
रा.इ.सू.प्रौ.सं
NIELIT
ISEA
सी डैक
CDAC
PROSPECTUS
Certification Scheme for I .T. SECURITY PROFESSIONALS
ISEA Certified Course
Level3
ISEA Certified Computer Forensic Professional [CCFP]
Or
ISEA Certified Information Systems Security Auditor [CISSA]
Or
ISEA Certified System Security Solution Designer [CSSSD]
Level2
ISEA Certified System Security Professional [CSSP]
Level1
ISEA Certified System Security Analyst [CSSA]
A Joint Certification Scheme by NIELIT & CDAC

Certification Scheme in Information Security

At A Glance

Level-3 ISEA Certified Information Systems Security Auditor [CISSA]*

- Security Standards & Information Security Policy
- Auditing, Penetration Testing & Information Security Risk Management
- Public Key Infrastructure and Trust Management
- Cyber Law and IPR Issues
- Industrial Projects

Level-3 ISEA Certified Computer Forensic Professional [CCFP]*

- Cyber Crime, Indian IT (Amendment) Act 2008 and Introduction to Computer Forensics
- Seizure & Imaging of Digital Evidence
- Analysis of Digital Evidence
- Computer Forensics for Windows & Linux Systems and Anti-forensics
- Industrial Projects

Level-3 ISEA Certified System Security Solution Designer [CSSSD]*

- Application Security & E-Commerce
- Public Key Infrastructure and Trust Management
- Security Standards & Information Security Policy
- Cyber Law and IPR Issues
- Industrial Projects

Level-2 ISEA Certified System Security Professional [CSSP]*

- Cryptography and Network Security
- System and Device Security
- Mobile and Wireless Security
- Database and Web Application Security

Level-1 ISEA Certified System Security Analyst [CSSA]

- Computer Fundamentals and Computer Networks
- Operating System Administration
- Information Security Concepts
- System Security

***Currently Registration is Open for CSSA Level -1 only .The CSSP Level-2 & CCFP/CSSSD/CISSA Level-3 would be launched shortly.**

National Institute of Electronics and Information Technology (NIELIT)
Centre for Development of Advanced Computing (CDAC)
(An Autonomous Scientific Society under the administrative control of Department of Electronics & Information Technology (DeitY), Ministry of Communications and Information Technology, Government of India,)
Electronics Niketan, 6, CGO Complex, New Delhi - 110003

CONTENTS

CONTENTS

1. About Information Security Education and Awareness (ISEA) Project

Keeping in view the pervasive nature and impact of cyber security on all walks of life - economic and social, Government of India has identified Information Security as one of the major thrust area for launching various development programs. One of the key elements essential for information security is availability of right kind of qualified and well trained human resources, who could take up Research & Development (R&D), develop indigenous solutions / software, secure and maintain various systems including critical infrastructure.

Department of Electronics & Information Technology (DeitY) has approved a project in 2005 entitled Information Security Education and Awareness (ISEA) which was completed in 2014 and Phase II of the said Project was approved in April 2014.

ISEA Project Phase II

Objectives

- Capacity building in the area of Information Security to address the human resource requirement of the country, by
  - Generation of core research manpower to undertake basic/fundamental research, applied research, research in the area of product/solution design and development and in selected thematic areas of national strategic importance to build indigenous capability
  - Introduction of Information Security curriculum in formal courses like M.Tech./M.E./M.S., B.Tech/B.E., Post Graduate Diploma courses, faculty training, modular/short term knowledge oriented courses etc. through academic institutions
  - Launching non-formal modular/short-term knowledge-cum-skill oriented courses etc. for working professionals at all levels including the flexible certificate programs, certification scheme through NIELIT, CDAC etc.
  - Launching formal courses on virtual mode using the NKN Network to expand the training capacities
- Training of Government Personnel
- Creation of mass information security awareness targeted towards
  - Academic Users: School level – Children, Parents & Teachers, College level – Students & Faculties
  - General Users: Small enterprise/Business users, SME Sector/Non IT industry, NGO's, CSCs, Cyber cafes and general public at large
  - Government Users: Central/State Government employees (non IT professionals), Legal / Police personnel's etc.

2. NIELIT - An Introduction

NIELIT (National Institute of Electronics And Information Technology) is an autonomous scientific society of the Department of Electronics & Information Technology, Ministry of Communications & Information Technology, Government of India with Head Quarters at New Delhi. It is envisioned to bring the most updated global industry relevant computer education, within the reach of more and more in the areas of Information, Electronics and Communication Technology (IECT). NIELIT is implementing a joint scheme of All India Council for Technical Education(AICTE) and Department of Electronics & Information Technology Government of India.

National Institute of Electronics & Information Technology (NIELIT) was set up to carry out Human Resource Development and related activities in the area of Information, Electronics & Communications Technology (IECT). NIELIT is engaged both in Formal & Non-Formal Education in the area of IECT besides development of industry oriented quality education and training programmes in the state-of-the-art areas. NIELIT has endeavored to establish standards to be the country's premier institution for Examination and Certification in the field of IECT. It is also one of the National Examination Body, which accredits institutes/organizations for conducting courses in IT in the non-formal sector.

At present, NIELIT has thirty one(34) offices located at Agartala, Aizawl, Ajmer, Aurangabad, Calicut, Chandigarh, Chennai, Chuchuyimlang, Churachandpur, Delhi, Gangtok, Gorakhpur, Guwahati, Imphal, Itanagar, Jammu, Jorhat, Kohima, Kolkata, Kokrajhar, Leh, Lucknow, Lunglei, Pasighat, Patna, Ranchi, Senapati, Shillong, Shimla, Srikakulam, Silchar, Srinagar, Tezpur, Tura with its Head quarters at New

Delhi. It is also well networked throughout India with the presence of about 900+ institutes accredited by it.

