Python & Java programming are also being taught as per discussions with CDAC Hyderabad & DSCI

Module 1: System Fundamentals

- Operating Systems Concepts:
  - Architecture of Operating Systems
    - Introduction to operating systems and terminologies
    - A typical monolithic-architecture of operating systems
    - Kernel Components and Non-kernel Components
    - User-space vs Kernel-space
    - User-mode vs Kernel- mode
    - Interrupt Management
    - H/W Interrupts/ handler
  - Process Management
    - H/W Clocks and Timers vs S/W Clocks and Timers
    - Process management
    - Process Scheduling
    - CPU Scheduling
    - Preemptive vs Non-Preemptive
    - Different types of Scheduling policies
    - Algorithm-FCFS,RR,PRIO,FAIR-SHARE,EDF
  - Memory Management
    - Virtual Memory Techniques
    - Page Replacement Algorithm
    - H/W Technologies available for memory management
    - Segmentation/ Paging
  - File System Management
    - File System Organization
    - Physical File System organization Techniques FAT/NTFS file system manager in the kernel
    - Disk-cache Management
- Introduction to Network topology, Open System, Interconnection mode- Working,
  - Working of Hub, bridge, switch, router collision, UTM
  - Working on Switch, Router remote administration of switch and routers in simulators
  - Overview of transmission media
  - UTP/STP/Coaxial/Fiber-spec./advantages and disadvantage
  - OSI layers
  - TCP/IP models
  - Functions/ protocols & devices at each layer
  - Overview of LAN
  - Ethernet
  - Gigabit Lan
  - Fiber Enabled Networking
  - Working with LAN, VLAN, Virtual Trunk Protocol, DTP, 802.1q in simulators
  - Subnetting
  - NAT
  - Working with Number systems, Fixed Length subnet masking, Variable Length subnet masking, Classless Inter Domain Routing, NAT, introduction to PAT

    - Static routing
    - Dynamic routing
    - Working on Inter VLAN routing, Static Routing, RIP, RIPv2, OSPF, EIGRP, IGRP using IPv4, Static Routing in Ipv6
- Protocols and mechanism,
    - Protocols & standards
    - Overview of WAN
    - Networking protocols
    - Protocol headers for frame, TCP, UDP, IP ,RTMP
- Know your operating systems: Windows & Linux, Configuring services, Active Directory, service security, Network configuration.
- **Windows Operating system :**
    - Overview of windows operating system
    - Overview of Administrative Tasks and Tools
    - Installation of windows operating system
    - Network Configuring
        - Designing a Windows network
        - Implementing the TCP/IP protocol
        - Configuring Sites
    - Implementation of infrastructure of windows networks
        - File system and disk management
        - Implementation, planning and maintaining of active directory infrastructure
        - Configuration of IIS SQL server, web server and Exchange server
        - Configuring Services
    - Implementing and administering Active Directory
        - User accounts and groups in an Active Directory Domain
        - Installing a domain name server (DNS)
        - Implementing and administering Active Directory
        - Integrating DNS and Active Directory
        - Administering group policy
        - Managing Active Directory performance
        - Implementing WINS and Dynamic Host
    - System Center Configuration management
    - System Center Endpoint Protection
    - Configuration Protocol (DHCP)
    - Deploying Windows 7/8 using WDS
    - Managing disks with Distributed File System (DFS)
    - Introduction to Microsoft Windows 7 & 8 security
        - Security issues at the Active Directory level
        - Authenticating users and clients
    - Planning the administrative structure for security groups
    - Using smart cards for network authentication
    - Securing file systems with EFS encryption
    - Evaluating and analyzing workstation security
    - Securing Windows services
    - Windows Hyper V

        - Windows Management On Virtual Infrastructure
- **LINUX Operating System**
    - Systems Concepts
    - Directory Structure
    - Working with the basic commands in Linux, Directory Structure
    - Installation of Linux
        - The interactive Anaconda installer
        - A hands-free method of installation
        - Understanding the boot procedure
        - Configuring the GRUB boot loader
        - The Initial RAM Disk
    - Understanding run levels
    - Repository & Package Management(RPM & DEB)
    - Shutdown and Installation concepts
    - Kick Start Configuration & Customization
    - User administration
    - Network address Ipv4/Ipv6
    - Using OpenSSH for network communications
    - NIS Configuration and FTP services
    - Disk management, System, print services
    - Services Management
    - System Configuration Files
    - Configuring NFS
    - The Samba Server: networking with Windows system
    - Configuring a Failover DHCP server
    - Configuring a Failover DNS server
    - Configuring the Apache web server
    - Apache security & Virtual Hosting
    - Configuring the Squid web proxy cache
    - Understanding e-mail delivery
    - Postfix Mail Server
    - Dovecot: an IMAP and POP server
    - Network Authentication: RPC, NIS and Kerberos
    - Apache Clustering
    - Load Balancer
    - Virtual Machine management
    - Virtual machine Network Configuration

