Systems Security Professional Essentials Labs

Course: **00111**
Filter: **Beginner**
Duration: **3 days**
Category:: **Cyber Security**
Price: **2800,00 €**

About Course

Learn the security techniques used by the Internet's most skilled professionals. This Systems Security Essentials lab bundle, which includes 32 distinct, hands-on labs, will prepare you with the essential principles of risk management, network security, identity and access management, security operations and more.

What you'll learn

- Practice the objectives presented in the (ISC)2 Certified Information Systems Security Professional certification
- Identify whether high-risk systems have been affected by an attack
- Identifier si les systèmes à haut risque ont été affectés lors d'une attaque
- Analyze, update and perform gap analysis on a sample of BCP/BIA/DRP/CIRP

Pre-requisites

- None

Curriculum

Module 1: Analyze and Update a Company BCP/BIA/DRP/CIRP

- Students will become familiar with the Business Continuity Plan (BCP), Business Impact Assessment (BIA), Disaster Recovery Plan (DRP) and Computer Incident Response Plan (CIRP).

Module 2: Analyze SQL Injection Attack

- Students will Identify the use of an SQL Injection through the use of Wireshark. The students will also isolate the different aspects of the SQL Injection and execute the selected code.

Module 3: Analyze Structured Exception Handler Buffer Overflow Exploit

- Students will identify the use of a Buffer Overflow exploit through the use of Wireshark and by analyzing items found in the captured traffic. The students will also find the exploit code and isolate the different aspects of a Buffer Overflow exploit.

Module 4: Applying Filters to TCPDump and Wireshark

- This lab exercise is designed to allow the trainee to become familiar with applying a capture filter to TCPDump and Wireshark using Berkley Packet Filter (BPF) syntax.

Module 5: Baseline Systems in Accordance with Policy Documentation

- Students are provided a whitelist of applications allowed for installation on a system. Students will compare the list against multiple hosts and remove the installed applications which are not on the list.

Module 6: 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 7: Creating a List of Installed Programs, Services and User Accounts from a WIN2K12 Server

- Students will create a list of installed programs, services, and accounts in a Windows 2012 server environment using various tools and methods.

Module 8: Creating a Secondary Baseline and Conducting Comparison

- Students will create a second baseline using the Window Forensic Toolchest (WFT) and compare it against a previously created baseline using KDiff3.

Module 9: Creation of Standard Operating Procedures for Recovery

- Students will have access to the results of a vulnerability scan run again a sample Windows 2008 Server. They will perform any necessary remediations to the server by applying a variety of patches

Module 10: Data Backup and Recovery

- Firewall Setup and Configuration In this lab you will perform the steps necessary to set up a pfSense fi

Module 11: Firewall Setup and Configuration

- In this lab you will perform the steps necessary to set up a pfSense firewall from the basic command line interface and then configure the firewall using the web configuration GUI on a Windows machine.

Module 12: 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 13: Identify Whether High-Risk Systems Were Affected

- Identify Whether High-Risk Systems Were Affected

Module 14: Identifying System Vulnerabilities with OpenVAS

- Students will scan a system in OpenVAS (Open Vulnerability Assessment) to discover and identify systems on the network that have vulnerabilities.

Module 15: IDS Setup

-

Module 16: Implementing Least-Privilege on Windows

- Least-privilege is an important concept across many domains (e.g., Windows server/workstation management, networking, Linux management, etc.) and requires great discipline to implement properly.

Module 17: Linux Users and Groups

- In this lab students will use command line tools to create, modify, and manage users and groups within the Linux operating environment.

Module 18: Log Correlation & Analysis to Identify Potential IOC

- When defending networked digital systems, attention must be paid to the logging mechanisms set in place to detect suspicious behavior.

Module 19: Manual Vulnerability Assessments

- Students will learn how to conduct manual scanning against systems using command line tools such as Netcat then they will login to a discovered system and enable object access verify that auditing to the object is enabled.

Module 20: Manually Analyze Malicious PDF Documents

- Several company employees have received unsolicited emails with suspicious pdf attachments. The CIO has asked you to look at the attachments and see if they are malicious.

Module 21: Manually Analyze Malicious PDF Documents 2

- Several company employees have received unsolicited emails with suspicious pdf attachments. The CIO has asked you to look at the attachments and see if they are malicious.

Module 22: Microsoft Baseline Security Analyzer

- In this lab you will use Microsoft Baseline Security Analyzer (MBSA) to perform scans of individual host computers and of groups of computers.

Module 23: Monitoring and Verifying Management Systems

- Students will analyze a MBSA Baseline report and compare it to current system configurations.

Module 24: Monitoring Network Traffic for Potential IOA/IOC

- In this lab we will replicate potentially malicious scans from the Internet against a corporate asset.

Module 25: Network Segmentation (FW/DMZ/WAN/LAN)

- In this lab we will take the concept of zones and create three zones and route traffic accordingly. We will have the trusted zones ZONE - LAN which will be the internal Local Area Network.

Module 26: Parse Files Out of Network Traffic

- This lab teach students how to extract various files from network traffic using Network Miner and Wireshark.

Module 27: Patch Installation and Validation Testing

- Students will identify if a vulnerability is present on two Windows systems and then move to remediate the vulnerability, if necessary.

Module 28: Performing Incident Response in a Windows Environment

- This next lab walks students through identifying a security incident, as well as handling and then responding to the incident.

Module 29: Scanning and Mapping Networks

- Students will use Zenmap to scan a network segment in order to create an updated network map and detail findings on the systems discovered.

Module 30: Securing Linux for System Administrators

- Linux environments are ubiquitous in many different sectors, and securing these environments is as important as securing Windows environments

Module 31: Use pfTop to Analyze Network Traffic

- Students will use pfTop, a network traffic monitoring/statistics plugin used in pfSense, to analyze and monitor network traffic.

Module 32: Vulnerability Identification and Remediation

- Learners will use Nmap and OpenVAS/Greenbone Vulnerability Scanner to confirm old vulnerable systems and to also discover new ones.