MANONMANIAM SUNDARANAR UNIVERSITY
TIRUNELVELI-627 012, TAMILNADU, INDIA

CENTRE FOR INFORMATION TECHNOLOGY AND ENGINEERING

Board of Studies Meeting held on 29-03-2022

Master of Science (M.Sc.) Degree course in
CYBER SECURITY

(CBCS-University Department)

Regulations, Scheme and LOCF based Syllabus
For those who joined from the academic year 2022-23 onwards

Submitted By
Chairman, BOS and Head ,
Centre for Information Technology and Engineering, MSU

To

The Registrar
Manonmaniam Sundaranar
University
Tirunelveli – 626 012

MANONMANIAM SUNDARANAR UNIVERSITY

TIRUNELVELI, TAMILNADU

DEPARTMENT OF CENTRE FOR INFORMATION TECHNOLOGY AND ENGINEERING

The Objective of CITE Department is to create IT manpower catering to the need and expectations of IT Industry capable of making decisions that demonstrate their standing of being an ethical computing professional; Impart Applied communication skills to students in order to promote ideas in IT engineering and technology fields.

Vision

The CITE Department Aims to become a Center of Excellence in Core fields of Information Technology and Engineering with its efficient teaching and innovative research environment that makes knowledgeable and competent professionals who are socially oriented human beings.

Mission

The mission of Information Technology and Engineering Department is to educate students in IT And Engineering fields by providing in state-of-art knowledge IT in order to enable them create and consume information for an Ever-Dynamic Information Society in an ethical way.

MANONMANIAM SUNDARANAR UNIVERSITY
TIRUNELVELI-627 012, TAMILNADU, INDIA

CENTRE FOR INFORMATION TECHNOLOGY AND ENGINEERING

Master of Science (M.Sc.) Degree course in
CYBER SECURITY
(CBCS-University Department)
Regulations, Scheme and LOCF based Syllabus
(For those who joined from the academic year 2022-23 onwards)

PREAMBLE

Objective of the Programme:

- ❖ Master of Science or MSc in Cyber Security is a 2-year long postgraduate level degree course indoctrinating the study of cyber laws and cyber security.
- ❖ It includes the study of communication networks and technologies along with the analysis of legal and ethical issues in cyber security.
- ❖ It also comprises essential skills desired to protect and defend computer systems and networks.

Curriculum Highlights:

- ➢ Master of Science or MSc in Cyber Security has a curriculum that the graduate is accomplished in gaining knowledge in different domains of the cyber security.
- ➢ As this programme is a multi-disciplinary, this curriculum focuses on the subdomains like malware analysis, web scecurity, IoT security and more.

Knowledge through MOOCs and Credit through University:

- ✓ Graduate can undergo any of the courses available on Massive Open Online Courses - MOOC platform SWAYAM, edX, etc that can be credit transferred to the course basket as equivalent to classroom-based courses based on the recommendations of Board of Studies approved from time-to-time.

A. Regulations

M.Sc. degree programme in Cyber Security exposes students, **Learn a practical skill-set in defeating all online threats**, including - advanced hackers, trackers, malware, zero days, exploit kits, cybercriminals and more.

A1: Duration of the Course:

The M.Sc. programme in Cyber Security is a 2 years full time programme spread over two years under semester pattern, with Choice Based Credit System (CBCS).

A2: Eligibility for Admission:

The minimum eligibility conditions for admission to the M.Sc. programme in Cyber Security are given below.

The candidates who seek admission into the first semester of the M.Sc. programme in Cyber Security course will be required to have passed the Bachelor's degree (B.Sc./ B.C.A./B.E. equivalent) from ManonmaniamSundaranar University or any other Indian University or equivalent in any one of the following disciplines:

1. Information Technology
2. Information Technology and E-Commerce
3. Computer Science
4. Computer Technology
5. Software Engineering
6. Computer Applications
7. Physics
8. Forensics
9. Electronics
10. Mathematics
11. Any other discipline with Mathematics or Computer Applications as a subject.
    The minimum percentage of marks required for admission is based on the periodic regulations made by the university and the government norms.

A3. Structure of the Programme:

This Master's programme will consist of:

a. *Core courses* and *Elective courses* which are compulsory for all students;

b. ***I Semester*****:** 4 Core, 1 Elective and 2 Practicals– ***II Semester*****:** 4 Core, 1 Elective, 1 supportive course and 2 Practicals **–** ***III Semester*****:** 3 Core, 1 Elective , 1 supportive course**,** 2 Practicals and 1 Mini Project **–** ***IV Semester*****:** 2 Electives and 1 Major Project

c. Supportive courses which students can choose from amongst the courses offered in other departments of this University

d. **Internship and Project** are compulsory and included as core.

A4: Credit Requirement for the Degree:

The general Regulations of the Choice Based Credit System programme of Manonmaniam Sundaranar University are applicable to this programme. The University requirement for the M.Sc. programme is completion of 91credits of course work, out of which 4 credits should be through the mini project, 10 credits should be through the 4th semester main project work, remaining 77 credits should be through Core, Elective and Supportive Course papers. A typical theory course has 4 credits for Core, 3 credits for Elective, 2 credits for Supportive Course and laboratory course weighs 2 credits. No candidate will be eligible for the Degree of Master of Science in Cyber Security, unless the candidate has undergone the prescribed courses of study for a period not less than 4 semesters and has acquired 91 credits and other passing requirements in all subjects of study. The marks, $M_i$obtained by the student in each subject, i shall be multiplied by the credit of that subject, C_i; such marks of all 'n' subjects are added up and divided by the total credit (91) to obtain the Consolidated Percentage of Marks.

$$\text{Consolidated Percentage of Marks} = \frac{\sum_{i=1}^{n} C_i \times M_i}{\sum_{i=1}^{n} C_i}$$

A5: Attendance Requirement:

A candidate will be permitted to appear for the semester examination only if the candidate keeps not less than 75 percent attendance. The University condonation rules are applicable for those who lack minimum of 75% attendance. The candidates with less than 60% attendance will have to repeat the concerned entire semester.

A6: Assessment

The assessment will comprise Continuous Internal Assessment (CIA) comprising of tests, seminars and assignments carrying a maximum of 25% marks and end-semester Examination carrying a maximum of 75% marks in each theory subject (Core/Elective/Supportive Course). For practical subjects, Mini Project and Major Project, the CIA is carried out for 50 marks and the External Assessment (Final Lab Exam, Lab Report, Viva-Voce for Practical Subjects and Final Project Presentation, Project Report, Viva-Voce for Mini Project and Major Project) is for

50 marks. Semester examination will be conducted for all subjects of study, at the end of each Semester.

A candidate has to go for Internship during their summer holidays (May-June) and submit the certificate in the 3rd semester for evaluation.

If a Student wants to carry out the final Major project as field work in 4th semester in an IT company, the student can get permission from the concerned Project Supervisor, Head of the Department and get approval from the Department council after submitting the Acceptance Letter from the IT Company.

A7: Passing Requirements

A candidate who secures not less than 50 percent marks in end-semester examination and not less than 50 percent of the total marks (Continuous Internal Assessment + end-semester examination) in any subject of study will be declared to have passed the subject.

A candidate should secure minimum of 38 marks out of maximum of 75 marks for all theory exams (Core, Elective and Supportive Course) and secure minimum of 25 marks out of maximum of 50 marks for practical's, mini project and major project in External Exam of each semester.

A Candidate who successfully completes the course and satisfies the passing requirements in all the subjects of study and curricular requirements will be declared to have qualified for the award of the Degree.

A8: Classification of successful candidates

The candidates who passed written papers, practical papers and Projects shall be classified as follows. Total Marks secured in written papers, practical papers and Project work altogether put as overall percentage along with the credits.

The classification is as follows,

	Marks Overall %	**Classification**
1.	75% and above with a First attempt Pass in all subjects	I Class with Distinction
2.	i) 75% above from multiple attempts	I Class
	ii) 60% to below 75%	I Class
3.	50% to below 60%	II Class

A9. Power to Modify

The University may from time to time revise, amend or change the regulations, scheme of examinations and syllabus, if found necessary and such amendments, changes shall come into effect from the date prescribed.

The academic year normally begins in July every year and ends in April. These regulations will come into effect from the academic year 2022-23 onwards.

PROGRAMME EDUCATIONAL OBJECTIVES (PEO)

PEO1: Graduates of the programme will be able communicate to effectively both orally and in writing in a variety of audiences.

PEO2: Graduates of the programme will be able to demonstrate critical thinking by analyzing situations and by constructing and selecting solutions to problems.

PEO3: Graduates of the programme will be able to understand and appreciate the legal and ethical environment impacting individuals as well as business organizations and have an understanding of the ethical implications of IT legal decisions.

PEO4: Graduates of the programme will be able to understand fundamentals and advanced issues of various threats faced by today’s cyberinfrastructure.

PROGRAM SPECIFIC OUTCOMES

PSO1: Evaluate the computer network and information security needs of an organization. Explain concepts and theories of networking and apply them to various situations, classifying networks, analyzing performance and implementing new technologies.

PSO2: Assess cyber-security risk management policies in order to adequately protect an organization's critical information and assets.

PSO3: Measure the performance of security systems within an enterprise-level information system. Troubleshoot, maintain and update an enterprise-level information security system.

PSO4: Implement continuous network monitoring and provide real-time security solutions.

PSO5: Formulate, update and communicate short- and long-term organizational cyber-security strategies and policies.

PSO6: Explain the concepts of confidentiality, availability and integrity in Information Assurance, including physical, software, devices, policies and people. Analyze these factors in an existing system and design implementations.

PSO7: Analyze and evaluate the cyber security needs of an organization.

PSO8: Manage multiple operating systems, systems software, network services and security. Evaluate and compare systems software and emerging technologies.

PSO9: Effectively communicate technical information verbally, in writing, and in presentations.

PSO10: Implement cyber security solutions. Be able to use cyber-security, information assurance, and cyber/computer forensics software/tools. Design operational and strategic cyber-security strategies and policies.

PEO vs. PSO Mapping

	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
PEO1 Career Accomplishments	S	S	S	S	S	S	S	S	M	S
PEO2 Research	M	L	M	L	M	S	L	M	S	S
PEO3 Sustained Learning	S	L	S	L	S	M	L	S	L	S
PEO4 Activity Skills	S	M	S	M	L	S	M	M	L	S

S- Strong

M – Middle

L – Low

B. Scheme of Examination
M.Sc. Cyber Security (CBCS) - FULL - TIME
(For those who joined from the academic year 2022-2023 onwards)
Duration: Two Years (Four Semesters – 91Credits)

Sem-ester	Title of the Subject	Status*	Hrs / week	Credits	Maximum Marks			Passing Minimum Percentage	
					Inte-rnal	Exte-rnal	Total	External	Total
FIRST SEMESTER									
I	Cyber Criminology and Cyber Forensics (e-pathshala)	C	4	4	25	75	100	50	50
I	Foundations of Information Security	C	4	4	25	75	100	50	50
I	Introduction to Computer Networking and Components	C	4	4	25	75	100	50	50
I	Data Privacy and Cloud Security	C	4	4	25	75	100	50	50
I	Elective A	E	3	3	25	75	100	50	50
I	Information Security Laboratory	L	4	2	50	50	100	50	50
I	Networking Laboratory	L	4	2	50	50	100	50	50
I Semester Total Credits				**23**					
SECOND SEMESTER									
II	MOOCSupportive Course	S	3	3	25	75	100	50	50
II	Cyber Laws, Regulations and Frauds in BFSI sector	C	4	4	25	75	100	50	50
II	Introduction to Digital Forensics	C	4	4	25	75	100	50	50
II	Intrusion Detection and Prevention System	C	4	4	25	75	100	50	50
II	Internet of Things	C	4	4	25	75	100	50	50
II	Elective B	E	3	3	25	75	100	50	50
II	Digital Forensics Laboratory	L	4	2	50	50	100	50	50
II	ID&PS using Python Laboratory	L	4	2	50	50	100	50	50
II Semester Total Credits				**26**					
THIRD SEMESTER									
III	MOOC	S	3	3	25	75	100	50	50

	Supportive Course								
III	Advanced Digital Forensics	C	4	4	25	75	100	50	50
III	Cryptography And Network Security	C	4	4	25	75	100	50	50
III	IT Governance, Risk and Compliance	C	4	4	25	75	100	50	50
III	Elective C	E	3	3	25	75	100	50	50
III	Cryptography using python Laboratory	L	4	2	50	50	100	50	50
III	Advanced Digital Forensics Laboratory	L	4	2	50	50	100	50	50
III	Internship	I	4	4	50	50	100	50	50
III Semester Total Credits				**26**					
FOURTH SEMESTER									
IV	Elective D1 (e-pathshala)	E	4	3	25	75	100	50	50
IV	Elective D2	E	4	3	25	75	100	50	50
IV	Major Project	P	6	10	50	50	100	50	50
IV Semester Total Credits				**16**					
OVERALL TOTAL CREDITS				**91**					

***Status C- Core, E-Elective, L-Laboratory, P-Project, I-Internship**

Subjects for Electives A									
Sl. No.	**Title of the Subject**	**Status**	**Hrs/week**	**Credits**	**Maximum Marks**			**Passing Minimum Percentage**	
					Inte-rnal	**Exte-rnal**	**Total**	**External**	**Total**
A1	Biometric Security	E	3	3	25	75	100	50	50
A2	Storage Management and Security	E	3	3	25	75	100	50	50
A3	Database Security	E	3	3	25	75	100	50	50
A4	Scripting Language	E	3	3	25	75	100	50	50
Subjects for Electives B									
B1	Fundamentals of Block chains and Crypto-currency	E	3	3	25	75	100	50	50
B2	Risk Management in Cyber Security	E	3	3	25	75	100	50	50
B3	Malware Analysis	E	3	3	25	75	100	50	50
B4	Android Mobile Application Development	E	3	3	25	75	100	50	50
Subjects for Electives C									
C1	Firewall and Internet Security	E	3	3	25	75	100	50	50
C2	Email, Mobile Devices Security	E	3	3	25	75	100	50	50
C3	Artificial Intelligence	E	3	3	25	75	100	50	50
C4	Big Data Security	E	3	3	25	75	100	50	50
Subjects for Electives D									
D1	Web application development (e-pathshala)	E	3	3	25	75	100	50	50
D2	Web Technology (e-pathshala)	E	3	3	25	75	100	50	50
D3	Information Security and Audit Monitoring	E	3	3	25	75	100	50	50
D4	Security Architecture	E	3	3	25	75	100	50	50

