Specialised Programme on Cyber Security & Forensics – 2 Weeks

Pre-requisites for the course

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

Aim

- ➢ To prepare the professionals to create awareness about threats, attacks and vulnerabilities and help in mitigation and identification of the footprints of the various cyber attacks
- ➢ To instill the mindset of understanding the continuous evolving cyber threats and attacks

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 of Networking

- Networking Basics
- OSI Model and Protocols
- TCP and UDP Header
- IPv4 Header and Address
- IPv6 Header and Address
- Router and Switch Configuration and Security

Introduction to Cyber Security

- Introduction to Basic Concepts of Cyber Security
- Cyber Security Threats like APT, Phishing, Spyware, Malware, Ransomware, BOT, BOTnet etc.

Cryptography and PKI

- Basics of Cryptography.
- Different types of ciphers –Symmetric and Asymmetric.
- Hashing& Digital Signatures.
- 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 Wireshark
- Examine real-world packet captures
- Introduction to IDS and IPS
- IDS /IPS
- VPN –Introduction, protocols/characteristics, Functions
- Introduction to UTM

Cyber Forensics

- Introduction to Cyber Forensics
- Digital Forensics: Computer
- Digital Objects (Evidence)
- Seizure of Digital Evidence
- Imaging of Digital Evidence
- Computer Forensics Tools & Toolkits
- Analysis of Digital Evidence
- Disk Forensics
- Network Forensics
- Cyber Forensics Analysis for Cyber Crime cases