**CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING**
**A-34, PHASE VIII, INDUSTRIAL AREA, MOHALI**
WHATSAPP NO. 76278 90037 TELEPHONE NO: 0172-2237052-55, 6619000
Email: enquiry-mohali@cdac.in, etd@cdac.in

# TRAINING ON CYBER SECURITY

**DURATION: 26 weeks**

## COURSE CONTENTS

### ❖ Network and Computer Security

- **Computer Networks Fundamentals**
  - ✓ ARP Protocol
  - ✓ Basic Network Devices & Their Functionality
  - ✓ IP Protocol and Addressing
  - ✓ Introduction to Networking with Lab
  - ✓ OSI Model, TCP/IP Headers
  - ✓ Routing process and Routing tables with Lab
  - ✓ Implementation and configuration of Routing protocols
  - ✓ Access Control Lists
  - ✓ Use cases of LAN and WAN topologies and restriction of user segments through ACLs
  - ✓ Network/Port address Translation

- **Introduction to Windows Server 2012**
  - ✓ Hardware Requirements
  - ✓ Installation and Deployment
  - ✓ Features and Security Improvements.

- **Server Role and Responsibility:**
- **Active Directory Domain Services (AD DS):**
  - ✓ Active Directory Domain Services Objects and Concepts.
  - ✓ Structure and Managing domain Environment.
  - ✓ Introduction to user Accounts and Groups.

- **Domain Name System :**
  - ✓ Type of DNS Servers, Types of Zones.
  - ✓ Configuration and management.

- **Group Policy:**
  - ✓ Working with group policy objects.
  - ✓ Using group policy to manage user environment.
  - ✓ Domain security policy, Password policy, Account lockout policy.
  - ✓ User right permissions, Local Security Policy, Domain - controller Security Policy
- **DHCP Server :**
  - ✓ Introduction, Configuration and Management.

### ❖ Cyber Security Concepts

- **Introduction:**
  - ✓ Security mindset and challenge of Survivability.
  - ✓ Security Concepts (CIA)
  - ✓ Threats, Attacks, and Assets

- **Introduction to Kali Linux:**
  - ✓ Kali Linux- An Introduction
  - ✓ Prerequisite and Installation
  - ✓ File Structure and Basic Commands

- **Cyber Attacks:**
  - ✓ Introduction, Impact of Cyber Attacks
  - ✓ Types of Cyber Attacks, Active Attacks, Passive Attacks
  - ✓ Prevention of Cyber Attacks, Basic Security Tips
  - ✓ How to Deal with Cyber-Attack
  - ✓ Phishing Scams
  - ✓ Man-in-Middle Attacks
  - ✓ Eavesdropping
  - ✓ Social Engineering

- **Network Analysis Techniques/Tools:**
  - ✓ Netstat,Tcpview,Currport,Regseeker
  - ✓ Nmap,DNS Interrogation
  - ✓ Network Scanning: finding services, version detection, OS Detection

- **Information Gathering :**
  - ✓ Footprinting,Scanning,Sniffing
  - ✓ Active and Passive Sniffing
  - ✓ Working on Sniffing Tools
  - ✓ Enumeration : Open source Search and Network Enumeration
  - ✓ Social Engineering, Information security Governance

- **Practical Network Packet Analysis**
  - ✓ Traffic Analysis-Fundamental
  - ✓ Packet Analysis and Network Basics
  - ✓ Tapping into the wire
  - ✓ Introduction to Wireshark
    - Navigating around Wireshark
    - Examination of Wireshark statistics
    - Stream reassembly
    - Finding content in packets
    - Wireshark display filters
  - ✓ Packet capturing and Its analysis
  - ✓ Application Protocol and Traffic analysis

- **Offensive Cyber Security:**
  - ✓ Introduction to Metasploit Framework
  - ✓ Security Terminology
  - ✓ Metasploit Interfaces
  - ✓ Intelligence Gatherings-passive and active intelligence gatherings
  - ✓ Exploit-DB-Exploits and advisories
  - ✓ Virtual Security Lab
  - ✓ Basic Exploitations
  - ✓ Exploiting your first machine

- **Application Security Attacks**
  - ✓ Injection (SQL Injection)
  - ✓ Broken Authentication and session management
  - ✓ Cross Site Scripting
  - ✓ Broken Access Control
  - ✓ Security Misconfigurations
  - ✓ Cross Site Request Forgery (CSRF)

- **Network Monitoring and Deep Packet Inspection**
  - ✓ Perimeter Security Fundamentals
  - ✓ Network Monitoring
  - ✓ Packet Crafting
  - ✓ PCAP (Packet) Capturing
  - ✓ Antivirus and Firewalls
  - ✓ Intrusion Detection/Prevention System (IDS/IPS)
  - ✓ Network Architectures
    - Instrumenting the network for traffic collection
    - IDS/IPS deployment strategies
    - Hardware to capture traffic
  - ✓ Introduction to IDS/IPS Analysis

- Function of an IDS
- The analyst's role in detection
- Flow process for Snort

✓ Snort

- Introduction to Snort
- Running Snort
- Writing Snort rules

- **Malware Analytics**
  - ✓ Malware Analysis a practical approach
  - ✓ Introduction to Mobile Device Security
  - ✓ Android Malwares types and Techniques
  - ✓ In-depth Malware Analysis
    - Reverse engineer malware and learn methods for malware analysis
    - Performing static and dynamic code analysis of malicious
    - Android Malware Analysis
  - ✓ Set up a safe virtual environment to analyze malware

**Project Work**