CSCO 462 – INTRODUCTION TO CYBER SECURITY

Course Objective:

The objective of the courses to

1) Understand the fundamental s of cyber security and cyber crimes.
2) Understand the tools and methods in cybercrimes and understanding computer forensics.

UNIT - I

INTRODUCTION TO CYBERCRIME [1st TEXTBOOK]

Cybercrime- Definition and Origins of the WordCybercrime and Information Security, Who are Cybercriminals? Classifications of Cybercrimes, A Global Perspective on Cybercrimes, Cybercrime Era: Survival Mantra for the Netizens. (1.2-1.5,1.9,1.10)

Cyberoffenses: How Criminals Plan Them:How Criminals Plan the Attacks, Social Engineering, Cyberstalking, Cybercafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Attack Vector, Cloud Computing. (2.2-2.8)

CYBERCRIME:

Mobile and Wireless Devices:Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication Service Security, Attacks on Mobile/Cell Phones, Mobile Devices: Security Implications for organizations, Organizational Measures for Handling Mobile, Organizational Security Policies and Measures in Mobile Computing Era, Laptops. (3.13.12) **12 Hours**

UNIT - II

TOOLS AND METHODS USED IN CYBERCRIME

Introduction, Proxy Servers and Anonymizers, Phishing, Password Cracking, Keyloggers and Spywares, Virus and Worms, Trojan-horses and Backdoors, Steganography, DoS and DDoS At-tacks, SQL Injection, Buffer Overflow, Attacks on Wireless Networks. (4.1-4.12)

Phishing and Identity Theft: Introduction to Phishing, Identity Theft (ID Theft). (5.2,5.3)

UNDERSTANDING COMPUTER FORENSICS

Introduction, Digital Forensics Science, The Need for Computer Forensics, Cyber forensics and Digital Evidence, Forensics Analysis of E-Mail, Digital Forensics Life Cycle, Chain of Custody Concept, Network Forensics, Approaching a Computer Forensics Investigation, Setting up a Computer Forensics Laboratory: Understanding the Requirements, Computer Forensics and Steganography, Relevance of the OSI 7 Layer Model to Computer Forensics. (7.1,7.3-7.13) **12 Hours**

UNIT - III

Forensics and Social Networking Sites: The Security/Privacy Threats, Computer Forensics from Compliance Perspective, Challenges in Computer Forensics, Special Tools and Techniques, Forensics Auditing, Antiforensics. (7.14-7.19)

INTRODUCTION TO SECURITY POLICIES AND CYBER LAWS [2nd Textbook]

Need for An Information Security Policy, Information Security Standards – ISO, Introducing Various Security Policies and Their Review Process, Introduction to Indian Cyber Law, Objective and Scope of the IT Act, 2000, Intellectual Property Issues, Overview of Intellectual Property Related Legislation in India, Patent, Copyright, Law Related to Semiconductor Layout and Design, Software License. (4.1-4.11)

12 Hours

Course Outcome:

At the end of the course student will be able to

1) Understand the basic concepts of cyber security and cyber crimes.
2) Understand the security policies and cyber laws.

TEXTBOOKS:

1. SunitBelapure and Nina Godbole, "Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives", Wiley India Pvt Ltd, ISBN: 978-81-265-21791, Publish Date 2013.
2. Dr. Surya PrakashTripathi, RitendraGoyal, Praveen Kumar Shukla, KLSI. "Introduction to information security and cyber laws". Dreamtech Press. ISBN: 9789351194736, 2015.

REFERENCE BOOKS:

1. Thomas J. Mowbray, "Cybersecurity: Managing Systems, Conducting Testing, and
2. Investigating Intrusions", Copyright © 2014 by John Wiley & Sons, Inc, ISBN: 978 - 1-118 -84965 -1.
3. James Graham, Ryan Olson, Rick Howard, "Cyber Security Essentials", CRC Press, 15-Dec 2010.
4. Anti- Hacker Tool Kit (Indian Edition) by Mike Shema, McGraw-Hill Publication.

SEMESTER III

CSCH 501: DIGITAL FORENSICS

Course Objective:

The objective of the courses to

1) Understanding the concepts of Digital forensics and mobile device forensics.
2) Getting in depth knowledge of volume analysis and file systems.

UNIT I

Introduction To Digital Forensics : Introduction, Evolution Of Computer Forensics, Stages Of Computer Forensics Process, Benefits Of Computer Forensics, Uses Of Computer Forensics, Objectives Of Computer Forensics, Role Of Forensics Investigator, Forensics Readiness, **Computer Forensics Investigation Process** : Introduction To Computer Crime Investigation, Assess The Situation, Acquire The Data, Analyze The Data, Report The Investigation, Digital Evidence And First Responder Procedure, Digital Evidence, First Responder Toolkit, Issues Facing Computer Forensics, Types Of Investigation, Techniques Of Digital Forensics **(16 hours)**

UNIT II

Understanding Storage Media And File System : Hard Disk Drive, Details Of Internal Structure Of Hdd, The Booting Process, File System, **Windows Forensics** : Introduction, Recovering Deleted Files And Partitions, More About Recovering Lost Files/Data, **Logs & Event Analysis And Password Cracking** : Introduction, Windows Registry, Windows Event Log File, Windows Password Storage, Application Passwords Crackers, **Network Forensics** : Introduction, Network Components And Their Forensics Importance, Osi, Forensics Information From Network, Log Analysis, Forensics Tools, **Wireless Attacks** : Introduction, 4.3wireless Fidelity (Wi-fi)(802.11), Wireless Security, Wireless Attacks Detection Techniques, Wireless Intrusion Detection Systems

(16 hours)

UNIT III

Investigating Web Attacks : Introduction, Types Of Web Attacks, Web Attack Forensics, Web Application Forensics Tools, **Investigating Email Attacks** :