MAHATMA GANDHI UNIVERSITY

SCHEME AND SYLLABI

FOR

M.TECH DEGREE PROGRAMME

IN

COMPUTER SCIENCE AND ENGINEERING

WITH SPECIALIZATION

IN

CYBER SECURITY

(2013 ADMISSION ONWARDS)

SCHEME AND SYLLABI FOR M .Tech DEGREE PROGRAMME IN COMPUTER SCIENCE AND ENGINEERING WITHSPECIALIZATION IN CYBER SECURITY

SEMESTER – II

SI NO.	Course No.	Subject	Hrs/Week			Evaluation Scheme(marks)					
			L	T	P	Sessional			ESE	Total	Credits (C)
						TA	CT	Sub Total			
1	MCSCB 201	Cyber Forensics	3	1	0	25	25	50	100	150	4
2	MCSCB 202	Security Threats	3	1	0	25	25	50	100	150	4
3	MCSCB 203	Ethical Hacking	3	1	0	25	25	50	100	150	4
4	MCSCB 204	Design of Secured Architectures	3	1	0	25	25	50	100	150	4
5	MCSCB 205	Elective – III	3	0	0	25	25	50	100	150	3
6	MCSCB 206	Elective – IV	3	0	0	25	25	50	100	150	3
7	MCSCB 207	Ethical Hacking Lab	-	-	3	25	25	50	100	150	2
8	MCSCB 208	Seminar- II	-	-	2	50	-	50	0	50	1
Total			**18**	**4**	**5**	**225**	**175**	**400**	**700**	**1100**	**25**

L – Lecture, **T** – Tutorial, **P** – Practical

Elective – III (MCSCB 205)		Elective – IV (MCSCB 206)	
MCSCB 205 -1	Coding and Information Theory	MCSCB 206 – 1	Cryptanalysis
MCSCB 205 -2	Storage Management And Security	MCSCB 206 - 2	Logical Foundations for Access Control
MCSCB 205- 3	Internet Information and Application Security	MCSCB 206 - 3	Game Theory
MCSCB 205 -4	Digital Watermarking	MCSCB 206 - 4	Database Security

TA – Teacher's Assessment (Assignments, attendance, group discussion, quiz, tutorials, Seminars, etc.)
CT – Class Test (Minimum of two tests to be conducted by the Institute)
ESE – End Semester Examination to be conducted by the University

MCSCB 201 **CYBER FORENSICS**

L	T	P	C
3	1	0	4

Module 1: Cyber forensics
Introduction to Cyber forensics, Type of Computer Forensics Technology- Type of Vendor and Computer Forensics Services. Information Security Investigations, Corporate Cyber Forensics, Scientific method in forensic analysis, investigating large scale Data breach cases, Analyzing Malicious software.

Module 2: Ethical Hacking
Essential Terminology, Windows Hacking, Malware, Scanning, Cracking.
Digital Evidence in Criminal Investigations. The Analog and Digital World, Training and Education in digital evidence, the digital crime scene, Investigating Cybercrime, Duties Support Functions and Competencies.
Computer Forensics Evidence and Capture- Data Recovery-Evidence collection and Data Seizure-Duplication and preservation of Digital Evidence-Computer image verification and Authentication

Module 3: Investigating Network Intrusions and Cyber Crime, Network Forensics and Investigating logs, Investigating network Traffic, Investigating Web attacks, Router Forensics.
Computer Forensics Analysis- Discovery of Electronic Evidence- Identification of data- Reconstructing Past events- networks

Module 4: Countermeasure: Information warfare- Surveillance tool for Information warfare of the future-Advanced Computer Forensics. Cyber forensics tools and case studies.

