Specialised Programme on Reducing Cyber Crime through Knowledge Exchange and Capacity Building (6 Weeks)

Objective:

- To understand the network concepts, terminology and its security
- To understand about various types of threats, vulnerabilities, risks and it's exploitation
- To prevent attacks and other threats in a network or internetwork and applying various countermeasures
- To enable participants to understand and investigate various types of cyber crimes
- To enable participants to understand the Mobile Android Operating systems, web application terminology and its Security.

Course Contents:

Introduction to Cyber Crime

- Definition
- Types of Cyber Crime
- Impact of Cyber Crime

Computer Network Fundamentals

- Networking Basics
- OSI Model and Protocols
- TCP and UDP Header

IP Protocol

- IPv4 Header and Address
- IPv4 Subnetting
- CIDR
- VLSM
- IPv6 Header and Address

Router Configuration and Security

- Router Modes
- Setting and Breaking the Router's Password
- IP Routing

- Configuring Dynamic Routing Protocol and Authentication (EIGRP and OSPF)

Switch Configuration and Security

- Setting and Breaking the Switch's Password
- Configuring Port Security
- Configuring VLAN and Inter-VLAN

Computer Network Security

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

Understanding and Securing Windows Server Computers

- Infrastructure and ADS
- User Authentication and Group
- Resource Security
- Encrypting File System
- Windows Firewall
- Virtual Private Network

Understanding and Securing Linux Computers

- Linux Operating System
- Linux Administration
- Linux Network Files, Network Commands
- LUKS Disk Encryption
- GNU Privacy Guard(GPG)
- Firewall using IPtables

Cryptography and PKI

- Cryptography basics
- Requirements for cryptography
- Different types of ciphers
- DES
- RSA
- Digital Signatures & PKI
- Authentication functions-Message authentication codes

- Algorithms (MD5, Secure Hash Algorithm)

Attack Techniques

- Information Gathering
- Sniffing,ARP Cache Poisoning & MITM Attack
- Brute Force Attack
- Virus,Trojan,Backdoors
- Recording Keystrokes
- Denial of Service Attack
- MAC Spoofing through Kali Linux
- E-Mail Spoofing & Phishing Attack
- Network Traffic Encryption

Web Application Security

- Web Application Security Risks
- OWASP Top 10 – 2021
- Injection and Inclusion
- Injection in stored procedures
- Cross Site Scripting
- Denial of Service
- Buffer Overflows and Input Validation
- Access Control
- Data Extraction
- Advanced Identification/Exploitation

Mobile Security

- Introduction to Android Architecture
- Android File Structure
- Android Build Process
- Android App fundamentals
- Android Security Model
- Device Rooting
- Android Emulator setup
- Penetration Testing Tools
- Attacks on Android Apps
- Smishing attack
- Web based attacks on Android devices

- Networks based attacks
- Social Engineering attacks
- Static and Dynamic Analysis of Android Apps using MobSF

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

- Acquring the hard disk, usb or other devices
- Analysis of the hard disk and other external devices
- Registry Analysis

Live Forensics

- Key Forensic Acquisition/Analysis Concepts
- Volatile Evidence Gathering and Analysis
- Live Response

Network Forensics

- Wireshark
- Email Tracing
- Steganography

Firewall and IDS

- De-militarized Zone
- Firewall types
- IDS