Kadi Sarva Vishwavidyalaya, Gandhinagar
MCA Semester III
MCA-32: Cyber Security & Forensic Science

Rationale:

- To understand the major concepts of Cyber Security and Forensics and to create the awareness through simple practical tips and tricks and to educate the students to learn how to avoid becoming victims of cyber crimes.
- The subject and the course content will help to the student who wish to take up cyber forensics as career as well as those who want to seek careers in cyber security.
- To gain experience of doing independent study and research in the field of cyber security and cyber forensics.

Prerequisite: Basic fundamental knowledge of Networking, Web Application, Mobile Application and Relational Database Management System

Teaching and Evaluation Scheme: Students are evaluated on the basis of continuous evaluation system both in theory and practical classes based on various parameters like term work, class participation, practical and theory assignments, presentation, class test, Regular Attendance, etc.

Sub Total Credit	Teaching scheme		Examination scheme				
	(per week)		MID	CEC	External		Total Marks
	Th	Pr	Th	Th	Th.	Pr.	
4	3	2	25	25	50	50	150

Course Contents:

UNIT 1: Cybercrime and Cyber Offenses [20%]

Introduction to Cybercrime:

Definition and Origins of Cybercrime, Cybercrime and Information Security, Cybercriminals Classifications of Cybercrimes: E-Mail Spoofing, Spamming, Cyber defamation, Internet Time Theft, Salami Attack/Salami Technique, Data Diddling, Forgery, Web Jacking, Newsgroup Spam/Crimes Emanating from Usenet Newsgroup, Industrial Spying/Industrial Espionage, Hacking, Online Frauds, Pornographic Offenses, Software Piracy, Computer Sabotage, E-Mail Bombing/Mail Bombs, Usenet Newsgroup as the Source of Cybercrimes, Computer Network Intrusions, Password Sniffing, Credit Card Frauds, Identity Theft

Cyber Offenses: How Criminals Plan Them

Introduction, Categories of Cybercrime, How Criminals Plan the Attacks: Reconnaissance, Passive Attack, Active Attacks, Scanning/Scrutinizing gathered Information, Attack (Gaining and Maintaining the System Access), Social Engineering, and Classification of Social Engineering, Cyberstalking: Types of Stalkers, How Stalking Works? Real-Life Incident of Cyberstalking, Cybercafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Cybercrime and Cloud Computing

UNIT 2: Cyber Crime: Computer and Human Devices [20%]

Cybercrime: Mobile and Wireless Devices

Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing Era: Types and Techniques of Credit Card Frauds, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices Authentication Service Security: Cryptographic Security for Mobile Devices, LDAP Security for Hand-Held Mobile Computing Devices, RAS Security for Mobile Devices, Media Player Control Security, Networking API Security for Mobile Computing Applications, Attacks on Mobile/Cell Phones: Mobile Phone Theft, Mobile Viruses, Mishing, Vishing, Smishing, Hacking Bluetooth, Mobile Devices: Unconventional/Stealth Storage Devices Threats through Lost and Stolen Devices, Protecting Data on Lost Devices, Educating the Laptop Users

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

UNIT 3: Cybercrime Weapons [20 %]

Password Cracking: Online Attacks, Offline Attacks, Strong, Weak and Random Passwords, Random Passwords

Keyloggers and Spywares: Software Keyloggers, Hardware Keyloggers, Antikeylogger, Spywares; Steganography: Steganalysis;

DoS and DDoS Attacks: DoS Attacks, Classification of DoS Attacks, Types or Levels of DoS Attacks, Tools Used to Launch DoS Attack, DDoS Attacks, How to Protect from DoS/DDoS Attacks SQL Injection: Steps for SQL Injection Attack, How to Avoid SQL Injection Attacks

Attacks on Wireless Networks: Traditional Techniques of Attacks on Wireless Networks, Theft of Internet Hours and Wi-Fi-based Frauds and Misuses, How to Secure the Wireless Networks

UNIT 4: Cyber Security & Cyber Law [20%]

Intrusion Detection: Component of intrusion detection framework, types, Function of lDS, strengths and limitations

DNS and DNS based vulnerabilities: DNS query, DNs cache, Poisoning cache, countermeasures

Email Security - PGP, S/MIME, Domain key identified mail, spam, protection against spam