MANONMANIAM SUNDARANAR UNIVERSITY
TIRUNELVELI, TAMILNADU
M.Sc CYBER SECURITY DEGREE PROGRAMME
LIST OF CORES
(For The Candidates Admitted From 2022-23 Onwards)

SI. No.	Course code	Course name
1.		Cyber Criminology and Cyber Forensics (e-pathshala)
2.		Foundations of Information Security
3.		Introduction to Computer Networking and Components
4.		Data Privacy and Cloud Security
5.		Information Security Laboratory
6.		Networking Laboratory
7.		Cyber Laws, Regulations and Frauds in BFSI sector
8.		Introduction to Digital Forensics
9.		Intrusion Detection and Prevention System
10.		Internet of Things
11.		Digital Forensics Laboratory
12.		ID&PS using Python Laboratory
13.		Advanced Digital Forensics
14.		Cryptography And Network Security
15.		IT Governance, Risk and Compliance
16.		Cryptography using Python Laboratory
17.		Advanced Digital Forensics Laboratory
18.		Internship
19.		Major Project

MANONMANIAM SUNDARANAR UNIVERSITY
TIRUNELVELI, TAMILNADU
M.Sc CYBER SECURITY DEGREE PROGRAMME
LIST OF ELECTIVES
(For The Candidates Admitted From 2022-23 Onwards)

SI. No.	Course code	Course name
1.		Biometric Security
2.		Storage Management and Security
3.		Database Security
4.		Scripting Language
5.		Fundamentals of Block chains and Crypto-currency
6.		Risk Management in Cyber Security
7.		Malware Analysis
8.		Android Mobile Application Development
9.		Firewall and Internet Security
10.		Email, Mobile Devices Security
11.		Artificial Intelligence
12.		Big Data Security
13.		Web application development (e-pathshala)
14.		Web Technology (e-pathshala)
15.		Information Security and Audit Monitoring
16.		Security Architecture

Core 1	Cyber Criminology and Cyber Forensics (e-pathshala)	Category	L	P	Credit
		C	4	0	4

Preamble

Cybercrime, or computer oriented crime, is crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.

Prerequisite

- Nil

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes (CO)		Bhoom’s level
CO1	Concepts of Criminology	Understand, Analyze
CO2	Apply theoretical concepts to different cybercrimes	Apply
CO3	Cyber Crime: Sociological and Criminological Perspectives	Apply
CO4	Describe various legal responses to cybercrime	Understand, Evaluate
CO5	Contemporary crime prevention approaches	Apply, Create

Mapping with Programme specific outcomes

COs	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1										M
CO2		S					S			S
CO3			S					L		
CO4				M	M				L	
CO5	L					L				

Assessment Pattern

Category	Continuous Internal Assessment(25)			Terminal Examination (75)
	I	II	III	
Remember	5	5	5	25
Understand	6	6	6	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate	2	2	2	5
Create	2	2	2	5

Syllabus

Unit 1: Cyber Crime: History & Evolution: Definition-History and Evolution of Cyber Crime- **Cyber Criminology: Evolution Contribution and Impact:** History, Evolution and Definition - Contribution and Impact-Appreciation– Challenges- **Basics of Internet & Cyber Crimes - Understanding the Internet:** Working Principle of Domain Name System- Basics of Email-Concepts of World Wide Web (WWW)- Website Creation- Database driven websites

(12hrs)

Unit 2: E-Commerce: General types of E commerce- Evolution of Internet for E commerce- Barriers to e-commerce in developing countries- Functions which are required in Electronic Commerce- Hacking: - Computer Hacking- Email Hacking- Ethical Hacking- Network Hacking- Password Hacking- Website Hacking- Preventive Measures- **Malicious Code -Computer Viruses, Worms, and Trojans:** Malicious Codes- Computer Viruses- Worms- Trojans- **Cyber Piracy** - Cyber Piracy and its forms- Legislative Underpinnings **(14hrs)**

Unit 3: Cyber Terrorism: Definition of Cyber Terrorism- Nature of Threat- Why Cyber Terrorism- Forms of Cyber Terrorism- Countering Cyber Terrorism- Terrorists use of Internet- **Cyber Warfare :** What is Cyber Warfare- Features of Cyber Warfare-Features of Cyber weapons- **Cyber Bullying:CyberStalking:Sexting:Revenge Porn:** O**nline Sextortion:** Characteristics of Online Sextortion- How sextortion differed earlier?- Impact on Victims

(10hrs)

Unit 4: **Child Pornography- Online Child Grooming** - How is grooming different online?- Patterns of Victimization- **Identity related Cyber Crimes: Cyber Obscenity and Pornography:** Cyber obscenity and pornography- Test for Obscenity- Legislations in India - **Online Gambling:**Participation in Economy- Features of Internet Gambling - Physical and Mental Health Comorbidities- Models to Understand online gambling behavior- **Space Transition Theory of Cyber Crimes: Routine Activities Theory and Cyber Crimes(12hrs)**

Unit 5: **Social Learning Theory and Cyber Crimes: De-individuation Theory and Cyber Crimes:** De-individuation theory- De-individuation theory and cyber crimes - **Cyber Policing and Cyber Crime Investigation Cyber Tribunals Cyber Security:** Cyber security- Security Attacks- Firewalls-Intrusion Detection Systems **-Ethical Hacking:** Filing a complaint on hacking - **Internet of Things:** Evolution of IoT- Applications of IoT- Security and privacy concerns of IoT

(12hrs)

TOTAL (60hrs)

Textbook

https://epgp.inflibnet.ac.in/ahl.php?csrno=1608

Core 2	**Foundations of Information Security**	Category	L	P	Credit
		C	4	0	4

Preamble

The module provides an overview over several foundational areas in information security. The core of the module is given over to a rigorous discussion of security models and their relation to access control models with selected issues in identification and authentication and their required trust and reputation models also covered.

Prerequisite

- Basic Computer Technology Security

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bhoom's level
CO1	Understand the conceptual foundation of information security awareness.	Understand, Remember
CO2	Analysis the risk events, treatment plans, assessment	Understand,
CO3	Detail evaluation of information classification, roles and responsibilities	Apply, evaluate
CO4	Examining the access controls, monitoring, management and review process	Apply, create
CO5	Study the physical and logical perimeters of information assets and its security.	Apply, analyze

Mapping with Programme specific outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	M									
CO2		M								S
CO3	S			L		L	S			
CO4			M		S			M		
CO5				S					L	M

Assessment Pattern

Category	Continuous Internal Assessment(25)			Terminal Examination (75)
	I	II	III	
Remember	5	5	5	25
Understand	6	6	6	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate	2	2	2	5
Create	2	2	2	5

Syllabus

Unit 1: The Need for Information Security: The Internet of Things Is Changing How We Live- Evolution of the Internet of Things - Converting to a TCP/IP World - IoT's Impact on Human and Business Life - Evolution from Bricks and Mortar to E-Commerce - Why Businesses Must Have an Internet and IoT Marketing Strategy - IP Mobility - Mobile Applications - New Challenges Created by the IoT **(13hrs)**

Unit 2: Malicious Attacks, Threats, and Vulnerabilities-Malicious Activity on the Rise - Attack Tools - Security Breach - Risks, Threats, and Vulnerabilities - Malicious Attack - Malicious Software - Common Types of Attacks – Countermeasure

(11hrs)

Unit 3: Security Operations and Administration-Security Administration – Compliance - Professional Ethics - The Infrastructure for an IT Security Policy - Data Classification Standards - Configuration Management - The Change Management Process - Application Software Security - Software Development and Security **(12hrs)**

Unit 4: Networks and Telecommunications-The Open Systems Interconnection Reference Model - The Main Types of Networks - TCP/IP and How It Works - Network Security Risks - Basic Network Security Defense Tools - Wireless Networks **(11hrs)**

Unit 5: Malicious Code and Activity-Characteristics, Architecture, and Operations of Malicious Software - The Main Types of Malware - A Brief History of Malicious Code Threats - Threats to Business Organizations - Anatomy of an Attack - Attack Prevention Tools and Techniques - Intrusion Detection Tools and Techniques **(13hrs)**

TOTAL (60Hrs)

Textbook:

1. Fundamentals of information systems security- Dividkim | Michael G.solomon - 3rd edition

Core 3	**Introduction to Computer Networking and Components**	Category	L	P	Credit
		C	4	0	4

Preamble

To study the interconnection of computing devices that can exchange data and share resources with each other. These networked devices use a system of rules, called communications protocols, to transmit information over physical or wireless technologies. To study the basic concepts of computer components like OS and database

Prerequisite

- Computer Basics

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bhoom's level
CO1	Learn basic components of information technology	Understand, Apply
CO2	Understand the interface of the components, roles and their difference	Understand, Evaluate
CO3	Study the back end of the system in database security issues	Apply, Remember
CO4	Grasp the knowledge in networking components with its architecture and protocols	Apply, Analyze
CO5	Know the standards for security in the cloud environment	Learn , Create

Mapping with Programme specific outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	S									
CO2		L					L	S		M
CO3			S	M		L			L	
CO4	S						M			
CO5					S					

Assessment Pattern

Category	Continuous Internal Assessment(25)			Terminal Examination (75)
	I	II	III	
Remember	5	5	5	25
Understand	6	6	6	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate	2	2	2	5
Create	2	2	2	5

Unit-1:Components of a computer – CMOS and BIOS – processors: types and functions – RAM: role and types – Hard disks – FAT and NTFS – RAID – Removable storage devices – Common forms of data ports – Display standards and cards – printers and scanners **Operating Systems and Interface** OS basics – functions of OS – Windows and Linux family of OS – Client and Server operating systems: principal roles and differences – Command line access – device drivers **(12hrs)**

Unit-2: Databases The evolution of databases – types of databases – relational databased management systems – ERP – security issues in RDBMS – databases as back-end to web sites – access control granularity in databases – SQL: process and vulnerabilities (**10hrs)**

Unit-3: Introduction - What is networking - Need for computer networks - Network Topologies - Types of networks - Hardware needed for setting up simple LAN, Wireless networks and for inter-connecting LANs and WAN -Communication media - Network topologies and access methods - IEEE 802 series standards - Wireless technology - Spread spectrum - WAP and WML - Access points - Service Set ID (SSID) - Authentication methods (OSA, SKA) - Devices used in networking – Hubs – Switches – Routers - Wireless Access Points etc - Physical connectivity between systems - Types of Cables – Ethernet - Token Ring - Optical Fibre - Introduction to MAC address - Introduction to IP address - Classes of IP address - Need for subnetting - Basics of IPV6 - Introduction to Unicast, Multicast and Broadcast**(13hrs)**

Unit 4:Routing - Fundamentals of routing - RIP – EIGRP – OSPF - Configuring Routers - Understanding the router architecture - Assigning IP address to the routers - Configuring routing protocols. **Packet Switched Connection -** Types of connections – Circuit switched, Packet switched - Why packet switched is preferred - Types of protocols and need for protocols - Packet switched Protocols - TCP/ IP O**SI Layers** - Interconnecting disparate systems/ networks – issues - Open Systems Interconnect - 7 layers and their functionality - **Introduction to TCP/ IP -** Origins of TCP/ IP and evolution of Internet - IP Layers Vs OSI - IP number concepts - Network address - Classes of Networks - Subnet masking - Static and dynamic IP numbers - UDP - Establishing a TCP session (Three way handshake) - Name to address translation - Domain Name System **(13hrs)**

Unit 5: Networking to the end user - Configuring Server for enterprise networking - Introduction to Domains and Work groups - Understanding DNS and configuring DNS - Introduction to ADS (Active Directory Service) - File sharing within network - Understanding DHCP - Introduction to Mail Exchange server and ISA server - Network operating system - Client Server applications - Peer to Peer Applications - Measuring performance - Monitoring tools.**(12hrs)**

Total(60 hours)

Books:

1. Basic of Networking – Prentice Hall (ISBN 8120324897)
2. Introduction to Networking – Prentice Hall (ISBN 8120313860)
3. Computer Networking First Step – Odom Wendell – (ISBN 8129706075)
4. Carl Hamacher V. Zvonko G.V. Safwat G. Z. (2002) Computer organization (5th ed.),Tata McGraw Hill
5. Morris Mano (2007) Computer System Architecture (3rd ed.), Pearson Education
6. Ramez, E. Shamkant, B. Navathe (2008) Fundamentals of database systems (5th ed.), Pearson Education
7. Date, C. J, (2012) An Introduction to Database Systems (8th ed.), Pearson Education

Reference Books:

1. Basic of Networking – Prentice Hall (ISBN 8120324897)
2. Introduction to Networking – Prentice Hall (ISBN 8120313860)
3. Computer Networking First Step – Odom Wendell – (ISBN 8129706075)

Core 4	**Data Privacy and Cloud Security**	Category	L	P	Credit
		C	4	0	4

Preamble

Data security and privacy are inevitable requirement of cloud environment. Massive usage and sharing of data among users open door to security loopholes.

