

## ITEC- 2022- 2023

### Specialized Training Programme in Cyber Security & Malware Analytics (Reverse Engineering) for Dominican Republic

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	17 <sup>th</sup> October, 2022 – 11 <sup>th</sup> November, 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.
	2. Work Experience	As per MEA guidelines
	3. Age Limit	As per MEA guidelines
	4. 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	<p>At the end of the course, Students will be able:</p> <ul style="list-style-type: none"> <li>• To understand the Cyber Security concepts &amp; terminology.</li> <li>• To understand different types of Cyber Attacks and their impacts.</li> <li>• To prevent attacks and other threats in a network or Internetwork.</li> <li>• To understand about vulnerabilities in existing networking infrastructure</li> <li>• Hands on practical packet analysis.</li> <li>• To facilitate network security using security methods.</li> <li>• Cyber Security Analytics</li> </ul>
F.	Details / Content of the Course	<p><b>1) Introduction to Computer Networks &amp; Linux</b></p> <ul style="list-style-type: none"> <li>• Introduction to Networking with Lab</li> <li>• OSI Model, TCP/IP Headers, IP Protocol and Addressing</li> <li>• Basic Network Devices &amp; Their functionality</li> <li>• Routing process and Routing tables with Lab, Access Control lists</li> <li>• System Administration tools</li> <li>• Linux Fundamentals and Commands, iptables</li> <li>• Network Designing, Configuring and</li> </ul>

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 Poisoning, 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

		<ul style="list-style-type: none"> <li>• Basic analysis <ul style="list-style-type: none"> <li>○ Basic static analysis</li> <li>○ Malware analysis in virtual machines</li> <li>○ Setup a safe virtual environment to analyse malware</li> <li>○ Basic Dynamic analysis</li> </ul> </li> <li>• Advanced static analysis <ul style="list-style-type: none"> <li>○ Buffer overflow analysis using immunity debugger</li> <li>○ IDA Pro</li> </ul> </li> </ul> <p><b>4) Malware Reverse Engineer</b></p> <ul style="list-style-type: none"> <li>• In-depth Malware Analysis <ul style="list-style-type: none"> <li>○ Reverse engineer malware and learn methods for malware analysis</li> <li>○ Performing static and dynamic code analysis of malicious Windows executables</li> <li>○ Set up a safe virtual environment to analyze malware</li> <li>○ Use key analysis tools like IDA Pro, OllyDbg, and WinDbg</li> </ul> </li> <li>• Advanced dynamic analysis <ul style="list-style-type: none"> <li>○ Debugging, malware functionality</li> <li>○ Malware behavior</li> <li>○ Signature generation</li> </ul> </li> </ul>
G.	Mode of Evaluation of Performance of the ITEC Participant	Theory, viva voce & Practical