**Specialized Training Program in** **Cyber Attacks and Prevention Techniques**

|  |  |  |
| --- | --- | --- |
| A. | **Name of the Institute** | Centre for Development of Advanced Computing, Mohali |
| B. | **Name/Title of the Course** | **Specialized Training Program in Cyber Attacks and Prevention Techniques** |
| C. | **Proposed Dates and Duration of the Course in weeks/ months** | Duration: **Eight weeks**  From: **6 May, 2019 to 28 June, 2019** |
| D. | **Eligibility Criteria for Participants** | |
| 1. Educational Qualification | Technical Graduate (Computer Science/ Electronics/Telecommunications/or equivalent) with working knowledge of computers. |
| 1. Work Experience | As per MEA guidelines |
| 1. Age Limit | As per MEA guidelines |
| 1. Target group (Level of participants and target ministry/department etc. may be identified) | Working Professional with knowledge of computers. |
| E. | Aims & Objectives of the Course | At the end of the course, Students will be able:   * To understand the Network and e-Security concepts & terminology. * To understand different types of Cyber Attacks and their impacts. * To prevent attacks and other threats in a network or Internetwork. * To understand about vulnerabilities in existing networking infrastructure * To facilitate secured communication using Cryptography. * To facilitate network security using security methods. |
| F. | Details / Content of the Course ***(please attach detailed Course Profile****)* | As per sheet attached |
| G. | Mode of Evaluation of Performance of the ITEC Participant | Theory, viva voce & Practical |

**Course Content:**

Duration of Module: 8 weeks

* **Computer Networking Fundamentals**
  + Networking Basics
  + OSI Model
  + TCP/IP Headers
  + TCP Flags
  + IP Addressing
  + Basic Network Devices
  + Subnet & Supernet
  + Domain Name System (DNS)
  + UDP Header and ICMP Message
  + ARP Process
  + Routing process and Routing tables
  + Access Control lists
  + System Administration tools
* **Cyber Attacks**
  + Introduction to Cyber Attacks
  + Impact of Cyber Attacks
  + Types of Cyber Attacks
    - Malwares
    - Password Attacks
    - DDos Attacks (Distributed Denial of Service Attacks)
    - Pop-Ups
    - Software Updates
    - Public Unsecured Wi-Fi Network Attacks
    - Phishing Scams
    - Cross Site Scripting
    - SQL Injection
    - Man-in-Middle Attacks
    - Eavesdropping
    - Session Hijacking
    - Social Engineering
  + Prevention of Cyber Attacks
    - Basic Security Tips
    - How to Deal with Cyber-Attack
* **Cyber Security Methods**
  + Perimeter Security Fundamentals
  + Administration and Security
  + Linux Commands
  + Network Monitoring
  + Packet Crafting
  + PCAP (Packet) Capturing
  + IPtables
  + Antivirus and Firewalls
  + Intrusion Detection/Prevention System (IDS/IPS)
  + Signature Generation
  + Vulnerability Assessment
  + Attacks (Test Cases)
* **Cryptographic Methodologies**
  + Understand Basic Encryption Concepts
  + Attacks Against Encryption
  + Understand Private Key Encryption
  + Understand Public Key Encryption
  + Cryptography Fundamentals
  + Symmetric Key Encryption Algorithms
    - Data Encryption Standard (DES) & Tripple DES
    - Blowfish
    - AES (Rijndael)
  + Public Key Algorithms
    - Diffie–Hellman Exponential Key Exchange
    - RSA
    - ElGamal
    - Schnorr’s Public-key Cryptosystem
  + Cryptographic issues
  + Secure Hash Functions
    - MD5
    - SHA1
  + Digital Signatures
  + HTTPS
  + PKI (Public Key Infrastructure)
    - What Is PKI?
    - Components of PKI
    - PKI Architecture & Working