FACULTY OF COMPUTER APPLICATIONS
Bachelor of Science-IT

- **Sem.** : 6
- **Subject Code** : 05BS0603
- **Subject** : Cyber Security
- **Course Objectives**:
  1. To understand the fundamental concepts of Cyber Security.
  2. Student should understand cyber-attack, types of cybercrimes.
  3. To understand different methodologies of attacks and prevention.
  4. To understand usage of different cybercrime and security tool.
  5. To understand legal aspect of Cyber Crime and Security.

Prerequisites : Basic knowledge of computers, Internet, operating system and Networking.

Unit No	Topics Covered	No of lectures required
1	**Introduction to Cyber Security** Cybercrime and origins of the world, Cybercrime and information security, Classifications of cybercrime, Cybercrime and the Indian ITA- 2000, A global Perspective on cybercrimes.	12
2	**Cyber offenses** How criminal plan the attacks, Social Engineering, Cyber stalking, Cyber café and Cybercrimes, Botnets, Attack vector	08
3	**Phishing and Identity Theft** Introduction, Phishing: Methods of Phishing, Phishing Techniques, Spear Phishing, Types of Phishing Scams, Phishing Toolkits and Spy Phishing, Phishing Countermeasures Identity Theft (ID Theft): Personally, Identifiable Information (PII), Types of Identity Theft, Techniques of ID Theft, Identity Theft-Countermeasures, How to Protect your Online Identity.	12
4	**Systems and Network Vulnerability Scanning** Overview of vulnerability scanning, Open Port/ Service Identification, Banner / Version Check, Traffic Probe, Vulnerability Probe, Vulnerability Examples, OpenVAS,	14

	Networks Vulnerability Scanning - Netcat, Socat, understanding Port and Services tools - Datapipe, Fpipe, WinRelay, Network Reconnaissance – Nmap, THC-Amap and System tools. Network Sniffers and Injection tools – Tcpdump and Windump, Wireshark, Ettercap, Hping.	
5	**Tools and Methods Used in Cybercrime** Introduction, Proxy Servers and Anonymizers, Password Cracking, Virus and Worms, Trojan Horses and Backdoors, Steganography, DoS and DDoS Attacks, SQL Injection. **Cybercrimes and Cybersecurity: The Legal Perspectives** Introduction, Why Do We Need Cyberlaws: The Indian Context, The Indian IT Act, Challenges to Indian Law and Cybercrime Scenario in India, Consequences of Not Addressing the Weakness in Information Technology Act, Amendments to the Indian IT Act, Cybercrime and Punishment. Digital Personal Data Protection (DPDP) Act, 2023 – Salient Features.	**14**

Course Outcomes:

1. Demonstrate understanding of basic concepts in cyber security
2. Analyze threats and risks within context of the cyber security architecture.
3. Examine the performance and troubleshoot Network and Cyber security systems.
4. Make use of various tools and methods used in cybercrime
5. Evaluate cyber activities which are considered as crime as per IT Act.

Course Outcomes – Program Outcomes Mapping Table:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1				H		M	M	L
CO2				H		M	M	L
CO3	H	H	H	M		H	M	H
CO4	H	H	H	M		H	M	H
CO5	L			H			M	

FACULTY OF COMPUTER APPLICATIONS
Bachelor of Science-IT

Text Book:

1. "Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Nina Godbole and Sunit Belpure, Wiley Publication, 1st Edition.
2. "Anti-Hacker Tool Kit (Indian Edition)", Mike Shema, Mc Graw Hill Publication, 4th Edition.

Reference Book:

1. "Cyber Security Essentials", James Graham, Richar Howard, Ryan Olson, CRC Press, Tailor and Francis Group, 1st Edition.
2. "Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions", Kenneth J. Knapp, IGI Global, 2009-1st Edition.
3. Cyber Security and Cyber Laws Paperback", Alfred Basta, Nadine Basta, Mary Brown, Ravinder Kumar, Cengage publication, 1st Edition.

Web References :

4. https://www.sans.org/cybersecurity
5. https://www.tecmint.com/
6. https://www.meity.gov.in/content/cyber-laws

Syllabus Coverage from Main reference:

Unit #	Chapter Numbers
1	Book 1 Chapter 1
2	Book 1 Chapter 2
3	Book 1 Chapter 5
4	Book 2: Chapter 4: 4.1 and 4.2, Chapter 7, 8, 9 ,10.1 to 10.5
5	Book 1 Chapter 4: 4.1 to 4.10, Chapter 6

Marwadi University

FACULTY OF COMPUTER APPLICATIONS
Bachelor of Science-IT

PRACTICALS

Practical No.	Problem Definition
1.	Installation of Kali operating system in virtual box and explore different utilities provided by the operating system.
2.	Explore google hacking database and perform different operational searching techniques.
3.	Perform following linux commands: ifconfig Command ip Command ifup Command ethtool Command ping Command traceroute Command netstat Command nc/netcat Command nmap Command host Command dig Command nslookup Command tcpdump Command FTP Command Netstat Command
4.	Perform network scanning using Nmap GUI or Linux Terminal: Basic options for scanning techniques (i.e. -sS, -sT, -sU and -sA)
5.	Perform network scanning using Nmap GUI or Linux Terminal: Perform host discovery using Nmap possible options.
6.	Perform network scanning using Nmap GUI or Linux Terminal: Perform port specification options using Nmap.
7.	Perform network scanning using Nmap GUI or Linux Terminal: Perform service version and OS detection using possible options of Nmap.
8.	TCP / UDP connectivity using Netcat.
9.	Perform Network vulnerability using OpenVAS.
10.	Perform steganography using kali tool.
11.	Perform password cracking using kali tool.
12.	Perform different attacks using DVWA.
13.	Implement different GHDB searching techniques.
14.	Perform DoS attack using LOIC GUI tool.

15.	Perform SQLInjection using SqlMap tool.