**Specialised Programme on Cyber Security & Forensics**

**Course Content**

**NETWORK MANAGEMENT**

**Computer Network Fundamentals**

* Introduction to Network
* Types of Networks
* OSI Reference Model
* TCP/IP Model
* Application Layer Protocol
* Transport Layer Protocol
* Network Layer Protocol
* Data Link Layer Protocol
* Network Topology
* Ethernet Cabling

**IPv4 Protocol**

* IPv4 Header
* IPv4 Addressing
* Subnetting
* CIDR
* VLSM

**Router Configuration and Security**

* Router Modes
* Setting the Router’s Password
* IP Routing
* Configuring Static Routing
* Configuring Default Route
* Dynamic Routing
* Configuring Dynamic Routing Protocol
* RIP
* RIPv2
* EIGRP
* OSPF

**Switch Configuration and Security**

* Setting and Breaking the Switch’s Password
* Configuring Port Security
* Configuring VLAN and Inter-VLAN
* Configuring VTP
* Configuring STP

**Computer Network Security**

* Introduction to Access Control List (ACL)
* Configuring ACLs
* Standard ACLs
* Extended ACLs

**Network Address Translation**

* Introduction to NAT
* Configuring NAT
* Static NAT
* Dynamic NAT
* PAT

**Wireless LAN**

* Wireless standard
* Wireless topologies
* Wireless Protocol
* Configuring Wireless Access Point

**Wide Area Network**

* Fundamentals of WAN Protocols
* Introduction and configuration of PPP
* Introduction to Frame Relay
* Introduction to ISDN

**IPv6 Protocol**

* IPv6 Header
* IPv6 Addressing
* Configuring Static Routing with IPv6
* Configuring RIPng
* Configuring EIGRPv6
* Configuring OSPFv3

**SERVER ADMINISTRATION**

###### Windows Administration

**Introducing Windows Server**

* Windows Server Editions
* Key benefits of Windows Server, Virtualization and Security
* New Features of Windows Server
* Server Manager, Server Core, Windows Deployment Services
* Installing and Configuring Windows Server
* Hardware requirements, Activating Windows
* Windows Deployment Methods & Installing Deployment Services
* WDS requirements, Install WDS, Creating Standard Server image, Configuring Windows Deployment services etc.

**Using Windows Server Roles and Features**

* Adding and Removing Roles and Features
* Remote management

**Monitoring and Maintaining Network Infrastructure Servers**

* Internet Protocol
* Dynamic Host Configuration Protocol
* Overview, Scopes, ports used by DHCP, options, DHCP management
* Domain Name System
* Names, Zones, WINS, resolving name to ip & vice versa, Transferring Zone & other features

**Monitoring and Maintaining Active Directory**

* Installing and Removing Active Directory Roles
* Active Directory Rights and Permissions
* Active Directory Users and Group Management
* Group Policy
* Active Directory Backup and Recovery
* Configuring Trust Relationship
* Configuring Forest and Domain

**Monitoring and Maintain File Servers**

* File Servers
* File server resource manager, shares, permissions, disk Quota
* Distributed File System

**Planning Windows Server Security**

* Encrypting File System
* Disk level security with BitLocker,configuring the partition, Encrypting files & folders
* Auditing for Server Security
* Auditing detailed active directory events, enabling object access
* Configuring Windows Firewall

 **Internet Information Services**

* Adding Role of IIS, configuring multiple sites, configuring multiple ftp sites etc.

**Managing Windows Registry**

* Registry hives, data type in registry, backup of registry, enabling & disabling options

**Configuring and Managing Backup**

###### Linux Administration

# Red Hat Linux Essentials

* Overview

Linux ideas & History, Linux Origins & Principles

* Command Line File system Browsing

Editing Files, Getting Help, File Hierarchy Concepts, Important Directories & browsing the file system

* The bash Shell

Scripting Basics, sample shell script, Exploring Bash shell, Bash Shell Scripting

* Users, Groups, and Permissions

Concepts of user & group accounts, Linux file security, permission

Precedence, permission types, changing file ownership, changing Permission, redirecting output to a file, Combining Output & Errors

* vi and vim Editor Basics

 Modifying file in insert mode, saving & exiting file

* The Linux File system

Tools for Extracting Text, Viewing file contents, extracting text by

Keyword from files, extracting text by column from files, tools for

Analyzing text, gathering text statistics, sorting text, eliminating

Duplicate lines, comparing files, spell checking

* Introduction to String Processing

String Processing with Regular Expressions

* Introduction to Processes

 Investigating & Managing Processes, Listing Process, Finding Process, sending signals to process, Crontab

#  Red Hat Enterprise Linux System Administration

* Installation
* System Initialization and Services

 Boot sequence, boot loader components, starting boot process, Kernel Services, init initialization, run levels, Configuration

* File system Management

Device recognition, disk partitioning, managing partitions, making file

System, file system labels, Mount points, creating logical volumes, Resizing logical volumes

* Network Configuration

Static Network interface configuration

* RPM

Package manager, installing, removing, updating software, rpm, Queries, using yum, configuring repositories

* Troubleshooting

Order of the boot process, file system corruption, recovery run levels, rescue environment

# Red Hat Linux Networking and Security Administration

* Introduction to System Services
* Organizing Networked Systems
* Network File Sharing Services
* Securing Networks
* Securing Services
* IP table configuration

**Configuration and Management of Servers**

* Web Server

Apache configuration, Virtual Hosting

* Mail Server

Dovecot configuration, Postfix configuration

* File Transfer protocol(FTP)

File sharing, authentication, FTP port options

* Domain Name Server(DNS)
* Samba Server

Authentication & authorization of users, file & printer sharing,browsing etc.