Over the last two decades, NIELIT has acquired very good expertise in IT training, through its wide repertoire of causes, ranging from 'O' Level (Foundation), 'A' Level (Advance Diploma), 'B' Level (MCA equivalent), 'C' Level (M-Tech level), IT literacy courses such as CCC (Course on Computer Concept), BCC (Basic Computer Course) and other such long term and short term course in the non formal sector like courses on Information Security, ITeS-BPO(Customer Care/Banking), Computer Hardware Maintenance (CHM-O/A level), Bio-Informatics(BI-O/A/B level), ESDM etc, besides, high end courses offered by NIELIT Centres at Post-Graduate level (M.Tech) in Electronics Design & Technology, Embedded Systems etc. which are not normally offered by Universities/Institutions in the formal sector, in association with the respective state Universities.

3.About CDAC

Centre for Development of Advanced Computing (C-DAC) is the premier R&D organization of the Department of Electronics and Information Technology (DeitY), Ministry of Communications & Information Technology (MCIT) for carrying out R&D in IT, Electronics and associated areas. Different areas of C-DAC, had originated at different times, many of which came out as a result of identification of opportunities.

- The setting up of C-DAC in 1988 itself was to built Supercomputers in context of denial of import of Supercomputers by USA. Since then C-DAC has been undertaking building of multiple generations of Supercomputer starting from PARAM with 1 GF in 1988.
- Electronic Research and Development Centre of India (ER&DCI) with various constituents starting as adjunct entities of various State Electronic Corporations, had been brought under the hold of Department of Electronics and Telecommunications (now DeitY) in around 1988. They were focusing on various aspects of applied electronics, technology and applications.

C-DAC has today emerged as a premier R&D organization in IT&E (Information Technologies and Electronics) in the country working on strengthening national technological capabilities in the context of global developments in the field and responding to change in the market need in selected foundation areas.

4. Certification Scheme in Information Security

One of the objectives of the ISEA project Phase-I was is to implement a robust certification mechanism in Information Security with technical experience and guidance from RC's (of ISEA Project) which will set the international acceptable standards with NIELIT as the implementing organization.

With the above objective in the mind, the NIELIT has launched the following certification scheme in Information security in 2009 with three levels of certification scheme as a part of Information security education and awareness project. NIELIT, Gorakhpur Centre is acting as nodal centre. However the national image of the scheme is being maintained by NIELIT, New Delhi as the implementing organization.

Now in ISEA Phase-II, the Certification Scheme in Information Security is being launched jointly by CDAC & NIELIT.

5. Course Objective

To implement a national level Certification Scheme in Information Security as part of the Information Security Education and Awareness Project of DeitY. The Course structure has been designed to conduct examination for three levels of certification i.e.

Level -1	**ISEA Certified System Security Analyst [CSSA]**
Level -2 (To be introduced later)	**ISEA Certified System Security Professional [CSSP]**
Level -3 (To be introduced later)	**ISEA Certified Computer Forensic Professional [CCFP] Or ISEA Certified Information Systems Security Auditor [CISSA] Or ISEA Certified System Security Solution Designer [CSSSD]**

6. Course Structure

Level – 1
ISEA Certified System Security Analyst

S. No.	Module Code	Module Name	Max. Marks
01.	IS-C1-01	Computer Fundamentals and Computer Network	125
02.	IS-C1-02	Operating System Administration	125
03.	IS-C1-03	Information Security Concepts	125
04.	IS-C1-04	System Security	125

7. Eligibility Criteria

- **ISEA Certified System Security Analyst (Level-1)**
  10 + 2 Any Stream with minimum 50% Marks **OR** Diploma in IT/Electronics/LCE (Final Year Students may also apply) **OR** NIELIT 'O' Level
- **ISEA Certified System Security Professional (Level-2)***
  Level 1 Passed **OR** B.Tech. (CS/IT/Electronics/Electrical Instrumentation)(Third Year Students may also apply) **OR** NIELIT 'A' Level/Any Graduate in CS/Electronics/IT with an mathematical back ground
- **ISEA Certified Computer Forensic Professional /Certified Information Systems Security Auditor /Certified System Security Solution Designer (Level - 3)**
  Level 1 and Level 2 Passed (OR) Any Graduate with Level 2 Passed (OR)B.E./B.Tech. (CS/IT/ECE) Passed with 60% Marks

  Note : NIELIT/CDAC Employees applying for the certification need to submit a letter from their employer indicating that they are in the job and given permission to appear in the certification.

8. Modes of Admission:

Admission can be taken in one of the following mode:

- **Regular Course (Classroom Mode):** Candidates will be provided Classroom Training, Hands on Lab, Course Materials etc. at NIELIT/CDAC Centres offering such training program.
- **Online Course (Self Study Mode):** Online Course mode is an option for candidates to enroll through sel**f-**study mode without attending the regular classes.

9. Rules and Regulations for Candidates Seeking Certification

i. A candidate could take regular study by taking admission at the Institute offering such training Programme at Level-1 as per eligibility criteria mentioned above.
ii. There is also an option for a candidate to enroll through Online Mode (self study mode) without attending regular course having eligibility criteria mentioned for different levels.
iii. Candidates can apply for any level at a time subjected to fulfilling eligibility criteria as mentioned at S.No. 7.
iv. A candidate may opt for any number of modules in each level as per the choice and preparation of the candidate. For this session the candidate may appear in August 2016 Examination proposed in 4th Week.
v. There is a cut-off date beyond which the registrants cannot take immediate examination. There should be a gap of minimum 25 days between date of registration and date of the examination.
vi. The candidate has to fill the Online Examination form which will be available on website http://www.isea-pmu.in. The candidate may apply examination form for any number of modules in each level as per preparation of the candidate

10. Training Centers

Training is provided for Regular Students at following Centres

NIELIT, Gorakhpur	C-DAC, Noida
NIELIT, Jammu/Srinagar	C-DAC, Mohali
NIELIT, Aurangabad	C-DAC, Trivandrum
NIELIT, Calicut	C-DAC, Kolkata
NIELIT, Agartala	C-DAC, Hyderabad
NIELIT, Chennai	C-DAC, Bangalore

11. Course Fee

Course Mode	Fee		
Regular [Class Room mode] [For ISEA CSSA(Level-1) Only]	Fee per Module		Rs. 5,000/-*
	For All Modules		Rs. 20,000/-*
* Training fee +Course Materials+ Registration Fee + Examination Fee +Including all applicable taxes			
Online Mode [For ISEA CSSA [Self Study Mode] (Level-1) Only]	S.No.	Course Code	Fee Per Module ^
	1	IS-C1-01	Rs1000.00^
	2	IS-C1-02	Rs1000.00^
	3	IS-C1-03	Rs1500.00^
	4	IS-C1-04	Rs1500.00^
^ Course Materials+ Registration Fee + Examination Fee +Including all applicable taxes			

12. Registration

Registration is a pre-requisite for appearing in the certification examination. Some important aspects of registration are:

- The registration of candidate would be achieved through ISEA website http://www.isea-pmu.in/
- Registration No is unique and will remain same for a particular level.
- Registration will be valid for a period of 2 years for a particular level after which re-registration is required.
- After completion of a particular level successfully registration is allowed for next higher level after paying the prescribed fee.