References:

1 Understanding Cryptography: A Textbook for Students and Practitioners: Christof paar, Jan Pelzl.
2 Live Hacking: The Ultimate Guide to Hacking Techniques & Countermeasures for Ethical Hackers & IT Security Experts Ali Jahangiri
3 Handbook of Digital and Multimedia Forensic Evidence [Paperback] John J. Barbara
4 Computer Forensics: Investigating Network Intrusions and Cyber Crime (Ec-Council Press Series: Computer Forensics)
5 Cyber Forensics: Understanding Information Security Investigations (Springer's Forensic Laboratory Science Series) by Jennifer Bayuk
6 Information warfare : Information warfare and security: (ACM Press) by Dorothy
Elizabeth Robling Denning
7 Cyberwar and Information Warfare : Springer's by Daniel Ventre
8 Computer forensics: computer crime scene investigation, Volume 1 (Charles River Media, 2008) By John R. Vacca

MCSCB 202 **SECURITY THREATS**

L	T	P	C
3	1	0	4

Module I: Introduction: Security threats - Sources of security threats- Motives - Target Assets and vulnerabilities – Consequences of threats- E-mail threats - Web-threats - Intruders and Hackers, Insider threats, Cyber crimes.

Module II: Network Threats: Active/ Passive – Interference – Interception – Impersonation – Worms – Virus – Spam's – Ad ware - Spy ware – Trojans and covert channels – Backdoors – Bots – IP Spoofing - ARP spoofing - Session Hijacking - Sabotage-Internal treats- Environmental threats - Threats to Server security.

Module III: Security Threat Management: Risk Assessment - Forensic Analysis - Security threat correlation – Threat awareness - Vulnerability sources and assessment- Vulnerability assessment tools - Threat identification - Threat Analysis - Threat Modeling - Model for Information Security Planning.

Module IV: Security Elements: Authorization and Authentication - types, policies and techniques – Security certification - Security monitoring and Auditing - Security Requirements Specifications - Security Policies and Procedures, Firewalls, IDS, Log Files, Honey Pots. Access control, Trusted Computing and multilevel security - Security models, Trusted Systems, Software security issues, Physical and infrastructure security, Human factors – Security awareness, training , Email and Internet use policies.

REFERENCES

1. Joseph M Kizza, "Computer Network Security", Springer Verlag, 2005.
2. Swiderski, Frank and Syndex, "Threat Modeling", Microsoft Press, 2004.
3. William Stallings and Lawrie Brown, "Computer Security: Principles and Practice", Prentice Hall, 2008.
4. Thomas Calabres and Tom Calabrese, "Information Security Intelligence: Cryptographic Principles & Application", Thomson Delmar Learning, 2004.

MCSCB 203 **ETHICAL HACKING**

L	T	P	C
3	1	0	4

Module I: Casing the Establishment - What is footprinting- Internet Footprinting. -Scanning- Enumeration - basic banner grabbing, Enumerating Common Network services. Case study- Network Security Monitoring Securing permission - Securing file and folder permission. Using the encrypting file system. Securing registry permissions. Securing service- Managing service permission. Default services in windows 2000 and windows XP. Unix - The Quest for Root. Remote Access vs Local access. Remote access. Local access. After hacking root.

Module II: Dial-up ,PBX, Voicemail, and VPN hacking - Preparing to dial up. War-Dialing. Brude-Force Scripting PBX hacking. Voice mail hacking . VPN hacking. Network Devices – Discovery, Autonomous System Lookup. Public Newsgroups. Service Detection. Network Vulnerability. Detecting Layer 2 Media.

Module III: Wireless Hacking - Wireless Foot printing. Wireless Scanning and Enumeration. Gaining Access. Tools that exploiting WEP Weakness. Denial of Services Attacks. Firewalls- Firewalls landscape- Firewall Identification-Scanning Through firewalls- packet Filtering- Application Proxy Vulnerabilities . Denial of Service Attacks - Motivation of Dos Attackers. Types of DoS attacks. Generic Dos Attacks. Unix and Windows DoS

Module IV: Remote Control Insecurities - Discovering Remote Control Software. Connection. Weakness.VNC . Microsoft Terminal Server and Citrix ICA .Advanced Techniques Session Hijacking. Back Doors. Trojans. Cryptography . Subverting the systems Environment. Social Engineering. Web Hacking. Web server hacking web application hacking. Hacking the internet User - Malicious Mobile code, SSL fraud, E-mail Hacking, IRC hacking, Global
Counter measures to Internet User Hacking.

