CURRICULUM FOR

ADVANCE DIPLOMA IN CYBER SECURITY (CB)

SCHEME : E

DURATION: ONE YEAR **PATTERN:** PART TIME **-** SEMESTER

ELIGIBILITY: Diploma (Electronics / Computer / Mechanical / Electrical Streams), B.Sc. (Physics / IT / Comp Sc. Streams) OR Higher.

(To be implemented from the Academic Year 2009 – 2010)

MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION. MUMBAI
(AUTONOMOUS)
ISO 9001-2000 Certified
49, Kherwadi, Aliyawer Jung Marg, Mumbai – 400 051

MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION, MUMBAI

TEACHNING AND EXAMINATION SCHEME

COURSE NAME : ADVANCE DIPLOMA IN CYBER SECURITY MANAGEMENT

COURSE CODE : CB

DURATION OF COURSE : ONE YEAR / TWO SEMESTER **WITH EFFECT FROM 2009-10**

SEMESTER : FIRST **DURATION : 16 WEEKS**

PATTERN : PART TIME - SEMESTER **SCHEME: E**

SR. NO.	SUBJECT TITLE	SUB CODE	TEACHING SCHEME			EXAMINATION SCHEME									
			TH	TU	PR	PAPER HRS	TH (1)		PR (4)		OR (8)		TW (9)		SW
							MAX	MIN	MAX	MIN	MAX	MIN	MAX	MIN	
1	Introduction to Computer Networking	11041	3	--	2	3	50	25	--	--	50@	25	--	--	50
2	Operating System Concepts	11042	3	--	2	3	100	50	--	--	50#	25	50@	25	
3	Forensic Science	11043	3	--	2	3	100	50	50#	25	--	--	50@	25	
4	System and Network Security	11044	3	--	4	3	100	50	50#	25	--	--	50@	25	
		TOTAL	**12**	**--**	**10**	**--**	**350**	**--**	**100**	**--**	**100**	**--**	**150**	**--**	**50**

Student Contact Hours Per Week: **22 Hrs.**

Theory and practical periods of 60 minutes each.

Total Marks **: 750**

@ Internal Assessment, # External Assessment, *# On Line Examination, [redacted] No Theory Examination.

Abbreviations: TH-Theory, TU- Tutorial, PR-Practical, ,OR-Oral, TW- Termwork, SW- Sessional Work

- Conduct two class tests each of 25 marks for each theory subject. Sum of the total test marks of all subject are to be converted out of 50 marks as sessional work.
- Progressive evaluation is to be done by subject teacher as per the prevailing curriculum implementation and assessment norms
- Code number for TH, PR, OR, TW and SW are to be given as suffix 1, 4, 8, 9 respectively to the subject code as mentioned.

MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION, MUMBAI

TEACHNING AND EXAMINATION SCHEME

COURSE NAME : ADVANCE DIPLOMA IN CYBER SECURITY MANAGEMENT

COURSE CODE : CB

DURATION OF COURSE : ONE YEAR / TWO SEMESTER **WITH EFFECT FROM 2009 - 10**

SEMESTER : SECOND **DURATION : 16 WEEKS**

PATTERN : PART TIME - SEMESTER **SCHEME: E**

SR. NO.	SUBJECT TITLE	SUB CODE	TEACHING SCHEME			EXAMINATION SCHEME									
			TH	TU	PR	PAPER HRS	TH (1)		PR (4)		OR (8)		TW (9)		SW
							MAX	MIN	MAX	MIN	MAX	MIN	MAX	MIN	
1	Cyber Security Management	11045	3	--	--	3	100	50	--	--	--	--	--	--	50
2	Intrusion Detection System	11046	3	--	2	3	100	50	50#	25	--	--	50@	25	
3	Mobile Security	11047	3	--	2	3	100	50	--	--	50#	25	50@	25	
4	Ethical Hacking	11048	3	--	2	3	100	50	50@	25	--	--	--	--	
5	Professional Practices	11049	--	--	4	--	--	--	50#	25	--	--	50@	25	
		Total	**12**	**--**	**10**	**--**	**400**	--	**150**	**--**	**50**	**--**	**150**	**--**	**50**

Student Contact Hours Per Week: **22 Hrs.**

Theory and practical periods of 60 minutes each.

Total Marks **: 800**

@ Internal Assessment, # External Assessment, *# On Line Examination, [ ] No Theory Examination.

Abbreviations: TH-Theory, TU- Tutorial, PR-Practical, ,OR-Oral, TW- Termwork, SW- Sessional Work

- Conduct two class tests each of 25 marks for each theory subject. Sum of the total test marks of all subject are to be converted out of 50 marks as sessional work.
- Progressive evaluation is to be done by subject teacher as per the prevailing curriculum implementation and assessment norms.
- Code number for TH, PR, OR, TW and SW are to be given as suffix 1, 4, 8, 9 respectively to the subject code as mentioned.

COURSE NAME : Advance Diploma in Cyber Security Management

COURSE CODE : CB

SEMESTER : First

SUBJECT TITLE : Introduction to Computer Networking

SUBJECT CODE : 11041

Teaching and Examination Scheme:-

TEACHING SCHEME			EXAMINATION SCHEME					
TH	TU	PR	PAPER HRS	TH	PR	OR	TW	TOTAL
3	--	2	3	50	--	50@	--	100

RATIONALE:

The Students will be able to understand the concepts of Networking. It will also help in understanding the importance of Networking.

OBJECTIVES: Students will be able to understand

1. The Basic Structure of the Networking.
2. The Architecture and Model of the Networking.
3. Configuring the Network.
4. Configuring hosts and access inter networks using TCP/IP protocols.
5. Identifying the role of each TCP/IP component.
6. Use of all major TCP/IP application services including: FTP, TELNET, HTTP and NFS.
7. Avoiding common internetworking problems.
8. Troubleshooting TCP/IP networks using protocol analysis techniques.
9. Employing popular Internet/intranet tools: FTP, Web browsers, WWW and other.