* Network File System (NFS )

Exported directory, mounting directory, permanent mounting NFS file system

* Proxy Server

Squid configuration, restricting IP, websites, MAC etc.

**Cryptography and PKI**

* Cryptography basics

History of Cryptography

Terminology

Concepts of Confusion and Diffusion

* Requirements for cryptography
* Different types of ciphers

Symmetric –Classic and Modern

Asymmetric

* Caesar Cipher

Concept

Algorithm (Encryption and Decryption)

 Examples and their solutions

Exercises

* Hill Cipher

Concept

Algorithm (Encryption and Decryption)

 Examples and their solutions

 Exercises

* Vernam Cipher

 Concept

Algorithm (Encryption and Decryption)

 Examples and their solutions

 Exercises

* DES

Concept

Algorithm (Encryption and Decryption)

 Examples and their solutions

 Exercises

* RSA

Concept

Algorithm (Encryption and Decryption)

Examples and their solutions

 Exercises

* Applications of Cryptography

Digital Signatures & PKI

What is PKI

What is Digital Signatures

Demonstration for generating Digital Signatures

Email Security

 Digital Certificates

* Authentication functions-Message authentication codes

MAC

 Concept

 Algorithm

HMAC

 Concept

 Algorithm

* Hash Algorithms (MD5, Secure Hash Algorithm)

Concept

Algorithm

Uses of Hashing

* Authentication Protocols

**CYBER SECURITY**

**Application Security**

**MySQL**

* Introduction to MySQL
* Installing and Configuring MySQL
* Queries in MySQL Database Security Principles
* Authentication Bypass
* Data Extraction
* Advanced Identification/Exploitation
* Order by/group by
* Encoding/decoding Injection in Insert/Update
* Other HTTP fields
* Injection in stored procedures

**Web Application Security**

* Web application Security Risks
* Identifying the Application Security Risks
* Threat Risk Modeling
* OWASP Top 10 Concepts

**Python**

* Introduction to Python
* Python basics
* Data Types and variables Operators
* Looping & Control Structure List
* Modules Dictionaries
* String Regular Expressions
* Functions and Functional Programming
* Object Oriented Linux Scripting Environment
* Classes, Objects and OOPS concepts
* File and Directory Access Permissions and Controls Socket
* Libraries and Functionality  Programming, Servers and Clients Web Servers and Client scripting
* Exploit Development techniques
* Writing plugins in Python
* Exploit analysis Automation Process
* Debugging basics
* Task Automation with Python

**Ethical Hacking**

* Basics of Information System
* Classification of Threads and attacks
* Protecting Information System Security
* Cyber Laws
* Security in mobile and Wireless Computing
* Security Policy
* Standards
* Social engineering
* Information Security risk analysis
* Data Privacy Fundamentals
* Penetration Testing fundamentals
* Foot printing and scanning
* Enumeration and Step-by-Step vulnerability finding
* Linux and Automated Security Assessment Tools
* Trojans and Backdoors, Viruses and worms, Sniffers, session Hijacking and Denial of Service, System Hacking, Web Server Hacking, Web application Vulnerabilities, Honey pots, Google dorks, Phishing

**CYBER FORENSICS**

* Introduction to Cyber Forensics
* Definitions
* Principles of Cyber Forensics
* Usage of Cyber Forensics
* Purpose of Forensics
* Types of Electronic Stored Information
* Location of Electronically Stored Evidence
* Evidence Collection
* Order of Volatility
* Hard Drive Basics

 **Disk Forensics**

* Acquiring the hard disk, usb or other devices
* Analysis of the hard disk and other external devices
* Registry Analysis
* Tools and Case Study

 **Live Forensics**

* Key Forensic Acquisition/Analysis Concepts
* Volatile Evidence Gathering and Analysis
* Live Response
* Forensic Evidence Acquisition and Imaging
* Tools and Case Study

**Network Forensics**

* Wireshark
* Log analysis
* Email Tracing
* Tools and Case Study

**Mobile Forensics**

* Accessing Mobile Devices
* Acquiring mobile devices
* Processing of SIM Cards
* Forensic Examination of Data
* Tools and Case Study

**Utilities**

* Recovery of passwords from documents
* Steganography
* Recovery of Data from Browser

**PROJECT WORK**