Digital Media Forensics Essentials Labs

Course: **00076**
Filter: **Beginner**
Duration: **2 days**
Category:: **Gouvernance, Risk and Compliance**
Price: **3000,00 €**

About Course

Learn the security techniques used by the Internet's most skilled professionals. This Digital Media Forensics Essentials lab bundle, which includes 19 distinct, hands-on labs, will provide you with an introduction to media collection, imaging and analysis.

What you'll learn

- Detect, identify, and analyze malicious activityUse detection various tools and tools like Wireshark and Snort to read, capture, and analyze trafficIdentify and remove trojans, malicious files, and/or processes

Pre-requisites

None

Curriculum

Module 1: Analyze Malicious Activity in Memory Using Volatility

- Students will use the open source Volatility tool to analyze a memory snapshot and determine what malicious software has infected the victim machine

Module 2: Conduct Log Analysis and Cross Examination for False Positives

- Students will confirm the validity of event-data analysis to eliminate false-positive events.

Module 3: Creating a Baseline Using the Windows Forensic Toolchest (WFT)

- Students will run Windows Forensic Toolchest against an existing system to create a baseline that will be used for future analysis.

Module 4: Data Recovery with Autopsy

- Students will ingest and process a previously acquired forensic image using Autopsy. The focus of the lab will be on recovering data from the image, reviewing the supplied forensic report and verifying that the image is forensically sound.

Module 5: Detect the Introduction and Execution of Malicious Activity

- In this lab, the student will simulate browsing and downloading a malicious file from a website then learn how to detect the introduction and executions of malicious activity on a Win7 machine

Module 6: Dynamic Malware Analysis Capstone

- Students will use utilize two virtual machines, inside a protected network, to observe configuration changes on a known good / clean system and all of the unusual network traffic generated by the suspect software they will be analyzing.

Module 7: Identify Access to a LINUX Firewall Through SYSLOG Service

- Students will identify access to a PFSENSE firewall through the forwarding of SYSLOG (System logs) from a Firewall to the SYSLOG service we have configured and set up on the Network. Students will then identify malicious activity through system logs.

Module 8: Identify and Remove Trojan Using Various Tools

- Students will detect malicious files and processes using various tools. Students will then remove the malicious files and/or processes.

Module 9: Identify Suspicious Information in VM Snapshots

- Students will identify known IOCs for Stuxnet and save them for analysis. Students will then identify malicious drivers associated with the malware, and identify AES keys in memory

Module 10: Identify Whether High-Risk Systems Were Affected

- The highest risk systems are the ones with Internet facing Applications. One an attacker from the Internet is able to compromise the internal network, then it is very likely they will attempt to move to other machines on the network.

Module 11: Image Forensics Capstone

- Students will create a live image using FTK Imager and verify that the image was created successfully.

Module 12: Live Imaging with FTK Imager Lite

- Students will use FTK Imager Lite to create a forensic image of a Windows 8 workstation. After they create the image they will perform a hash check to ensure that the image that was created is the same as what is currently running on the live system.

Module 13: Memory Extraction and Analysis

- This is one of the labs for the Advanced Digital Media Forensics class.

Module 14: Network Miner

- This lab exercise is designed to allow the trainee to become familiar with using Network Miner.

Module 15: Open Source Password Cracking

- Students will use John the Ripper and Cain and Abel to crack password protected files.

Module 16: Participate in Attack Analysis Using Trusted Tool Set

- Students will participate in attack analysis/incident response, including root cause determination, to identify vulnerabilities exploited, vector/source and methods used (e.g., malware, denial of service).

Module 17: Using Snort and Wireshark to Analyze Traffic

- In this lab we will replicate the need for Analysts to be able to analyze network traffic and detect suspicious activity. Tools like Wireshark and Snort can be utilized to read, capture, and analyze traffic.