Prerequisite

- Computer Basics

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bhoom's level
CO1	Know the sensitive online information and its privacy policies.	Understand, Remember
CO2	Basic concepts in Cloud computing	Understand
CO3	Different Infrastructure Security in Cloud	Apply, Evaluate
CO4	Policy and Compliance in Cloud Environment	Understand
CO5	Cloud computing service for real world problem	Create, Apply

Mapping with Programme specific outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	M		S				M		L	
CO2		S								
CO3				M	M			S		
CO4			L				L			
CO5		M	M			S				M

Assessment Pattern

Category	Continuous Internal Assessment(25)			Terminal Examination (75)
	I	II	III	
Remember	5	5	5	25
Understand	6	6	6	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate	2	2	2	5
Create	2	2	2	5

Syllabus

Unit 1: Information Privacy Concepts: Key Privacy Terminology, Privacy by Design, Privacy Engineering, Privacy and Security, Privacy Versus Utility, Usable Privacy. **Information Privacy Requirements and Guidelines:** Personally Identifiable Information and Personal Data, Personal Information That Is Not PII , Fair Information Practice Principles, Privacy Regulations, Privacy Standards, Privacy Best Practices **(11hrs)**

Unit 2: **Introduction to Cloud Computing and Security:** Understanding Cloud Computing, The IT Foundation for Cloud, An Historical View: Roots of Cloud Computing, A Brief Primer on Architecture, Security Architecture: Cloud Computing Architecture: **Security Concerns, Risk Issues, and Legal Aspects:** Cloud Computing: Security Concerns, Assessing Your Risk Tolerance in Cloud Computing, Legal and Regulatory **Issues, Securing the Cloud: Architecture:** Security Patterns and Architectural Element, Cloud Security Architecture, planning Key Strategies for Secure Operation **(11hrs)**

Unit-3: Securing the Cloud: Data Security : Overview of Data Security in Cloud Computing, Data Encryption: Applications and Limits, Cloud Data Security: Sensitive Data Categorization, Cloud Data Storage, Cloud Lock-in (the Roach Motel Syndrome), Securing the Cloud: Key Strategies and Best Practices:Overall Strategy: Effectively Managing Risk,Overview of Security Controls, The Limits of Security Controls, Best Practices , Security Monitoring **(13hrs)**

Unit-4: Security Criteria: Building an Internal Cloud, Private Clouds: Motivation and Overview, Security Criteria for Ensuring a Private Cloud, Security Criteria: Selecting an External Cloud Provider, Selecting a CSP: Overview of Assurance, Selecting a CSP: Overview of Risks, Selecting a CSP: Security Criteria, **Evaluating Cloud Security:** An Information Security Framework:Evaluating Cloud Security, Checklists for Evaluating Cloud Security, Metrics for the Checklists **(12hrs)**

Unit 5: Understand core Azure services: Understand the core Azure architectural components- Describe some of the core products available in Azure - Describe some of the solutions available on Azure - Understand Azure management tools, Understand security, privacy, compliance, and trust : Understand securing network connectivity in Azure, Describe security tools and features of Azure. **(13hrs)**

Total(60hrs)

Textbook:

1. Information Privacy Engineering and Privacy by Design Understanding Privacy Threats, Technology, and Regulations Based on Standards and Best Practices By William Stallings · 2019
2. Cloud Security and Privacy, An Enterprise Perspective on Risks and Compliance byTim Mather, SubraKumaraswamy, and ShahedLatif, Oreilly
3. Securing the Cloud: Cloud Computer Security Techniques and Tactics by Vic (J.R.) Winkler, Technical Editor Bill Meine
4. Mather, Kumaraswamy and Latif: Cloud Security and Privacy – An Enterprise Perspective on Risk and Compliance, O'Reilly
5. Kurtz and Vines: Cloud Security: A Comprehensive guide to secure cloud computing, Wiley
6. Buyya, Broberg and Goscinski: Cloud Computing – Principles and Paradigms, Wiley
7. Exam Ref AZ-900 Microsoft Azure Fundamentals By Jim Cheshire · 2019

	Information Security Laboratory	**L**	**T**	**P**	**C**
				4	**2**

1. User Identity and Access Management
2. Account Authorization
3. Access and Privilege Management
4. System and Network Access Control
5. Operating Systems Access Controls
6. Monitoring Systems Access Controls
7. Event Logging
8. Dumpsec tool

	Networking Lab	**L**	**T**	**P**	**C**
				4	**2**

1. Understanding network commands.
2. Understanding Client – Server Architecture.
3. Understanding the basics of cabling.
4. Understanding Domain controller.
5. Understanding User Controller and assigning the user rights.
6. Study of the following network devices: Repeater, Hub, Switch, Bridge, Router, Gateway
7. Study of network IP: Classification of IP, Subnetting, super netting
8. Connect the computers in LAN
9. Study Of Network Simulator (Ns)
    i. Network Topology Date: Bus Topology, Ring Topology
    ii. Simulation Of Stop And Wait Protocol And Sliding Window Date: Protocol

Core 5	Cyber Laws, Regulations and Frauds in BFSI sector	Category	L	P	Credit
		C	4	0	4

Preamble

To know the various cyber attacks and crimes. Cyber crimes are criminal offenses committed via the Internet or otherwise aided by various forms of computer technology. A cyber security regulation comprises directives that safeguard information technology and computer systems with the purpose of forcing companies and organizations to protect their systems and information from cyber attacks like viruses, worms, Trojan horses, phishing, denial of service attacks, unauthorized access and control system attacks.

Prerequisite

- Cyber Criminology and Cyber Forensics

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bhoom's level
CO1	Learn the Banking and Financial Services Operations	Remember, Understand
CO2	Understand the Computerized CBS	Apply, Evaluate
CO3	Know the Security and Controls	Remember, Apply
CO4	Study the Money Laundering Controls	Analyze ,Apply
CO5	Know the Regulatory Frameworks	Remember ,Apply

Mapping with Programme specific outcomes

COs	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	M								L	
CO2		S	L							M
CO3				M				S		
CO4	L					L	S			
CO5					M					M

Assessment Pattern

Category	Continuous Internal Assessment(25)			Terminal Examination (75)
	I	II	III	
Remember	5	5	5	25
Understand	6	6	6	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate	2	2	2	5
Create	2	2	2	5

Syllabus

Unit 1: Cyber Laws Indian Information Technology Act, as amended up to data - rules framed under the Act; in particular the rules relating to regulation of cyber cafes, certification authority and digital signature and other commercially significant aspects – selected comparative cyber laws in other countries,Related Laws Indian Penal Code, Evidence Act, Bankers Book Evidence Act, Negotiable Instruments Act, Contracts Act and Reserve Bank of India Act – selected comparative laws of other countries and their use in a cyber environment, UNCITRAL model law on electronic commerce **(10hrs)**

Unit 2:Cyber Fraud: Principles, Trends, and Mitigation Techniques-Executive Summary - Cyber Fraud Model - The Model Made Real: The Carding Underground in 2007 - The Evolution of Cyber Fraud Techniques: Phishing and Pharming - The Evolution of Cyber Fraud Techniques: Trojans and Toolkits - The Evolution of Cyber Fraud Techniques: Direct Attacks - The Evolution of Cyber Fraud Techniques: Pump-and-Dump **(14hrs)**

Unit 3:Banking Trojans: An Overview-Executive Summary – Introduction - Stages of Attack. - Techniques and Malicious Code Evolution - Most Common Banking Malicious Software in the Wild - Command-and-Control (C&C) Servers and Drop Sites -Minimizing Financial Impact - Future Trends **(13hrs)**

Unit 4: Distributed Denial of Service (DDoS) Attacks: Motivations and Methods-Executive Summary – Introduction - Denial of Service (DoS) and Botnets - Quantifying DDoS attacks - The Law - The Torpig Trojan Exposed-The Torpig Group, Part 1: Exploit Server and Master Boot Record Rootkit - The Torpig Group, Part 1: Exploit Server and Master Boot Record Rootkit. **(10hrs)**

Unit 5: Preventing Malicious Code from “Phoning Home”-Executive - Outbound Channel Methods - Mitigating Outbound Channels. - Mobile Malicious Code Trends-Executive Summary - Introduction to Mobile Communications - Bluetooth, Short Messaging Service (SMS), and Multimedia Messaging Service (MMS) for Mobile Communications - Development Platforms - The Rise of Mobile Malicious Code - Mobile Malicious Code Summary - Mobile Malicious Code Trend Analysis - Device Convergence - Personal Computer Integration - Best Security Practices for Mobile Malicious Codes **(14hrs)**

TOTAL (60hrs)

Textbook:

1. Cyber law by Nandankamath, Fifth Edition, Universal law Publication, 01 Jan 2012
2. Intellectual property by Robert P Merges, 3rd Edition, Aspen Publication, 2003

3. Computers , Technology and the new internet laws by Karnika Seth, Updated Edition, Lexis nexis Publication, 01 Jan 2013

4. Legal dimensions of cyber space by S.K.Verma, Volume 1, Ashgate Publication, 01 Jan 2001

5. Cyber fraud - Tactics, Techniques, and Procedures: Kellie, Bryan Kristen ,Dunnesen, Jayson Jean ,Eli Jellenc ,Josh Lincoln, Michael Ligh, Mike La Pilla, Ryan Olson ,Andrew ,Scholnick, Greg Sinclair, Tom Wills, Kimberly Zenz

Core 6	Introduction to Digital Forensics	Category	L	P	Credit
		C	4	0	4

Preamble

Digital forensics is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. The term digital forensics was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data.

Prerequisite

- Introduction to Data privacy

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bhoom's level
CO1	Study the different forms in digital forensic investigations and its life cycle	Understand, Remember
CO2	Understand the digital data that are used in digital data that are used in digital forensic investigation	Understand, Apply
CO3	Learn the various forensic principles propounded by different person that are applied to digital space	Understand, Apply
CO4	Study the principles in collecting the digital evidence	Understand, Evaluate
CO5	Learn the best practice guidelines and standards for digital evidence examination	Create, Apply

Mapping with Programme specific outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	S									S
CO2		L								
CO3					L	M			M	
CO4			M					L		
CO5				S			L			S

Assessment Pattern

Category	Continuous Internal Assessment(25)			Terminal Examination (75)
	I	II	III	
Remember	5	5	5	25
Understand	6	6	6	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate	2	2	2	5
Create	2	2	2	5

Syllabus

Unit 1: Introduction - Forensic Science? - Digital Forensics? - Uses of Digital Forensics - Locard's Exchange Principle - Scientific Method - Organizations of Note - Role of the Forensic Examiner in the Judicial System **(12hrs)**

Unit 2: Key Technical Concepts-Introduction - Bits, Bytes, and Numbering Schemes - File Extensions and File Signatures - Storage and Memory - Computing Environments - Data Types - File Systems - Allocated and Unallocated Space – V - Basic Computer Function—Putting it All Together **(13hrs)**

Unit 3: Labs and Tools-Introduction - Forensic Laboratories - Policies and Procedures - Quality Assurance - Digital Forensic Tools – Accreditation – Collecting Evidence-Introduction - Crime Scenes and Collecting Evidence - Documenting the Scene - Chain of Custody – Cloning - Live System versus Dead System – Hashing **(13hrs)**

Unit 4: Windows System Artifacts -Introduction - Deleted Data - Hibernation File (Hiberfile.sys) – Registry - Print Spooling - Recycle Bin – Metadata - Thumbnail Cache - Most Recently Used (MRU) - Restore Points and Shadow Copy – Prefetch - Link Files **(10hrs)**

Unit 5: Antiforensics-Introduction - Hiding Data - Password Attacks – Steganography - Data Destruction Legal-Introduction - The Fourth Amendment - Criminal Law—Searches without a Warrant - Searching with a Warrant - Electronic Discovery (eDiscovery) - Expert Testimony **(12hrs)**

Total (60Hrs)

Textbook:

The Basics of Digital Forensics: The primer for getting started in Digital Forensics by John Sammons

References:

1) Computer Forensics, Computer Crime Investigation by John.R.Vacca, 2002, Firewall Media
2) Computer Intrusion Forensics by George Mohay et al, 2003, Artech House
3) Handbook of Digital Forensics by Eoghan Casey, 2010, Elsevier
4) NIST guidelines on digital forensic processes

Core 7	**Induction Detection and Prevention System**	Category	L	P	Credit
		C	4	0	4

Preamble

To prepare students to know regarding the common threats faced today and the necessity of intrusion detection systems for securing the systems. To understand the essential concepts of intrusion detection and prevention.

Prerequisite

- Foundations of Information Security

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bhoom's level
CO1	The physical location, the operational characteristics and the various functions performed by the intrusion detection and prevention system.	Remember, Apply
CO2	Describe the detection approaches. The taxonomy of the anomaly detections using fuzzy logic.	Create, Understand
CO3	To detect network attacks and troubleshoot network problems.	Understand, Remember
CO4	The concepts of Prior strong experience in operating system and prior hands-on experience	Evaluate, Apply
CO5	The tiered architecture and its implementation.	Understand, Apply

Mapping with Programme specific outcomes

COs	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	S									
CO2	S			M					L	
CO3			L				S			
CO4		M						S		
CO5					S	L				L

Assessment Pattern

Category	Continuous Internal Assessment(25)			Terminal Examination (75)
	I	II	III	
Remember	5	5	5	25
Understand	6	6	6	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate	2	2	2	5
Create	2	2	2	5

Syllabus

UNIT 1: INTRODUCTION

Network Attacks – Attack Taxonomies – Probes – Privilege Escalation Attacks – Denial of Service – Distributed Denial of Service – Worm Attacks – Routing Attacks(12 hrs)

Unit 2 :Understanding Intrusion Detection –Intrusion detection and prevention basics –IDS and IPS analysis schemes, Attacks, Detection approaches –Misuse detection – anomaly detection – specification-based detection – hybrid detection. (12 hrs)

UNIT 3: THEORETICAL FOUNDATIONS OF DETECTION

Taxonomy of anomaly detection system –fuzzy logic –Bayes theory –Artificial Neural networks Support vector machine –Evolutionary computation –Association rules –Clustering. (12 hrs)

UNIT 4: ARCHITECTURE AND IMPLEMENTATION

Centralized – Distributed –Cooperative Intrusion Detection -Tiered architecture – Intrusion Response - JUSTIFYING INTRUSION DETECTION - Intrusion detection in security –Threat Briefing –Quantifying risk –Return on Investment (ROI) (12 hrs)

UNIT 5: CASE STUDY

Tool Selection and Acquisition Process - Bro Intrusion Detection – Prelude Intrusion Detection - Cisco Security IDS -Snorts Intrusion Detection –NFR security Legal Issues And Organizations Standards: Law Enforcement / Criminal Prosecutions –Standard of Due Care –Evidentiary Issues, Organizations and Standardizations. (12hrs)

Books for References:

1. Ali A. Ghorbani, Wei Lu, “Network Intrusion Detection and Prevention: Concepts and

Techniques”, Springer, 2010.

