TRUSTWAVE SPIDERLABS TRAINING

# Practical Incident Response

## Introduction

Practical Incident Response is a five-day instructor led course designed for IT staff and/or System Administrators who wish to learn how to effectively identify and handle a cyber security breach. These team members typically have strong information technology skills and experience working in a business computing environment but may be new to investigating information security incidents.

After completing this course, the student will possess the skills needed to successfully conduct a basic cyber security investigation which adheres to a formal methodology and ensures proper evidence collection and preservation. Students will also learn to efficiently process evidence with a variety of free and open source tools and use those results to investigate and clearly describe the incident.

Trustwave SpiderLabs is an industry leader in providing Incident Response to worldwide customers from several industries who have suffered data compromises or security breaches involving APTs, unauthorized access, credit card fraud, data theft, insider threat, and malware outbreaks. This training is based on our experience and has been built and is focused on teaching and demonstrating the various aspects related to developing and building a cyber Security Incident Response capability that works in the real world.

## Learning Objectives

By the end of this course students will be able to:

1. Identify different types of cyber-attacks, describe malware and attack vectors, explain attribution and evaluate the consequences of these attacks.
2. Conduct a network intrusion scope assessment and determine the potential extent of the subsequent investigation.
3. Identify and describe the phases of the investigative process.
4. Identify and evaluate the potential sources of evidence relating to a cyber security incident.
5. Evaluate and use tools needed for forensic data collection (both volatile and non-volatile).
6. Identify and preserve computer-based evidence in a forensically sound manner.
7. Identify and preserve network-based evidence in a forensically sound manner.
8. Analyze memory dumps.
9. Analyze volatile data including, but not limited to, event logs, user account data, open network ports, file and directory lists, open handles and registry hives.
10. Analyze disk images including, but not limited to, MACB timelines, directory listings, hash analysis, keyword searches, signed executables, file packers and more.
11. Correlate multiple sources of evidence to re-construct the incident.
12. Describe the content of an investigation report.

# Course Length

Five days, 8 hours per day, total of 40 hours.

# Intended Audience

This course is designed for anyone who works with computer systems and needs to learn how to effectively identify and handle a cyber security breach.

Examples of strong candidates include:

- SOC Analysts
- Network and Systems Engineers
- Computer Support Specialists
- System Administrators
- Security Specialists

# Prerequisites

There are no formal prerequisites, though prior exposure to the following concepts and skills are recommended:

1. Basic knowledge of computer hardware, network devices and TCP/IP.
2. Experience working with and managing the Microsoft Windows family of operating systems.
3. Familiarity of basic computer security terms and concepts.
4. Comfortable using the Microsoft Windows or Linux command shell.

# Topic Outline

The topics of this course are built around the investigation process of detection, triage, evidence collection, analysis, containment and remediation.

### Course Introduction

- Welcome, instructor and student introductions

### Computer Crimes, Actors and Impacts

- Types of cybercrime
- Malware overview
- Threat actors and organized criminal enterprise
- Attribution

### The Investigative Process

- Overview of the Investigation Process
- Principles of Digital Forensics and Incident Response
- What Makes a Good Investigator?
- Incident Triage

### Forensic Tools and Media Preparation

- Open Source forensic tools
- File systems and their limitations
- Media preparation

## Data Collection and Chain of Custody

- *Live Data Collection*
  - Order of Volatility
  - Windows Memory capture
  - Volatile data capture with TWI
- *Static Data Collection*
  - Disk Imaging
  - *RAID and LVM concerns*
- *Network Data Collection*
  - Sources
  - Methods of preservation
- Triage Imaging
- Chain of Custody

## Live Investigations

- IOC scanning
- EDR tools
- Live system review, including:
  - Process trees
  - Network connections
  - Persistence

## Offline Forensic Analysis - Windows

- Analyzing Windows memory
- Contextual and keyword searches
- Registry analysis
- Event log analysis
- Browser analysis
- Timeline analysis

## The Bigger Picture

- Log analysis and correlation
  - Graphical approaches
  - Text approaches
- Switches\Routers\Firewalls
- SIEM
- NIDS/NIPS
- Enterprise AV
- Web Proxies
- Active Directory Fundamentals

## Report Writing and Review

- Common mistakes
- Being objective
- Being succinct and factual

## Teaching Methodology

The foundation principle of these classes is to ensure that students are able to use the knowledge gained in the real world. In order to ensure this, all theory is applied in practical hands on labs, using open source and free software. This approach ensures that the student is able to apply their learning to their workplace, either using their existing tools, or the ones covered in the class.

Students are provided with sample tools.

## Class Size

Maximum 25 per instructor.

## Materials Provided

To achieve the course objectives, you will learn through instructor-led training, demos and hands-on activities and labs. The course materials used in this course include:

- **Student Guides** – The Student Guide contains all speaking points that the instructor will deliver throughout this course. The headings in the student guide correspond directly to the headings in the Instructor slides to make it easy for you to follow along. Many of the concepts and tools that you will learn about throughout this course are presented graphically to help you better understand the course content. To help you practice and test your knowledge, the following hands-on elements, as appropriate, are included in the Student Guide.
- **Activities** – Modules have paper-based hands-on activities that enable you to check your knowledge of the lesson content.
- **Labs** – Modules have hands-on case-based lab exercises. Each lab identifies high-level tasks to perform as well as step-by-step instruction. More complex labs will be instructor-led.

## Equipment/Software Students Must Furnish:

Students must furnish their own laptop capable of running VMware Workstation 14 or higher on a Windows-based operating system and approximately 100GB of free disk space. While it may be possible to utilize other virtual machine environments or host operating systems, due to class time constraints, instructors will be unable to provide support or assistance in configuring these environments.