- For applicants in Online Mode, the registration is open throughout the year and valid for a specified number of consecutive examinations taking into account the cut-off date for the next immediate examination after registration. There is a cut-off date beyond which the registrants cannot take immediate examination. There should be a gap of minimum 25 days between date of registration and date of the examination.
- For More Information visit ISEA Website http://www.isea-pmu.in/

Registration Process

1. Visit "Certification Scheme in Information Security" Section on https://www.isea-pmu.in/
2. Download Course Brochure and Read the Instructions carefully.
3. Create an account at https://www.isea-pmu.in/ by entering the following details to register and complete the Registration Form.
   - Name
   - Email
   - Password
   - Gender
   - Date of Birth
   - Contact No.

   Note: Email ID (valid email ID to which a web link will be mailed to complete the registration process).This will be your username.

4. Login with the user/password created in step 3.
5. Update User Profile e.g Personal, Academic Details etc.
6. Fee Payment
   - The applicants who fulfill the admission criteria specified above should Register and Update their user profile online (https://www.isea-pmu.in/).
   - Deposit Course fee(in accordance with the number of course modules, mode of admission regular or Online etc) by using following payment Mode. The candidate must note the transaction details.
     - ✓ **NEFT/RTGS** to the respective institute where candidate desired to seek admission.
     - ✓ **CHALLAN** based fee deposit at the respective institute where candidate desired to seek admission.
     - ✓ **Demand Draft (DD)** in Favor of respective Institute.
     - ✓ **Cash/PoS** Deposit at the respective institute where candidate desired to seek admission.

   Note: To calculate the desired fee and get the bank details of respective institute, the Applicant may go to "Apply for Certificate" under dashboard and could see details by selecting one or more parameter.

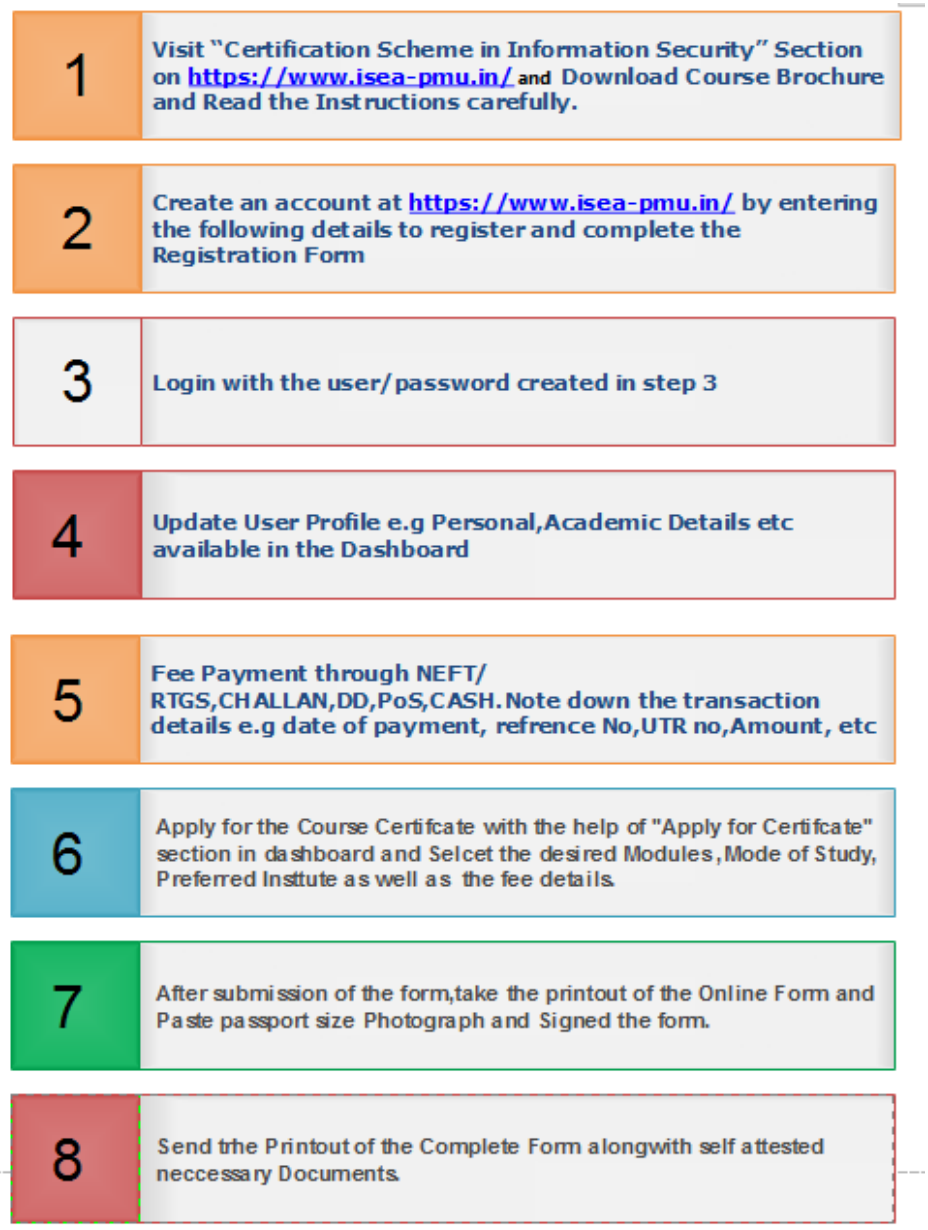
7. After payment is done through above given payment mode, click on "Apply for Certificate" in dashboard and enter the details of Module, Mode of Admission, Preferred Institute to be linked and Payment details.
8. **Submission of Application Form**

   After online submission of Application Form, Candidate need to take the printout of the application form, paste the recent passport sized photograph and signed the documents. The hard copy of application as well as supporting documents needs to be sent to the respective institute at the address mentioned in the printed application form.