2. Carl Enrolf, Eugene Schultz, Jim Mellander, “Intrusion detection and Prevention”, McGraw

Hill, 2004.

3. Paul E. Proctor, “The Practical Intrusion Detection Handbook “, Prentice Hall, 2001.

4. AnkitFadia and MnuZacharia, “Intrusion Alert”, Vikas Publishing house Pvt., Ltd, 2007.

5. Earl Carter, Jonathan Hogue, “Intrusion Prevention Fundamentals”, Pearson Education, 2006.

Core 8	**Internet of Things**	Category	L	P	Credit
		C	4	0	4

Preamble

In order to gain knowledge on bases of Internet of Things (IoT), IoT Architecture, and the Protocols related to IoT; and understand the concept of the Web of Thing and the relationship between the IoT and WoT.

Prerequisite

- Computer Network

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bhoom's level
CO1	Learn the basics of IoT	Remember, Apply
CO2	Study the IoT architecture	Understand, Remember
CO3	Understand the IoT protocols	Understand, Create
CO4	Learn the IoT in Web	Apply, Evaluate
CO5	Know the applications	Apply, Create

Mapping with Programme specific outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	S									
CO2	M			M					L	
CO3			S				M			
CO4		M						S		
CO5					M	L				L

Assessment Pattern

Category	Continuous Internal Assessment(25)			Terminal Examination (75)
	I	II	III	
Remember	5	5	5	25
Understand	6	6	6	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate	2	2	2	5
Create	2	2	2	5

Syllabus

UNIT I INTRODUCTION To IoT: Internet of Things - Physical Design- Logical Design- IoT Enabling Technologies - IoT Levels and Deployment Templates - Domain Specific IoTs - IoT and M2M - IoT System Management with NETCONF-YANG- IoT Platforms Design Methodology. **(12hrs)**

UNIT II IoT ARCHITECTURE: M2M high-level ETSI architecture - IETF architecture for IoT - OGC architecture - IoT reference model - Domain model - information model - functional model - communication model - IoT reference architecture **(10hrs)**

UNIT III IoTPROTOCOLS: Protocol Standardization for IoT – Efforts – M2M and WSN Protocols – SCADA and RFID Protocols – Unified Data Standards – Protocols – IEEE 802.15.4 – BACNet Protocol – Modbus– Zigbee Architecture – Network layer –LowPAN - CoAP - Security **(13hrs)**

UNIT IV WEB OF THINGS: Web of Things versus Internet of Things – Two Pillars of the Web – Architecture Standardization for WoT– Platform Middleware for WoT – Unified Multitier WoT Architecture – WoT Portals and Business Intelligence. Cloud of Things: Grid/SOA and Cloud Computing – Cloud Middleware – Cloud Standards – Cloud Providers and Systems – Mobile Cloud Computing – The Cloud of Things Architecture. **(13hrs)**

UNIT V APPLICATIONS: The Role of the Internet of Things for Increased Autonomy and Agility in Collaborative Production Environments - Resource Management in the Internet of Things: Clustering, Synchronisation and Software Agents. Applications - Smart Grid – Electrical Vehicle Charging. **(12hrs)**

Total (60Hrs)

Text Books

1. ArshdeepBahga, Vijay Madisetti, “Internet of Things – A hands-on approach”, Universities Press, 2015.
2. Dieter Uckelmann, Mark Harrison, Michahelles, Florian (Eds), “Architecting the Internet of Things”, Springer, 2011.
3. Jan Ho¨ ller, VlasiosTsiatsis , Catherine Mulligan, Stamatis , Karnouskos, Stefan Avesand. David Boyle, "From Machine-to-Machine to the Internet of Things - Introduction to a New Age of Intelligence", Elsevier, 2014.
4. Networks, Crowds, and Markets: Reasoning About a Highly Connected World - David Easley and Jon Kleinberg, Cambridge University Press - 2010.
5. Olivier Hersent, David Boswarthick, Omar Elloumi , “The Internet of Things – Key applications and Protocols”, Wiley, 2012.

	Digital Forensics Laboratory	**L**	**T**	**P**	**C**
				4	**2**

1. **The Practice of Digital Forensics -** Boot Process – Partitions - File Systems - Procedures
2. **Forensic Hardware and Software tools –** Cyber Check Suite - Email Tracer – FTK - Open Source Tools
3. **Forensic Imaging Process –Acquiring the Digital Evidence -** FTK - Open Source Tools.
4. **Windows Forensics** - Windows dates and times - Adjusting for time zone offsets - Recycle Bin and INFO records - Windows Recycle Bin - Link files - Windows folders - Recent folder - Desktop folder - My Documents folder - Send To folder - Temp folders - Favorites folder - Windows Low folders - Cookies folder - History folder - Temporary Internet files - Swap file -Hibernation file - Printing artifacts - Windows volume shadow copy - Windows event logs.
5. Data Loss Prevention software tools and techniques

	ID&PS Laboratory	**L**	**T**	**P**	**C**
				4	**2**

1. Using Python
   a. Program using basics of python.
   b. Program for WEBSERVER FINGER PRINTING
   c. Program for PORT SCANNING
   d. Program for TRANSMISSION OF TRAFFIC IN THE NETWORK
   e. Program for WEB APP TESTING
2. Using Tools
   a. OSSEC – Open Source host-based security
   b. SNORT
   c. SURICATA

	Internship	**4**

1. Industrial Training

Core 9	Advanced Digital Forensics	Category	L	P	Credit
		C	4	0	4

Preamble

Advanced digital forensics is education intended as an upgrade on basics of digital forensics. Goal is to introduce attender to advanced and more complex usage of digital forensics in real situations.

Prerequisite

- Introduction to Digital Forensics

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bhoom’s level
CO1	Learn the windows & virtual machine forensics	Apply,Understand
CO2	Study the forensic analysis of storage media and web	Understand, Remember
CO3	Understand the concepts to managing Forensic Data	Understand, Evaluate
CO4	Learn the forensics in memory	Apply, Create
CO5	Know the form of Forensics in cloud and social media	Apply, Create

Mapping with Programme specific outcomess

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	S									
CO2	M			M					L	
CO3			S				M			
CO4		M						S		
CO5					M	L				L

Assessment Pattern

Category	Continuous Internal Assessment(25)			Terminal Examination (75)
	I	II	III	
Remember	5	5	5	25
Understand	6	6	6	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate	2	2	2	5
Create	2	2	2	5

Syllabus

Unit-1: Overview of Computer Forensics Technology: Computer Forensics Fundamentals, Types of Computer Forensics Technology, Types of Computer Forensics Systems, Vendor and Computer Forensics Services **(10hrs)**

Unit-2: Windows Forensics Introduction, What Is "Registry Analysis"?, What Is the Windows Registry?, Registry Structure. Tools: Introduction, Live Analysis, Security and SAM Hives, System Hive, Software Hive, BCD Hive **(10hrs)**

Unit-3: Memory Forensics Volatility framework - Memory acquisition -Windows Objects and Pool allocation - Process, Handles and Tokens - Process Memory internals - Hunting Malware in Process Memory - Event Logs - Registry in Memory - Kernel forensics and rootkits - Disk artifacts in memory - Event reconstruction – Timelining - Linux Memory Forensics - Linux memory acquisition - Linux OS - Process and Process Memory - Process Address space - Open File Handles - Saved Context state - Bash Memory Analysis - Networking artifacts-Network socket file descriptors - Network connections - Network interfaces -ARP cache - Kernel memory artifacts - Physical Memory maps **(14hrs)**

Unit 4:Memory Forensics Virtual memory maps - Kernel debug buffer - Loaded kernel modules - File systems in memory - Mounted file systems - Listing files and directories - Extracting file metadata -Recovering file contents Rootkits -Shell code injection - Process hollowing - Shared library injection - Rootkits - overwrites - Inline hooking - Kernel Mode Rootkits - Accessing kernel mode - Hidden kernel modules - Hidden processes - Elevating privileges - System call handler hooks - Keyboard notifiers - Network protocol structures - Net filter hooks - Inline code hooks. Mac acquisition and internals - Mac design - Memory acquisition - Mac volatility profiles **(14hrs)**

Unit-5: Forensics of cloud and social media Cloud Storage Forensic Framework - Evidence Source Identification and preservation in the cloud storage - Collection of Evidence from cloud storage services - Examination and analysis of collected data - Microsoft SkyDrive Cloud Storage Forensic Analysis - Evidence Source Identification and Preservation in Microsoft SkyDrive - Preservation of evidence collected from cloud storage devices -Examination and analysis of collected data – Skype forensics – Facebook and Twitter forensics – LinkedIn forensics**(12hrs)**

Total (60hrs)

Textbooks:

1. Computer Forensics by John R. Vacca , 2nd Edition
2. Windows Registry analysis by Harlan Carvey, 2010
3. The Art of Memory Forensics by Michael Hale Ligh, Andrew Case, Jamie Levy, Aron Walters
4. Cloud Storage Forensics by Darren Quick, 2014

References:

Malware Forensics Field Guide for Windows System , CameroH.Malin, Eoghan Casey, James M.Acuilina, Curtis W.Rose, Syngress, 2012 Books

Core 10	**CRYPTOGRAPHY AND NETWORK SECURITY**	Category	L	P	Credit
		C	4	0	4

Preamble

To attain the extensive knowledge on the information security, specifically, network security, software security, cryptography, authentication protocols, and protection of intellectual property, from the various viewpoints of the advanced information security.

Prerequisite

- Network Security

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bhoom's level
CO1	Understand the concepts in cryptology	Understand, Apply
CO2	Know about Symmetric Encryption and Message Confidentiality	Understand, Create
CO3	Study the Authentication Applications	Apply, Evaluate
CO4	Learn the IP security	Apply, Create
CO5	Understand the concepts of Digital Rights Management	Understand, Evaluate

Mapping with Programme specific outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1					M					
CO2	S		L				M			
CO3			L					L		M
CO4		M		M		L				
CO5	L						L		M	

Assessment Pattern

Category	Continuous Internal Assessment(25)			Terminal Examination (75)
	I	II	III	
Remember	5	5	5	25
Understand	6	6	6	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate	2	2	2	5
Create	2	2	2	5

Syllabus

Unit I Introduction - Security trends – Legal, Ethical and Professional Aspects of Security, Need for Security at Multiple levels, Security Policies – Model of network security – Security attacks, services and mechanisms – OSI security architecture – Classical encryption techniques: substitution techniques, transposition techniques, steganography- Foundations of modern cryptography: perfect security – information theory – product cryptosystem – cryptanalysis. **(11hrs)**

Unit II Symmetric Encryption and Message Confidentiality - Symmetric Encryption Principles, Symmetric Block Encryption Algorithms, Stream Ciphers and RC4 ,Chipher Block Modes of Operation, Location of Encryption Devices, Key Distribution. Public-key Cryptography and Message Authentication: Approaches to Message Authentication, Secure Hash Functions and HMAC, Public-Key Cryptography Principles, Public-Key Cryptography Algorithms, Digital Signatures, Key Management. **(12hrs)**

Unit III Authentication Applications - Kerberos, x.509 Authentication Service, Public-Key Infrastructure. Electronic Mail Security: Pretty Good Privacy (PGP), S/MIME. **(10hrs)**

Unit IV IP Security - IP Security Over view, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations. Web Security: Web Security Considerations, Secure Socket Layer(SSL) and Transport Layer Security(TLS), Secure Electronic Transaction(SET).Network Management Security: Basic Concepts of SNMP, SNMPv1 Community Facility, SNMPv3. **(13hrs)**

Unit V Intruders - Intruders, Intrusion Detection, Password Management.**Malicious Software:** Virus and Related Threats, Virus Countermeasures, Distributed Denial of Service Attacks. **Firewalls:** Firewall Design Principles, Trusted Systems, Common Criteria for Information Technology Security Evaluation. **(14hrs)**

TOTAL (60Hrs)

Text books

1. Behrouz A. Ferouzan, “Cryptography & Network Security”, Tata McGraw Hill, 2007, Reprint 2015.

2. Stallings William, “Cryptography and Network Security - Principles and Practice 2017.

3. William Stallings, “Network Security Essentials Applications and Standards ”Third Edition, Pearson Education, 2008.

References

1. Man Young Rhee, “Internet Security: Cryptographic Principles”, “Algorithms And Protocols”, Wiley Publications, 2003.

2. Charles Pfleeger, “Security In Computing”, 4th Edition, Prentice Hall Of India, 2006.

3. Ulysess Black, “Internet Security Protocols”, Pearson Education Asia, 2000.

4. Charlie Kaufman AndRadia Perlman, Mike Speciner, “Network Security, Second Edition, Private Communication In Public World”, PHI 2002.

5. Bruce SchneierAndNeils Ferguson, “Practical Cryptography”, First Edition, Wiley Dreamtech India Pvt Ltd, 2003.

6. Douglas R Simson “Cryptography – Theory And Practice”, First Edition, CRC Press, 1995.

7. Http://Nptel.Ac.In/.

Core 11	**IT Governance, Risk and Compliance**	Category	L	P	Credit
		C	4	0	4

Preamble

IT GRC ensures that Activities and functions of IT organization(s) support objectives investments are maximised.IT delivers envisioned benefits against the strategy, costs are optimized, and relevant best practices incorporated. The optimal investments is made in IT and critical IT resources are responsibly, effectively and efficiently managed and used.