Cybercrimes and Cyber Security: The Legal Perspectives

Introduction, Why Do We Need Cyberlaws: The Indian Context, The Indian IT Act: Admissibility of Electronic Records: Amendments made in the Indian ITA 2000, Positive Aspects of the ITA 2000, The Weak Areas of the ITA 2000, Challenges to Indian Law and Cybercrime Scenario in India, Consequences of Not Addressing the Weakness in Information Technology Act

UNIT 5: Forensics [20%]

Introduction, Historical Background of Cyberforensics, Digital Forensics Science, The Need for Computer Forensics, Cyberforensics and Digital Evidence: The Rules of Evidence,Forensics Analysis of E-Mail: RFC282, Digital Forensics Life Cycle: The Digital Forensics Process,The Phases in Computer Forensics/Digital Forensics, Precautions to be Taken when Collecting Electronic Evidence, Chain of Custody Concept, Network Forensics, Approaching a Computer Forensics Investigation: Typical Elements Addressed in a Forensics Investigation Engagement Contract, Solving a Computer Forensics Case, Setting up a Computer Forensics Laboratory:

Challenges in Computer Forensics: Technical Challenges: Understanding the Raw Data and its Structure, The Legal Challenges in Computer Forensics and Data Privacy Issues, Special Tools

and Techniques: Digital Forensics Tools Ready Reckenor, Special Technique: Data Mining used in Cyberforensics, Forensics Auditing, Antiforensics

Cybercrime: Illustrations, Examples and Mini-Cases, Scams
(Only for the referential context should not be asked in the examination)

Real-Life Examples

Example 1: Official Website of Maharashtra Government Hacked
Example 2: E-Mail Spoofing Instances
Example 3: I Love You Melissa – Come Meet Me on the Internet
Example 4: Ring-Ring Telephone Ring: Chatting Sessions Turn Dangerous
Example 5: Young Lady's Privacy Impacted
Example 6: Indian Banks Lose Millions of Rupees
Example 7: "Justice" vs. "Justice": Software Developer Arrested for Launching Website Attacks
Example 8: Parliament Attack
Example9: Pune City Police Bust Nigerian Racket

Mini-Cases:

Mini-Case 1: Cyberpornography Involving a Juvenile
Criminal Mini-Case 2: Cyberdefamation: A Young
Couple Impacted Mini-Case 12: Internet Used for
Murdering
Mini-Case 13: Social Networking Victim – The MySpace Suicide Case
Mini-Case 16: NASSCOM vs. Ajay Sood and Others

Online Scams:

Scam No. 1 – Foreign Country Visit Bait
Scam No. 2 – Romance Scam
Scam No. 3 – Lottery Scam
Scam No. 4 – Bomb Scams
Scam No. 5 – Charity Scams
Scam No. 6 – Fake Job Offer Scam

Financial Crimes in Cyber Domain:

Financial Crime 1: Banking Related Frauds
Financial Crime 2: Credit Card Related Frauds

Text Books:

Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives – Nina Godbole, Sunit Belapur, Wiley India Publications Released: April 2011

Chapter & Topics –

Chapter 1: 1.1 to 1.5
Chapter 2: 2.1 to 2.8
Chapter 3: 3.1 to 3.12
Chapter 4: 4.1 to 4.12
Chapter 5: 5.1, 5.2, 5.3
Chapter 6: 6.1, 6.3, 6.4, 6.5, 6.6, 6.8, 6.9, 6.10
Chapter 7: 7.1 to 7.14, 7.16, 7.17, 7.18, 7.19
Chapter 8: 8.1, 8.3, 8.4, 8.8

Reference Book:

- Internet Forensics: Using Digital Evidence to Solve Computer Crime Robert Jones, O'Reilly Media, Released: October 2005
- Windows Forensics: The field guide for conducting corporate computer investigations Chad Steel, Wiley India Publications Released: December 2006

Experiment List:

1. TCP scanning using NMAP
2. Port scanning using NMAP
3. TCP or UDP connectivity using Netcat
4. Web application testing using DVWAlCustomize web application
5. Manual SQL injection using DVWAlCustomize web application
6. XSS using DVWAlICustomize web application
7. Automated SQL injection with SqlMap
8. Vulnerability detection in Web application
9. Exploitation
10. Snort, Wiresharkuser.
11. Implement the information hiding and stegenography. (Snort).
12. Recover the deleted data and files. (recoverjpeg, recovermov, foremost)