Subject Code: 01CE0604

Subject Name: – Cyber Security

B.Tech. Year - III

Objective: Objective of this course that provides students basic knowledge and skills in the fundamental theory and practical of Cyber Security.

Credits Earned: 05 Credits

Course Outcomes

- Understanding the basic technical, social and law suits aspect of Cyber Security (Remember)
- Integrate the ethical hacking process and scripting. (Create)
- The students can use basic security tools to enhance cyber security. (Analyse)
- Understand the security management methods and auditing. (Evaluation)
- Apply the security principles to system design. (Apply)

Pre-requisite of course: NA.

Teaching and Examination Scheme

Teaching Scheme (Hours)			Credits	Theory Marks			Tutorial/ Practical Marks		Total Marks
Theory	Tutorial	Practical		ESE (E)	Mid Sem (M)	Internal (I)	Viva (V)	Term work (TW)	
4	0	2	5	50	30	20	25	25	150

Contents:

Unit	Topics	Contact Hours
1	**Introduction:** Introduction to Cyber Security, Importance and challenges in Cyber Security, Cyberspace, Cyber threats, Cyberwarfare, CIA Triad, Cyber Terrorism, Cyber Security of Critical Infrastructure, Cybersecurity - Organizational Implications.	11
2	**Hackers and Cyber Crimes:** Types of Hackers, Hackers and Crackers, Cyber-Attacks and Vulnerabilities, Malware threats, Sniffing, Gaining Access, Escalating Privileges, Executing Applications, Hiding Files, Covering Tracks, Worms, Trojans, Viruses, Backdoors.	11
3	**Ethical Hacking and Social Engineering:** Ethical Hacking Concepts and Scopes, Threats and Attack Vectors, Information Assurance, Threat Modelling, Enterprise Information Security Architecture, Vulnerability Assessment and Penetration Testing, Types of Social Engineering, Insider Attack, Preventing Insider Threats, Social Engineering Targets and Defence Strategies.	12
4	**Cyber Forensics and Auditing:** Introduction to Cyber Forensics, Computer Equipment and associated storage media, Role of forensics Investigator, Forensics Investigation Process, Collecting Network based Evidence, Writing Computer Forensics Reports, Auditing, Plan an audit against a set of audit criteria, Information Security Management System Management. Introduction to ISO 27001:2013	11
5	**Cyber Ethics and Laws:**	11

	Introduction to Cyber Laws, E-Commerce and E-Governance, Certifying Authority and Controller, Offences under IT Act, Computer Offences and its penalty under IT Act 2000, Intellectual Property Rights in Cyberspace.	
	Total Hours	56

References:

1. Donaldson, S., Siegel, S., Williams, C.K., Aslam, A., Enterprise Cybersecurity -How to Build a Successful Cyberdefense Program Against Advanced Threats, A-press
2. Nina Godbole, SumitBelapure, Cyber Security, Willey
3. Hacking the Hacker, Roger Grimes, Wiley
4. Cyber Law By Bare Act, Govt Of india, It Act 2000.

Suggested Theory distribution:

The suggested theory distribution as per Bloom's taxonomy is as per follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

Distribution of Theory for course delivery and evaluation				
Remember	Apply	Analyse	Evaluate	Create
20%	25%	20%	15%	20%

Suggested List of Experiments:

1. Install VM Workstation in Ubuntu and set up windows and kali.
2. Set up nginx and provide password credentials with Secure Socket Layer.
3. Write a program to sniff packet sent over the local network.
4. To perform DNS Pharming attack using any method on computers in a LAN Environment.
5. Implement system hacking using tools.
6. Create virus with python script and implement attack and analyse the effect of various viruses.
7. Sniffing Website Credentials using Social Engineering Toolkit.
8. Study and Audit Marwadi University IT Infrastructure.