



University of Mauritius
C-DAC School of Advanced Computing



Executive Development Programme

Training Workshop on Network Forensics

(MQA approved)

27-29 October 2009, University of Mauritius

Introduction

Today's information society requires that everyone be aware of the potential threats, the limitations and the respective countermeasures of the extended use of IT networks. Awareness and training are of utmost importance to ensure that the society is well-equipped with the essential know-how and expertise to handle security risks and threats. This Executive Development Programme will be a stepping stone towards the development of a culture of IT security in Mauritius.

Network forensics is the use of scientifically proven techniques to capture, record, and analyse network events in order to discover the source of security attacks or other problem incidents. It is basically about monitoring network traffic, determining if there is an anomaly in the traffic and whether the anomaly can be an attack.

Objectives

The main objective of this Training Workshop is to bring together IT and security professionals, industry experts, academicians, analysts and students to share their experiences, acquire knowledge and gain an understanding of the key tools, techniques and strategies needed to safeguard organisation's most valuable asset – information. It also aims to:

- understand various cyber attacks and approaches to mitigate these attacks.
- develop means to identify if the organisation is adequately prepared to deal with such a disaster.
- protect critical infrastructure through effective intrusion prevention strategies against cyber threats.

Methodology

The Training Workshop will employ a right mix of lectures, hands-on sessions, demonstrations, and case studies. Real-world examples will be used throughout the course in conjunction with numerous tutorial exercises to develop field-proven, practical forensics skills. Participants will receive training binders and a set of demo CDs of Cyber Forensics tools.

Audience

The Training Workshop will help Law Enforcement Personnel, Information Security Professionals, Corporate Business and Management Executives, and Network Administrators to understand how to secure their resources from cyber attacks. Participants will acquire real-world knowledge and skills to analyze network traffic from criminals' computers, improve network security and reliability, and protect networks from malicious and criminal attacks.

Certificate of Attendance will be issued to all the participants.

Resource Persons

- ✓ Mr. V.K. Bhadran, Director, Resource Centre for Cyber Forensics, C-DAC, Ministry of Communications & IT, India.

V.K. Bhadran, an expert in network security and forensics, has 25 years work experience in the ICT sector. He is heading a group of scientists involved in the development of tools for cyber forensics, cyber crime investigation and training activities. He was the lead in developing network forensics tools such as Forensics Log Analyser and Network Session Analyser, to support the investigation of network crimes and analysis. Bhadran is currently developing a package for Enterprise Security and Forensics Systems which helps organisations in securing the transactions over their network.

- ✓ Mr. Peter Kruse, Head, Research & Intelligence, CSIS Security Group, Denmark.

Peter Kruse is known and recognized as being amongst the best reverse engineers and eCrime researchers in the world and has worked in these fields for more than 15 years. In the past Peter has worked with Norwegian antivirus vendor Norman as a virus signature developer and malware specialist. He has also been working as the head of security in Nordic telecom giants such as TDC and Telia. He is a member of the Conficker and Malware Working Groups and work closely with security vendors such as F-Secure, Symantec, MacAfee and TrendMicro. Peter is known to be a colourful and strong speaker at various high tech security conferences around the world.

Programme Outline

Day 1

- Network forensics overview
- Network forensics tools
- Understanding normal network traffic
- Tracking IP addresses
- Analysing TCP and UDP port numbers
- Domain Name System (DNS)
- E-mail tracing
- Reconstructing a suspect's Web-browsing activity
- Demo of e-mail tracing and practical

Day 2

- Capturing network traffic
- Reconnaissance missions
- Security breaches
- Live attacks
- Reconnaissance and attack signatures
- Demo of Cyber Investigator and practical

Day 3

- Introduction to server logs
- Introduction to routers and switch forensics
- Introduction to log file analysis
- Introduction to packet analysis
- Demo of Network Session Analyzer and practical
- Case studies

Fees

- Rs 15,000 per participant for general candidates.
- Discount rate of Rs 12,000 per participant for a corporate batch of minimum 10.
- Special rate of Rs 12,000 per participant from government/parastatal sectors.
- Special rate of Rs 12,000 per participant for C-SAC/UoM alumnus.
- Sponsored rate of Rs 7,500 per participant for students of C-SAC/UoM/UTM.

Since the Training Workshop is MQA approved, participants could avail HRDC refund as applicable.

Organisers

C-DAC School of Advanced Computing: C-SAC was set up in Mauritius in 2002 to promote education, training, research and consultancy in the field of ICT and its applications in Mauritius. C-DAC is an R&D organisation of the Government of India and is involved in design, development and deployment of advanced ICT based solutions and ICT training. www.csac.mu

University of Mauritius: UoM is a dynamic and internationally recognised university with a long established tradition in providing excellence in education. www.uom.ac.mu

Contact Persons

1. Dr. C.P. Johnson
Resident Director & Head
C-DAC School of Advanced Computing
24, St. Jean Road, Quatre Bornes, Mauritius
Tel: 230-4255849; Tel/Fax: 230-4275516
E-mail: johnson@csac.mu , info@csac.mu
2. Mr. Kavi Khedo
Head, Department of Computer Sciences
University of Mauritius
Réduit, Mauritius
Tel: 230-4037400; Fax: 4657144
E-mail: k.khedo@uom.ac.mu