**ITEC- 2022- 2023**

**Specialized Training Programme in** **Cyber Security & Malware Analytics**

**(Reverse Engineering)**

|  |  |  |
| --- | --- | --- |
| A. | Name of the Institute | Centre for Development of Advanced Computing, Mohali |
| B. | Name/Title of the Course | Specialized Training Programme in Cyber Security & Malware Analytics (Reverse Engineering) |
| C. | Proposed Dates and Duration of the Course in weeks/ months | 16th May, 2022 – 10th June, 2022  Duration: Four week(s) |
| 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 Cyber 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 * Hands on practical packet analysis. * To facilitate network security using security methods. * Cyber Security Analytics |
| F. | Details / Content of the Course | **1) Introduction to Computer Networks & Linux**   * Introduction to Networking with Lab * OSI Model, TCP/IP Headers, IP Protocol and Addressing * Basic Network Devices & Their functionality * Routing process and Routing tables with Lab, Access Control lists * System Administration tools * Linux Fundamentals and Commands, iptables * Network Designing, Configuring and Administration   **2) Cyber Security Attacks**   * Cyber Security Overview * Introduction to Cyber Attacks * Impact of Cyber Attacks * Types of Cyber Attacks   + Layer-2 Threats: MITM, ARP Poising, Spoofing etc.   + Malwares   + Password Attacks   + DDoS Attacks (Distributed Denial of Service Attacks)   + Pop-Ups   + Software Updates   + Public Unsecured Wi-Fi Network Attacks   + Phishing Scams   + Man-in-Middle Attacks   + Eavesdropping   + Social Engineering * Application Security Attacks   + Injection (SQL Injection)   + Broken Authentication and session management   + Cross Site Scripting   + Broken Access Control   + Security Misconfigurations   + Cross Site Request Forgery (CSRF) * Cyber Security Methods   + Perimeter Security Fundamentals   + Network Monitoring   + PCAP (Packet) Capturing   + Antivirus and Firewalls   + Intrusion Detection/Prevention System (IDS/IPS)   + Honeypots/Honeynets   + Vulnerability Assessment   + Attacks (Test Cases)   **3) Malware Analytics**   * Introduction to malware analysis * Malware Analysis a practical approach * Malware analysis techniques- Dynamic and static analysis * Basic analysis   + Basic static analysis   + Malware analysis in virtual machines   + Setup a safe virtual environment to analyse malware   + Basic Dynamic analysis * Advanced static analysis   + Buffer overflow analysis using immunity debugger   + IDA Pro   **4) Malware Reverse Engineer**   * In-depth Malware Analysis   + Reverse engineer malware and learn methods for malware analysis   + Performing static and dynamic code analysis of malicious Windows executables   + Set up a safe virtual environment to analyze malware   + Use key analysis tools like IDA Pro, OllyDbg, and WinDbg * Advanced dynamic analysis   + Debugging, malware functionality   + Malware behavior   + Signature generation |
| G. | Mode of Evaluation of Performance of the ITEC Participant | Theory, viva voce & Practical |