Prerequisite

- Nil

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bhoom's level
CO1	Study of GRC basics	Understand, Remember
CO2	Learn best practices for IT governance	Understand, Create
CO3	Understand the information security governance concepts	Understand, Evaluate
CO4	Know the ISG practices	Apply, Remember
CO5	Detail study of the compliance	Apply, Evaluate

Mapping with Programme specific outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	S									
CO2		S					S			L
CO3			S						L	
CO4				L		M				
CO5					M			M		

Assessment Pattern

Category	Continuous Internal Assessment(25)			Terminal Examination (75)
	I	II	III	
Remember	5	5	5	25
Understand	6	6	6	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate	2	2	2	5
Create	2	2	2	5

Syllabus

Unit 1: GRC Basics Governance, Risk & Compliance definition, Scope and Objectives - IT Governance Metrics & Framework – BASEL – OECD – NIST - ITGI **(10hrs)**

Unit 2: Best Practices for IT GovernanceITIL - ISO/IEC 27001 - Control Objectives of Information and Related Technology (COBIT) - The Information Security Management Maturity Model - Capability Maturity Model – Other emerging standards **(12hrs)**

Unit 3: Information Security Governance concepts Effective Information Security Governance - Importance of Information Security Governance - Outcomes of Information Security Governance - Strategic alignment - Value Management - Risk Management - Performance Measurement - Information System Strategy - Strategic Planning - Steering Committee - Policies and Procedures **(12hrs)**

Unit 4: Information Security Governance Practices Information Security Management - Performance Optimization - Roles and Responsibilities - Auditing IT Governance Structure - Evaluation Criteria & Benchmark - Assessment Tools - Case Study Analysis - Risk Management Process - Developing a Risk Management Program - COSO – NIST Risk Assessment & Risk Mitigation model - Evaluation & Assessment **(12hrs)**

Unit 5: Compliance Audit, Assessment and review - The Role of the Compliance Officer - The duties and responsibilities of the compliance officer and the function of compliance - The requirements of a Compliance Officer - Drafting compliance reports - Designing an Internal Compliance System - Regulatory principles – Issues - Developing high-level compliance policies - Defining responsibility for compliance - The compliance function - Specific internal compliance control issues - Audit Reports - Best Practices for IT compliance and Regulatory Requirements - IT Compliance requirements under clause 49 of SEBI Listing agreement - IT Compliance requirements under Sarbanes Oxley Act of USA. **(14hrs)**

TOTAL (60Hrs)

Books:

1. Information Security Governance: Guidance for Information Security Managers by W. KragBrotby, 1st Edition, Wiley Publication, 13 April 2009
2. Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition by W. KragBrotby, 2nd Edition, ISACA Publication, 01 Mar 2006
3. Security Governance Checklists: Business Operations, Security Governance, Risk Management, and Enterprise Security Architecture by Fred Cohen, Large Print Edition, Fred Cohen &Assosciates Publication, 2005
4. CISSP All-in-One Exam Guide by Shon Harris and Fernando Maymi, 7th Edition, McGraw-Hill Education, 1 June 2016
5. IT Compliance and Controls: Best Practices for Implementation by James J., IV DeLuccia, Illustrated Edition, Wiley Publication, 2008
6. The IT Regulatory and Standards Compliance Handbook: How to Survive Information Systems Audit and Assessments by Craig S. Wright, Brian Freedman, Dale Liu, 1st Edition, Syngress Publication, 2008

7. Auditor's Guide to Information Systems Auditing by Richard E. Cascarino, 2nd Edition, Wiley Publication, 03 Apr 2012.

	Cryptography using Python Laboratory	**L**	**T**	**P**	**C**
				3	**2**

1. Implement the following SUBSTITUTION & TRANSPOSITION TECHNIQUES concepts:

a) Caesar Cipher

b) Playfair Cipher

c) Hill Cipher

d) Vigenere Cipher

e) Rail fence – row & Column Transformation

2. Implement the following algorithms

a) DES

b) RSA Algorithm

c) Diffiee-Hellman

d) MD5

e) SHA-1

3. Implement the Signature Scheme - Digital Signature Standard

4. Demonstrate how to provide secure data storage, secure data transmission and for creating digital signatures (GnuPG)

5. Setup a honey pot and monitor the honeypot on network (KF Sensor)

6. Installation of rootkits and study about the variety of options

7. Perform wireless audit on an access point or a router and decrypt WEP and WPA. (NetStumbler)

8. Demonstrate intrusion detection system (ids) using any tool (snort or any other s/w)

	Advanced Digital Forensics laboratory	**L**	**T**	**P**	**C**
				3	**2**

1. Ethical hacking in mobile, system
2. Perform an experiment on Active and Passive finger printing using XProbe2 or nmap
3. Perform an experiment for Port Scanning with nmap, superscan or any other Equivalent software
4. Generate minimum 10 passwords of length 12 characters using OpenSSL command
5. Performa a experiment to demonstrate how to sniff for router traffic by using the tool Cain and Abel / Wireshark / tcpdump
6. Implement the Signature Scheme - Digital Signature Standard
7. Email and Internet Analysis – Web cache, history, bookmarks – Mail header analysis Email server analysis – Building time lines
8. Rootkit analysis
9. NTFS analysis
10. Comparison of two Files for forensics investigation by Compare IT Software

	Dissertation and Viva Voce	

Preamble of this course is to facilitate transfer of knowledge acquired by a student to a field of his chosen specialization for application to solving a problem. The Co-ordinator of Students' Project works from the department shall coordinate this course. Student is expected to collect and study relevant material under mentorship of a Project Supervisor, identify a suitable problem and propose methodology towards its solution. Alternately a student can explore hardware / software implementation of existing solution(s).

The student will be tested for his understanding of basic principles of the core Specializations. The internal assessment will be made by Project Supervisor. The Project Supervisor will conduct three reviews in each level of progress. On completion of the work, a thesis report should be prepared in the prescribed format and submitted to the department. The end-semester university examination will have a thesis presentation and Viva-Voce examination conducted by a committee of one external examiner and one internal examiner appointed by the HOD/Professor/ Co-ordinator of Students' Project works.

MANONMANIAM SUNDARANAR UNIVERSITY
TIRUNELVELI, TAMILNADU
M.Sc CYBER SECURITY DEGREE PROGRAMME
LIST OF ELECTIVES

(For The Candidates Admitted From 2022-23 Onwards)

SI. No.	Course code	Course name
Electives – Group A		
1.		Biometric Security
2.		Storage Management and Security
3.		Database Security
4.		Scripting Language
Electives – Group B		
5.		Fundamentals of Block chains and Crypto-currency
6.		Risk Management in Cyber Security
7.		Malware Analysis
8.		Android Mobile Application Development
Electives – Group C		
9.		Firewall and Internet Security
10.		Email, Mobile Devices Security
11.		Artificial Intelligence
12.		Big Data Security
Electives – Group D		
13.		Web application development (e-pathshala)
14.		Web Technology (e-pathshala)
15.		Information Security and Audit Monitoring
16.		Security Architecture

	Biometric Security	Category	L	P	Credit
		E	3	0	3

Preamble

To study a security mechanism that recognizes people by verifying their physical or behavioral characteristics.

Prerequisite

- Network Security

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bhoom's level
CO1	The basic physical and biological science and engineering principles underlying biometric systems.	Understand, Remember
CO2	Biometric systems at the component level and be able to analyze and design basic biometric system applications.	Understand, analyze
CO3	Be able to work effectively in teams and express their work and ideas orally and in writing.	Apply, Create
CO4	Identify the sociological and acceptance issues associated with the design and implementation of biometric systems	Apply, Remember
CO5	Various Biometric security issues.	Understand, Evaluate

Mapping with Programme specific outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	S									
CO2		L		M						
CO3						M				S
CO4					L		L	M		
CO5			S						L	

Assessment Pattern

Category	Continuous Internal Assessment(25)			Terminal Examination (75)
	I	II	III	
Remember	5	5	5	25
Understand	6	6	6	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate	2	2	2	5
Create	2	2	2	5

Syllabus

UNIT-I

Biometrics- Introduction- benefits of biometrics over traditional authentication systems -benefits of biometrics in identification systems-selecting a biometric for a system–Applications – Key biometric terms and processes - biometric matching methods -Accuracy in biometric systems.

(12HRS)

UNIT-II

Physiological Biometric Technologies: Fingerprints – Technical description –characteristics - Competing technologies - strengths – weaknesses – deployment - Facial scan - Technical description - characteristics - weaknesses-deployment - Iris scan – Technical description – characteristics - strengths – weaknesses – deployment- Retina vascular pattern (12HRS)

UNIT-III

Technical description – characteristics - strengths – weaknesses – deployment - Hand scan - Technical description-characteristics - strengths – weaknesses deployment – DNA biometrics.
Behavioral Biometric Technologies: Handprint Biometrics – DNA Biometrics. (12HRS)

UNIT-IV

Signature and handwriting technology - Technical description – classification – keyboard / keystroke dynamics- Voice – data acquisition - feature extraction - characteristics - strengths – Weaknesses-deployment. (12HRS)

UNIT-V

Multi biometrics and multi factor biometrics - two-factor authentication with passwords - tickets and tokens – executive decision - implementation plan. (12HRS)

Total (60Hrs)

TEXT BOOKS:

1. Samir Nanavathi, Michel Thieme, and Raj Nanavathi : “Biometrics-Identity verification in a network”, 1st Edition, Wiley Eastern, 2002.
2. John Chirillo and Scott Blaul : “Implementing BiometricSecurity”, 1st Edition, Wiley Eastern Publication, 2005.

REFERENCES:

1. John Berger: “Biometrics for Network Security”, 1st Edition, Prentice Hall, 2004.

	Storage management & security	Category	L	P	Credit
		E	3	0	3

Preamble

Storage security is the collective processes, tools and technologies that ensure that only authorized and legitimate users store, access and use storage resources. It enables better security of any storage resource through the implementation of required technologies and policies on storage access and consumption and the denial of access to all unidentified and potentially malicious users.

Prerequisite

- Nil

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bhoom's level
CO1	Study the concepts in storage systems	Understand, Remember
CO2	Understand the idea of networking in network area	Understand, Apply
CO3	Learn backup and recovery mechanisms	Apply, Evaluate
CO4	Know the storage security	Understand, Create
CO5	Study the storage infrastructure management	Understand, Apply

Mapping with Programme specific outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	M									
CO2		M		S				S		
CO3					L					L
CO4			S				L			
CO5						M			M	

Assessment Pattern

Category	Continuous Internal Assessment(25)			Terminal Examination (75)
	I	II	III	
Remember	5	5	5	25
Understand	6	6	6	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate	2	2	2	5
Create	2	2	2	5

Syllabus

Unit – I – Introduction to Storage Systems: Storage System - Introduction to Information Storage and Management, Storage System Environment, Data Protection Raid, Intelligent Storage System. **(12hrs)**

Unit – II – Storage Area Networking: Storage Networking Technologies and Virtualization, Storage Networks, Network Attached Storage, IP SAN, Content Addressed Storage, Storage Virtualization. **(12hrs)**

Unit – III - Backup and Recovery Mechanisms: Introduction to Business Continuity, Backup and Recovery, Local Replication, Remote Replication. **(12hrs)**

Unit – IV – Storage Security: Securing the storage Infrastructure, Storage Security Framework, Risk Triad, Storage Security Domains, Security Implementation in Storage Networking. **(12hrs)**

Unit – V – Storage Infrastructure Management: Managing the Storage Infrastructure, Monitoring the Storage Infrastructure, Storage Management Activities, Developing an Ideal Solution, Concepts in Practice. **(12hrs)**

Total (60Hrs)

Reference Books:

1. Information Storage and Management, “Storing, Managing, and Protecting Digital Information”, Wiley; 1 edition, EMC Corporation, 2009.
2. John Chirillo, Scott Blaul, “Storage Security: Protecting SAN, NAS and DAS”, Wiley Publishers, 2003.
3. David Alexander , Amanda French , David Sutton ,”Information Security Management Principles” The British Computer Society, 2008.

	Database Security	Category	L	P	Credit
		E	3	0	3

Preamble

To study the different models involved in database security and their applications in real time world to protect the database and information associated with them.

Prerequisite

- Introduction to Computer Networks and Components

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bhoom’s level
CO1	Identify the security issues and solve them using appropriate security models.	Understand, Remember
CO2	Implement security mechanisms in a database system and provide a secured information flow.	Apply, Create
CO3	Design secured software using the methodological approach	Apply, Create
CO4	Design and implement secure database systems	Understand, Apply
CO5	Solve Complex Problems in a Team of database works	Apply, Remember

Mapping with Programme specific outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1		M								M
CO2		S			S		M			S
CO3			M						L	
CO4	S				M			M		
CO5			L			L				

Assessment Pattern

Category	Continuous Internal Assessment(25)			Terminal Examination (75)
	I	II	III	
Remember	5	5	5	25
Understand	6	6	6	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate	2	2	2	5
Create	2	2	2	5

Syllabus

Unit 1: INTRODUCTION: introduction to Databases Security Problems in Databases Security Controls Conclusions Security Models - Introduction Access Matrix Model Take-Grant Model Acten Model PN Model Hartson and Hsiao's Model Fernandez's Model Bussolati and Martella's Model for Distributed databases **(12hrs)**

Unit 2:SECURITY MODELS Bell and LaPadula's Model Biba's Model Dion's Model Sea View Model Jajodia and Sandhu's Model the Lattice Model for the Flow Control conclusion Security Mechanisms Introduction User Identification/Authentication Memory Protection Resource Protection Control Flow Mechanisms Isolation Security Functionalities in Some Operating Systems Trusted Computer System Evaluation Criteria. **(14hrs)**

Unit 3:SECURITY SOFTWARE DESIGN Introduction A Methodological Approach to Security Software Design Secure Operating System Design Secure DBMS Design Security Packages Database Security Design Statistical Database Protection & 58Intrusion Detection Systems Introduction Statistics Concepts and Definitions Types of Attacks Inference Controls evaluation Criteria for Control Comparison .Introduction IDES System RETISS System ASES System Discovery. **(10hrs)**

Unit 4: MODELS FOR THE PROTECTION OF NEW GENERATION DATABASE SYSTEMS 1- Introduction A Model for the Protection of Frame Based Systems A Model for the Protection of Object Oriented Systems SORION Model for the Protection of Object-Oriented Data. SYSTEMS 2 - A Model for the Protection of New Generation Database Systems: the Orion Model Jajodia and Kogan's Model a Model for the Protection of Active Databases Conclusions **(12hrs)**

Unit 5: CASE STUDY :Database Watermarking – Basic Watermarking Process - Discrete Data, Multimedia,andRelational Data – Attacks on Watermarking - Single Bit Watermarking, Multi bit Watermarking. **(12hrs)**

TOTAL (60hrs)

Textbook

1. Hassan A. Afyouni, " Database Security and Auditing" , India Edition, CENGAGE Learning, 2009.
2. Castano ," Database Security" , Second edition, Pearson Education, 2002.
3. Alfred basta, melissazgola, " Database security", CENGAGE learning, 2014.
4. Michael Gertz and SushilJajodia, " Handbook of Database Security: Applications and Trends",
Springer, 2010.
5. Osama S. Faragallah, El-Sayed M. El-Rabaie, Fathi E. Abd El-Samie, Ahmed I. Sallam, and Hala S. ElSayed, Multilevel Security for Relational Databases", ISBN 978-1-4822- 0539-8. CRC Press, 2014.
5. https://www.techopedia.com/definition/29841/database-security
6. https://www.sisense.com/glossary/database-security/
7. https://www.cs.uct.ac.za/mit_notes/database/pdfs/chp12.pdf.

