FOUR YEAR GRADUATE PROGRAMME (FYUGP) IN CYBER SECURITY
DETAILED SYLLABUS OF 3RD SEMESTER

Course Code	:	**SEC331**
Title of the Course	:	**Cyber Security Management**
Nature of Course	:	**Skill Enhancement Course (SEC)**
End Semester	:	**60 Marks**
In Semester	:	**40 Marks**
Course Credit	:	**03**

COURSE OBJECTIVES:

- To equip students with the technical knowledge and skills needed to protect and defend against cyber threats.
- To develop skills in students that can help them plan, implement, and monitor cyber security mechanisms to ensure the protection of information technology assets.
- To expose students to responsible use of online social media networks.
- To systematically educate the necessity to understand the impact of cyber-crimes and threats with solutions in a global and societal context.

Unit	Topic	L	T	P	Total
1 **(12 Marks)**	**Network Fundamentals:** Introduction to Networks • Type of Networks OSI Layer Architecture • IP Addressing • Subnetting • Working of Switch • VLAN, Working of Router Routing Protocols, Basic Network Protocols Wireshark	6	1	8	15
2 **(12 Marks)**	**Server Administration Fundamentals:** Introduction to Operating System • Manage Identity • Plan Desktop and device deployment • Plan and implement Microsoft Active Directory Manage Networks, storage, data access & protection Manage remote access, Apps, updates & recovery OS password Recovery	6	1	8	15
3 **(12 Marks)**	**Security Fundamentals:** Security Jargons • Confidentiality, Integrity and Availability • Vulnerability threat and Risk • Cyber Kill Chain Type of Threat Vectors & Threat Actors Industries prone to Cyber Attacks	3	1	0	4
4 **(12 Marks)**	**Cryptography:** Introduction • Symmetric Cryptography • Asymmetric cryptography Hashing	2	1	1	4

	Ethical Hacking:	4	1	2	7
5 **(12 Marks)**	Introduction • Introduction to Ethical Hacking • Foot printing and Reconnaissance • Scanning Networks Enumeration Vulnerability Analysis System Hacking, Malware Threats • What is Web Application Security Testing and VA/PT? • VA through Tools, Kali overview Penetration testing and CTF challenges Auditing, Compliance and Monitoring				
	Total	21	05	19	45

Where,   *L: Lectures*   *T: Tutorials*   *P: Practicals*

MODES OF IN-SEMESTER ASSESSMENT: **(40 Marks)**
- Two In-Semester (Sessional) Examinations   = 20 Marks
- Evaluation will be based on the following: = 20 Marks
  - ➢ Conduction of test
  - ➢ Practical Note Book
  - ➢ Performance in the laboratory

COURSE OUTCOMES:

After the completion of thiscourse, the learner will be able to -

CO 1: Analyze and evaluate the cyber security needs of an organization.

CO 2: Analyze software vulnerability and Security Solutions to reduce the risk of exploitation.

CO 3: Measure the performance and troubleshoot cyber security systems.

CO 4: Explore the ethical hacking features and opportunities.