REFERENCES:

1. Stuart McClure, Joel Scambray and Goerge Kurtz, “Hacking Exposed Network Security Secrets & Solutions”, Tata Mcgrawhill Publishers, 2010.
2. Bensmith, and Brian Komer, “Microsoft Windows Security Resource Kit”, Prentice Hall of India, 2010.

MCSCB 204 **DESIGN OF SECURED ARCHITECTURES**

L	T	P	C
3	1	0	4

Module I: Architecture and Security - Architecture Reviews-Software Process-Reviews and the Software Development Cycle-Software Process and Architecture Models-Software Process and Security- Architecture Review of System-Security Assessments-Security Architecture Basics- Architecture Patterns in Security.

Module II: Low-Level Architecture - Code Review-importance of code review- Buffer Overflow Exploits- Countermeasures against Buffer Overflow Attacks-patterns applicable-Security and Perl- Byte code Verification in Java-Good Coding Practices Lead to Secure Code- Cryptography- Trusted Code - Secure Communications

Module III: Mid-Level Architecture - Middleware Security- Middleware and Security- The Assumption of Infallibility. High-Level Architecture - Security Components- Secure Single Sign-On- Public-Key Infrastructures- Firewalls- Intrusion Detection Systems-LDAP and X.500 Directories- Kerberos- Distributed Computing Environment-The Secure Shell, or SSH-The Distributed Sandbox- Security and Other Architectural Goals- Metrics for Non-Functional Goals-Force Diagrams around Security- High Availability- Robustness-Reconstruction of Events- Ease of Use- Maintainability, Adaptability, and Evolution-Scalability- Interoperability- Performance- Portability.

Module IV: Enterprise Security Architecture - Security as a Process-Security Data-Enterprise Security as a Data Management Problem- Tools for Data Management- David Isenberg and the "Stupid Network"-Extensible Markup Language- The XML Security Services Signaling Layer-XML and Security Standards- The Security Pattern Catalog Revisited-XML-Enabled Security Data-HGP: A Case Study in Data Management. Business Cases and Security: Building Business Cases for Security

REFERENCES

1. Jay Ramachandran, "Designing Security Architecture Solutions", Wiley Computer Publishing, 2010.
2. Markus Schumacher, "Security Patterns: Integrating Security and Systems Engineering", Wiley Software Pattern Series, 2010.

MCSCB 205-1 **CODING AND INFORMATION THEORY**

L	T	P	C
3	0	0	3

Module I: Source Coding - Introduction to information theory, uncertainty and information, average mutual information and entropy, source coding theorem, Shannon-fano coding, Huffman coding, Arithmetic coding, Lempel-Ziv algorithm, run-length encoding and rate distortion function.

Module II: Channel capacity and coding - channel models, channel capacity, channel coding, information capacity theorem, random selection of codes. Error control coding: linear block codes and their properties, decoding of linear block code, perfect codes, hamming codes, optimal linear codes and MDS codes.

Module III: Cyclic codes - polynomials, division algorithm for polynomials, a method for generating cyclic codes, matrix description of cyclic codes, burst error correction, fire codes, golay codes, CRC codes, circuit implementation of cyclic codes. BCH codes: minimal polynomials, generator polynomial for BCH codes, decoding of BCH codes, Reed-Solomon codes and nested codes.

Module IV: Convolutional codes - tree codes and trellis codes, polynomial description of convolutional codes, distance notions for convolutional codes, generation function, matrix description of convolutional codes, viterbi decoding of convolutional codes, distance bounds for convolutional codes, turbo codes and turbo decoding. Trellis Coded Modulation - concept of coded modulation, mapping by set partitioning, ungerboeck's TCM design rules, TCM decoder, Performance evaluation for Additive White Gaussian Noise (AWGN) channel, TCM for fading channels.