	Scripting Language	Category	L	P	Credit
		E	3	0	3

Preamble

This course gives introduction to the concepts of ASP, VB Script and Java Script, Working with ASP.NET to enhance communication and security and to develop web page.

Prerequisite

- Nil

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bhoom’s level
CO1	Client-side scripting language, ASP, VB Script and Java Script, Working with ASP.NET to enhance communication and security and to develop web page.	Understand, Remember
CO2	Develop applications by using scripting concepts. exhibit the knowledge of programming with basic building blocks of scripting language	Apply, Create
CO3	Gain deep knowledge in different controls using client server	Apply, Evaluate
CO4	Validation controls in developing client-side scripting language. the features of all objects, caching and session management for every client.	Understand, Apply
CO5	Applications which connect client servers using scripting language	Apply, Understand

Mapping with Programme specific outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	S	M								M
CO2		S					M			S
CO3			M					S		
CO4					M				L	
CO5						L				

Assessment Pattern

Category	Continuous Internal Assessment(25)			Terminal Examination (75)
	I	II	III	
Remember	5	5	5	25
Understand	6	6	6	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate	2	2	2	5
Create	2	2	2	5

Syllabus

Unit 1: INTRODUCTION : Introduction To` Vbscript - Adding Vbscript Code To An Html Page - Vb Script Basics – Vbscript Data Types - Vbscript Variables - Vbscript Constants -Vbscript Operators – Mathematical- ComparisonLogical - Using Conditional Statements - Looping Through Code - Vbscript Procedures – Type Casting Variables - Math Functions – Date Functions – String Functions – Other Functions - Vbscript Coding Conventions - Dictionary Object In Vbscript - Err Object.**(12hrs)**

Unit 2:JAVA SCRIPT Introduction To Javascript – Advantages Of Javascript – Javascript Syntax – Data Type –Variable - Array – Operator &Expression – Looping – Control Structures - Constructor Function – User Defined Function Dialog Box**(14hrs)**

Unit 3: OBJECT MODEL Javascript Document Object Model – Introduction – Object In HTML – Event Handling – Window Object – Document Object – Browser Object – Form Object – Navigator Object – Screen Object – Build In Object – User Defined Object – Cookies

(10hrs)

Unit 4: ASP.NET Language Structure – Page Structure – Page Event, Properties &Compiler Directives. HTML Server Controls – Anchor, Tables, Forms, Files. Basic Web Server Controls – Lable, Text Box, Button, Image Links, Check & Radio Button, Hyperlink, Data List Web Server Controls – Check Box List. Radio Button List, Drop down List, List Box, Data Grid, Repeater

(12hrs)

Unit 5: Request And Response Objects, Cookies, Working With Data – OLEDB Connection Class, Command Class, Transaction Class, Data Adaptor Class, Data Set Class. Advanced Issues – Email, Application Issues, Working with IIS and Page Directives, Error Handling. Security – Authentication, IP Address, Secure By SSL & Client Certificates.

(12hrs)

TOTAL (60hrs)

Textbook

1. I.Bayross,"Web Enable Commercial Application Development using HTML, DHTML, Javascript", Perl CGI, BPB Publications,2000.
2. A.RussellJones , "Mastering Active Server Pages 3", BPB Publications, 2000.
3. Hathleen ,Kalata." Internet Programming with VBScript and JavaScript" , Thomson Learning, 2000.
4. Mike McGrath, "XML Harness the Power of XML in easy steps", Dreamtech Publications.
5. T.A. Powell , "Complete Reference HTML", TMH, 2002.
6. J.Jaworski , "Mastering Javascript" , BPB Publications, 1999.

	Fundamentals of Blockchains and Crypto-currency	Category	L	P	Credit
		E	3	0	3

Preamble

Blockchain and Cryptocurrencies are fast becoming a worldwide Tour De Force that is taking all markets and industries by storm.

Prerequisite

- Network Security

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bhoom's level
CO1	Learn basic concepts of block-chains	Understand, Remember
CO2	Understanding the crypto-currency technology	Create, Apply
CO3	Know the block chain architecture	Create, Evaluate
CO4	Study the block chain applications	Understand, Apply
CO5	Learn the regulatory frameworks	Understand, Create

Mapping with Programme specific outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1										
CO2	S	S				S		S		M
CO3				M			S		M	
CO4			L		L			L		
CO5	M	L				M				M

Assessment Pattern

Category	Continuous Internal Assessment(25)			Terminal Examination (75)
	I	II	III	
Remember	5	5	5	25
Understand	6	6	6	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate	2	2	2	5
Create	2	2	2	5

Syllabus

Unit 1: Currency-Technology Stack: Blockchain, Protocol, Currency - The Double-Spend and Byzantine Generals' Computing Problems - Cryptocurrency Works **(12hrs)**

Unit 2: Contracts-Financial Services – Crowdfunding - Bitcoin Prediction Markets - Smart Property - Smart Contracts - Blockchain 2.0- Protocol Projects - Wallet Development Projects - Blockchain Development Platforms and APIs –BlockchainEcosystem:Decentralized Storage, Communication, and Computation - Ethereum: Turing-Complete Virtual Machine - Dapps, DAOs, DACs, and DASs: Increasingly Autonomous Smart Contracts 22 Dapps - The Blockchain as a Path to Artificial Intelligence **(12hrs)**

Unit 3: Justice Applications Beyond Currency, Economics, and Markets-Blockchain Technology Is a New and Highly Effective Model for Organizing Activity - Extensibility of Blockchain Technology Concepts - Fundamental Economic Principles: Discovery, Value Attribution, and Exchange - Distributed Censorship-Resistant Organizational Models - Namecoin: Decentralized Domain Name System - Digital Identity Verification - Digital Art: Blockchain Attestation Services (Notary, Intellectual Property Protection) - Blockchain Government**(12hrs)**

Unit 4: Efficiency and Coordination Applications Beyond Currency, Economics, and Markets: Blockchain Science: Gridcoin, Foldingcoin - Blockchain Genomics - Blockchain Health - Blockchain Learning: Bitcoin MOOCs and Smart Contract Literacy - Blockchain Academic Publishing: Journalcoin - The Blockchain Is Not for Every Situation - Centralization-Decentralization Tension and Equilibrium **(12hrs)**

Unit 5: Advanced Concepts-Terminology and Concepts - Currency, Token, Tokenizing - Currency Multiplicity: Monetary and Nonmonetary Currencies - Demurrage Currencies: Potentially Incitory and Redistributable. Limitations-Technical Challenges - Business Model Challenges - Scandals and Public Perception Government Regulation - Privacy Challenges for Personal Records - Overall:centralization Trends Likely to Persist **(12hrs)**

TOTAL (60Hrs)

Textbook:

Blockchain - Blueprint for a New Economy :Melanie Swan, OREILLY

	Risk Management in Cyber Security	Category	L	P	Credit
		E	3	0	3

Preamble

This course will address the issues faced by management responsible for ensuring the security of organizational technology, communications and data infrastructure.

Prerequisite

- Nil

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bhoom's level
CO1	Current Threat Landscape, Current Organizational Risk Trends	Understand, Remember
CO2	Cyber Risk Management Fundamentals, Understand Key Frameworks and Methodologies	Understand, Apply
CO3	Identify Cyber Security Risks, Articulate Cyber Security Risks as Business Consequences	Apply, Create
CO4	Risk Management Life Cycle	Understand, Evauate
CO5	Business Cost-Benefit Analysis Techniques	Apply, analyze

Mapping with Programme specific outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1		M								M
CO2	S	S					M			S
CO3			M					S		
CO4				S	M				L	
CO5						L				

Assessment Pattern

Category	Continuous Internal Assessment(25)			Terminal Examination (75)
	I	II	III	
Remember	5	5	5	25
Understand	6	6	6	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate	2	2	2	5
Create	2	2	2	5

Syllabus

UNIT I INTRODUCTIONTO CYBERSECURITY

The Security Environment: Threats, vulnerabilities, and consequences - Advanced persistent threats - The state of security today. Principles of Cybersecurity: The interrelated components of the computing environment - Cybersecurity models - Variations on a theme: computer security, information security, and information assurance. Cybersecurity Management Concepts: Management models, roles, and functions. Enterprise Roles and Structures: Information security roles and positions. (12hours)

UNIT II STRATEGIC PLANNING AND SECURITY PLANS

Strategy and Strategic Planning: Strategy - Strategic planning and security strategy - The information security lifecycle - Architecting the enterprise. Security Plans and Policies: Levels of planning - Planning misalignment - The System Security Plan (SSP)- Policy development and implementation. Security Standards and Controls: Security standards and controls - Certification and accreditation (C&A). (12hours)

UNIT III RISK MANAGEMENT

Risk Management: Principles of risk - Types of risk - Risk strategies - The Risk Management Framework (RMF). Physical Security and Environmental Events: Physical and environmental threats - Physical and environmental controls. Contingency Planning: Developing a contingency plan - Understanding the different types of contingency plan - Responding to events. (12hours)

UNIT IV SECURITY AWARENESS

Security Education, Training, and Awareness: Human factors in security - Developing and implementing a security training plan - Cross-domain training (IT and other security domains). The future of cyber security: Key future uncertainties - Possible future scenarios - How to apply what you've learned. (12hours)

UNIT V CASE STUDY

Case Study on Pune Citibank MphasiS Call Center Fraud – The Bank NSP Case – UTI Bank hooked in a phishing attack – Mumbai Police can now nail web offenders – Orkut: The new danger. (12hours)

Total: 60 Hours

Books for References:

1. Rhodes-Ousley, Mark. "Information Security: The Complete Reference, Second Edition, . Information Security Management: Concepts and Practice", New York, McGraw-Hill, 2013.
2. Whitman, Michael E. and Herbert J. Mattord, " Roadmap to Information Security for IT and Infosec Managers", Boston, MA: Course Technology, 2011.
3. Michael E. Whitman and Herbert J. Mattord, "Principles of Information Security", Course Technology, Cengage Learning, Fourth Edition, Nov, 2014.

Web Resources:

1.file:///C:/Users/admin/Desktop/Online%20work/Course/Risk%20management%20in%20Cyber%20Security/Whitman.pdf
2. https://www.cyberralegalservices.com/detail-casestudies.php.
3.https://rtinagpur.cag.gov.in/uploads/CaseStudies/CaseStudiesonCyberCrimesNOTSENT/CaseStudiesonCyberCrimes.pdf.

	Malware Analysis	Category	L	P	Credit
		E	3	0	3

Preamble

The purpose is to understand the purpose of malware, work with examples of famous virus and worms.

Prerequisite

- ✓ Network Security

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bhoom’s level
CO1	The purpose of computer infection program.	Understand, Remember
CO2	The covert channel and mechanisms.	Apply, Understand
CO3	Test and exploit various malware in open-source environment.	Apply, Evaluate
CO4	Analyze and design the famous virus and worms.	Analyze, Create
CO5	Analyze the given Portable Executable and Non-Portable Executable files using Static and dynamic analysis techniques	Analyze, Apply

Mapping with Programme specific outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1		M								M
CO2		S				S	M			S
CO3	S		M					M		
CO4				S	M				L	
CO5						L				

Assessment Pattern

Category	Continuous Internal Assessment(25)			Terminal Examination (75)
	I	II	III	
Remember	5	5	5	25
Understand	6	6	6	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate	2	2	2	5
Create	2	2	2	5

Syllabus

Unit 1 ; Malicious software: Definition - Needs - Goals - Requirements - Environment setup – Types of malicious software analysis, Types of malicious software. Dynamic Analysis: PE structure - Tools needed for malware analysis - steps to take care of to protect our host - steps to analyse a file and giving reputation - Advanced dynamic analysis - windbg - How to analyse DLL files - Malicious network traffic analysis – creating YARA rules. (12hrs)

Unit 2: Analysing Non-PE files: File structures of Non-PE file - Importance of working with Non-PE files - Tools required to analyse Non-PE files - how to analyse Microsoft document file – how to analyse PDF files - how to analyse flash files. (12hrs)

Unit 3: Static Analysis: Importance of PE are disassemblers structures - Packers -compilers - crypters - Tools used for static analysis - debuggers - packing and unpacking a malware - Types Of Debugging - OllyDbg - virustotal - hashing - Shell code Analysis – Analyzing Malicious Windows Programs - Why antivirus needed - how antivirus works - how to create signature for a malware to support antivirus - analysing antivirus signatures. (12hrs)

Unit 4: Exploit writing/analysis: Introduction to exploit analysis - Anti-disassembly techniques - VM detection - bypassing anti-disassembly - basics of exploit writing - shellcode analysis - working with exploit writing - Hardware based malware - Ducky scripts - Throwstarlantap pro.

