 2000	03

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 and Lawrie Brown, Computer Security Principles and Practices, Pearson Education
2. Pfleeger and Pfleeger, Security in Computing, Pearson Education.
3. Raghu Santanam, Sethumadhavan, Mohit Virendra, Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives, IGI Global.
4. Chris Davis, IT Auditing Using controls to protect Information Assets, TMH.

Suggested List of Experiments:

Sr. No.	Title	Hours
1.	To learn various network commands and use them to analyze network performance	04
2.	To retrieve information under communication between various nodes using Wireshark tool	02
3.	To write a simple socket program for sending and receiving messages	04
4.	To implement Key exchange scheme using Diffie Hellman in Practical 3	02
5.	To encrypt the file using simple encrypting schemes and key 1) Getting Started with Cloud KMS (0.5) 2) Cloud IAM: Qwik Start (0.3) 3) Cloud Security Scanner: Qwik Start (0.2)	04
6.	To implement the Buffer Overflow Attacks and VPC network Controlling Access using Qwiklabs	04

	7.	To develop a Secured Database through - User authentication using hashing mechanism	04
	8.	To secure the data stored in database using suitable encryption mechanism	02
	9.	To implement the RSA Algorithm	02
	10.	To study various open source/free tools for hacking and identify mechanisms to overcome the issue	02
Suggested Case List:	-NA-		