   Submission of the duly signed hard copy of online application form must be sent along with following required documents
   - ✓ Proof for date of birth (Secondary Education Board [Class X or equivalent] or any certificate issued by the Government authorities)
   - ✓ Mark Sheet of 10 th and 12th (or) Equivalent examination(s)

- ✓ Mark Sheet of Graduation/Diploma in line with the eligibility criteria.
- ✓ Details and proof of fee payment in case of payment made by NEFT/RTGS, PoS or CASH deposit.

Registration Process of ISEA CSSA LEVEL-1



13. Calendar of Events for Certification

13.1 For Regular Students

Start date for submission of application form in Online	Last date for submission of Application form in Online	Commencement date of classes
04th July 2016	17th July 2016	18th July 2016

13.2 For Online Mode Students

Schedule For July, 2016 Batch of "Certification Scheme in Information Security' Level-1
Last Date for submission of Registration Form
For applicants in Online Mode, the registration is open throughout the year and valid for a specified number of consecutive examinations taking into account the cut-off date for the next immediate examination after registration. There is a cut-off date beyond which the registrants cannot take immediate examination. There should be a gap of minimum 25 days between date of registration and date of the examination.

14. Examination Pattern

The examination for Information Security Certification Scheme will be conducted on following pattern:

i. Each Centre would conduct the examination on 4th Saturday of the months of August, November, February & May in an academic year
ii. At the time of registration, the candidate would be given an option to choose the preferred centre out of all 12 CDAC/NIELIT centres. Based on the centre's preference at the time of registration, examination body would be linked
iii. The Theory/Practical examination of each paper will contain objective questions of Total 125 per Module, Out of which Theory section would carry 75 Marks and Practical Section would carry 50 Marks.
iv. To qualify for a pass in a module, a candidate must obtained at least 50% in each module examination.
v. There will be an online application form for examination and for each examination the candidate has to fill in the said form. Online Examination form will be available on website http://www.isea-pmu.in
vi. A candidate would be provided with the Grade Sheet and Participation Certificate upon successful completion of any module with at least 50% marks by respective centres.
vii. A candidate would be provided with the Grade Sheet and Professional Certificate upon successful completion of all the modules of a particular level (L1/L2/L3) with at least 50% marks by respective centre.

15. Examination Centre

Examination is proposed to be conducted at the centres all over india as given below:

JAMMU & KASHMIR	DELHI / NCR	MAHARASHTRA	KARNATAKA	UTTAR PRADESH
Jammu Srinagar	New Delhi Noida	Aurangabad	Bangalore	Lucknow Gorakhpur
Chandigarh	**Kerala**	**West Bengal**	**Tamil Nadu**	**Andhra Pradesh**
Mohali	Calicut Trivandrum	Kolkata	Chennai	Hyderabad
Tripura	**Karnataka**	**Bihar**		
Agartala	Bengaluru	Patna		

Note: NIELIT/CDAC reserves the right to change/cancel any centre mentioned above. In such case candidates who have applied for that centre will be allocated their second choice/nearest examination centre.

APPENDIX-A

ISEA CERTIFIED SYSTEM SECURITY ANALYST [LEVEL-1]

IS-C1-01: Computer Fundamentals and Computer Networks

S. No.	Topics
1.	Overview of PC architecture
2.	Different bus standards (ISA, PCI, PCMCIA)
3.	Different Add-on Cards like memory, Graphics etc.
4.	Operating system architecture
5.	Process Management
6.	Memory Management
7.	File system Management
8.	Introduction to Network OS
9.	Basics of Communication Systems
10.	Transmission Media
11.	OSI ,TCP/IP Models
12.	Local Area Networks
13.	Wide Area Networks
14.	Networking Protocols
15.	IP addressing & Routing
16.	Understanding & recognizing TCP, IP, UDP, ICMP,Ethernet Packets Internetworking Devices (Hub, Switch, Router etc.)
17.	Wireless Networks

Overview of PC Architecture

What is a Computer , How computers operate ,Types of computers , The computing environment, The Enterprise Computer Environment , Types of computers in the enterprise, Where the PC fits in the enterprise environment ,Computers and PC Hardware Architectural Components ,CPUs, Chipsets, Memory ,I/O ,Component interaction ,PC Software ,CISC versus RISC computer models ,Software ,Assembly, interpreted, and compiled software, Mother Board Components ,CPU ,Chipsets ,Interrupt and DMA controllers and how they work ,Memory ,Static and dynamic RAM and their derivations BIOS ,CMOS RAM ,I/O subsystem ,Embedded and add-in devices

Different BUS standards

Serial Interconnects and Layered Protocols ,Parallel models ,Serial models, Synchronous versus asynchronous operation , Physical Layer Function and Services , Logical Sub-Block, Expansions Slots and Add-In Cards , Bus evolution and the bus wars , ISA , EISA , MCA ,PCI, PCI-X, PCI Express ,PCMIA, Video and Monitor Types , Ports Serial and parallel , USB and FireWire , Ethernet , Mass Storage Devices , Floppy and hard drives , High and low level formatting , CDs and DVDs ,Types, speeds, and formatting

Different Add-on cards

Add-on Video Cards ,Add-on Memory Cards , Add-on Graphics Cards

Operating System Architecture

Introduction to Operating Systems, OS Internals and Architecture, Memory management, processes and threads, Files, file systems and directory structure, The Boot Process, POST, Windows boot process, Linux boot process, Basic OS Configuration

Process Management

Types of Process ,Multitasking, Input, Output & Error redirection, Managing running process, Killing Started process, Understanding the init process, Parent processes, Tools for working with processes, Process scheduling , Inter process communication, Signals, Pipes , FIFO , Queues , Semaphores ,Shared Memory