References:

1. Lin S. and D. J. Costello, "Error Control Coding — Fundamentals and Applications", Second Edition, Pearson Education Inc., NJ., USA, 2004
2. Shu Lin and Daniel J. Costello, "Error Control Coding", Second Edition, Prentice Hall, 1983.
3. Ranjan Bose, "Information Theory, Coding and Cryptography", Tata McGraw-Hill, 2003.
4. E. R. Berlekamp, "Algebraic Coding Theory", McGraw-Hill, New York, 1968.
5. R. E. Blahut, "Algebraic Codes for Data Transmission", Cambridge University Press Cambridge, UK, 2003.
6. Ranjan Bose, "Information theory, coding and cryptography", Tata McGraw Hill, 2002.
7. Viterbi, "Information theory and coding", McGraw Hill, 1982.
8. John G. Proakis, "Digital Communications", 2nd Edition, McGraw Hill, 1989.

MCSCB 205-2 **STORAGE MANAGEMENT AND SECURITY**

L	T	P	C
3	0	0	3

Module 1: Introduction, History: computing, networking, storage, Need for storage networking , SAN, NAS, SAN/NAS Convergence, Distributed Storage Systems, Mainframe/proprietary vs. open storage, Storage Industry Organizations and Major Vendors Market, Storage networking strategy (SAN/NAS) Technology

Module 2: Storage components, Data organization: File vs. Block, Object; Data store; Searchable models; Storage Devices (including fixed content storage devices), File Systems, Volume Managers, RAID systems, Caches, Prefetching. Error management: Disk Error Management, RAID Error Management, Distributed Systems Error Management.

Module 3: Large Storage Systems: Google FS/Big Table, Cloud/Web - based systems (Amazon S3), FS+DB convergence, Programming models: Hadoop. *Archival Systems*: Content addressable storage, Backup: server less, LAN free, LAN Replication issues, Storage Security, Storage Management, Device Management, NAS Management, Virtualization, Virtualization solutions, SAN Management: Storage Provisioning, Storage Migration

Module 4: Securing the storage Infrastructure, Storage Security Framework, Risk Triad, Storage Security Domains, Security Implementation in Storage Networking. Managing the Storage Infrastructure, Monitoring the Storage Infrastructure, Storage Management Activities, Developing an Ideal Solution, Concepts in Practice.

References:

1. EMC Education Services “Information Storage and Management: Storing, Managing, and Protecting Digital Information” , John Wiley & Sons, 2010
2. John Chirillo, ScottBlaul “ Storage Security: Protecting SANs, NAS and DAS”, Wiley, 2003.
3. David Alexander, Amanda French, Dave Sutton “Information Security Management Principles” BCS, The Chartered Institute, 2008.
4. Gerald J. Kowalski, Mark T. Maybury “ Information Storage and Retrieval Systems: Theory and Implementation, Springer, 2000.
5. Foster Stockwell , “A history of information storage and retrieval” McFarland, 2001.
6. R. Kelly Rainer, Casey G. Cegielski , “Introduction to Information Systems: Enabling and Transforming Business, John Wiley & Sons, 2010.