CONTENTS: Theory

Chapter	Contents	Hours	Marks
1	**Basic concepts of Networking** a) Define Network b) Characteristics of good network c) Uses of network d) Network Architecture e) Network topologies f) Different types of Networking Devices g) Protocols h) Types of Protocol i) Internet/ Intranet/ Extranet/ Internet works a) Types of Network b) OSI Model j) TCP/IP Model	06	04
2	**Network Hardware Requirement** a) Cables and Connectors b) Network Interface Card (NIC) c) Transceiver d) Repeater e) Switch f) Hub g) Bridge h) Router i) Gateways	04	08
3	**Internet & TCP/IP Suite** a) TCP/IP : key application services and multivendor capabilities b) TCP/IP and the Internet c) Internet RFCs and STDs affect TCP/IP **Introduction to TCP/IP protocol architecture** a) Protocol layering concepts b) TCP/IP layering c) Components of TCP/IP networks **The Internet Protocol (IP)** **Internet Layer functions** a) Fundamental internetworking concepts b) Connecting networks c) Provision of Physical Layer independence d) Internet addressing: IP address classes A, B, C, D, E **Address resolution** a) Resolving MAC addresses with ARP b) Avoiding duplicate IP addresses with RARP, BOOTP and DHCP **IP address resolution** a) Building own IP network b) NIC-registered addresses	10	12

	c) Use of private IP addresses: application proxy firewalls d) IPv6 **IP on different physical networks** a) IP on non-Ethernet LANs: SNAP and LLC b) Using IP on WANs c) IP on ATM d) IP on DSL		
4	**Internetworking with IP Routers** **Implementing routed networks** a) The Role of IP router b) Common IP routing protocols: RIP, OSPF c) Troubleshooting router problems **Intranet** a) Subdividing IP networks (subnetting) b) Control messages on IP networks: ICMP c) Subnetting and supernetting calculation formulas d) Classless Inter-Domain Routing (CIDR) e) Network Address Translation (NAT)	06	08
5	**Transport and Protocols: TCP and UDP** **Transport Layer fundamentals** a) The Role of the transport protocol b) Comparison of Reliable with best-effort services **The Transmission Control Protocol (TCP)** a) Reliable data delivery with TCP b) Stating remote applications using port numbers and process addressing c) TCP packet structure d) TCP performance issues e) Troubleshooting the protocol **User Datagram Protocol** a) Connectionless protocol operation b) Providing reliability at the Application Layer	06	04
6	**Applications and Management Protocols** **Functions and operation of application protocols** a) File transfer protocols: FTP, TFTP b) Network Virtual Terminal (TELNET) c) Employing DNS BIND d) SMTP e) Utilizing workstation mail: POP3, IMAP4 f) Mechanisms of VoIP **Vendor implementations** a) File sharing with NFS b) NFS protocols: RPC, XDR and other protocols c) TCP/IP for Windows Server 2003/NT and XP and UNIX **Managing TCP/IP networks** a) SNMP management paradigm b) Simple Network Management Protocol (SNMP)	10	12

	c) Management database: MIB d) SNMP evolution: MIB I and II, RMON, SNMPv2, SNMPv3		
7	**Exploring Internet Services** **Internet service access methods** a) Permanent direct connection **b)** Building virtual private networks (VPNs) with PPP **Internet service tools** a) Retrieving files using Anonymous FTP b) Using World Wide Web (WWW) tools	06	02
	TOTAL	**48**	**50**

LIST OF PRACTICALS:

1. Configuring a Network.
2. Deploying protocol analysis techniques for Internet protocols: IP, ARP, TCP, UDP and HTTP.
3. Solving duplicate IP address problems.
4. Troubleshooting IP configuration problems.
5. Building internets with IP routers: configuration and testing.
6. Troubleshooting TCP/IP networks with ICMP and ping.
7. Exploiting FTP and TELNET.
8. Performing detailed protocol analysis of FTP sessions.
9. Decoding HTTP traffic.

Reference Books:

Sr. No	Title	Author	Publisher
1	Data Communications and Networking	Behrouz A Forouzan and Behrouz Forouzan	Tata McGraw Hill
2	Computer Networks (4th Edition)	Andrew S. Tanenbaum	Prentice Hall Ptr
3	Computer Networking with Internet Protocols	William Stallings	Person Education Ltd.
4	Data and Computer Communications (8th Edition)	William Stallings	Prentice Hall of India Pvt. Ltd.
5	MCSE Guide to Networking Essentials	David Johnson and Ed Tittel	Thomson Leaning

Website references:

1 .http://www.interhack.net/pubs/network-security/

2. http://www.networkcomputing.com/

COURSE NAME : Advance Diploma in Cyber Security Management

COURSE CODE : CB

SEMESTER : First

SUBJECT TITLE : Operating System Concepts

SUBJECT CODE : 11042

Teaching and Examination Scheme:-

TEACHING SCHEME			EXAMINATION SCHEME					
TH	TU	PR	PAPER HRS	TH	PR	OR	TW	TOTAL
3	---	2	3	100	--	50#	50@	200

RATIONALE:

The Students will be able to understand the concepts of Operating systems. It will also help in understanding the importance of operating system.

OBJECTIVES: Students will be able to understand

1. Operating System and Technique involved in designing the Operating System.
2. Functioning of operating system.
3. Structure of operating system.
4. Function of thread, process.
5. Concept of CPU Scheduling.
6. Memory management.
7. Process of handling deadlock.
8. System management.

CONTENTS: Theory

Chapter	Contents	Hours	Marks
1	**Introduction to OS** a) Functions of Operating Systems b) Computer-System Organization c) Computer-System Architecture d) Operating-System Structure e) Operating-System Operations f) Process Management g) Memory Management h) Storage Management i) Protection and Security j) Distributed Systems k) Special-Purpose Systems l) Computing Environments	04	08
2	**Operating system structures** a) Operating-System Services b) User Operating-System Interface c) System Calls d) Types of System Calls e) System Programs f) Operating-System Design and Implementation g) Operating-System Structure h) Virtual Machines i) Java j) Operating-System Generation k) System Boot	04	08
3	**Processes** a) Process Concept b) Process Scheduling c) Operations on Processes d) Inter process Communication e) Examples of IPC Systems f) Communication in Client-Server Systems	03	04
4	**Threads** a) Overview b) Multithreading Models c) Thread Libraries d) Java Threads e) Threading Issues f) Operating System Examples	03	08

5	**CPU scheduling** a) Basic Concepts b) Scheduling Criteria c) Scheduling Algorithms d) Multiple-Processor Scheduling e) Thread Scheduling f) Operating System Examples g) Java Scheduling h) Algorithm Evaluation	04	08
6	**Process Synchronization** a) Background b) The Critical-Section Problem c) Peterson's Solution d) Synchronization Hardware e) Semaphores f) Classic Problems of Synchronization g) Monitors h) Java Synchronization i) Synchronization Examples	04	08
7	**Deadlocks** a) System Model b) Deadlock Characterization c) Methods for Handling Deadlocks d) Deadlock Prevention e) Deadlock Avoidance f) Deadlock Detection g) Recovery from Deadlock	04	12
8	**Memory Management** **Main Memory** a) Definition of Memory b) Logical versus Physical address space c) Swapping d) Contiguous Memory Allocation e) Paging f) Structure of the Page Table g) Segmentation **Virtual Memory** a) Background b) Demand Paging c) Copy-on-Write d) Page Replacement e) Allocation of Frames f) Thrashing g) Memory-Mapped Files h) Allocating Kernel Memory i) Other Considerations j) Operating-System Examples	08	12

