Kadi Sarva Vishwavidyalaya

Faculty of Engineering & Technology

Fourth Year Bachelor of Engineering (Computer/IT)

(To be Proposed For: Academic Year 2021-22)

Subject Code: CT702-N	Subject Title: Cyber Security
Pre-requisite	Computer Networks and Cryptography & network security

Teaching scheme				Total Credit	Evaluation Scheme					Total Marks
L	T	P	Total		Theory		IE Marks	CIA Marks	Pract. Marks	
Hrs	Hrs	Hrs	Hrs		Hrs	Marks				
03	00	02	05	04	03	70	30	20	30	150

LEARNING OBJECTIVES:

- Identify the malicious activities taking place in their system/network.
- Protect themselves from the cyber attacks.
- Understand ethics behind hacking and vulnerability discovery.
- Gain the knowledge of cyber laws and find their importance

OUTLINE OF THE COURSE:

Sr. No	Title of the Unit	Minimum Hours
1	Introduction to Cyber Crime	5
2	Information Security Concepts	5
3	Phishing and Identity Theft	6
4	Security Threats and Vulnerabilities	6
5	Privacy control concept	7
6	Access Control and Intrusion Detection	5
7	Cybercrimes and Cyber Security: The Legal Perspectives	5
8	Legal, Ethical and Professional Issues in Information Security	5
9	Hands on Open source	4

Total hours (Theory): 48
Total hours (Lab): 32
Total hours: 80

DETAILED SYLLABUS:

Sr. No	Topic	Lecture Hours	Weightage (%)
1	**Introduction to Cyber Crime** Cyber Crime and Information Security, Classification of Cyber crime-E-mail Spoofing, Spamming, Internet Time Theft, Salami Attack, Data Hacking, Credit Card Frauds, Identity Theft, Password Sniffing, Software Piracy, Web Jacking, Forgery, Online Frauds.	5	10
2	**Information Security Concepts** Information Security Overview , Information Security Services , Goals for Security, E-commerce security, Computer Forensics, Digital Forensics Science, Digital Forensics Life Cycle.	5	10
3	**Phishing and Identity Theft** Methods of Phishing, Phishing Techniques, Spear phishing, Types of phishing scams, Phishing Toolkits and Spy Phishing, Phishing Countermeasures, Identity Theft, Types and Techniques of identity thefts and its counter measures.	6	13
4	**Security Threats and Vulnerabilities** Overview of Security threats, Attacks, Hacking Techniques, Insecure Network connections.	6	13
5	**Privacy Control Concept** What is Privacy? Methods to control Privacy, Data Collection from Social Networks, Challenges, Opportunities and pitfalls in securities, Credibility and reputation in social system. Privacy policing and preserving. Information Privacy disclosure, revelation and its effect in OSM and networks.	7	15
6	**Access Control and Intrusion Detection** Overview of Authentication and Authorization, Overview of Intrusion Detection System, IDS Types and Detection Models, IDS Features and Intrusion Prevention Systems.	5	10
7	**Cybercrimes and Cyber Security: The Legal Perspectives** Indian Context, The Indian IT Act –Positive Aspect of the ITA 2000, Weak Areas of ITA 2000.	5	10
8	**Legal, Ethical and Professional Issues in Information Security** Laws and Ethics in information Security, Relevant US Laws, Ethics and Information Security, Codes of Ethics and Professional Organization.	5	10

9	**Hands on Open source.** IPV4, IPV6, IP assigning, MAC, Bridging, Raid protocols, Linux remote connection: (Remote login, transfer file), Remote session(OpenSSh Configuration), Logs introduction, log files(Messages, dmesg, Audit log), cron.	**4**	**9**
	Total	**48**	**100**

Instructional Method and Pedagogy: (Continuous Internal Assessment (CIA) Scheme)

- At the start of course, the course delivery pattern, prerequisite of the subject will Be discussed.
- Lectures will be conducted with the aid of multi-media projector, black board, OHP etc.
- Attendance is compulsory in lecture and laboratory which carries 10 marks in overall evaluation.
- One internal exam will be conducted as a part of internal theory evaluation.
- Assignments based on the course content will be given to the students for each unit and will be evaluated at regular interval evaluation.
- Surprise tests/Quizzes/Seminar/tutorial will be conducted having a share of five marks in the overall internal evaluation.
- The course includes a laboratory, where students have an opportunity to build an appreciation for the concepts being taught in lectures.
- Experiments shall be performed in the laboratory related to course contents

Learning Outcome:

At the end of the course the students will be able to do following:

- Trace Back the Intrusion/Hacking.
- Responding to the Cyber Crime
- Preserving and creating controlled environment for Digital evidence.

REFERENCE BOOKS:

- ✓ Rhodes-Ousley, Mark. Information Security: The Complete Reference, Second Edition, . Information Security Management: Concepts and Practice. New York, McGraw-Hill, 2013.
- ✓ Whitman, Michael E. and Herbert J. Mattord. Roadmap to Information Security for IT and InfoSec Managers. Boston, MA: Course Technology, 2011.
- ✓ Cyber Security, by Nina Godbole and Sunit Belapure, Wiley Publication
- ✓ Gray Hat Hacking: The Ethical Hackers' Handbook, Shon Harris, Allen Harper, Chris Eagle and Jonathan Ness, TMH Edition .

LIST OF PRACTICAL:

Sr. No.	Name of experiment
1	To study about cyber security and analysis intruders and threats.
2	To study Linux advance commands for cyber security.
3	Implementation of methods using Phishing Toolkits
4	Implementation of methods penetration techniques.
5	Implementation of methods to Controls to enforce security services
6	Hardening OS by IP Tables Implementations.
7	Server Configuration for security.
8	To study about cyber security and analysis intruders and threats.
9	To analysis Insecure Network connections by different tools.
10	Identifying security breach in Social Medial network.