MCSCB 205-3 **Internet Information and Application Security**

L	T	P	C
3	0	0	4

Module 1: Web application security- Key Problem factors – Core defense mechanisms- Handling user access- handling user input- Handling attackers – web spidering – Discovering hidden content. Transmitting data via the client – Hidden form fields – HTTP cookies – URL parameters – Handling client-side data securely – Attacking authentication – design flaws in authentication mechanisms –securing authentication Attacking access controls – Common vulnerabilities – Securing access controls

Module 2: SQL Injection - How it happens - Dynamic string building - Insecure Database Configuration - finding SQL injection – Exploiting SQL injection – Common techniques – identifying the database – UNION statements – Preventing SQL injection Platform level defenses - Using run time protection - web application Firewalls – Using ModSecurity - Intercepting filters- Web server filters - application filters – securing the database – Locking down the application data – Locking down the Database server

Module3: Mod Security - Blocking common attacks – HTTP finger printing – Blocking proxies requests – Cross-site scripting – Cross-site request forgeries – Shell command execution attempts – Null byte attacks – Source code revelation – Directory traversal attacks – Blog spam – Website defacement – Brute force attack – Directory indexing – Detecting the real IP address of an attacker

Module 4: Web server Hacking - Source code disclosure – Canonicalization attacks – Denial of service – Web application hacking – Web crawling Database Hacking – Database discovery – Database vulnerabilities

References:

1. Dafydd Stuttard, Marcus Pinto, The Web Application Hacker’s Handbook, 2nd Edition, Wiley Publishing, Inc.
2. Justin Clarke, SQL Injection Attacks and Defense, 2009, Syngress Publication Inc.
3. Magnus Mischel , ModSecurity 2.5, Packt Publishing
4. Stuart McClure Joel, ScambRay, George Kurtz, Hacking Exposed 7: Network Security Secrets & Solutions, Seventh Edition, 2012, The McGraw-Hill Companies

MCSCB 205-4 **DIGITAL WATERMARKING**

L	T	P	C
3	0	0	3

Module 1: Watermarking host signals: Image, Video, and Audio. Multimedia compression and decompression, Lossless compression, Models watermarking, Communication-based models of watermarking, Geometric models of watermarking, modeling watermark detection by correlation

Module 2: Basic message coding, Mapping message in message vectors, Error correction coding, Detecting multi-symbol watermarks, Watermarking with side information, Inform(embedding, Informed coding.

Module 3: Structured dirty-paper codes, Analyzing errors, Message errors, ROC curves, The effect of whitening on error rates, Analysis of normalized correlation, Using perceptual mode, Evaluating perceptual impact of watermarks.

Module 4: General forms of perceptual model, Perceptual adaptive watermarking, Robust watermarking, Watermark security, Watermark security and cryptography, Content authentication, Exact authentication, Selective, authentication, Localization, Restoration.

References:

1. Cox I., M. Miller, J. Bloom, J. Fridrich and T Kalker, "Digit Watermarking and Steganography", Second Edition, Morg Kaufmann Publishers, 2008.
2. E. Cole, R. Krutz, and J. Conley, Network Security Bible, Wiley-Dreamtech, 2005.
3. W. Stallings, Cryptography and Network Security Principles and practice, 3/e, Pearson Education Asia, 2003.
4. C. P. Pfleeger and S. L. Pfleeger, Security in Computing, 3/e, Pearson Education, 2003.
5. M. Bishop, Computer Security: Art and Science, Pearson Education, 2003.

MCSCB 206-1 **CRYPTANALYSIS**

L	T	P	C
3	0	0	3

Module 1: Cryptanalysis of classical ciphers: Vigenere cipher, Affine cipher, Hill-cipher Linear Shift Register Random Bit Generator: Berlekamp- Massey algorithm for the cryptanalysis of LFSR, Correlation attack on LFSR based stream ciphers, Cryptanalysis of ORYX, Fast algebraic attack.

Module 2: Cryptanalysis of Block Ciphers: Man in the middle attack double DES, Linear and Differential cryptanalysis. Algorithmic Number Theory: Stein's binary greatest common divisor algorithm, Shanks Tonelli algorithm for square roots in Fp, Stein's greatest common divisor algorithm for polynomials.

Module 3: Algorithms for DLP: Pollard Rho method for DLP, Shank's baby step Giant step algorithm for DLP Silver-Pohling-Hellman algorithm for DLP, Index calculus for DLP algorithms: Trial division, Fermat method, Legendre-congruence, Continued fraction method, Pollard Rho method, Elliptic curve method, Quadratic sieve.