9	**Storage Management** **File-System Interface** a) The Concept of a File b) Access Methods c) Directory Structure d) File-System Mounting e) File Sharing f) Protection **File-System Implementation** a) File-System Structure b) File-System Implementation c) Directory Implementation d) Allocation Methods e) Free-Space Management f) Efficiency and Performance g) Recovery h) Log-Structured File Systems i) NFS j) Example: The WAFL File System **Mass-Storage Structure** a) Overview of Mass-Storage Structure b) Disk Structure c) Disk Attachment d) Disk Scheduling e) Disk Management f) Swap-Space Management g) RAID Structure h) Stable-Storage Implementation i) Tertiary-Storage Structure	06	12
10	**I/O Systems** a) Overview b) I/O Hardware c) Application I/O Interface d) Kernel I/O Subsystem e) Transforming I/O f) Requests to Hardware Operations g) STREAMS h) Performance	04	08

11	**Protection And Security** **Protection** a) Goals of Protection b) Principles of Protection c) Domain of Protection d) Access Matrix e) Implementation of Access Matrix f) Access Control g) Revocation of Access Rights h) Capability-Based Systems i) Language-Based Protection **Security** j) The Security Problem k) Program Threats l) System and Network Threats m) Cryptography as a Security Tool n) User Authentication o) Implementing Security Defenses p) Fire walling to Protect Systems and Networks q) Computer-Security r) An Example: Windows XP	04	12
	Total	**48**	**100**

Case Studies:

Any Operating system as per the choice of the students

LIST OF PRACTICALS:

1. Installation of Window and Linux, operating System.
2. Adding devices (printer, fax machine, Scanner, Mouse etc.)
3. Adding or removing Program / Software.
4. Configuring Local Security Policy, Event Viewer, Performance, Service of the System.
5. Creating, deleting, updating user account.
6. Confirming Firewall.
7. Setting up wi-fi connectivity.
8. Setting up home or small office network.
9. Setting Program Access & Default.
10. Configuring & Setting Internet properties.
11. Configuring Security.

Reference Books:

Sr. No	Title	Author	Publisher
1	Operating System Concepts (7th Edition)	Abraham Silberschatz, Peter Baer Galvin, and Greg Gagne	John Wileye & Sons
2	Applied Operating System Concepts	Abraham Silberschatz, Peter Baer Galvin, Peter Galvin, and Avi Silberschatz	John Wileye & Sons Inc (sea) Pvt. Ltd.
3	Advanced Concepts In Operating Systems	Mukesh Singhal and Niranjan Shivaratri	McGraw Hill
4	Operating Systems: Concepts and Examples	William Stallings	Prentice Hall
5	Distributed Operating Systems: Concepts and Design	Pradeep K. Sinha	Prentice Hall of India Pvt. Ltd.

Website references:

1. http://computer.howstuffworks.com/operating-system.htm
2. http://www.computerhope.com/os.htm#01
3. http://en.wikipedia.org/wiki/Operating_system

COURSE NAME : Advance Diploma in Cyber Security Management

COURSE CODE : CB

SEMESTER : First

SUBJECT TITLE : Forensic Science

SUBJECT CODE : 11043

Teaching and Examination Scheme:-

TEACHING SCHEME			EXAMINATION SCHEME					
TH	TU	PR	PAPER HRS	TH	PR	OR	TW	TOTAL
3	--	2	3	100	50#	--	50@	200

RATIONALE:

The students will be able to recover important data by using various technologies.

It will help in minimizing the data loss which could happen frequently.

OBJECTIVES: Students will be able to understand

1. Basics of forensic science.
2. Requirement for recovering data.
3. Investigations techniques of computer crime using forensic science.
4. Storage device information.
5. Use of different technologies for data recovery.
6. Methods, techniques and tools for data recovery.
7. Digital picture recovery.
8. Formation of Incident Response Team.

CONTENTS: Theory

CHAPTER	CONTENTS	Hours	Marks
1	**Overview** a) Introduction to Forensic Science b) Types of Forensic Science c) Impact of computer forensic on judiciary d) Forensic process	08	12

2	**Storage device** a) Introduction b) Types of Storage devices c) Architecture of storage device d) Application of storage device	08	12
3	**Forensic Investigator** a) Role of Computer Forensic Investigator b) Analysis of Computer by Forensic Investigator c) Procedure to be adopted by Computer Forensics Investigator d) Responsibility of Computer Forensic Investigator e) Case Study	08	20
4	**Evidence** a) Definition of evidence b) Life cycle of evidence c) Types of evidence d) Rules for evidence e) Evidence Storage and Security f) Case Study	08	20
5	**Incident Response** a) Introduction b) Investigations c) Pre Incident Preparation d) Formation of Incident Response Team e) Role of Incident Response Team f) Case Study	08	16
6	**Data recovery** a) Definition of data recovery b) Data recovery mechanism. c) Techniques for recovering data d) Tools for recovering data e) Case Study	08	20
	Total	**48**	**100**

LIST OF PRACTICALS:

Forensic Science

1. Documentary evidence and presenting it in court for legal proceeding
2. Recovering data from formatted and corrupted disk
3. Translating data in different language to readable form
4. Recovering cookies ,data from cache memory
5. Reading and interpreting log sheets
6. Getting logged to remote machines
7. Recovering deleted pictures/images from the system

Reference Books:

Sr. No	Title	Author	Publisher
1	Forensic Science: The Basics	Jay A. Siegel	Crc Press
2	Crime Science: Methods of Forensic Detection	Joe Nickell and John F. Fischer	University Press of Kentucky
3	Forensic Science: Fundamentals and Investigations	Anthony J. Bertino	South Western Educational Publishing
4	Forensic Science: An Introduction to Scientific and Investigative Techniques, 2nd edition	Stuart H. James and Ph.D., Jon J. Nordby	Crc Press
5	The Casebook of Forensic Detection: How Science Solved 100 of the World's Most Baffling Crimes	Colin Evans	John Wiley & Sons
6	Criminalistics: An Introduction to Forensic Science (College Version) (9th Edition)	Richard Saferstein	Prentice Hall
7	The Forensic Casebook: The Science of Crime Scene Investigation	Ngaire E. Genge	Ballantine Books
8	Fundamentals of Forensic Science	Max M. Houck and Jay A. Siegel	Academic Press
9	Forensic Science (2nd Edition)	Andrew R.W Jackson and Julie M. Jackson	Pearson Prentice Hall
10	Forensic Science: and Practical Skills in Forensic Science	Andrew R.W Jackson, Julie M Jackson, Alan M Langford, and John Dean	Prentice Hall
11	The Complete Idiot's Guide to Forensics, 2nd Edition (Complete Idiot's Guide to)	Ph.D., Alan Axelrod and J.D., Guy Antinozzi	Alpha Books
12	Forensic Science Handbook, Volume 1 (2nd Edition) (Forensic Science Handbook)	Richard Saferstein	Prentice Hall
13	Forensic Science (DK Eyewitness Books)	Chris Cooper	DK Publishing (Doorling Kindersley)
14	Forensic Science Laboratory Manual and Workbook, Revised Edition	Thomas Kubic and Nicholas Petraco	Crc Press
15	Forensic Science of CSI	Katherine M. Ramsland	Berkley Publishing Group
16	Introduction to Forensic Science and Criminalistics	Robert E Gaensslen, Howard Harris, and Henry C Lee	McGraw Hall Humanities/ Social Sciences/Langua
17	Forensic Science: Modern Methods of Solving Crime	Max M. Houck	Praeger Publisher
18	Ethics in Forensic Science:	Peter D. Barnett	Crc Press

