Specialized Programme on Reducing Cyber Crime through Knowledge Exchange and Capacity Building

A. NAME OF INSTITUTE	Centre For Development of Advanced Computing
B. NAME/TITLE OF THE COURSE	**Specialized Programme on Reducing Cyber Crime through Knowledge Exchange and Capacity Building**
C. COURSE DATES WITH DURATION IN WEEKS	**From October 27th, 2014 to December 19th, 2014** **In weeks: 8 Weeks**
D. ELIGIBILITY CRITERIA FOR PARTICIPANTS: 1. EDUCATIONAL QUALIFICATIONS 2. WORK EXPERIENCE required, if any 3. AGE LIMIT 4. Target Group *[Level of participants and target ministries/departments etc. may be indicated]*	1) Two years technical course or Graduation with knowledge of: →Windows Operating System preferably familiarity with its administration though not essential. →Understanding of Networking, OSI Model & Concept of protocols 2) ------- 3) ------ 4) Should meet the above educational requirements and should know English language
E. AIMS AND OBJECTIVES OF THE COURSE	<u>Objective:</u> • To make the participants aware about the Cyber crime, it's impact, types of cyber crime etc. • To give information to participants relating to reducing Cyber Crime by implementing security at various levels e.g desktop, server, network etc. Participants would also be trained in Cyber Forensics to help them in dealing with their investigations in Cyber Crimes.
F. MODE OF EVALUATION OF PERFORMANCE OF THE TRAINEE	Lab Work

Objective:

At the end of the course, Students will be able:

- To understand the Network and e-Security concepts & terminology.
- To understand about vulnerabilities in existing networking infrastructure
- To have information relating to Info security, Internet Security & Network Security to facilitate secured communication through enterprise Networking.
- To prevent attacks and other threats in a network or Internetwork.

Course Content

1. Introduction to Cyber Crime

- Definition
- Types of Cyber Crime
- Impact of Cyber Crime

2. Computer Networks

- Networking Basics
- Types of Networks
- OSI reference model
- IP addressing scheme
- What is subnetting
- Configuring Subnet mask

3. Advanced TCP/IP

- The Concepts of TCP/IP
- The Suite and the Services
- Internet Protocol Security (IPSec)
- Internet Protocol version 6 (IPv6)

4. IP Packet Structure and Routing and Access Control Lists

- Network Monitor
- The IP Header
- The TCP Header
- Connections
- The UDP Header andThe ICMP Message
- Configuring RIP
- Configuring IGRP
- Configuring EIGRP

- The ARP Process
- Cisco Routing Modes
- The Routing Process
- Routing Tables
- Access Control Lists
- Implementing ACLs

5. Cryptography and PKI

- Cryptography basics
- Requirements for cryptography
- Different types of ciphers
  - Caesar Cipher
- Hill Cipher
- Vernam Cipher
- DES
- RSA
- MD5
- SHA1
- PKI
- Digital Signatures

6. Securing Windows Computers

- Windows 2008 Infrastructure and ADS
- Windows 2008 Authentication
- Windows 2008 User and Group Security
- Windows 2008 Resource Security
- Windows 2008 Encrypting File System
- Windows 2008 Network Security

7. Securing Linux Computers

- Linux Operating System
- Linux Administration and Security
- Key Linux Network Files, Network Processes, Network Commands
- Hardening Linux
- Portmap and Linux
- Network File System (NFS) and Linux SAMBA Security
- Linux Web Server Security
- Linux Mail Server Security
- IPtables

- Auditing and Syslog
- Vulnerability Assessment

8. Cyber Forensics

- Introduction to Cyber Forensics
- Computer Forensics
- Disk Forensics
- Network Forensics
- Device Forensics
- Tools demonstration

9. Attack Techniques

- Network Reconnaissance & Footprinting
- Mapping the Network
- Viruses, Worms, and Trojan Horses
- Gaining Control over the System
- Recording Keystrokes
- Cracking Encrypted Passwords
- Reveal Hidden Passwords
- Social Engineering
- Gaining Unauthorized Access
- Hiding Evidence of an Attack
- Performing a Denial of Service