Module 4: Lattice based Cryptanalysis. Direct attacks using lattice reduction, Coppersmith's attacks. Attacks on cryptographic hash functions: Birth day paradox, Birthday for paradox for multi collisions, Birthday paradox in two groups, Application of Birthday paradox in Hash functions, Multicollisions attack on hash functions.

References:

1. Antoine Joux, "Algorithmic Cryptanalysis", Chapman & Hall/CRC Cryptography and Series, 2009.
2. Song Y Yang, "Number Theory for Computing", Second Edition,SpringerVerlag, 2010.
3. Gregory V. Bard, "Algebraic Cryptanalysis", Springer, 2009.
4. Hffstein, Jeffray, Pipher, Jill and Silverman, "An Introduction to Mathematical Cryptography", Springer, 2010.

MCSCB 206-2	LOGICAL FOUNDATIONS FOR ACCESS CONTROL	L	T	P	C
		3	0	0	3

Module 1: Mathematical Logic: Mathematical systems, Propositions and connectives, Statement formulae and truth tables, Logic variables, Logic Functions, Logic expressions, Equivalences of Logic functions, complete sets of logic functions.

Module 2: Propositional & Predicate Calculus: Propositional and Predicate Calculus: Language of Propositional and Predicate Logic - Logic Programming, Formulas, Models,

Module 3: Normal Forms— CNF, DNF, SNF, PNF, Satisfiability, consequences and Interpretations, Tableaux, Resolution, Soundness and completeness of Tableaux and Resolution, Semantic Tableaux complete Systematic Tableaux, Decision Methods, Security Models:Biba, Bell LaPadula, Chinese wall, Lattice model, SPKI/SDSI –PKIin first order logic, security of distributed systems using Datalog with constraints,

Module 4: Executional specification of security policies in a logic programming framework, Delegation logic, trust management systems, Case studies of specific logic programming models for distributed systems security such as SD3, SecPAL, RT etc.

References:

1. John W Lloyd, "Foundations of Logic Programming (Symbolic E Artificial Intelligence)", Springer, 1993
2. J. W Lloyd and John Lloyd, 'Logic and Learning: Knowledge -tation, Computation and Learning in Higher-order Logic", ES—L'11 Heidelberg, 2003.
3. Mordechai Ben-Ad, "Mathematical Logic for Computer Science", B". on, Springer International Edition, 2008.
4. George Matakides and Anil Nerode, "Principles of Logic and Logic — North Holland, 1996.
5. Alessandro Aldini, Gilles Barthe, Roberto Gorrieri, " Foundations of Security Analysis and Design V, Volume 5,Springer, 2009.

MCSCB 206-3 **GAME THEORY**

L	T	P	C
3	0	0	3

Module I: Fundamentals: Conflict, Strategy and Games, Game theory, The Prisoner's Dilemma, Scientific metaphor, Business case, Games in normal and extensive forms – Representation, Examination, Examples.

Module II: Non Cooperative Equilibrium in Normal Games: Dominant Strategies and Social Dilemmas, Nash Equilibrium, Classical Cases in Game theory, Three person games, Introduction to Probability and Game theory, N-Person games.

Module III: Cooperative Solutions: Elements of Cooperative Games- Credible commitment, A Real Estate Development, Solution Set, Some Political Coalitions, Applications of the Core to Economics – The Market Game, The Core of a Two Person Exchange Game, The Core with More than Two Pairs of Traders, The core of Public Goods Contribution Game, Monopoly and Regulation .

Module IV: Sequential Games: Strategic Investment to Deter Entry, The Spanish Rebellion, Again, Imbedded Games – Planning Doctoral Study, Centipede Solved, Repeated play-Campers Dilemma, Pressing the shirts, Indefinitely Repeated Play – A Repeated Effort Dilemma, The Discount Factor. Applications: Voting Games, Games and Experiments, Auctions, Evolution and Boundary Rational Learning.