	Professional Standards for the Practice of Criminalistics (Protocols in Forensic Science)		
19	Physical Evidence in Forensic Science	Henry C. Lee and Howard A. Harris	Lawyers and Judges Publishing

Website reference:

1. www.computerforensics.com
2. www.datapriage.com
3. http://en.wikipedia.org/wiki/Computer_forensics
4. http://www.computerforensicsworld.com/

COURSE NAME : Advance Diploma in Cyber Security Management
COURSE CODE : CB
SEMESTER : First
SUBJECT TITLE : System and Network Security
SUBJECT CODE : 11044

Teaching and Examination Scheme:-

TEACHING SCHEME			EXAMINATION SCHEME					
TH	TU	PR	PAPER HRS	TH	PR	OR	TW	TOTAL
3	---	4	3	100	50#	--	50@	200

RATIONALE: In today's Internet-dependent business environment, organizations must link their systems across enterprise-wide and virtual private networks, as well as connect mobile users. Each connection increases exposure to customers, competitors and hackers, magnifying vulnerability to attack. In this course, the students will learn how to analyze risks to networks and the steps needed to select and deploy the appropriate countermeasures to reduce exposure to network threats.

.

OBJECTIVES: Students will be able to understand

1. Analyzing exposure to security threats and protects organization's systems and data.
2. Reducing susceptibility to an attack by deploying firewalls and data encryption.
3. Assessing alternative user and host authentication mechanisms.
4. Managing risks emanating from inside the organization and from the Internet.
5. Protecting network users from hostile applications and viruses.
6. Identifying the security risks that need to be addressed within the organization.

CONTENTS: Theory

Chapter	Contents	Hours	Marks
1	**Real threats that impact security** a) Hackers b) Eavesdropping c) Spoofing d) Sniffing e) Trojan horses f) Viruses g) Wiretaps **Security policy as the foundation of protection** a) Defining information assurance objectives b) Assessing exposure	08	12
2	**Securing data with symmetric encryption** a) Choosing algorithm: DES, AES, RC4 and others b) Assessing key length and key distribution **Solving key distribution issues with asymmetric encryption** a) Generating keys b) Encrypting with RSA c) Working with PGP and GnuPG d) Evaluating Web of Trust and PKI **Ensuring integrity with hashes** a) Hashing with MD5 and SHA b) Protecting data in transit c) Building the digital signature	08	20
3	**Assessing traditional static password schemes** a) Creating a good quality password policy. b) Protecting against social engineering attacks c) Encrypting passwords vs. replay attacks **Evaluating strong authentication methods** a) Challenge-response to prevent man-in-the-middle attacks b) Preventing password replay using one-time and tokenized passwords c) Employing biometrics as part of two-factor authentication **Authenticating hosts** a) Shortcomings of IP addresses b) Address-spoofing issues and countermeasures c) Solutions for wireless networks	08	16

4	**Discovering system vulnerabilities** a) Searching for operating system holes b) Discovering file permission issues c) Limiting access via physical security **Encrypting files for confidentiality** a) Encryption with application-specific tools b) Recovering encrypted data **Hardening the operating system** a) Locking down user accounts b) Securing administrator's permissions c) Protecting against viruses	06	12
5	**Scanning for vulnerabilities** a) Restricting access to critical services b) Preventing buffer overflows **Reducing denial-of-service (DoS) attacks** a) Securing DNS b) Limiting the impact of common attacks : **Deploying firewalls to control network traffic** c) Analyzing shortcomings of stateless packet filters d) Contrasting stateful packet filters with application proxies e) Preventing intrusions with filters **Building network firewalls** a) Evaluating firewall features b) Selecting an architecture and a personal firewall	08	12
6	**Threats from the LAN** a) Sniffing the network b) Mitigating threats from connected hosts c) Partitioning the network to prevent data leakage d) Identifying wireless LAN vulnerabilities **Confidentiality on external connections** a) Ensuring confidentiality with encryption b) Securing data-link layer with PPTP and L2TP c) Middleware information assurance with SSL and TLS d) Deploying SSH (the Secure Shell) **Protecting data with IPsec** a) Authenticating remote locations b) Tunneling traffic between sites c) Exchanging keys	06	16
7	**Managing Organization's Security** a) Developing a security plan b) Responding to incidents c) Enumerating the six critical steps d) Security policy for organization	04	12
	TOTAL	**48**	**100**

List of Practical:

1. Cracking passwords.
2. Scanning systems with Microsoft Baseline Security Analyzer (MBSA).
3. Restricting computer access with biometrics.
4. Preventing unwanted network access with a personal firewall.
5. Encrypting and signing important data.
6. Discovering security best practices.

Reference Books:

Sr. No	Title	Author	Publisher
1	Cryptography and Network Security: Principles and Practice (3rd Edition)	William Stallings	Prentice Hall
2	Computer System and Network Security (Computer Science & Engineering)	Gregory B. White, Eric A. Fisch, and Udo W. Pooch	Crc Press
3	Integrated Security Systems Design: Concepts, Specifications, and Implementation	CPP, PSP, CSC, Thomas L. Norman	Butterworth Heinemann
4	Network Security Hacks	Andrew Lockhart	O'Reilly Media, Inc
5	Computer Network Security	Joseph M. Kizza	Springer
6	Network Security: The Complete Reference	Mark Rhodes-Ousley, Roberta Bragg, and Keith Strassberg	McGraw Hill Osborns Media
7	Incident Response: A Strategic Guide to Handling System and Network Security Breaches (Landmark)	E. Eugene Schultz and Russell Shumway	Sams
8	Fundamentals of Network Security Companion Guide (Cisco Networking Academy Program) (Cisco Networking Academy Program)	Cisco Systems Inc. and Cisco Networking Academy Program	Cisco Press
9	Security of e-Systems and Computer Networks	Mohammad Obaidat and Noureddine Boudriga	Cambridge University Press
10	Information Security Policies and Procedures: A Practitioner's Reference, Second Edition	Thomas R. Peltier	Crc Pree
11	Network Security Technologies and Solutions (CCIE Professional Development Series) (CCIE Professional Development)	Yusuf Bhaiji	Cisco Press

12	Fundamentals of Network Security Lab Companion and Workbook	(Cisco Networking Academy Program)	Cisco Press

Website reference:

1. http://mail.colonial.net/~abeckwith/encrypt.htm
2. http://www.pgpi.org/doc/pgpintro/#p1
3. http://mail.colonial.net/~abeckwith/encrypt.htm

COURSE NAME : Advance Diploma in Cyber Security Management

COURSE CODE : CB

SEMESTER : Second

SUBJECT TITLE : Cyber Security Management

SUBJECT CODE : 11045

Teaching and Examination Scheme:-

TEACHING SCHEME			EXAMINATION SCHEME					
TH	TU	PR	PAPER HRS	TH	PR	OR	TW	TOTAL
3	---	--	3	100	--	--	--	100

RATIONALE:

Students will be able to understand the concepts of Cyber Law.

