

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 | 16 th May, 2022 – 10 th 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. |
| | 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"> • 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 | <p>1) Introduction to Computer Networks & Linux</p> <ul style="list-style-type: none"> • 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 |

| | | |
|--|--|--|
| | | <ul style="list-style-type: none">• Linux Fundamentals and Commands, iptables• Network Designing, Configuring and Administration <p>2) Cyber Security Attacks</p> <ul style="list-style-type: none">• Cyber Security Overview• Introduction to Cyber Attacks• Impact of Cyber Attacks• Types of Cyber Attacks<ul style="list-style-type: none">○ 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<ul style="list-style-type: none">○ Injection (SQL Injection)○ Broken Authentication and session management○ Cross Site Scripting○ Broken Access Control○ Security Misconfigurations○ Cross Site Request Forgery (CSRF)• Cyber Security Methods<ul style="list-style-type: none">○ Perimeter Security Fundamentals○ Network Monitoring○ PCAP (Packet) Capturing○ Antivirus and Firewalls○ Intrusion Detection/Prevention System (IDS/IPS)○ Honeypots/Honeynets○ Vulnerability Assessment○ Attacks (Test Cases) |
|--|--|--|

| | | |
|----|---|---|
| | | <p>3) Malware Analytics</p> <ul style="list-style-type: none"> • Introduction to malware analysis • Malware Analysis a practical approach • Malware analysis techniques- Dynamic and static analysis • Basic analysis <ul style="list-style-type: none"> ○ Basic static analysis ○ Malware analysis in virtual machines ○ Setup a safe virtual environment to analyse malware ○ Basic Dynamic analysis • Advanced static analysis <ul style="list-style-type: none"> ○ Buffer overflow analysis using immunity debugger ○ IDA Pro <p>4) Malware Reverse Engineer</p> <ul style="list-style-type: none"> • In-depth Malware Analysis <ul style="list-style-type: none"> ○ 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 <ul style="list-style-type: none"> ○ Debugging, malware functionality ○ Malware behavior ○ Signature generation |
| G. | Mode of Evaluation of Performance of the ITEC Participant | Theory, viva voce & Practical |