Specialised Programme on Cyber Security & Forensics – 2 Weeks

Pre-requisites

- Participants should be comfortable of using Windows and Linux Operating system.
- Understanding of Basic Networking concepts is necessary.

Aim

- To prepare the professionals and build proficiency in Threat Intelligence and Risk Management.
- To build resilience against cyberattacks.
- To foster ethical behaviour and promote cyber security practices.

Objectives

- Identify and comprehend the various types of cyber threats like malware, phishing and other attack vectors.
- Help understand the encryption, network security basics.
- Gain the hands –on experience on Ethical Hacking tools and techniques.
- Implement and manage security measures to protect network infrastructure using Firewalls, IDPS, UTM.
- Acquire knowledge of cyber forensics tools and methodologies for the investigating cyber crimes.
- Explain the importance of staying updated on the latest cyber security trends and technologies.

Course Contents

Introduction to Cyber Security

- Introduction to Basic Concepts of Cyber Security
- Cyber Security Threats, Vulnerabilities and Attacks
- Introduction to Cyber Crime

Initiatives taken by The Indian Government on Cyber Security

- The Indian Computer Emergency Response Team (CERT-In)
- Cyber Surakshit Bharat
- National Critical Information Infrastructure Protection Centre (NCIIPC)
- Appointment of Chief Information Security Officers
- Personal Data Protection Bill
- Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre)
- National Cyber Security Policy

Introduction to Threat Intelligence

- Introduction
- Types of Threat Intelligence
- Relevance of Threat Intelligence
- Threat Intelligence Life Cycle
- Threat Intelligence vs Threat Hunting

Cryptography and PKI

- Basics of Cryptography
- Different types of ciphers –Symmetric and Asymmetric
- Hashing& Digital Signatures
- Introduction to Digital Certificates
- Introduction to PKI

Cyber Attacks and their Countermeasures

- Types and methods of hacking and counter measures
- Password Attacks and their countermeasures
- Distributed Denial of Services (DDoS)
- Man-in-Middle Attacks and their countermeasures
- Phishing and Spoofing attacks and their countermeasures
- Malware Attacks and their countermeasures
- Cross Site Scripting Attack and their countermeasures
- SQL Injection Attack and their countermeasures

Network Security

- Introduction to Firewalls
- Types of Firewalls
- Introduction to IDS and IPS
- IDPS
- Introduction to UTM

Cyber Forensics

- Introduction to Cyber Forensics
- Chain of Custody document
- Digital Evidence
- Phases of an Investigation
- Computer Forensics Tools & Toolkits
- Analysis of Digital Evidence
- Disk Forensics
- Network Forensics
- Cyber Forensics Analysis for Cyber Crime cases