(12hrs)

Unit 5 : Web Exploits analysis: What are the severity of web exploits - why its carried on - how its carried on - tools required to analyse web exploits - Environment setup -Exploit kit analysis - vulnerabilities used in Exploit kits - how vulnerabilities are used to create exploit kits - Introduction to Linux and Mac OS malware analysis. (12hrs)

Total (60hrs)

Textbook

1. Michael Sikorski and Andrew Honig, "Practical Malware Analysis" ,No starch press, February, 2012.
2. Michael Ligh, Steven Adair, Blake Hartstein, Matthew Richard , "Malware Analyst's Cookbook" , John Wiley & Sons, October, 2010.
3. Mark Russinovich, David A. Solomon, Alex Ionescu "Windows Internals", Microsoft Press, 6th edition, 2012

	ANDROID MOBILE APPLICATION DEVELOPMENT	L	T	P	C
		3			3

Preamble

The mobile application development landscape uses Android as the platform. The basics of the Android platform, Android application components, Activities and their lifecycle, UI design, Multimedia, 2D graphics and networking support in Android.

Prerequisite

- Nil

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bhoom's level
CO1	Learn the basic elements in module computing	Apply, Remember
CO2	Know the concepts of android	Understand, Create
CO3	Understand the android activities and GUI design concepts	Understand, Apply
CO4	Know the advanced UI programming	Analyze, Create
CO5	Learn toast, menu dialog, list and adapters	Understand, Evaluate

Mapping with Programme specific outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	M	M								S
CO2								L		
CO3		M		S	L				L	
CO4						M				
CO5			S				S			

Assessment Pattern

Category	Continuous Internal Assessment(25)			Terminal Examination (75)
	I	II	III	
Remember	5	5	5	25
Understand	6	6	6	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate	2	2	2	5
Create	2	2	2	5

Syllabus

UNIT –I Introduction to Mobile Computing: Mobile Communication Concept - generations of wireless technology – Basics concept of cell, cluster and frequency reuse - Noise effects on mobile - Understanding GSM and CDMA - Basics of GSM architecture, its services like voice call, SMS, MMS, LBS, VAS - Different modes used for Mobile Communication - Architecture of Mobile Computing(3 tier) - Design considerations for mobile computing - Mobile Communication Characteristics - Mobile communication Application - Mobile Computing Security Concerns - Middleware and Gateway needed for mobile Computing - Making Existing Application Mobile Enable - Mobile IP - Basic Mobile Computing Protocol - Mobile Communication through Satellite (Low orbit satellite, Medium orbit satellite, Geo stationary satellite, Satellite phones) **(14hrs)**

UNIT–II Introduction to Android: Overview of Android - What does Android run On - Internals of Android? - Android for mobile apps development - Environment setup for Android apps Development - Framework - Android - SDK, Eclipse - Emulators –What is an Emulator / Android AVD **(10hrs)**

UNIT –III Android Activities and GUI Design Concepts: Android Application Design criteria: Consideration for Hardware Design, Design Demands For Android application, Intent, Activity, Activity Lifecycle and Manifest - Creating Application and new Activities - Simple UI - Layouts and Layout properties : Introducing Android UI Design, Introducing Layouts - XML Introduction to GUI objects viz.: Push Button, Text / Labels , EditText, ToggleButton , Padding **(13hrs)**

UNIT –IV Advanced UI Programming: Event driven Programming in Android - (Text Edit, Button clicked etc.) - Activity Lifecycle of Android **(11hrs)**

UNIT –V Toast, Menu, Dialog, List and Adapters Menu: Basics, Custom v/s System Menus, Create and Use Handset menu Button (Hardware) - Dialog : Creating and Altering Dialogs - Toast : List & Adapters - Demo Application Development and Application Launching - Basic operation of SQLite Database - Priorities for Android Application **(12hrs)**

Total(60hrs)

Books:

1J.F.De Marzio, Android –A Programmer's Guide, McGraw Hill Pub, 2008.
2. Building Android Apps IN EASY STEPS McGraw - Hill Education
3.Professional Android 2 Application Development by Reto Meier, Wiley India Pvt Ltd.,2012
4.Beginning Android by Mark L Murphy,Wiley India Pvt Ltd.,2015
5. Pro Android, by Sayed Y Hashimi and SatyaKomatineni Wiley India Pvt Ltd., 2015

	Firewall and Internet Security	Category	L	P	Credit
		E	3	0	3

Preamble

This course introduces the basic concept of Firewalls, fundamentals of internet security and security architecture, the different kinds of security threats in networks, databases and their solutions.

Prerequisite

- Nil

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bhoom's level
CO1	Fundamentals of firewalls and internet security. malicious and non-malicious code.	Understand, Create
CO2	List and explain various type of threats in networks.	Apply, Evaluate
CO3	The concept of controls against program threat and to find the vulnerabilities in programs.	Apply, Understand
CO4	The concept of database security and to write secured transactions in databases.	Understand, Evaluate
CO5	The security requirements and multilevel database. To expose the students to the proposals for multilevel security.	Apply, Remember

Mapping with Programme specific outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1		M								M
CO2		S					M			S
CO3	S		M	S					L	
CO4					M			S		
CO5						L				

Assessment Pattern

Category	Continuous Internal Assessment(25)			Terminal Examination (75)
	I	II	III	
Remember	5	5	5	25
Understand	6	6	6	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate	2	2	2	5
Create	2	2	2	5

Syllabus

UNIT I FIREWALLS AND SECURITY MECHANISM

Introduction – Types of Firewalls – Packet filters – Application gate ways – Limitations of firewalls - Internet Security - Email security – PGP - S/MIME - IP security – Overview – IP Security Architecture - Web security - SSL, TLS, SET. (12hrs)

UNIT III PROGRAM SECURITY

Secure programs – Non-malicious Program Errors – Viruses – Targeted Malicious code – Controls against Program Threat – Control of Access to General Objects – User Authentication – Good Coding Practices – Open Web Application Security Project Top 10 Flaws – Common Weakness Enumeration Top 25 Most Dangerous Software Errors. (12hrs)

UNIT III OPERATING SYSTEM SECURITY

Protected objects and methods of protection- Memory address protection- Control of access to general objects- File protection mechanism-Authentication: Authentication basics- Password-Challenge response- Biometrics. (12hrs)

UNIT IV SECURITY IN DATABASES

Security requirements of database systems – Reliability and Integrity in databases – Two Phase Update – Redundancy/Internal Consistency – Recovery – Concurrency/Consistency – Monitors – Sensitive Data– Types of disclosures – Inference. (12hrs)

UNIT V SECURITY IN NETWORKS AND CASE STUDY

Threats in networks – Encryption – Virtual Private Networks – PKI – SSH – SSL – IPSec – Content Integrity – Access Controls – Wireless Security – Honeypots – Traffic Flow Security – Firewalls – Intrusion Detection Systems – Secure e-mail. (12hrs)

Total: 60 Hours

Books for References:

1. Charles P. Pfleeger, Shari Lawrence Pfleeger, “Security in Computing”, Fourth Edition, Pearson
Education, 2007.
2. Matt Bishop, “Computer Security: Art and Science”, Pearson Education, 2003.
3. William Stallings, “Cryptography and Network Security: Principles and Practices”, Fifth Edition,
Prentice Hall, 2010.
4. Michael Howard, David LeBlanc, John Viega, “24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them”, First Edition, McGraw Hill Osborne Media, 2009.
5. Kaufman, Perlman, Speciner, “Network Security”, Prentice Hall, 2nd Edition, 2003.
6. Eric Maiwald, “Network Security: A Beginner’s Guide”, TMH, 1999.
7. Macro Pistoia, Java Network Security, Pearson Education, 2nd Edition, 1999.
8. Whitman, Mattord, Principles of Information Security, Thomson, 2nd Edition, 2005.

	Email, Mobile Devices Security	Category	L	P	Credit
		E	3	0	3

Preamble

Email security is a priority for all businesses, with the growing threat of hackers, viruses spam, phishing and identity theft, as well as the need to secure business information. Mobile security is the protection of smartphones, tablets, laptops and other portable computing devices, and the networks they connect to, from threats and vulnerabilities associated with wireless computing. Mobile security is also known as wireless security.

Prerequisite

- Network Security

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bhoom's level
CO1	Understanding basics of email	Understand, Remember
CO2	Study about simple mail transfer protocol	Apply, Create
CO3	Learn focused attacks against email systems	Understand
CO4	Understand the spam and phishing concepts	Analyze
CO5	Study about mobile and wireless devices	Apply, Evaluate

Mapping with Programme specific outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	S									
CO2		L		M					L	
CO3					S	M				
CO4							S	L		
CO5			S							M

Assessment Pattern

Category	Continuous Internal Assessment(25)			Terminal Examination (75)
	I	II	III	
Remember	5	5	5	25
Understand	6	6	6	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate	2	2	2	5
Create	2	2	2	5

Syllabus

Unit 1: Basics of email - How email works - The role of Mail User Agent, Mail Delivery Agent, Mail Transfer Agent, and DNS servers - An overview of various protocols (SMTP, POP, IMAP) involved in a typical email infrastructure - A brief introduction to security issues relevant to emails as well as the typical email infrastructure. **(9hrs)**

Unit 2: Simple Mail Transfer Protocol - SMTP model including the basic structure as well as the extension model - The SMTP terminology - SMTP procedures (session initiation, mail transaction, forwarding mail, relaying, mail gatewaying, support for mailing lists as well as aliases, termination etc) - Important SMTP commands including their sequencing as well as the corresponding replies / response codes - Commands for debugging addresses - SMTP trace information - Address resolution & mail handling - Problem detection & handling - Security considerations **(14hrs)**

Unit 3: Focused attacks against email systems - Common attacks against SMTP, POP3 and IMAP services - Vulnerabilities in web mail systems - Exploits targeting the supporting infrastructure - Cryptographic techniques to protect against email eavesdropping and masquerading attacks - Architectural guidelines for secure mail infrastructure - Hardening email infrastructure **(10hrs)**

Unit 4: Spam & Phishing - History of Spam - Harvesting email addresses - Anonymous emails - forging headers, using open relays & proxy servers, employing proxy chaining techniques, botnets - Sending Spam - Tools of trade - Historical anti-spam approaches - Language classification and statistical filtering anti-spam techniques - Anti-spam solution offerings - Definitions - What is phishing and what's not - Email security issues that aid in phishing - Role of emails in common types of phishing attacks (impersonation, forwarding and popups) - Anti-phishing solution offerings **Email Forensics -** Understanding message headers - Forging message headers and identifying forged headers - General approaches to tracking the email sender - General approaches to inspect attachments - Spam and steganography. **(14hrs)**

Unit -5 Mobile & Wireless Devices : Introduction – Types of Mobiles and wireless devices and their functionalities - Proliferation of Mobile and Wireless Devices - Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing - Types and Techniques of Credit Card Frauds - Security Challenges Posed by Mobile Devices - Registry Settings for Mobile Devices Authentication Service Security - Mobile phone camera and microphone hacking - On-Screen Keyboard keyloggers - : 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: Security Implications for Organizations: Managing Diversity and Proliferation of Hand-Held Devices, Unconventional/Stealth Storage Devices Threats through Lost and Stolen Devices, Protecting Data on Lost Devices, Importance of Security Policies relating to Mobile Computing Devices, Operating Guidelines for Implementing

Mobile Device Security Policies, Organizational Policies for the Use of Mobile Hand-Held Devices, Laptops: Physical Security Countermeasures **(15hrs)**

TOTAL (60hrs)

Reference Books:

1.Mobile Security and Privacy1st EditionAdvances, Challenges and Future Research Directions by Man Ho Au Raymond Choo

	Artificial Intelligence	Category	L	P	Credit
		E	3	0	3

Preamble

The course will address key AI technologies in an attempt to help in understanding their role in cyber security and the implications of these new technologies to the world of politics. AI deficiently will complement and strengthen the cyber security practices and will improve their applications in enhancing
our security.

Prerequisite

- Nil

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bhoom's level
CO1	Understand the Future of Artificial Intelligence and cyber security.	Understand, Analyze
CO2	Analyze the different Problem Solving Approaches.	Apply, Create
CO3	Evaluate the security issues of web applications, services and severs.	Apply, Create
CO4	Analyze software agents and applications.	Understand, Remember
CO5	Assess different Cyber Security Vulnerabilities	Apply

Mapping with Programme specific outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1		M								M
CO2	S	S					M			S
CO3			M					L		
CO4				S	M					
CO5						L			S	

Assessment Pattern

Category	Continuous Internal Assessment(25)			Terminal Examination (75)
	I	II	III	
Remember	5	5	5	25
Understand	6	6	6	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate	2	2	2	5
Create	2	2	2	5

Syllabus

UNIT I INTRODUCTION TO ARTIFICIAL INTELLIGENCE

Introduction–Definition – Future of Artificial Intelligence – Characteristics of Intelligent Agents– Typical Intelligent Agents – Problem Solving Approach to Typical AI problems-Algorithms and Optimization Problems -Searching with Partial Observations – Constraint Satisfaction Problems – Constraint Propagation – Backtracking Search – Game Playing – Optimal Decisions in Games – Alpha – Beta Pruning – Stochastic Games. (12hrs)

UNIT II SOFTWARE AGENTS AND APPLICATIONS

Architecture for Intelligent Agents – Agent communication – Negotiation and Bargaining – Argumentation among Agents – Trust and Reputation in Multi-agent systems- AI applications – Language Models – Information Retrieval- Information Extraction – Natural Language Processing – Machine Translation – Speech Recognition – Robot – Hardware –Perception – Planning – Moving. (12hrs)

UNIT III CYBER SECURITY VULNERABILITIES AND SAFEGUARDS

Cyber Security Vulnerabilities-Overview- vulnerabilities in software-System administration-Complex Network Architectures- Open Access to Organizational Data-Weak Authentication-Unprotected Broadband communications-Poor Cyber Security Awareness- Cyber Security Safeguards- Access control- Cryptography- Deception-Denial of Service Filters-Ethical Hacking- Firewalls-Intrusion Detection Systems- Threat Management. (12hrs)

UNIT IV SECURING WEB APPLICATION, SERVICES AND SERVERS

Basic security for HTTP Applications and Services- Basic Security for SOAP Services- Identity Management and Web Services- Authorization Patterns- Security Considerations- Challenges - Malware infection, Intrusion detection and Prevention Techniques, Anti-Malware SoftwareBotnet detection-Spam filter applications-Hacking incident forecasting-cyber security ratings. (12hrs)

UNIT V CYBER FORENSICS AND CASE STUDIES

Introduction to Cyber Forensics- Conducting disk-based analysis- Investigating Informationhiding-Scrutinizing E-mail- Tracing Internet access- Tracing memory in real-time-Case study: Cyber Security Regulations- Roles of International Law- Cyber Security Standards-The INDIAN Cyberspace- National Cyber Security Policy 2013. (12hrs)

Total: 60 Hours

Books for References:

1. Stuart Russell and Peter Norvig, "Artificial Intelligence: A Modern Approach", 3rd Edition, 2010.
2. James Graham, RicharHoward,Ryan Olson, "Cyber Security Essentials", CRC Press, Tailor and Francis Group, 2011.
3. Nina Godbole, SunitBelapur, "Cyber Security Understanding Cyber Crimes, ComputerForensics and Legal Perspectives", Wiley India Publications, April, 2011.
4. https://www.cyberralegalservices.com/detail-casestudies.php.