It will also help to understand the application of laws for different kind of cyber crime.

OBJECTIVES: Students will be able to understand

1. The importance of Cyber Crime Law.
2. The legal aspects of the Cyber crime and the punishments thereto.
3. Contracts in the InfoTech World.
4. Jurisdiction in the Cyber World.
5. Batting Cyber Squatters and Copyright Protection in the Cyber World.
6. E-Commerce Taxation or real problems in the virtual world.
7. Digital Signature, Certifying Authorities and E-Governance.
8. Indian Evidence Act 1872 and the IT Act 2000.

CONTENTS: Theory

Chapter	Contents	Hours	Marks
1	**Cyber Crime and Criminal Justice: Penalties, Adjudication and Appeals under the IT Act, 2000** 1.1 Concept of 'Cyber Crime' and the IT Act, 2000 1.2 Hacking 1.3 Teenage Web Vandals 1.4 Cyber Fraud and Cyber Cheating 1.5 Virus on the Internet 1.6 Defamation, Harassment and E-mail Abuse 1.7 Cyber Pornography 1.8 Other IT Act Offences 1.9 Monetary Penalties, Adjudication and Appeals Under IT Act, 2000 1.10 Network Service Provides 1.11 Jurisdiction and Cyber Crimes 1.12 Nature of Cyber Criminality, Strategies to Tackle Cyber Crime and Trends 1.13 Criminal Justice in India and Implication on Cyber Crime	07	16
2	**Contracts in the InfoTech World** 2.1 Contracts in the InfoTech World 2.2 Click-Wrap and Shrink-wrap Contracts: Status under the Indian Contract Act, 1872 2.3 Contract Formation under the Indian Contract Act, 1872 2.4 Contract Formation on the Internet 2.5 Terms and Condition of Contracts	06	12
3	**Jurisdiction in the Cyber World** 3.1 Questioning the Jurisdiction and Validity of the Present Law of Jurisdiction 3.2 Civil Law of Jurisdiction in India 3.3 Cause of Action 3.4 Jurisdiction and the Information Technology Act,2000 3.5 Foreign Judgments in India 3.6 Place of Cause of Action in Contractual and IPR Disputes 3.7 Exclusive Clauses in Contracts 3.8 Abuse of Exclusive Clauses 3.9 Objection of Lack of Jurisdiction 3.10 Misuse of the Law of Jurisdiction 3.11 Legal Principle on Jurisdiction in the United States of America 8.12 Jurisdiction Disputes with respect to the Internet in the United States of America	07	16

4	**Batting Cyber Squatters and Copyright Protection in the Cyber World** 4.1 Concept of Domain Name and Reply to Cyber Squatters 4.2 Meta-Tagging 4.3 Legislative and Other Innovative Moves against Cyber Squatting 4.4 The Battle between Freedom and Control on the Internet 4.5 Works in Which Copyright Subsists and Meaning of Copyright 4.6 Copyright Ownership and Assignment 4.7 License of Copyright 4.8 Copyright Term and Respect for Foreign Works 4.9 Copyright Infringement, Remedies and Offences 4.10 Copyright Protection and Content on the Internet; Copyright Notice, Disclaimer and Acknowledgement 4.11 Downloading for Viewing Contents on the Internet, Hyper-linking and framing 4.12 Liability of ISPs for Copyright Violation in the Cyber World: Legal Developments in the US 4.13 Napster and its Cousins: A Revolution on the Internet And the Crisis for Copyright Owners 4.14 Computer Software Piracy	07	16
5	**E-Commerce Taxation: Real Problems In the Virtual World** 5.1 A Tug of War on the Concept of 'Permanent Establishment' 5.2 Finding the PE in Cross Border E-Commerce 5.3 The United Nation Model Tax Treaty 5.4 The Law of Double Taxation Avoidance Agreements and Taxable Jurisdiction over Non-Residents, under the Income Tax, 1961 5.5 Tax Agents of Non-Residents under the Income Tax Act, 1961 and the Relevance to E-Commerce 5.6 Source versus Residence and Classification between Business Incomes 5.7 The Impact of the Internet on Custom Duties 5.8 Taxation Policies in India	07	16
6	**Digital Signature, Certifying Authorities and E-Governance** 6.1 Digital Signature 6.2 Digital Signature Certificate 6.3 Certifying Authorities and Liabilities in the Event of Digital Signature 6.4 E-Governance in India	07	12
7	**Indian Evidence Act 1872 vs. IT Act 2000** 7.1 Status of Electronic record as evidence 7.2 Proof and management of electronic record 7.3 Proving Digital Signature 7.4 Proof of Electronic Agreement 7.5 Proving of Electronic Message	07	12
	Total	**48**	**100**

Reference Books:

Sr. No	Title	Author	Publisher
1	Cyber Security by Edward Amoroso Computer Network Security and Cyber Ethics, 2nd edition	Joseph Migga Kizza	Mc Farland & Company
2	Data Warehousing and Data Mining Techniques for Cyber Security (Advances in Information Security)	Anoop Singhal	Springer
3	Security Operations Management, Second Edition	Robert McCrie	Butterworth - Heinemann
4	Risk Management for Computer Security: Protecting Your Network & Information Assets	Andy Jones and Debi Ashenden	Butterworth - Heinemann
5	Risk, Crisis and Security Management	Edward Borodzicz	Wiley
6	Cyber Warfare and Cyber Terrorism (Premier Reference)	Lech J. Janczewski and Andrew M. Colarik	IG1 Global
7	CYBER SECURITY: Economic Strategies and Public Policy Alternatives	Michael P. Gallaher, Albert N. Link, and Brent R. Rowe	Edward Elgar Publishing
8	The Transnational Dimension of Cyber Crime and Terrorism (Hoover National Security Forum Series)	Mariano-Florentino Cuellar, Ekaterina A. Drozdova, David D. Elliott, and Seymour E. Goodman	Hoover Institution Press
9	KNOW Cyber Risk: By Managing Your IT Security!	James P. Litchko and Al Payne	KNOW Book Publishing
10	Cyber Security: Turning National Solutions into International Cooperation (Csis Significant Issues Series)	James Andrew Lewis	Center for Strategic & International Studies
11	International Guide to Cyber Security	Jody R. Westy	American Bar Association
12	Fundamentals of Computer Security Technology	Edward Amoroso	Prentice Hall PTR