REFERENCES

1. Roger A. McCain, "Game Theory – A Non-Technical Introduction to the Analysis of Strategy", Thomson South-Western, 2005.
2. Tirole, "Game Theory", Mit press 2005.
3. Osborne, "An Introduction to Game Theory", Oxford Press 2006.
4. E. N. Barron, "Game Theory: An Introduction", Wiley India Pvt Ltd, 2009.

MCSCB 206-4 **DATABASE SECURITY**

L	T	P	C
3	0	0	3

Module 1: Introduction to databases: database modeling, conceptual database design, overview of SQL and relational algebra, Access control mechanisms in general computing systems: Lampson's access control matrix. Mandatory access control.

Module 2: Authentication mechanisms in databases, DAC in databases: Griffiths and Wade, MAC mechanisms in databases: SeaView. RBAC in databases. Authentication and password security – Weak authentication options, Implementation options, Strong password selection method, Implement account lockout, Password profile.

Module 3: SQL Injection, Auditing in databases, Statistical inference in databases, Private information retrieval viewed as a database access problem. Privacy in data publishing, Virtual Private Databases, Security of outsourced databases.

Module 4: Securing database to database communication – Monitor and limit outbound communication, Protect link usernames and passwords – Secure replication mechanisms. Trojans- Types of DB Trojans, Monitor for changes to run as privileges, Traces and event monitors. Encrypting data- in transit, Encrypt data-at-rest. Database security auditing categories.

References:

1. Ron Ben Natan, "Implementing Database Security and Auditing", Elsevier, 2005.
2. Hassan A. Afyouni, "Database Security and Auditing: Protecting Data Integrity and Accessibility", Course Technology, 2005.
3. Michael Gertz and Sushil Jajodia, "Handbook of Database Security-Applications and Trends", Springer, 2008.
4. Database Security, Cengage Learning; 1 edition (July 12, 2011),Alfred Basta . Melissa Zgola
5. Data warehousing and data mining techniques for cyber security, Springer's By Anoop Singha.
6. Carlos Coronel, Steven A. Morris, Peter Rob, "Database Systems: Design, Implementation, and Management", Cengage Learning, 2011.
7. Vijay Atluri, John Hale, "Research Advances in Database and Information Systems Security", Springer, 2000.
8. Pierangela Samarati, Ravi Sandhu," Database Security X: Status and prospects, Volume 10",Springer, 1997.

MCSCB 207 **ETHICAL HACKING LAB**

L	T	P	C
0	0	3	2

1. Working with Trojans, Backdoors and sniffer for monitoring network communication
2. Denial of Service and Session Hijacking using Tear Drop, DDOS attack.
3. Penetration Testing and justification of penetration testing through risk analysis
4. Password guessing and Password Cracking.
5. Wireless Network attacks , Bluetooth attacks
6. Firewalls , Intrusion Detection and Honeypots
7. Malware – Keylogger, Trojans, Keylogger countermeasures
8. Understanding Data Packet Sniffers
9. Windows Hacking – NT LAN Manager, Secure 1 password recovery
10. Implementing Web Data Extractor and Web site watcher.
11. Email Tracking.
12. Configuring Software and Hardware firewall.
13. Firewalls, Packet Analyzers, Filtering methods.

MCSCB 208 **SEMINAR - II**

L	T	P	C
0	0	2	1

Each student shall present a seminar on any topic of interest related to the core / elective courses offered in the second semester of the M. Tech. Programme. He / she shall select the topic based on the References: from international journals of repute, preferably IEEE journals. They should get the paper approved by the Programme Co-ordinator/ Faculty member in charge of the seminar and shall present it in the class. Every student shall participate in the seminar. The students should undertake a detailed study on the topic and submit a report at the end of the semester. Marks will be awarded based on the topic, presentation, participation in the seminar and the report submitted.