Memory Management

What is Memory Management , Abstract Model of Virtual Memory , Demand Paging Swapping , Shared Virtual Memory , Physical & Virtual addressing Modes , Access Control, Caches , Buffer Cache, Page Cache , Swap Cache , Hardware Caches , Page Tables, Page Allocation & de-allocation , Memory Mapping, Demand Paging, Page Cache , Swapping out & discarding Pages , Reducing Size of Page & buffer cache , Swapping out system shared memory pages, Swap, Cache , Swapping Pages in

File System Management

Types of file system, Comparison of file system, Virtual file System, Program used to manage file system, Making a file system, Checking a file system, File System Fragmentation, File Fragmentation, Free Space Fragmentation, Related file Fragmentation

Introduction to Network operating System

Networking OS Software, Network basics and network models, Protocols, OSI and TCP Drivers

Basics of Communication Systems

Basic Telecommunication System, Types of Communication, Transmission Impairments, Analog Versus Digital Transmission, Components, Data representation, Data Flow, Issues in Computer Networking, The Beginning of the Internet, Service and Applications, Packet Switching Concepts, Virtual Circuit, Datagram Service, Source Routing, Issues in Computer Networking

Transmission Media

Twisted Pair Cable, Coaxial Cable, Fiber Optic Cable, Unguided Media: Wireless Radio Waves, Micro Waves, Infrared

OSI Model, TCP/IP Model

OSI Model, Layered Architecture, Peer to Peer Process, Encapsulation, Layers in the OSI Model, Physical Layer, Data Link Layer, Network Layer, Transport Layer, Session Layer, Presentation Layer, Application Layer, Summary of Layers, TCP/IP Protocol Suite, Physical and Data Link Layers, Network Layer, Transport Layer

Local Area Networks

The Ethernet LAN , LAN Protocol , CSMA/CD protocol , Ethernet Addresses , Ethernet Frame Format , LAN Transmission Media , LAN Topologies , Medium Access Control Protocols in LANs, LAN Standards, LAN Bridge , Wireless LANs

Wide Area Networks

Issues in Wide area Networking, X.25 Protocol , Overview of X.25 , A Satellite-Based X.25 Networks , Addressing in X.25 Networks

Networking Protocols

Internetworking, Need for Network Layer, Internet as a datagram network, Internet as a connection less network, IPv4, Datagram , Fragmentation, Checksum, IPv6, Advantages of Packet Format, Extension Headers

IP Addressing and Routing

IPV 4 Address , Address Space, Notations, Classful Addressing, Classless Addressing, Network Address Translation (NAT), IPv6 Address, Structure, Address Space, Routing protocols, Direct Delivery, Indirect Delivery, Routing Tables and next-Hop Routing Adaptive routing, Routing within Autonomous systems, Open shortest path First (OSPF), Flooding, Routing between autonomous systems, Exterior gate way protocol, Border Gate way Protocol

Understanding and Recognizing TCP,IP UDP, ICMP, Ethernet Packets

TCP (Transmission Control Protocol), Flow Control and Acknowledgments, Stop-and-wait Protocol , Sliding Window Protocol, Congestion Control, IP (Internet Protocol), Overview of IP, Internet Addressing Scheme, Dotted Decimal notation, Address Resolution Protocol, Reverse Address resolution protocol, IP Datagram format, UDP (User Datagram Protocol), UDP Datagram format, Overview of ICMP, Overview of Ethernet Packets

Internet Working Devices

HUB, Switch and Routers

Wireless Networks

Introduction to personal Area Networks, Overview of Blue tooth, Home RF, IRDA, IEEE 802.1X

References
1. A+ Jumpstart PC Hardware and O.S. Basics by Faithe Wemben,BPB.
2. A+ Complete study Guide by Quentum Doctor.,BPB
3. CCNA study Guide by Todd Lammale,BPB
4. N+ study Guide 4th Edition David Groth,BPB

IS-C1-01: Computer Fundamentals and Computer Networks

Practical Assignments

1. To study various motherboards.
2. To study various data bus, slot and connectors.
3. To study assembling and disassembling of a PC.
4. To install Windows XP/Client operating system.
5. To study DOS commands.
6. To study CMOS setup.
7. To install hard disk drive in master slave mode.
8. To study and configure running process using task manager.
9. To configure virtual memory
10. To study file system such as FAT16, FAT32 and NTFS.
11. To install network card (Ethernet based NIC) and configuring TCP/IP.
12. To analyze various transmission media and it connectors.
13. To study different connectivity and internetworking devices such as Hub , Switch & Router.
14. To construct a Straight through and Cross over cable.
15. To connect two PC using Cross over cable.
16. To connect two or more PC using 8/16 port Hub/Switch.
17. To share files and folders and accessing it over network.
18. To study various TCP/IP troubleshooting utilities.
19. To study wireless networking using Adhoc mode.
20. To study wireless networking using infrastructure mode using Access Point.
21. To configure a PC for Internet connection.
22. To configure a Router on a multihomed PC.

IS-C1-02: Operating System Administration

S. No. Topic

WINDOWS OPERATING SYSTEM

1. Introduction to Windows Operating System
2. Installation and Configuration
3. Configuring and Troubleshooting Domain Name System
4. Maintaining Active Directory Domain Services
5. Managing User and Service Accounts
6. Implementing a Group Policy Infrastructure
7. Managing User Desktops with Group Policy
8. Installing, Configuring, and Troubleshooting the Network Policy Server Role
9. Implementing Network Access Protection
10. Implementing Remote Access
11. Optimizing File Services
12. Configuring Encryption and Advanced Auditing
13. Deploying and Maintaining Server Images
14. Implementing Update Management
15. Monitoring Windows Server 2012

LINUX OPERATING SYSTEM

16. Introduction to Linux
17. Linux Installation
18. Booting Procedures
19. Linux Commands and Shell Programming
20. System Administration
21. X Windows
22. Performance Tuning

Windows Operating System

Introduction to Windows Operating System

Windows 2012 Server, System Requirement, Architecture, Groups, Domains and Active Directory.

Installation and Configuration

Hardware Requirement, Preparation for Installation, Disk Partitioning, Dual Booting Feature, Remote Installation Server, Troubleshooting during Installation.