Website references:

1. www.legalserviceindia.com
2. www.mit.gov.in
3. http://www.us-cert.gov/cas/tips/ST04-001.html

COURSE NAME : Advance Diploma in Cyber Security Management

COURSE CODE : CB

SEMESTER : Second

SUBJECT TITLE : Intrusion Detection System

SUBJECT CODE : 11046

Teaching and Examination Scheme:-

TEACHING SCHEME			EXAMINATION SCHEME					
TH	TU	PR	PAPER HRS	TH	PR	OR	TW	TOTAL
3	---	2	3	100	50#	--	50@	200

RATIONALE:

Students will be able to understand the concepts of Intrusion Detection System and As well as distinguish between available security system and IDS. Students will also understand security provision, uses of IDS, vulnerabilities and use of IDS to resolve the particular vulnerability.

OBJECTIVES: Students will be able to understand

1. The Importance of IDS System.
2. Uses of intrusion detection system.
3. The Security problems and solutions.
4. Security providing using IDS and architecture of IDS.
5. Securing servers and workstations.
6. Handling intrusion.
7. Alarm management.
8. Administering an intrusion detection system.
9. Tools for detecting Intrusion and analyzing vulnerability.

CONTENTS: Theory

Chapter	Contents	Hours	Marks
1	• Overview of intrusion detection system • Uses of intrusion detection systems • Classification of intrusion detection system • Secure Intrusion Detection Environment	06	12

2	• A General IDS model • Alarm monitoring • Alarm Management • IP Blocking Configuration	07	12
3	• Secure Intrusion Detection System Architecture • Common security threats and their characteristics	07	12
4	• Security problems with TCP/IP: fragmentation, ICMP, OS fingerprinting, DNS, SYN flood, etc. • Tools for detecting Intrusion and analyzing vulnerability and commercial use of free software	07	16
5	• Architecture of an intrusion detection system: IDS vs. IPS, physical and logical location in the network, system disturbance analysis and system abuse detection, alarms, logging, link with the security gateway and false positives • Securing servers and workstations	07	16
6	• Trace analysis • Plan for handling intrusions • Maintaining intrusion detection system	07	16
7	• Administering an intrusion detection system • Techniques in intrusion detection system • Case studies: exercises, trace analyses	07	16
	Total	**48**	**100**

Reference Books:

Sr. No	Title	Author	Publisher
1	Implementing Intrusion Detection Systems: A Hands-On Guide for Securing the Network	Tim Crothers	Wiley Pub 2002
2	Cisco Secure Intrusion Detection System	Earl Carter	Cisco Press 2001
3	Cisco Security Professional's Guide to Secure Intrusion Detection Systems	Michael Sweeney, C. Tate Baumrucker, James. D. Burton, and Ido Dubrawsky	Syngress 2003
4	Intrusion Detection Systems, Second Edition	Robert Barnard	Butterworths 1988
5	Intrusion Detection Systems (Advances in Information Security)	Roberto Di Pietro and Luigi V. Mancini	Springer 2008
6	CCSP Self-Study: Cisco	Earl Carter and Cisco	Cisco Press

	Secure Intrusion Detection System (CSIDS) (2nd Edition) (Self-Study Guide)	Systems Inc.	
7	Intrusion Detection in Distributed Systems: An Abstraction-Based Approach (Advances in Information Security)	Peng Ning, Sushil Jajodia, and Xiaoyang Sean Wang	Springer
8	Computer Immune System for Intrusion and Virus Detection - Adaptive Detection Mechanisms and their Implementation	Markus Unterleitner	VDM Verlag Dr. Mueller e. k.
9	Intrusion Detection Systems: Annotated Instructor's Guide, (33402-03)	NCCER	Prentice Hall
10	Intrusion Detection Systems: 33402-03, Trainee Guide	NCCER	Pearson Education Ltd.

Website reference:

1. http://www.intrusion-detection-system-group.co.uk/
2. http://www.intrusion-detection-system-group.co.uk/faq.htm
3. http://www.webopedia.com/TERM/I/intrusion_detection_system.html
4. http://www.nerc.com/files/CIP-003-1.pdf

COURSE NAME : Advance Diploma in Cyber Security Management

COURSE CODE : CB

SEMESTER : Second

SUBJECT TITLE : Mobile Security

SUBJECT CODE : 11047

Teaching and Examination Scheme:-

TEACHING SCHEME			EXAMINATION SCHEME					
TH	TU	PR	PAPER HRS	TH	PR	OR	TW	TOTAL
3	---	2	3	100	--	50#	50@	200

RATIONALE:

Students will be able to understand the importance of mobile computing and as well as and importance of security in mobile computing.

OBJECTIVES: Students will be able to understand

1. Importance of Mobile Technology.
2. Security is provided to mobile computing and the tools, techniques used for establishing secure mobile network.
3. Backup and restoration of mobile.
4. Different mobile related crimes.
5. Ways to detect mobile crime.
6. VOIP technology.

CONTENTS: Theory

Chapter	Contents	Hours	Marks
1	**Introduction** 1.1 Mobile –Working Principles, functioning 1.2 Wireless handheld device 1.3 Service providers 1.4 Working of mobile phone network 1.5 WAP 1.6 I-mode 1.7 Messaging services	04	12

2	**Wireless network** 2.1 WLAN 2.2 IEEE 802.11 standards 2.3 HIPERLAN European alternative WWAM 2.4 WPN 2.5 Fixed wireless	06	12
3	**Technologies in Mobile Computing** 3.1 Wireless communication technologies 3.2 Wireless access technologies 3.3 Location based services and technologies 3.4 E-businesses	06	12
4	**Mobile Related Crimes** 5.1 Bluetooth hacking 5.2 Mobile Dos attack 5.3 Different types of attacks 5.4 SMS attack 5.5 Mobile IMEI number attack	06	12
5	**Detection Mobile Crimes** 6.1 Unblock 6.2 SIM card Cloning 6.3 Tool and techniques for detecting mobile crime 6.4 Detection of SMS attack	08	12
6	**Security Tips and Tricks of** 7.1 Displaying the International Mobile Equipment Identity number 7.2 Displaying the serial number 7.3 Displaying the mobile software firmware version 7.4 Unlocking the service provider lock	06	12
7	**Mobile Backup** 8.1 Mobile Backup and Restoration 8.2 Hardware tools for Mobile Backup 8.2.1 USB SIM Card Reader/writer 8.2.2 Data Cable	06	12
8	**VOIP Technology** 9.1 Functionality 9.2 Methods for connecting call 9.3 Benefits of VOIP 9.4 Challenges of VOIP	06	16
	Total	**48**	**100**

