Course Title:

Cyber Threat Intelligence & Spyware Hunting Workshop

Duration:

15-20Hrs

Class Format Options:

Instructor-led classroom – Practical Training.

Who Should Attend:

- Cyber Security Professionals
- SOC Managers
- SOC Engineers
- IT Auditors
- System Administrators
- IS Managers
- IT Managers

Prerequisites:

A general knowledge of information systems and security including spyware tools and cyber intelligence.

Provided Materials:

- Softcopy Materials.
- Workshop tools.

This training course is **practical training course** on which each trainee will learn how to configure spyware tools, how to detect and eradicate the spyware tools.

Course Overview

The **Cyber Threat Intelligence & Spyware Hunting Workshop** is an advanced **defensive cyber security course** from **BLUE Team** training path aims to teach trainees to install, detect, remove spy tools. by understanding how these programs work and the modern methods used by cyber criminals. CTISH relies on intelligence gathering using open source intelligence, social media intelligence, human intelligence, technical intelligence. **Cyber Threat Intelligence & Spyware Hunting Workshop** will allow trainees to gain the practical experience to manage and learn how spyware tools work, furthermore cyber threat intelligence whereby trainees to **understand the adversary's decision-making process**.

Cyber Threat Intelligence & Spyware Hunting Workshop is designed for those people who wish to become cyber security professionals, Spyware and Malware Hunter, Information Security Assurance specialists, the course covers:

- Develop key sources of threat intelligence
- Malware and spy software in computers - Practical using tools.
- Analyzing image with advance memory forensics labs.

Upon completion trainees will be able to:

- Protection. Detection & Removal of Potentially Unwanted Programs.
- Have the knowledge to perform OSSIM Installation.
- Have the knowledge to accurately detect spyware tools from analyzing the RAM image.

Day 1 Agenda

> Training Course Paths
> BLUE Team vs RED Team
> Defense Against Attacks
> Training Course Type
> Key Loggers Lab
> Soft Activity Lab
> **Threat Intelligence Introduction**
> Threat Intelligence
> Intelligence Definition
> Threat Intelligence Definition
> What Is CNE
> What Is CNA
> What Is CND
> Key Objective Of **CND**

Day 2 Agenda

> CND Tools
> IDS VS IPS
> Anti-Malware
> NAC
> Next Generation Firewall
> Next Generation Firewall VS UTM
> UTM
> Intrusion Kill Chain
> Why Incident Handling? Other Reasons
> Forensics vs Incident Handling & Response
> What is DATA
> What is Information
> What is Intelligence
> Relationship of Data, Information, & Intelligence
> Drowning in Data

Day 2 Agenda- Cont

> The Adaptive Security Architecture
> Purpose of Threat Intelligence
> The Intelligence Phases
> Phase 1 | Direction
> Phase 2 | Collection
> Phase 3 | Processing
> Phase 4 | Analysis & Production
> Phase 5 | Dissemination
> Phase 6 | Feedback
> The Threat Intelligence Lifecycle

Day 3 Agenda

> OSSIM Introduction Lab
> The OSSIM Platform
> Asset Discovery
> Vulnerability Assessment
> Intrusion Detection
> Behavioural Menu
> Security Intelligence
> Architecture
> General Preinstall Checklist
> OSSIM Installation Requirements
> Installing OSSIM
> Configure The Network Settings
> Login To The OSSIM Machine
> Setting Date And Time And Time Zone
> Adding Assets
> Scan Local Network
> Update Managed Assets
> Surface, Deep & Dark Web

Day 4 Agenda

> Image dumping tools - lab
> Memory Analysis using Volatility
> RAM Overview
> Volatility Framework
> KDMP - Kernel Debugging Data Block
> PEB - Process Environment Block
> Capturing Volatile Memory
> Volatile Memory Overview
> Memory Dumping Tools
> Volatility Commands

Day 5 Agenda

> Final Scenario