Configuring and Troubleshooting Domain Name System

Configuring the DNS Server Role, Configuring DNS Zones, Configuring DNS Zone Transfers, Managing and Troubleshooting DNS

Maintaining Active Directory Domain Services

Overview of AD DS, Implementing Virtualized Domain Controllers, Implementing RODCs, Administering AD DS, Managing the AD DS Database

Managing User and Service Accounts

Configuring Password Policy and User Account Lockout Settings, Configuring Managed Service Accounts

Implementing a Group Policy Infrastructure

Introducing Group Policy, Implementing and Administering GPOs, Group Policy Scope and Group Policy Processing, Troubleshooting the Application of GPOs

Managing User Desktops with Group Policy

Implementing Administrative Templates, Configuring Folder Redirection and Scripts, Configuring Group Policy Preferences, Managing Software with Group Policy

Installing, Configuring, and Troubleshooting the Network Policy Server Role

Installing and Configuring a Network Policy Server, Configuring RADIUS Clients and Servers, NPS, Authentication Methods, Monitoring and Troubleshooting a Network Policy Server

Implementing Network Access Protection

Overview of Network Access Protection, Overview of NAP Enforcement Processes, Configuring NAP, Configuring IPsec Enforcement for NAP, Monitoring and Troubleshooting NAP

Implementing Remote Access

Overview of Remote Access, Implementing Direct Access by Using the Getting Started Wizard, Implementing and Managing an Advanced Direct Access Infrastructure, Implementing VPN, Implementing Web Application Proxy

Optimizing File Services

Overview of FSRM, Using FSRM to Manage Quotas, File Screens, and Storage Reports, Implementing Classification and File Management Tasks, Overview of DFS, Configuring DFS Namespaces, Configuring and Troubleshooting DFS Replication

Configuring Encryption and Advanced Auditing

Encrypting Drives by Using Bit Locker, Encrypting Files by Using EFS, Configuring Advanced Auditing

Deploying and Maintaining Server Images

Overview of Windows Deployment Services, Managing Images, Implementing Deployment with Windows Deployment Services, Administering Windows Deployment Services

Implementing Update Management Overview of WSUS,Deploying Updates with WSUS

Monitoring Windows Server 2012

Monitoring Tools, Using Performance Monitor, Monitoring Event Logs

LINUX OPERATING SYSTEM

Introduction to Linux

Development of Linux, Various Distribution of Linux, Linux System Concepts- Directory Structure and File Structure.

Linux Installation

System Requirement, Different types of Installation- CD ROM, Network and quick Start, Different types of Linux Installation Server, Workstation and Customs, Disk Partitioning Auto and Manual, Boot Loader, Packet Selection, Network and Authentication Support.

Booting Procedures

LILO / GRUB Configuration, Server Security, Run Level, Initialization Script, Devices Initialization and their Access, Shut Down Procedures.

Linux Commands and Shell Programming

Concepts of Processes, Commonly used user Commands, vi Editor, Various Shells and Shell Programming.

System Administration

Services- Initialization and Status, Creating and Maintaining of User Account, and Group Account, Disk and Device Management, Backup Concepts, Installation and Maintenance of various Servers Apache, Squid, NFS, DHCP, NIS and Printer Server, Open LDAP, Samba Server.

Xwindows

Introduction, Installation and Configuration of XWindows, Working with X- Windows GNOME, KDE, Window Manager.

Performance Tuning

Logrotate, Backup Strategy, Study of various Services for Performance Tuning, Enhancement and Optimization.

References
1.Red Hat Linux Security and Optimization. Red Hat press.
2.Building Secure Server with Linux. O'Reilly Publishers
3.Linux Security by Hontanun. BPB Techmedia

IS-C1-02: Operating System Administration

Practical Assignments

Windows Practical List

1. Installation of WINDOWS 2012 Server.
2. Creation and administration of user and group accounts
3. Understanding files and folder permission w.r.t FAT32 and NTFS
4. Configuring Disk quotas and EFS
5. To study backup types (Normal, Copy, Incremental, Differential) and recovery.
6. Managing and Configuring file sharing, printer, network printer.
7. Installing and managing Domain Name System(DNS) server (primary and Secondary)
8. Installing and Uninstalling Active directory verifying installation and managing it.
9. Configuring Win2012 as DHCP Server (Scopes, Super scope and authorization).
10. Creating and configuring DFS roots links and configure client computer to use DFS
11. Configuring and managing Win2012 as Win Server.
12. Managing Disks/volume their creation and conversion, recovering from disk failure.
13. To study IIS and configuring its component (http, ftp) for web and ftp server.
14. To create Terminal server and terminal services clients in application server mode and remote administration mode.
15. To study Internet connection sharing (ICS)
16. To Install and configure RIS (Remote Installation Service)
17. Using the Emergency Repair Disk to restore a System.
18. To monitor Win2012 performance using system and Network Monitor.

Linux Practical List

1. To Install RHEL (Red Hat Enterprise Linux).
2. To study basic commands in Linux.
3. To study various shell interfaces in Linux.
4. To study GNOME desktop.
5. To study KDE desktop.
6. To manage RPM packages.
7. To study user and group management.
8. To study Network Configuration (IP Addressing, TCP/IP).
9. To configure and manage Telnet.
10. To configure and manage FTP (file transfer protocol).
11. To configure and manage DHCP server using dhcpd daemon.
12. To configure and manage DNS server (Domain Name System).
13. To configure and manage SQUID (proxy Server) and proxy clients.
14. To configure and manage NFS file server.
15. To configure and manage NIS (Network Information Service) server and clients.
16. To configure and manage SAMBA server.
17. To configure and manage APACHE Server (web server).
18. To configure and manage E-mail services.
19. To configure and manage a print server (CUPS).
20. To configure Linux system for using Internet.
21. To Configure Open LDAP Server

IS-C1-03: Information Security Concepts

S.No.	Topic
1	Basics of Information Security
2	Security threats and Vulnerabilities
3	Cryptography
4	Identification and Authentication
5	Network Security
6	Security Tools and Techniques
7	Internet Security
8	E-mail Security
9	Wireless Security
10	Risk Assessment and Disaster Recovery
11	Computer Forensics
12	Information Security laws