LIST OF PRACTICALS:

Mobile Security

1. Setting up wireless communication technology connectivity.
2. Hands on different Mobile Related Crimes
3. SIM card cloning

4. Tool and Techniques for detecting mobile crime
5. Defining the International Mobile Equipment Identity number, Serial number
6. Trace Handset, Bluetooth device, SMS

Reference Books:

Sr. No	Title	Author	Publisher
1	Mobile Security	Kai-Oliver Detken	Hanser Fachbuchverlag
2	Wireless Security Essentials: Defending Mobile Systems from Data Piracy	Russell Dean Vines	John Wiley & Sons, 2002
3	Embedded Java Security: Security for Mobile Devices	Mourad Debbabi, Mohamed Saleh, Chamseddine Talhi, and Sami Zhioua	Springer
4	Mobile and Wireless Network Security and Privacy	S. Kami Makki, Peter Reiher, Kia Makki, and Niki Pissinou	Springer
5	Mobile Phone Programming: and its Application to Wireless Networking	Frank H.P. Fitzek and Frank Reichert	Springer
6	Resource, Mobility, and Security Management in Wireless Networks and Mobile Communications	Yan Zhang, Honglin Hu, and Masayuki Fujise	Auerbach Publication
7	Wireless Personal Area Networks: Performance, Interconnection, and Security with IEEE 802.15.4 (Wireless Communications and Mobile Computing)	Jelena Misic and Vojislav Misic	John Wiley & Sons Ltd
8	AAA and Network Security for Mobile Access: Radius, Diameter, EAP, PKI and IP Mobility	Madjid Nakhjiri and Mahsa Nakhjiri	Wiley
9	Malicious Mobile Code: Virus Protection for Windows (O'Reilly Computer Security)	Roger Grimes	O'Reilly Media, Inc
10	Advances in Security and Payment Methods for Mobile Commerce	Chung-wei Lee, Weidong Kou, and Wen Chen Hu	Idea Group Publishing
11	CDMA Cellular Mobile Communications and Network Security	Man Young Rhee	Prentice Hall
12	Disruptive Security Technologies with Mobile Code and Peer-to-Peer Networks	Richard R. Brooks	Crc Press
13	Security for Mobile Networks	Selim Aissi, Nora	Artech House

	and Platforms (Artech House Universal Personal Communications)	Dabbous, and Anand R. Prasad	Publisher
14	Security of Mobile Communications	Noureddine Boudriga	Crc Press Auerbach Publication

Website reference:

1. www.intel.com/in
2. www.techgadgets.in/mobile
3. www.rimweb.in
4. http://www.informit.com/guides/content.aspx?g=security&seqNum=92

COURSE NAME : Advance Diploma in Cyber Security Management

COURSE CODE : CB

SEMESTER : Second

SUBJECT TITLE : Ethical Hacking

SUBJECT CODE : 11048

Teaching and Examination Scheme:-

TEACHING SCHEME			EXAMINATION SCHEME					
TH	TU	PR	PAPER HRS	TH	PR	OR	TW	TOTAL
3	---	2	3	100	50@	--	--	150

RATIONALE:

Students will be able to understand the concepts of hacking, types of hacking attacks, spoofing concepts and role of hackers.

OBJECTIVES: Students will be able to understand

1. Concepts of Hacking.
2. Types of hacking attacks and solution for such kind of attacks.
3. Session Hijacking and protection against such kinds of hijacking.
4. Concept of spoofing.
5. Denial of service attack, buffer overflow attack.
6. Preventing DOS attack and buffer overflow attack.
7. Password security.
8. Information gathering techniques.

CONTENTS: Theory

Chapter	Contents	Hours	Marks
1	**Introduction** 1.1 The Golden Age of Hacking. 1.2 The Problem and its security. 1.3 Measures adopted by Companies. 1.4 Defense.	06	12
2	**How And Why Hackers Attack** 2.1 Definition of Exploit 2.2 The Attacker's Process 2.3 Types of Attacks. 2.4 Categories of Exploits. 2.5 Routes attackers. 2.6 Goals of attackers.	06	12
3	**Information Gathering** 3.1 Steps for Gathering Information. 3.2 Information Gathering Summery. 3.3 Red Teaming.	06	12
4	**Spoofing** 4.1 Spoofing 4.2 Types of Spoofing.	04	04
5	**Session Hijacking** 5.1 Spoofing versus Hijacking. 5.2 Types of Session Hijacking. 5.3 TCP/IP Concept. 5.4 Detailed Description Of Session Hijacking. 5.5 ACK Storms. 5.6 Protection Against Session Hijacking.	08	08
6	**Denial Of Service Attacks** 6.1 Denial Of Service Attacks 6.2 Distributed Denial Of Service Attacks 6.3 Types of Denial of Service Attacks. 6.4 Tools for Running DOS Attacks. 6.5 Prevention Denial of Service Attacks 6.6 Prevention Distributed Denial Of Service Attacks	04	12
7	**Buffer Overflow Attacks** 7.1 Buffer Overflow attack 7.2 Working of Buffer Overflow Attack 7.3 Types of Buffer Overflow Attacks. 7.4 Reason of Programs Vulnerable 7.5 Protecting Our Sample Application. 7.6 Protecting Against Buffer Overflow Attacks.	04	12
8	**Password Security** 8.1 Typical Attack. 8.2 Current State Of Passwords. 8.3 History of Passwords. 8.4 Future of Passwords. 8.5 Password Management. 8.6 Password Attacks.	04	12

9	**Other Types Of Attacks** 9.1 Bind 8.2 NXT Exploit. 9.2 Cookies Exploit. 9.3 SNMP Community Strings. 9.4 Sniffing And Dsniff. 9.5 PGP ADK Exploit. 9.6 Cisco IOS Password Vulnerability. 9.7 Man-In-The-Middle Attack Against Key Exchange. 9.8 HTTP Tunnel Exploit.	06	16
	Total	**48**	**100**

LIST OF PRACTICALS:

Hacker's techniques & Exploits

1. Find open port or access port and Port scanning , nslookup, whois, ping (information gathering)
2. Perform various type of spoofing attack(IP, Email, wed Spoofing)
3. Monitor and hijack connection on single host.(TTY&IP watcher)
4. Preventing Distributed Denial of service attacks (scanning , zombie tools)
5. Protecting against buffer overflow attacks.
6. Password recovery of Applications System.

