

CAP791:SECURING NETWORK AND IT INFRASTRUCTURE-LABORATORY

Course Outcomes: Through this course students should be able to

CO1 :: study the need of system security concepts issues in computer security and user authentication mechanisms

CO2 :: explain some common need and issues of software and application level security

CO3 :: demonstrate of the working of cryptographic algorithms

CO4 :: analyze the underlying vulnerabilities of Network Security

List of Practicals / Experiments:

System Security

- Internet Attacks
- Authentication of a User or Program
- Ethical Issues in Computer Security
- Access Control
- File Protections in a Unix or Windows File System

Security and Cryptography

- Private Key and Public Key Cryptographic Systems
- Classical Encryption Techniques: Substitution and Transposition
- Encryption and Decryption of RSA – Public Key Cryptography Algorithm
- Intrusion detection System (IDS) Tool

Application Security

- Protecting and Securing MS Office Products
- Protect your PC by Creating User Accounts and Passwords
- Types of Malicious Codes
- Passwords Cracking Techniques
- Avoid viruses and other Malware on one's PC

Network Security

- Wireless Network Components
- Mobile Security Apps
- Firewall Security in Windows
- Security of Web Browser
- Vulnerabilities for Hacking a Web Applications

Text Books: 1. SECURITY IN COMPUTING by CHARLES P. PFLEEGER, PEARSON

References: 1. COMPUTER SECURITY: PRINCIPLES AND PRACTICE by WILLIAM STALLINGS AND LAWRIE BROWN, PEARSON