Detailed Syllabus

Basics of Information Security
Introduction to Information Security, History of Information Security, Need for computer security Confidentiality, Integrity, Availability, Authenticity, Accountability, non-repudiation, Authorization, Security threats, Intrusion, Hacking, Security mechanisms Prevention, Detection, Recovery, Anti virus, Encryption, Firewall, VPN, Access control, Smart card, Biometrics, Intrusion Detection, Policy management, Vulnerability Scanning, Physical security, Backup, Auditing, Logging ,National & International Scenario

Security threats, Vulnerabilities
Overview of Security threats, Vulnerabilities, Access Attacks Snooping, Eavesdropping Interception, Modification Attacks Changes, Insertion, Deletion, Denial-of-Service Attacks - Denial of Access to Information, Applications, Systems, Communications, Repudiation Attacks Masquerading, Denying an Event, Malicious code - Viruses, worms, Trojan horses, how they work and how to defend against them, Sniffing, back door, spoofing, brute force attack, Social Engineering, Vulnerable Configurations, Security of Hard drives, laptops & mobile devices

Cryptography
Symmetric versus asymmetric cryptography, Advantages & disadvantages of Symmetric versus asymmetric cryptography, How to mix and match both in practical scenario, Key management, Digital Signature & other application of cryptography, PKI CA, RA, Subscriber etc, PKI usage, From user side, CA/RA side etc, Type of PKI hierarchy, Single CA, trust models etc, Certificate management

Identification and Authentication
Access Control models Mandatory Access Control, Discretionary Access Control, Role based Access Control, Methods of Authentication Kerberos, CHA, Certificates, Username/Password, Tokens, Biometrics, Multi-factor, Mutual

Network Security
Network Infrastructure Security Workstation, Server, Router, Switch, Modem, Mobile devices, Firewalls and packet filtering, Proxy or application level gateways security devices, VPN, Intrusion detection System , Electronic payment System Introduction to IPSec, PPTP,L2TP

Security Tools and Technologies
Network scanners, Vulnerability scanners, OS fingerprinting: nmap, nessus, MBSA, SAINT, John the Ripper, Forensic tools, Others.

Internet Security
Recognize and understand the following Internet security concepts ,Customizing Browser Security Settings, Vulnerabilities Cookies, Java Script, ActiveX, Applets, Buffer overflows, Anonymous surfing, Phishing, HTTP/S, SSL/TLS and Certificates Internet use - best practices

E-mail Security
POP3 vs Web-based e-mail, Encrypting and signing messages, S/MIME, PGP, Vulnerabilities Spam, E-mail hoaxes , Email use - best practices

Wireless Security
Wired/Wireless networks, Ad-hoc network and sensor networks, WTSL, 802.11 and 802.11x, WEP/WAP(Wired Equivalent Privacy /Wireless Access Protocol), Vulnerabilities , Site Surveys, DOS and DDOS attack**s**

Risk Assessment and Disaster Recovery
Asset classification, Information classification, Organization level strategy, Process level strategy, Risk assessment methods, Risk classification, Business continuity plan , Business impact analysis, Event logs, Security Auditing , Disaster Recovery Plan , Backup, Secure Recovery- Alternate sites, Security Policies & Procedures

Computer Forensics
Nature and types of cyber crime- Industrial espionage, cyber terrorism, Principles of criminal law, Computer forensic investigation Digital evidence, Forensic analysis

Information Security laws
IT-Act, The rights the various parties have with respect to creating, modifying, using, distributing, storing and copying digital data. Concurrent responsibilities and potential liabilities, Intellectual property issues connected with use and management of digital data

Recommended Books

Main reading

1. Network Security Bible Eric cole and Ronald L KrutzWile dreamtech India Pvt Ltd, New Delhi
2. Fundamentals of Network Security by Eric Maiwald , Dreamtech Press
3. Absolute Beginner's Guide To: Security, Spam, Spyware & Viruses By Andy Walker, Publisher: Que
4. Computer Security Basics, 2nd Edition By Rick Lehtinen, Publisher: O'Reilly

Supplementary Reading

1. Network Security Essentials: Applications and standards Stallings, Pearson Education Pvt. Ltd, Delhi
2. Computer viruses, Computer Security, A Global challenge by Cohen Elsevier Press

IS-C1-03: Information Security Concepts

PRACTICAL ASSIGNMENT

1. Practical on Packet Sniffing tool Ethereal.
2. Practical on Discovery and scanning techniques (who is domain search query, ping, nslookup, traceroute, visual traceroute, DNS query).
3. Configuring IPSec on Windows.
4. Configuring Kerberos
5. Configuring SSH
6. Configuring SSL
7. Practical on password cracking tools john crack, Lophtcrack.
8. Practical on Denial of Service, IP spoofing.
9. Practical on network vulnerabilities assessment tools like jakal, NetRecon, NMAP.
10. Managing web and certificate services.
11. Installation and configuration of wireless NIC.
12. Installation and configuration of Access Point.
13. Setup of WLAN using infrastructural mode.
14. Security Implementation in WLAN.
15. Configuration of Access point as a Bridge.
16. Point to Point and Point to Multipoint configuration.
17. Detecting wireless Network activity and security lack using Netstumbler.
18. Implementing WEP.
19. Using Access point as a DHCP server.

IS-C1-04: System Security

Outline of the Syllabus

Sr.no	Topic
01.	Design of Secure Operating System
02.	Design of Trusted Operating System
03.	Operating System Hardening
04.	Operating System Controls
05.	Internet Protocols and Security
06.	Application Security
07.	WWW Security
08.	HTTPS (Secure HTTP)
09.	SMIME (Secure Multipurpose Internet Mail Extension)
10.	PGP
11.	SET (Secure Electronic Transaction)
12.	E-mail security and Instant Message Security
13.	Access Control
14.	Internet Security Protocols
15.	Managing Personal Firewall and Antivirus
16.	Remote Access Security
17.	Secure Configuration of Web Server
18.	Secure Configuration of Database Server
19.	Secure Configuration of Email Server

Detailed Syllabus

Design of Secure Operating System
Introduction of a Secured System, Drawbacks of Existing Operating System (Bugs, Fault Isolation, Huge size Kernel Program etc.), Patching Legacy Operating System, Paravirtual Machines Concept, Future System