Module 2: Introduction to cyber security

- Fundamentals of information security - CIA Triad
    - Understanding the core CS principles and the associated impact on Security
- Cyber Security Controls
    - Logical Controls
    - Physical Controls
    - Tools & Techniques

- Understanding threats, attacks categories, hacking process
    - Vulnerability, Threat & Risk (with examples)
    - Types of Attacks (with examples)
    - Threats to Network, Web, Storage & Devices
- Understanding the network security,
    - Network Layer protocol
    - Dynamics of Network Security-end to end attacks
    - Mitigation Techniques
- basics of cryptography
    - Fundamentals of cryptography-encryption, decryption, keys
    - Basic Algorithms-AES, RSA, DES and others
    - PKI
- fundamental of web/mobile application security,
    - Web Application Attacks(SQL Injection, Cross site scripting etc.)
    - Mobile Application Attacks
    - Secured Software Development
- data centre security, cloud computing and data security
    - Cloud Deployment Models and Security concerns
    - Best Practices for secure data storage
    - Data Loss Prevention
    - Disaster Recovery
    - Incident Response

Module 3: Cryptography

- Introduction to cryptography
    - Introduction to Cryptography
    - Basic Encryption Concepts
    - File Encryption
    - Encryption folders(Graphical/ using cipher)
    - Data recovery agent

- Symmetric-Asymmetric cryptography & cryptographic algorithms
    - Cryptographic fundamentals
    - Private key encryption
    - Public key encryption
    - Cryptographic algorithm and protocols
    - Protocols (history, usage, key generation, ciphering message)
    - Symmetric key encryption algorithm
    - DES/3DES
    - IDEA,RC5
    - AES
    - Public key algorithm
    - Diffie-Hellman exponential key exchange

    - RSA
    - ELgamal

- Hash functions
    - MD5-message digest algorithm
    - SHA-1 Secure Hash algorithm
    - HMAC
    - Secure Email Implementation
    - gpg
    - Compression
    - Algorithm for gpg
    - S/MIME
- Applications of cryptography- IPsec
    - Attacks against encryption
    - Cryptographic issues
    - Strong authentication
    - Sign on solutions
    - Kerberos
    - Policies
    - SSL
    - TLS
    - Public Key Infrastructure Setup using openca
    - PKI Standards and Management
    - X.500
    - X.509
    - ETF
    - IRTF
    - Secure Key Generation and distribution
    - PKI Fundamentals
    - CA
    - Enrollment
    - Revocation
    - Certificate templates
    - SA
    - AH
    - ESP
    - SASL
    - SAML
- Pretty Good Privacy
- Secure Socket Layer (SSL)
    - TLS Understanding digital certificates and signatures.

Module 4: Network Security and countermeasures

Introduction to network security – topology, Network configuration, understanding ports, protocols -TCP/IP, UDP, ARP, Operational processes, Network scanning, understanding packets and network specific attacks, vulnerabilities, DMZ, Packet filtering, firewalls, Iptables, TMG threat management gateway, network security tools (scanners, sniffers etc) and countermeasures

- Introduction to Information Security
- Why Information Security?
- Security: The money factor involved
- Internet Statistics - Study from a security perspective
- Vulnerability, Threat and Risk
- Risk Management, Exposure and Countermeasure
- Firewall
- De-militarized Zone
- Two methods of implementing firewall
- Packet Filtering
- Screened Host Firewall
- Stateful Inspection Firewall
- NextGen Firewall app controls
- iptables - Linux Firewall
- Automating iptables and scripting
- Wireshark
- Create a filters for data collection and display
- Examine real-world packet captures
- Linux Software Firewall(ClearOS Pfsense)
- Nginx & Squid Reverse Proxy
- UTM
- Server Load Balancing
- VPN – Introduction
- VPN protocols/characteristics
- VPN Functions
- Types of VPN
- SecureVPN
- Trusted VPN
- Introduction to IDS and IPS
- IDS / IPS
    - Types of Attacks
- IDS
- Security Events
- Vulnerability/design/implementation
- Attacks-traditional/distributed
- Intruder types
- Types of IDS
- IPS categories
- Defence in depth
- IDS and IPS analysis scheme

- Detection methodologies
- Principles of IDS
- Introduction Of Log Analyser
- Log
- SIEM Log Correlation and event triggering
- Introduction Of SIEM
- SIEM Log Forwarding Configuration
- SIEM Log Correlation and event triggering

Module 5: Web Server and Application Security

Client-Server Relationship, Vulnerabilities in web server and applications, Attack methods- Buffer overflow, SQl injection, cross site scripting, session hijack etc. , Secure Coding Practices, OWASP top 10 vulnerabilities and mitigation techniques, Web Application vulnerability scanning tools (Nesus), Web application security challenges.

