Security Essentials Labs

Course: **00108**
Filter: **Beginner**
Duration: **2 days**
Category:: **Systems & Network Security**
Price: **1500,00 €**

About Course

Learn the security techniques used by the Internet's most skilled professionals. This Security Essentials lab bundle, which includes 19 distinct, hands-on labs, will prepare you with the essential principles of network security and risk management.

What you'll learn

- Practice the objectives presented in the CompTIA's Security+ certificationAnalyze, update, and perform a gap analysis on a sample BCP/BIA/DRPPerform a backup in a server environmentFacilitate open source collection by using intimate network discovery techniques

Pre-requisites

- None

Curriculum

Module 1: BCP DRP and Test Planning

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

-). During the course of the lab, students will perform a gap analysis on the provided BCP, BIAs and DRP, and make the necessary fixes to those documents
- . After revising the previous documents the students will create a test for the covered assets, procedures and personnel

Module 2: BitLocker Setup

- This lab shows the student how to setup BitLocker on a Windows 8.1 Professional system.
- Block Incoming Traffic on Known Port
- In this lab, the student will respond to an incident by blocking incoming traffic on a known port from a specific IP. Comparing Controls
- Students will evaluate policies in place on a domain and apply those policies in accordance to organizational standards.

Module 3: 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 4: Creation of BCP and DRP

- Students will be required to create two documents: a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP).

Module 5: Data Backup to Prep for Recovery

- In this lab we will simulate the recovery phase where we must perform a backup in a server environment.
- Event Log Collection
- In this lab you will use Splunk Enterprise to ingest logs from a local host for analysis

Module 6: Host Data Integrity Baselining

- This lab takes the trainee into basic concepts regarding establishing baselines of files and directories with Kali Linux and Windows 7.

Module 7: Installing Patches and Testing Software

- Students will identify if a vulnerability is present in the systems and remediate the vulnerability if necessary

Module 8: Network Discovery

- The Network Discovery lab is designed to help students facilitate open source collection by teaching them how to use more intimate network discovery techniques.

Module 9: 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 10: Network Topology Generation

- Students will utilize Zenmap to generate a visual network topology.

Module 11: Open Source Collection

- The Open Source Collection lab is designed to familiarize students with the advanced functionality of Google, default webpages used for web-servers, and the specifics of Google Hacking database.

Module 12: Open Source Password Cracking

- Students will use John the Ripper and Cain and Abel to crack password protected files
- 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 13: Scanning from Windows

- Students will leverage Scalnline, a windows network discovery and mapping tool, to identify the systems on a network of responsibility.

Module 14: Windows Event Log Manipulation via Windows Event Viewer

- In this lab you will use Windows Event Viewer to view and filter the security event log on a Windows 7 client computer specifically for account logons.

Module 15: Wireshark

- This lab exercise is designed to allow the trainee become familiar with the use of Wireshark.