Design of Trusted Operating System
Introduction, Security Assurance Evaluation, Need for Trusted Operating System Features of Trusted OSs

Operating System Hardening
Function of Operating system , Types of OS (Real time OS, Single User Single task OS, Single User-Multi tasking System, Multiuser System), Task of OS , Process Management, Memory Management, Device Management, Storage Management, Application Interface, User Interface, Security Weakness, Operating System, Windows Weakness, LINUX Weakness, Hardening OS during Installation, Secure User Account Policy, Strong User Password Policy, Creating list of Services and Programs running on Server, Patching Software, Hardening Windows, Selecting File System, Active Directory / Kerberos, General Installation Rules, Hardening Linux, Choose the correct installation procedure , different installation tools, Partitions and Security, Network Services, Boot Loaders, Reverse Engineering

Operating System Controls
Introduction - How the Computer System Works, Purpose of an Operating System Types of Operating System, Wake up Call, Power on Self Test, BIOS, Boot Loader Task of an Operating System

Internet Protocols and Security
Introduction of Internet Protocols, IPSec Operation, IPSec Implementation, IPV4 Network Versus IPV6 Network, Problems with IPSec

Application Security
Hacking WEB Applications, How are the WEB applications attacked, Input Validation attack, Full Knowledge Analysis

WWW Security
Web Security Considerations, Hacking Web Platforms, Web Platform Security Best Practices, Web Authentication threats, Bypassing Web Authentication, (Token Relay, Identity Management, Client-Side Piggybacking), Attacking Web Authorization

HTTPS (Secure HTTP)
Introduction, Overview of HTTPS

SMIME (Secure Multipurpose Internet Mail Extension)
Introduction, Functionality, Digital Signature, Message Encryption, Triple-Wrapped Messages, S/MIME Certificates, Usage of S/MIME in various e-mail software, Obstacle of Deploying S/MIME, CAVEATS

PGP
Introduction, Use of PGP, Encryption and Decryption in PGP, PGP Services, Message, Key Management

SET (Secure Electronic Transaction)
Introduction of SET, SET Technology, Symmetric and Asymmetric encryption in SET, Transaction Authenticity, Importance of secure transactions

E-mail security and Instant Message Security
Introduction, E-mail Attack, Use of Digital Certificate to prevent attack, Introduction to IM Security, Best Practices for IM security

Access Control
Access Control Basics, Access Control Technique, Access Control Administration, Centralized Access Control, Decentralized Access Control, Accountability, Access Control Models, Identification and Authentication Methods, Biometric Authentication

Internet Security Protocols
IP Security Architecture, Authentication Header, Encapsulating Security Payload Combining Security Associations, Key Management

Managing Personal Firewall and Antivirus
Managing Logs, Upgrades, SNMP, Internet Service Provider Issues, Defense in Depth

Remote Access Security
Business Requirement of Remote Access, Remote Access Technologies, VPN, Extranet and Intranet Solution, Use of VPN for Remote Access Security, IPSec, Point to Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), SSL Authenticated access of files through SAMBA for different OS, Overview of RAS Server for Small Enterprise Application, Overview of Remote Access through ISP, Remote Administration

Secure Configuration of Web Server
Protecting Directories and Files against Profiling, IIS Hardening, Apache Hardening, Analyzing Security Logs, Web Authorization / Session Token Security, IE Security Zones, Low Privilege Browsing, Server Side countermeasure

Secure Configuration of Database Server
Access control policy, Protecting Read Only Accounts, Protecting high risk stored procedures and extended functionality, Patch updates

Secure Configuration of Email Server
Vulnerabilities of Mail Server, Improving the Security through appropriate planning Security Management Practices and Controls, Secured OS and Secured Application Installation, Improving the Security through Secured Network Infrastructures

References
1. Network Security Bible, Cole, WILEY
2. Designing Security Architecture Solutions, Ramachandran, WILEY
3. Network Security Essentials: Applications and Standards,William Stallings.
4. Hacking Web Applications Exposed, TATA McGraw-HILL By Joel Scambray, MikeShema, Caleb Sima

IS-C1-04: System Security

PRACTICAL ASSIGNMENTS

1. Practical on OS finger printing using NMAP.
2. Practical on operating system Hardening tool Bastille.
3. Practical on secure E-mail PGP.
4. Secure Configuration of web server like APACHE,IIS.
5. To study viruses, worms, trozen horses and viruses protection, detection and recovery.
6. Installation and secure configuration of E-mail server like send mail, Microsoft Exchange server.
7. Practical on useful utility for Security Administrator like Netcat, TCPdump, LSOf, Ngrep.
8. Practical on monitoring system processes.
9. Practical on Access control in Linux.
10. Practical on Access control in Windows.
11. Practical on SHTTP, SMIME and SET (Secure Electronic Transaction).
12. Installation and Secure configuration of Database Server Oracle /MYSQL/Postgres.
13. Configuring a Personal Firewall like Zone Alarm.
14. To study CISCO Router and its interface.
15. To bring up a Router first time logging in to a router, basic commands saving NVRAM configuration.
16. To configure a Router for different LAN segments.
17. To study IP Routing by creating static Routes.
18. To study IP routing by using RIP (Routing Information Protocol).
19. To study IP Routing by using IGRP (Interior Gateway Routing Protocol).
20. To study IP Routing by using EGRP (Enhanced IGRP).
21. To study IP Routing by using OSPF (Open Shortest Path first).
22. To study VLANS and Routing between VLANS.
23. To study Inter-VLAN Routing.
24. To backup Router IOS (Internetworking Operating System).
25. To upgrade or restore Router IOS.
26. To perform password recovery in Router.
27. To backup Router configuration and restoring it.
28. Using Telnet for configuring Router.
29. Configuring a Firewall. (Linux/Windows).
30. Configuring and securing VPN (Virtual Private Network).
31. Practical on Intrusion Detection System using Snort/Tripwire.
32. Practical on Firewall Testing using NMAP.
33. Practical on NAT (Network Address Translation).
34. Configuring a Proxy Server.(Linux/Windows).
35. Practical on Network vulnerabilities, assessment tools like Jakal, NetRecon, NMAP.