Cyber Forensics

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.

Day 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

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

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

Corporate Regulation and Privacy Issues

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

Evidence Control and Documentation

- Evidence Collection and Inventory
- Chain of Custody
- Evidence Storage and Security

Building a Forensics Laboratory

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

COMMERCIAL FORENSICS SOFTWARE TOOLS

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

Day 2

Open Source FORENSICS TOOLS

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

Open Source Disk Imaging Tools

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

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

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

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

Linux Forensics

- Network connections,
- Services
- Logging and log files in UNIX
- Linux forensics tools
- Demo - Real Time Command Logging
- Forensic Analysis using OSSEC HIDS

CONCLUDING THE INVESTIGATION

- Documentation
- Preparation
- Concluding a Corporate Investigation
- Testifying in Court
- Ethical Responsibilities

Deliverables to Participant after the conduction of workshop

1. Software toolkit to each participant.
2. Training Material (eBooks) for each participant.