- Web Application Security Risks
- Identifying the Application Security Risks
- Identify all risks and vulnerabilities of web applications using tools
- Data Extraction
- Advanced Identification/Exploitation
- Find vulnerability of data extraction/exploitation of a web application.
- Other HTTP fields
- Injection in stored procedures
- Find vulnerabilities of HTTP Methods (1.0 & 1.1).
- Analyse web application with the help of Wireshark.
- Threat Risk Modelling
- OWASP Top 10
- Denial of Service
- Injection and Inclusion
- Give SQL queries to bypass authentication.
- Try DOS attack to denial a service of any server.
- Buffer Overflows and Input Validation
- Cross site scripting
- Access control
- Make your own cross site script and apply in any web application.
- Case Study On Web Application Framework
- Use browser-jsguard firefox addon also to detect Malicious and Suspicious Webpages.
- Port Scanning, Network Scanning and Vulnerability Scanning
- Understand various Scanning Methodologies
- SYN, Stealth, XMAS, NULL, IDLE and FIN Scans
- Use NMAP,WHOIS,Shadon, for Reconnissance.
- Host and Port Discovery (using NMAP) etc.

- Use Nessus also to find Vulnerability.
- Security challenges

Module 6: Security Auditing

- Audit planning (scope, pre-audit planning, data gathering, audit risk)
    - Audit Scope
    - Audit Classification
    - Pre audit planning
    - Data gathering Audit Risk
    - Types of audit Risk

- Risk management
    - Overall Audit Risk
    - Risk based approach
    - Evidence
    - Evidence gathering techniques
    - Sampling
    - Control Self-Assessment

- Risk analysis
    - Purpose of risk analysis
    - Risk based auditing
    - Types of Control
    - Risk Assessment using SimpleRisk or Eramba (Open source Tools)

- 3 phase approach – Risk assessment
    - IT/IS Audit
    - Introduction of Audit Audit Planning
    - Risk management
    - Risk Analysis
    - 3 phase approach-Risk assessment, mitigation, reassessment

- mitigation and reassessment
- Log analysis
    - Log Parser
    - Windows Auditing
    - Using Microsoft Security Assessment Tool
    - Using Microsoft Security Baseline Analyzer
    - Configuring Windows File system auditing.
    - Using Sysinternal Toolkit - Process Monitor, Process Explorer, Autoruns etc.

- OS auditing: Windows auditing

- Event ID Log Analysis
- OS and Application specific auditing
- Windows auditing
- Linux Auditing
- Vulnerability Assessment using Nessus
- Performing Risk Assessment based on ISO27001 using ISO27001 security toolkit
- Preparing Audit Questionnaire and Performing Audit for ISO27001 Standard.

- Linux auditing and Device auditing.
  - Linux Auditing
  - IT/IS Audit
  - Configuring Linux File system auditing using auditd.
  - Using Linux Commands for auditing - top, ps, find, who, netstat etc.
  - Using Lynis to perform Linux auditing

Module 7: Cyber Forensics

- Cyber Forensics phases (Preservation, Identification, Extraction, Documentation Interpretation)
  - Overview - Computer Forensics
  - What is Computer Forensics?
  - Difference – Computer Crime & Un-authorized activities.
  - Process of Computer Forensics (six)
  - Need for forensics investigator
  - Computer Forensics Involves
  - Preservation
  - Identification
  - Extraction
  - Documentation
  - Interpretation
  - Goals of Forensics Analysis
  - Cyber forensics Procedures
  - Preparation
  - What to do before the incident
  - Incident response plan
  - Incident response team
  - Detecting Incidents
  - Incident Detecting
  - Chain of custody

- EDR
  - Evidence Checkout Log
  - Handling Evidence
  - First Response

    - Formulate/Execute Response Strategy
    - Forensic duplication
    - Authenticate the Evidence
    - Investigation
    - Common Mistakes
    - Detection

- tools and standard operating procedures for Disk forensics
    - The Initial Assessment
    - Incident Notification Checklist
    - Hexadecimal notation
    - Practical Bits
    - Slight diversion
    - What is use of Hexadecimal
    - Encoding And Encryption
    - The Hex Editor
    - Files
    - Hashing
    - Hashing DLs
    - MD5 Hash collisions
    - Hash Collisions
    - Bit Rot
    - Standard Operating Procedures
    - Digital Forensics Laboratory

- Social media and network forensics
    - Forensics Implications
    - Accreditation Standards
    - Performing a Cyber Forensics Investigation
    - Privacy and Cyber Forensics

- Mobile and CDR forensics.
    - Demo and lab sessions on Cyber Check Suit