	Big Data Security	Category	L	P	Credit
		E	3	0	3

Preamble

Big Data security is the processing of guarding data and analytics processes, both in the cloud and on-premise, from any number of factors that could compromise their confidentiality.

Prerequisite

- Information security

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bhoom's level
CO1	Know the big data privacy, ethics and security	Understand, Remember
CO2	Study the security, compliance, auditing and protection of data	Understand, Create
CO3	Learn hadoop security design	Apply, Analyze
CO4	Understand hadoop ecosystem security	Apply, Remember
CO5	Know data security and event logging	Understand

Mapping with Programme specific outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	M									
CO2		L				M				
CO3		S		M				M		
CO4							S		L	S
CO5			S		L					

Assessment Pattern

Category	Continuous Internal Assessment(25)			Terminal Examination (75)
	I	II	III	
Remember	5	5	5	25
Understand	6	6	6	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate	2	2	2	5
Create	2	2	2	5

Syllabus

UNIT I – BIG DATA PRIVACY, ETHICS AND SECURITY Privacy – Reidentification of Anonymous People – Why Big Data Privacy is self-regulating? – Ethics – Ownership – Ethical Guidelines – Big Data Security – Organizational Security.

(12hrs)

UNIT II - SECURITY, COMPLIANCE, AUDITING, AND PROTECTION Steps to secure big data – Classifying Data – Protecting – Big Data Compliance – Intellectual Property Challenge – Research Questions in Cloud Security – Open Problems.

(12hrs)

UNIT III – HADOOP SECURITY DESIGN Kerberos – Default Hadoop Model without security - Hadoop Kerberos Security Implementation & Configuration.

(12hrs)

UNIT IV – HADOOP ECOSYSTEM SECURITY Configuring Kerberos for Hadoop ecosystem components – Pig, Hive, Oozie, Flume, HBase, Sqoop. **(12hrs)**

UNIT V – DATA SECURITY & EVENT LOGGING Integrating Hadoop with Enterprise Security Systems - Securing Sensitive Data in Hadoop – SIEM system – Setting up audit logging in hadoop cluster

(12hrs)

TOTAL (60hrs)

Books:

1. Mark Van Rijmenam, “Think Bigger: Developing a Successful Big Data Strategy for Your Business”, Amazon, 1 edition, 2014.
2. Frank Ohlhorst John Wiley & Sons, “Big Data Analytics: Turning Big Data into Big Money”, John Wiley & Sons, 2013.
3. SherifSakr, “Large Scale and Big Data: Processing and Management”, CRC Press, 2014.
4. Sudeesh Narayanan, “Securing Hadoop”, Packt Publishing, 2013.
5. Ben Spivey, Joey Echeverria, “Hadoop Security Protecting Your Big Data Problem”, O’Reilly Media, 2015.

1. Top Tips for Securing Big Data Environments: e-book (http://www.ibmbigdatahub.com/whitepaper/top-tips-securing-big-data-environments-ebook)
2. http://www.dataguise.com/?q=securing-hadoop-discovering-and-securing-sensitive-Datahadoop-data-stores

8. Gazzang for Hadoophttp: // www.cloudera.com/ content/cloudera/ en/ solutions/ Enterprise solutions / security-for-hadoop.html
9. eCryptfs for Hadoop https://launchpad.net/ecryptfs.
10. Project Rhino - https://github.com/intel-hadoop/project-rhino/

	Web application development (e-pathshala)	Category	L	P	Credit
		E	3	0	3

Preamble

design and develop websites for a variety of devices. The course focuses on HTML, cascading style sheets, and digital imaging with Adobe Photoshop. Students will also be introduced to JavaScript.

Prerequisite

- Nil

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bhoom's level
CO1	The principles of creating an effective web page, including an in-depth consideration of information architecture.	Understand, Apply
CO2	Become familiar with graphic design principles that relate to web design and learn how to implement theories into practice.	Apply, Analyze
CO3	Develop skills in analyzing the usability of a web site.	Apply, Create
CO4	Understand how to plan and conduct user research related to web usability.	Understand, Evaluate
CO5	Learn the language of the web: HTML and CSS.	Apply

Mapping with Programme specific outcomes

COs	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1		M								M
CO2	S	S					M			S
CO3			M						L	
CO4					M			S		
CO5				S		L				

Assessment Pattern

Category	Continuous Internal Assessment(25)			Terminal Examination (75)
	I	II	III	
Remember	5	5	5	25
Understand	6	6	6	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate	2	2	2	5
Create	2	2	2	5

Syllabus

Unit 1: Introduction to Web Application Development and HTML – HTML HTML Form - In stalling WAMP and PHP Basics - Constant, Expression statements and PHP Control Statement - PHP Function - PHP Function -II - Array – I , Array – II

Unit 2: OOP - I in PHP - OOP - II in PHP - OOP - III in PHP - OOP - IV in PHP - Strings with PHP - Numbers and Dates with PHP - Regular Expressions in PHP

Unit 3: File Handling – I - File Handling – II - Exception Handling - Introduction to relation databases

Unit 4: MySQL - SQL in MySQL – I - - SQL – II in MySQL - SQL – III in MySQL - PHP and MySQL - COOKIE and SESSION

Unit 5: Stored Procedures in MYSQL - Triggers in MySQL - Triggers in MySQL (contd.) - Integrating PHP and MySQL - Email and Frameworks in PHP - Introduction to Java Script - Event Handling and Validation using JavaScript in PhP

Text book

https://epgp.inflibnet.ac.in/Home/ViewSubject?catid=iLkSuZZ5a+koxhsE1m+YjQ==

	Web Technology (e-pathshala)	Category	L	P	Credit
		E	3	0	3

Preamble

Understand the principles of creating an effective web page, including an in-depth consideration of information architecture. Become familiar with graphic design principles that relate to web design and learn how to implement theories into practice. Develop skills in analyzing the usability of a web site.

Prerequisite

- Nil

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bhoom's level
CO1	Learn techniques of responsive web design, including media queries.	Understand, Apply
CO2	Develop basic programming skills using XML	Apply, Create
CO3	Develop basic programming skills using Javascript and jQuery	Apply, Create
CO4	Develop basic programming skills using JDBC	Understand, Evaluate
CO5	Develop basic programming skills using web services	Apply, Remember

Mapping with Programme specific outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1		M								M
CO2	S	S					M			S
CO3			M						L	
CO4				S	M					
CO5						L		S		

Assessment Pattern

Category	Continuous Internal Assessment(25)			Terminal Examination (75)
	I	II	III	
Remember	5	5	5	25
Understand	6	6	6	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate	2	2	2	5
Create	2	2	2	5

Syllabus

Unit 1: Web Technology : Introduction - World Wide Web WWW - Services on Internet - Markup Languages –

Unit 2: XML DTD - XML SCHEMA (PART I) - XML SCHEMA (PART II) - XML DOM - XML DOM and Java

Unit 3: JAVA – CSS – X-path – XSLT –Java script basics , objects – Java script and HTML DOM

Unit 4: JDBC – JAVA SERVELTS

Unit 5: JSP - PHP – WEB SERVICES – JMS

Book for reference

https://epgp.inflibnet.ac.in/Home/ViewSubject?catid=fBYckQKJvP3a/8Vd3L08tQ==

	Information Security and Audit Monitoring	Category	L	P	Credit
		E	3	0	3

Preamble

This course focuses on concepts related to audit and assurance mechanisms related to information security mechanisms such as security policies, their enforcement through software, authentication, cryptography and physical security and their progression through the course of time.

Prerequisite

- Nil

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bhoom's level
CO1	Students should be able understand the need and methods of writing un-ambiguous, usable, and precise security policies.	Understand, Apply
CO2	Describe fundamental concepts of information security and systems auditing	Apply, Create
CO3	Analyze the latest trend of computer security threats and defense	Analyze, Understand
CO4	Identify security weaknesses in information systems, and rectify them with appropriate security mechanisms	Understand, Create
CO5	Critically evaluate the security of information systems	Analyze, Remember

Mapping with Programme specific outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1		M						S		M
CO2		S		S			M			S
CO3			M							
CO4	S				M				L	
CO5						L				

Assessment Pattern

Category	Continuous Internal Assessment(25)			Terminal Examination (75)
	I	II	III	
Remember	5	5	5	25
Understand	6	6	6	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate	2	2	2	5
Create	2	2	2	5

Syllabus

Unit- I

Information Security Performance Metrics and Audit: Security Metrics and Reporting, Common Issues and Variances of Performance Metrics, Introduction to Security Audit, Servers and Storage devices, Infrastructure and Networks, Communication Routes, Information Security Methodologies (Black-box, White-box, Greybox), Phases of Information Security Audit and Strategies, Ethics of an Information Security Auditor etc. Maintain Healthy, Safe & Secure Working environment (NOS 9003) (12hours)

Unit- II

Information Security Audit Tasks, Reports and Post Auditing Actions: Pre-audit checklist, Information Gathering, Vulnerability Analysis, External Security Audit, Internal Network Security Audit, Firewall Security Audit, IDS Security Auditing, Social Engineering Security Auditing, Web Application Security Auditing, Information Security Audit Deliverables & Writing Report, Result Analysis, Post Auditing Actions, Report Retention etc. Provide Data/Information in Standard formats (NOS 9004) (12hours)

Unit- III

Vulnerability Management: Information Security Vulnerabilities – Threats and Vulnerabilities, Human-based Social Engineering, Computer-based Social Engineering, Social Media Countermeasures, Vulnerability Management – Vulnerability Scanning, Testing, Threat management, Remediation etc. (12hours)

Unit -IV

Information Security Assessments: Vulnerability Assessment, Classification, Types of Vulnerability Assessment, Vulnerability Assessment Phases, Vulnerability Analysis Stages, Characteristics of a Good Vulnerability Assessment Solutions &Considerations, Vulnerability Assessment Reports – Tools and choosing a right Tool, Information Security Risk Assessment, Risk Treatment, Residual Risk, Risk Acceptance, Risk Management Feedback Loops etc. (12hours)

Unit -V

Configuration Reviews: Introduction to Configuration Management, Configuration Management Requirements-PlanControl, Development of configuration Control Policies, Testing onfiguration Management etc. (12hours)

Text Books:

1. Assessing Information Security (strategies, tactics, logic and framework)
by A Vladimirov, K.Gavrilenko, and A.Michajlowski

2. “The Art of Computer Virus Research and Defense by Peter Szor.”

b) Reference Books:

1. https://www.sans.org/readingroom/whitepapers/threats/implementing-vulnerability-management-process-34180

2. http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf

	Security Architecture	Category	L	P	Credit
		E	3	0	3

Preamble

This course introduces the basic concepts of Security and its needs, architecture and models and the students gain knowledge about security, information, components, issues, analysis, architecture, various models, security types and its applications.

Prerequisite

- Nil

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bhoom's level
CO1	To understand the basics of security concepts and its advantages	Understand
CO2	Become proficient in concepts like Security components, balancing and Access.	Apply
CO3	To understand the basics of security needs in business, threats etc.,	Apply
CO4	Become proficient in security technologies like IDS, cryptography.	Understand
CO5	To understand the concepts of Access control, physical security and personnel	Apply

Mapping with Programme specific outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1		M								M
CO2		S		S			S			S
CO3	S		M					S		
CO4					M					
CO5						L			L	

Assessment Pattern

Category	Continuous Internal Assessment(25)			Terminal Examination (75)
	I	II	III	
Remember	5	5	5	25
Understand	6	6	6	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate	2	2	2	5
Create	2	2	2	5

Syllabus

UNIT I SECURITY INTRODUCTION

Introduction: Information Security, Critical Characteristics of Information, Components of an Information System, Securing the Components, Balancing Security and Access, **(**12 hours)

UNIT II SECURITY ANALYSIS

Need for security, Business needs, Threats, Attacks, Legal, Ethical and Professional Issues. **(**12 hours)

UNIT III LOGICAL DESIGN

Blueprint for security, Information Security policy, NIST Models, VISA International security Models, Design of Security Architecture, planning for continuity. **(**12 hours)

UNIT IV PHYSICAL DESIGN

Security Technology, IDS, Cryptography, Access Control Devices, Physical Security, Security and Personnel. **(**12 hours)

UNIT V ARCHITECTURE TYPES AND CASE STUDY

Architecture: Types- Low-level, Mid-level and High-level Architecture, Case study- Business cases for Security**.** **(**12 hours)

Total: 60 Hours

Books for References:

1. Matt Bishop, “Computer Security Art and Science”, Addison Wesley, 2018.

2. Micki Krause, Harold F. Tipton, “ Handbook of Information Security Management”,

Vol 1-3, CRC Press LLC, 2004.

3. Michael E Whitman and Herbert J Mattord, “Principles of Information Security”, Vikas

Publishing House, New Delhi, 4th Edition, 2012.