System Forensics for Incident Responders

Course Summary

Description

Identify, Respond, and Recover from a Security Breach.

This comprehensive, technically detailed course enables you to successfully respond to incidents and reinforce your security posture.

Objectives

After taking this course, students will be able to understand:

- Computer forensics process
- How to create evidentiary disk images
- How to respond to unlawful access and information theft
- Incident response procedures for Unix and Microsoft Windows systems

Topics

- Introduction
- Preparation
- Legal Concerns
- UNIX and Linux Incident Response
- Windows Incident Response
- File Carving and Toolkit Building
- Network-Based Monitoring
- File System Forensics
- Advanced Topics

Audience

This course is designed for incident responders, security operations center personnel, and cyber security managers.

Prerequisites

Before taking this course, students should have a basic understanding of the Windows and Linux Operating Systems, and some programming knowledge.

Duration

Five days

ProTech protechtraining.com *"Charting the Course ...*

... to Your Success!"

System Forensics for Incident Responders

Course Outline

I. Introduction
- A. Course Content and Format
- B. Principles of Forensics and Incident Response (IR)

II. Preparation
- A. Data Collection Techniques
- B. Chain of Custody
- C. Pre-Incident Preparation
- D. Forensic Hardware
- E. Basic Incident Response Process
- F. Documentation Requirements

III. Legal Concerns
- A. Federal Laws - ECPA and USC
- B. Interception of Data
- C. Stored Communications
- D. Unauthorized Access
- E. Child Pornography
- F. Patriot Act, Gramm-Leach-Bliley Act, and Sarbanes-Oxley
- G. Acceptable Use Policies

IV. UNIX and Linux Incident Response
- A. Live Response Best Practices and Order of Volatility
- B. Unix/Linux File Permissions
- C. Unix/Linux Live Response
- D. Following the Process Tree

V. Windows Incident Response
- A. Installed Software and Hotfixes
- B. Persistence Mechanisms
- C. Windows Audit Policies
- D. Malware Analysis
- E. Alternate Data Streams
- F. Windows Registry

VI. File Carving and Toolkit Building
- A. File Carving
- B. Building a Response Kit
- C. Determining File Headers
- D. Scripting a Response Step by Step
- E. Extracting Specific File Types

VII. Network-Based Monitoring
- A. Sources of Network Data
- B. Placement of Monitoring Devices in Network Monitoring Hardware

VIII. File System Forensics
- A. Common File System Types
- B. Image File Formats
- C. Hard Drive Types
- D. Deleted Files
- E. File Systems

IX. Advanced Topics
- A. Memory Analysis and Rootlet Detection
- B. Extracting Registry Values from Memory Dumps