Ethical Hacking Essentials Labs

Course: **00083**
Filter: **Beginner**
Duration: **20 hours**
Category:: **Data Privacy**
Price: **3000,00 €**

About Course

Learn the hacking techniques used by the Internet's most skilled professionals. This Ethical Hacking Essentials lab bundle, which includes 22 distinct, hands-on labs, will prepare you to exploit networks in the manner of an attacker in order to discover how protect the system from them, ensuring you're ready to fill the role of an ethical hacker.

What you'll learn

- Practice the objectives presented in the EC-Council's Certified Ethical Hacker certificationExploit networks like an attacker and discover how protect the system from themDetermine the type of attack used and pinpoint exploit code in network trafficLeverage network and discovery mapping tools to identify systems on a network

Pre-requisites

None

Curriculum

Module 1: Scanning Options

- Students will leverage Nmap, a network discovery and mapping tool, to identify the systems on a network of responsibility. Students will utilize non-traditional scans to attempt avoiding an Intrusion Detection System (IDS).

Module 2: Analyze Browser-Based Heap Spray Attack

- Students will identify a browser-based attack used against a corporate asset using a network protocol analyzer. Students will determine the type of attack used and pinpoint exploit code in network traffic.

Module 3: 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 4: Analyze Various Data Sources to Confirm Suspected Infection

- Students will review network traffic to confirm the presence of malicious activity using various tools including Wireshark and VirusTotal.com.

Module 5: Automated Vulnerability Assessments

- Students will use Core Impact to conduct an automated vulnerability scan of specific systems in order to identify potential threat vectors.

Module 6: Automated Vulnerability Assessments

- Students will use Core Impact to conduct an automated vulnerability scan of specific systems in order to identify potential threat vectors.

Module 7: Core Impact Web Application Penetration Testing

- This lab introduces students to the web application penetration testing suite within the Core Impact application.

Module 8: 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 9: 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 10: Creating Recommendations Based on Vulnerability Assessments

- Students will use nmap and OpenVAS / Greenbone Vulnerability Scanner to confirm old vulnerable systems and discover new ones.

Module 11: Cybersecurity Testing with Core Impact

- Students will use Core Impact to enumerate a LAN and determine any vulnerable virtual machines through the use of a vulnerability scan.

Module 12: DNS as a Remote Shell

- This lab exercise is designed to allow the trainee to become familiar with recognizing remote shells that operate using well known ports such as DNS.

Module 13: 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 14: 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 15: 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 16: 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 17: Open Source Password Cracking

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

Module 18: Preliminary Scanning

- Students will utilize Nmap, a network discovery and mapping tool, to identify the systems on a network of responsibility.

Module 19: Scanning from Windows

- Students will leverage Scalnline, a windows network discovery and mapping tool, to identify the systems on a network of responsibility. Students will utilize non-traditional scans to attempt avoiding an Intrusion Detection System (IDS).

Module 20: Vulnerability Scan Analysis

- Students will run a Core Impact or Nessus Scan and identify vulnerabilities. Students will then view the report and prioritize vulnerabilities according to risk.

Module 21: Vulnerability Scanner Set-up and Configuration

- Students will setup and configure Core Impact in preparation of a vulnerability scan against an internal network.

Module 22: Vulnerability Scanner Set-up and Configuration, Pt. 2

- Students will utilize OpenVAS to identify hosts on a network and assess their vulnerabilities