Cyber Forensics & Crime Investigation

This workshop is dedicated on Cyber Forensics & Crime Investigation. Computer Forensics is a detailed and scientific study, research and implementation of computer science subjects for the purpose of gathering digital evidence in cases of cyber crimes or for other scientific research purposes also it introduces the needs of the current cyber security sector.

Topics to be covered:

1.Understanding of an Organization's IT Environment

Concept of Zoning – Demilitarized Zone, Militarized Zone
Basic Servers being used in the IT Environment and their positioning in different Zones
Brief Insight of the IT Security Devices used

2.What is Computer Forensics all about?

Difference – Computer Crime & Un-authorized activities.
6 steps involved in Computer Forensics – Description of what is to be carried in each step
Need for forensics investigator

3.Security Incident Response

What is a Security Incident
Role of the Investigator in investigating a Security Incident
Evidence Control and Documentation
Skills and Training of a Forensics Investigator – Technical, Presentation, Professional

4.Corporate Regulation and Privacy Issues

Computer Abuse in the Corporate World
Security Policies
Security and Acceptable-Use Policies

5.Evidence Control and Documentation

Document, Documents, Document.
Evidence Collection and Inventory
Chain of Custody
Evidence Storage and Security

6. Building a Forensics Laboratory

Laboratory Standards
Facility Physical Security
Evidence Security
Software
Hardware
Portable Forensics Labs

7. COMMERCIAL FORENSICS SOFTWARE TOOLS

The Case for Commercial Tools
Encase
Access Data Forensics Tool Kit
DriveSpy and Paraben

8. Open Source FORENSICS TOOLS

Windows Forensic Analysis Tools Open Source
Process Explorer from SysInternals
WhatsRunning
Registry Decoder CPORTS
Windows File Analyzer
Windows File Checksum Integrity Verifier
Registry Ripper
Microsoft Log Parser Tool

9. Open Source Disk Imaging Tools

What is Disk Imaging
Utilities of Disk Imaging Disk Imaging Utilities
Access Data FTK Imager
DixmlSetup

10. File Analysis

What is File Analysis?
File Attributes
Unix File Permissions
Known File Type Signatures & Hashes
Malware Infected Files
Virus Characteristics
Indications of a Trojan Infection
Worms Windows File Analyzer- File Analysis Software

11. Log analysis

Why Log Analysis
Windows Log analysis
Tools for Log Analysis
OSSEC HIDS
Installation Logs
Windows Event Logs
UNIX Syslogs
Firewall and IDS/IPS Logs
Apache Access Logs & Error Logs

12. Windows Forensics

LIVE VS DEAD RESPONSES – WHEN AND WHY
NETWORK CONNECTIONS TCP-States
Demo-Whats Up Running Tool
Demo-Process Explorer Tool
Demo-CPorts
Windows Processes
Demo-Services.msc
Hidden Files
Concept of ADS (Alternate Data Stream)
Demo-Windows File Analyser Tool
AUDITING & THE SECURITY EVENT LOG

Demo- Windows File Checksum Integrity Verifier

Demo- Access Data Forensics Tool Kit

Create a Disk Image

13. Linux Forensics

Network connections,

Services

Logging and log files in UNIX

Linux forensics tools

Demo - Real Time Command Logging

Forensic Analysis using OSSEC HIDS

14. CONCLUDING THE INVESTIGATION

Documentation

Preparation

Concluding a Corporate Investigation

Testifying in Court

Ethical Responsibilities

Duration: The duration of this workshop will be two consecutive days, with eight hour session each day in a total of sixteen hours properly divided into theory and hands on sessions.

Fees: Rs. 1350/- per head inclusive of all taxes.