Cyber Security for IT Teams (CS112)

40 Hours

Outline

That unique program is intended to provide the theoretical and practical knowledge required for integrating in main position of leading IT teams in the cyber security industry. The program provides advanced thinking skills, technique for complex defensive and offensive operations, advance monitoring and prevention and the most updated platforms and tools that will gain your arsenal of knowledge.

Target Audience

This course is intended for IT teams, SOC teams and People that almost integrated in the information security industry and want to gain their practical and theoretical skill.

Objectives

On completing this course, delegates will be able to:

- Understand The Hacker Point of View
- Improve Skills on Cyber Security
- Gain New Techniques For the Best Investigation

Contents

Day 2

Module 3: Network Security

- Virtualization
- Prepare Your Lab
    - Installation
    - Configuration
- Basics of Penetration Tasting
- Metasploit Basics
- Metasploit Auxiliary
- Meterpreter
- Creating Your Own Exploits
- Simulated Penetration Test
- Intelligence Gathering
- Anti-Forensic
- Thinking Anonymous
- Secure Log & Data Deletion
- Overwriting Metadata
- Preventing Data Creation
- Finding Important Files
- Auto-Start Directories
- WMI
- PowerShell Scripts

Day 3

Module 4: SOC Training

- Introduction to SIEM
- SIEM Architecture
- Log Monitoring
- SIEM Platforms
- Investigation Techniques and Nodes

- Analytical Reporting
- IDS and IPS
- Anti-Virus and Signatures
- Firewall Types and Configurations

Module 5: Prepare Your Forensics Lab

- Determining Lab Requirements
- Key Components of a Forensics Lab
- Forensics Tools
    - Autopsy
    - Volatility
    - NirSoft
    - FTK Imager
    - HxD
    - Bulk Extractor
    - Forensics Common Frameworks for Investigation

Day **4**

Module 6: Windows Forensics

- File System Types
- Hard Disc Types
- Open Source Tools
- Recovering Deleted Files
- Browsers and Internet Evidence Collecting
- Collecting RAM Information
- Key Files = Key Evidences
- Image Mounting and Analyze
- File Carving
- Pagefile.sys, Hiberfil.sys and Unallocated Space Analysis

Day **5**

Module 7: Network Forensics

- Introduction to Network Forensics
- Wireshark
- CAP Files Manipulation
- Package Structure and Analysis
- Internet Traffic Analyze
- Network Forensics Investigation Process
- Professional Report Writing

Module 8: Log Analysis

- Defining Log Data
- System Audit Policies
- Network Activity Logging
- Log Sources
- Log Analysis Tools
- Common Manipulation Methods
- Windows Event Viewer