Reference Books:

Sr. No	Title	Author	Publisher
1	Ethical Hacking	EC-Council	Osb Publisher Pte Ltd.
2	The Unofficial Guide to Ethical Hacking, Second Edition	Ankit Fadia	--
3	The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking	Ronald L. Krutz and Russell Dean Vines	Wiley
4	CEH: Official Certified Ethical Hacker Review Guide: Exam 312-50	Kimberly Graves	Sybex
5	Hands-On Ethical Hacking and Network Defense	Michael T. Simpson	Course Technology
6	Certified Ethical Hacker Exam Prep (Exam Prep 2 (Que Publishing)	Michael Gregg	Que (April 17, 2006)
7	Ethical Hacking ; An Introduction	Ravi Kumar Jain B.	Institute of chartered financial
8	The Ethical Hack: A Framework for Business Value Penetration Testing	James S. Tiller	Auerbach Publications
9	Network Security and Ethical Hacking	Rajat, Khare	Luniver Press

10	Intrusion Alert: An Ethical Hacking Guide to Intrusion Detection	Ankit Fadia	Vikas Publishing House
11	Hacker's Challenge 3 (Hacking Exposed)	David Pollino, Bill Pennington, Tony Bradley, and Himanshu Dwivedi	Mc Graw Hill Osbarne Media
12	The Complete Hacker's Handbook : Everything You Need to Know About Hacking in the Age of the Web	Dr. X and Dr. X	Carlton Books LTD
13	Google Hacking: An Ethical Hacking Guide to Google	Ankit Fadia	Course Technology

Website reference:

1. http://www.research.ibm.com/journal/sj/403/palmer.html
2. http://www.hackertopsites.com/
3. http://www.research.ibm.com/journal/sj/403/palmer.html

COURSE NAME : Advance Diploma in Cyber Security Management

COURSE CODE : CB

SEMESTER : Second

SUBJECT TITLE : Professional Practices

SUBJECT CODE : 11049

Teaching and Examination Scheme:-

TEACHING SCHEME			EXAMINATION SCHEME					
TH	TU	PR	PAPER HRS	TH	PR	OR	TW	TOTAL
--	--	4	--	--	50#	--	50@	100

RATIONALE:

The Students will be able to solved present bridges taking place in the Cyber world. It will also help in minimizing crime done by using technology.

OBJECTIVES: Students will be able to understand

1. Types of computer crimes taking place.
2. Principles used in Cyber Security breaches to gain access to Cyber Security System.
3. Various data recovery service
4. Top virus threats, spy ware threats
5. Unauthorized access to web site and its prevention.
6. Configuring user authentication
7. Opening Proxy Server Statistics and Defacement Statistics
8. Encryption of confidential data exchange with client

CONTENTS: Theory

Chapter	Contents
1	**Different Utilities and Tools** • Dos Emergency Scan**:** Virus Cleaning. Copy to C:\, Restarting PC in MS-Dos Mode and Run zvdos.exe • Scanner for Sality_M, Sality_J, Brontok, Parite, Funlove, Passma Unzip to a folder and run "Passmacleaner.exe" • Windows based win32.Parite.B Cleaning Utiltiy • "Severe Problem / Access Denied" Solution for Win XP Sp2 PCs • Unhide folders on Pen Drives / Memory cards / Cameras hidden by viruses • Deleting the Activation Code from PC, for Renewal and Demo to full • Autorun and Browser Entries • Old version customers hot-fix for sohandad type Virus • Strong Delete file on Re-Boot • Deleting fujacks desktop.ini files • Save to Desktop, copy to floppy / CD boot using 98 bootable CD and copy to C:\winnt\system32 folder
2	**Data Recovery Services** • Emergency, Weekend, and Priority Service. • Hard disk drive data repair and recovery. • Floppy, zip disk, CD and DVD recovery. • Magnetic tape recovery. • RAID Repair and Recovery - (RAID 0, 1, 5, 0+1, 10). • Corrupted File System repair and recovery. • Media and Data Conversion. • Data Destruction and Drive Sanitation
3	**Top Virus Threats** • Virtob.x / Virut.o • VBS.Pica.E (ms32dll.dll) • Trojan.VB.Po (Surabya Thumbs.db) • DuncoDakno fun.exe • Orkut / Firefox Banned
4	**Top Spy ware Threads** • Fujacks • Fakefolder.A • FakeRecycled.C • PWS.OnlineGames • FotoMoto.E • Viking
5	**Incidents in Events and their Solutions**
6	**Virus Alerts** • Zonebac Trojan • Scrapkut Orkut Worm • MBR Rootkit • MMS Worm BESELO
7	**Open Proxy Server Statistics**

8	**Defacement Statistics**
9	**Overview of securing website and application** • Process for securing web site and application
10	**Reducing the attack surface of the web server** • Enabling only Essential windows server 2003 components and services • Enabling only Essential IIS component and services • Enabling only Essential web service Extension • Enabling only Essential MIME Type
11	**Preventing unauthorized access to web site and application** • Storing content on Dedicated disk Volume • Setting IIS web site permission • Setting IP address and domain name Registration • Setting NTFS Permission
12	**Isolating web site and application** • Evaluating the Effect of Impersonation on Application Compatibility • Configuring web sites and application for Isolation • Adding web site to an IIS server
13	**Configuring user authentication** • Configuring web site authentication • Selecting web site authentication method • Configuring FTP site Authentication
14	**Encrypting confidential data exchange with client** • Using SSL to encrypt confidential data • Using IPsec or VPN with remote Administration

Reference Books:

Sr. No	Title	Author	Publisher
1	Wireless Hacking: Projects for Wi-Fi Enthusiasts	Lee Barken, Eric Bermel, John Eder, and Matt Fanady	Syngress
2	Network Security: A Hacker's Perspective	Ankit Fadia	Course Technology PTR
3	Hack Proofing Your Web Applications	Ryan Russell and Syngress Publishing	Syngress
4	Crime and the Internet	David Wall	Routledge
5	The CISSP Prep Guide: Mastering the Ten Domains of Computer Security	Ronald L. Krutz, Russell Dean Vines, and Edward M. Stroz	Wiley
6	Information Ethics: Privacy and Intellectual Property	Lee Freeman and A. Graham Peace	Information Science Publishing
7	Complete Hackers Handbook PB	Dr K	Carlton Book LTD
8	Internet Security: Hacking, Counterhacking and Security	Kenneth Einar Himma	Jones & Bartlett Publication
9	Hacking the Code: ASP.NET Web Application Security	Mark Burnett	Syngress
10	Testing Code Security	Maura A. van der Linden	Auerbach Publication
11	Hacking iPod and iTunes (ExtremeTech)	Scott Knaster	Wiley

12	The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers	Kevin D. Mitnick and William L. Simon	Wiley Publication Inc
13	Steal This Computer Book 4.0: What They Won't Tell You About the Internet	Wallace Wang	No Starch Press
14	Current Security Management & Ethical Issues of Information Technology	Rasool Azari	Irm Press
15	Build Your Own Security Lab: A Field Guide for Network Testing	Michael Gregg	Wiley; Pap/Dvdr edition

Website reference

1. http://www.computerworld.com/mobiletopics/mobile/story/0,10801,91313,00.html
2. http://en.wikipedia.org/wiki/Internet_security