**Specialized Training Program 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 Program in Cyber Security & Malware Analytics (Reverse Engineering)** |
| C. | **Proposed Dates and Duration of the Course in weeks/ months** | Duration: **Eight weeks**From: **09 March, 2020 to 01 May, 2020** |
| 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 ***(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

**1) Introduction to Computer Networks**

* Introduction to Networking with Lab
* OSI Model, TCP/IP Headers
* TCP Flags
* IP Protocol and Addressing
* Basic Network Devices & Their functionality
* Domain Name System (DNS)
* UDP Header and ICMP Message
* ARP Protocol
* Routing process and Routing tables with Lab
* Access Control lists
* System Administration tools
* 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
* Prevention of Cyber Attacks
	+ Basic Security Tips
	+ How to Deal with Cyber-Attack
* Application Security Attacks
	+ Injection (SQL Injection)
	+ Broken Authentication and session management
	+ Cross Site Scripting
	+ Broken Access Control
	+ Security Misconfigurations
	+ Cross Site Request Forgery( CSRF)

**3) Cyber Security Methods**

* Perimeter Security Fundamentals
* Administration and Security
* Linux Fundamentals and Commands
* Network Monitoring
* Packet Crafting
* PCAP (Packet) Capturing
* IPtables
* Antivirus and Firewalls
* Intrusion Detection/Prevention System (IDS/IPS)
* Honeypots/Honeynets
* Vulnerability Assessment
* Attacks (Test Cases)

**4) 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
		- TCPDUMP- writing tcpdump files
* Packet Capturing and Its analysis
* Application Protocol and Traffic analysis

**5) Network Monitoring and Deep Packet Inspection**

* 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
	+ Solutions for dealing with false negatives and positives
	+ Tips for writing efficient rules

**6) Cyber Analytics**

* Introduction to Cyber Analytics Studio
* Apply programming skills to develop Cyber Security data analytics
* Usage of Programming Language- R, Python to contextualize and visualize Cyber Security data
	+ Introduction to R language
	+ Python Programming
	+ Hands on and usage of R tools
	+ Practical exposure to Python Programming in Cyber Security
* Building the analytical models of Cyber Security Attack detection and visualization
* Clustering and Classification to identify new threats.
* Cyber Attack Data Mining using R- tools
* Deep Learning in Cyber Security

**7) Malware Analytics**

* Malware Analysis a practical approach
* 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
* Offensive Security & Penetration testing