TRUSTWAVE SPIDERLABS TRAINING

Advanced Linux Forensics

Introduction

The Advanced Linux Forensics program is a five-day instructor led course designed for law enforcement agents who will be required to acquire and analyze Linux systems as part of their investigations. It is expected that students are familiar with the fundamentals of digital forensics and want to enhance their expertise in dealing with Linux-based systems.

After completing this course, the agent will possess the skills to successfully conduct a Linux investigation that adheres to a formal methodology to ensure the admissibility of evidence in a court of law.

Learning Objectives

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

1. Acquire memory and volatile data from live Linux systems.
2. Analyze memory images of Linux and Unix systems.
3. Identify the risks and benefits of conducting live analysis versus powering down the system.
4. Conduct live and static forensic analysis of Linux systems.
5. Compare the differences between common Linux distributions.
6. Describe the different partition and volume systems frequently used on Linux systems.
7. Analyze common Linux filesystems, including EXT2,3 & 4 and XFS.
8. Analyze the main artefacts of common Linux filesystems.
9. Judge how different user and operation systems actions will change filesystem date time records.
10. Generate timelines of system artifacts.
11. Evaluate how key artefacts can be used to identify user activity.
12. Analyze operating system and application logs in order to describe user activity.
13. Evaluate application logs to detect anomalous activity.
14. Use built-in Linux utilities to conduct analysis.
15. Prioritize analysis steps in sequence most likely to address investigation needs.
16. Compose an analysis report of a Linux system.

Copyright © 2019 Trustwave Holdings, Inc. All rights reserved.

Course Length

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

Prerequisites

Exposure to the following concepts and skills will assist students in completing the course:

- Knowledge of computer hardware and network devices
- Experience working within the Microsoft Windows family of operating systems
- Basic knowledge of Linux operating systems
- Familiarity with fundamental digital forensic tools, techniques, and processes
- Experience conducting forensic analysis of windows operating systems
- Ability to use a hex editor/viewer to decode binary data

Topic Outline

Overview of the Linux Operating System

- Distributions
    - difference between user and server systems
    - Comparison of Redhat and Debian based distributions.
    - Common workstation and server distributions.
- Package management.
- Directory structures.
    - Configuration files
    - Applications
    - Logs
    - User home directories
- Common applications, both user and server.
- Common desktop environments.
- Comparison of Windows and Linux

File Systems and Disk Management

- Volume and partitioning systems.
- EXT filesystems.
- File system temporal analysis.
- Fixed and dynamic volume mounting.
- File permissions.
- Encryption

Evidence Collection and Acquisition

- Memory Acquisition.
- Preservation of Volatile data.
- Live disk imaging.
- Working with cloud-based systems.

Copyright © 2019 Trustwave Holdings, Inc. All rights reserved.

Operating System Artefacts

- Key features of Debian and Redhat configuration and log files
    - Mount points
    - Network configuration
    - Start-up scripts and scheduled jobs
    - Timezone settings
    - User accounts
    - User login (local and remote)
    - USB devices

Services

- ssh
- Webservers
- File shares (nfs & Samba)
- Iptables (firewall)
- Email
- Databases

Userland

- User environments
- User startup
- User activity
    - Editors
    - Command history (bash, sudo)
    - Browsers
    - File managers
    - Email
    - Office suites
    - Cloud shares

Hacking

- Common hacking tools and related artefacts

Teaching Methodology

- Lectures
- Hands-on labs
- Demonstrations

Classroom Environment

This training environment takes advantage of Virtual Machines located on external USB drives. Using this technology, students will engage in hands-on labs and instructor demonstrations of Linux concepts in a “real-world” environment. Each VM is pre-configured to mimic the different Distributions, network environments and user settings that may be encountered in the field.

Class Size

- Minimum 10, Maximum 30.

Copyright © 2019 Trustwave Holdings, Inc. All rights reserved.

- Class size may exceed 30, however additional instructors will be required.

Materials Provided

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

- **Annotated Slides** – Students will be provided with annotated copies of the slides, containing all speaking points that the instructor will deliver throughout the course.
- **Activities** – Modules have paper-based hands-on activities that enable students to check their knowledge of the lesson content.
- **Labs** – Modules have hands-on case-based lab exercises where students use Virtual Machines (VM) to perform technical tasks. Each lab identifies high-level tasks to perform as well as step-by-step instruction. More complex labs will be instructor-led.
- **Job Aids** – The Job Aid guide is comprised of cheat sheets, quick tips and other useful tools that can used on the job.

Equipment/Software Students Must Furnish:

Students must furnish their own laptop running VMware Workstation or Player running on a 64bit operating system. VMWare Workstation version 14 running on a Windows system is preferred. If you do not currently own a copy of VMWare Workstation 14, you can download an evaluation version from www.vmware.com prior to the class. While it is technically feasible to utilize a Linux system running VMWare Workstation or an OS X system running VMWare Fusion, due to time constraints of the class, instructors will not be able to troubleshoot compatibility issues with those systems. Students will be provided an external USB3 hard drive for use during the course. If you wish to copy the course material and virtual machine used during the training, you will need approximately 75G of free space. The USB3 drives must be returned to the course instructor at the completion of the training.

Copyright © 2019 Trustwave Holdings, Inc. All rights reserved.