Business & IT Center
Tel: +961 (0)1 362 289
Mob:+961 (0)3 615 786

www.bitc-edu.com
info@bitc-edu.com

Course Outline: Penetration Tester Course

Duration: 4 days

Price: 1,500 USD

Prerequisites: Basic knowledge of Windows and Linux

Who should attend:

This course will provide students with basic to intermediate knowledge in Ethical Hacking and Penetration Testing, significantly benefiting any professional who is involved in the area of Information Security as well as new individuals wanting to begin a career in IT Security.

Overview

This course teaches the fundamentals of penetration testing and will illustrate how to think like an attacker and use industry standard tools to perform penetration testing. The course is aligned with the CREST CRT technical syllabus.

Students will learn and perform the different phases of penetration testing assessments. The students will practice using Kali Linux and its tools to perform information gathering, target discovery and enumeration, Vulnerability mapping, social engineering, system exploitation, privilege escalation, and maintaining access to compromised systems. The students will also learn to report the results of their assessments.

What is included:

- eBook
- Lab Guide
- 6 months 24x7 remote access to a virtual lab
- 2 exam vouchers (Theoretical & Practical Exam)
- Online Exam Proctoring
- Certificate of Attendance (Digital)

Outline:

Module 1: Introduction to Pen Testing

- The need for Pen Testing
- Methodology of Pen Testing
- Ethics and Compliance to Legal Systems

Module 2: Pen Testing Engagement Lifecycle

- Pen Testing Scope and Boundaries

Business & IT Center
Tel: +961 (0)1 362 289
Mob:+961 (0)3 615 786

www.bitc-edu.com
info@bitc-edu.com

Module 3: The Basics

- Networking Concepts
- Operating System Security
- Application Layer Protocols
- Cryptography Concepts Review
- Wireless and Database Concepts Review

Module 4: Information Gathering & Social Engineering

- Creating USB Payloads for Social Engineering Attacks
- Gathering DNS Registration Information
- Gathering Router, Firewall and IPS Information
- Gathering Email Addresses from Public and Social Websites
- Reading Metadata of Files Revealing Target Information
- Hiding Attacks Using Onion Routing Network

Module 5: Target Discovery Fingerprinting & Enumeration

- Discovering the Operating System Details
- Port and Services Discovery using NMAP

Module 6: Vulnerability Mapping

- Understanding Vulnerability Taxonomy
- Discovering and Analyzing Weaknesses

Module 7: Target Exploitation & Privilege Escalation

- Escalation for Windows and Linux
- Choosing Attack Vectors
- Performing Local and Remote Attacks
- Gathering and Cracking Password Hashes using Mimikatz and John the Ripper
- Attacking a Target through a Compromised Target (Pivoting)
- Creating Man In The Middle Attacks through Spoofing
- Sniffing Authentication Packets Revealing Passwords
- Cracking Default Passwords with Password Lists and Rainbow Tables

Module 8: Maintaining Access & Covering Tracks

- Creating Metasploit Backdoor Payloads
- Antivirus, Firewall, and IPS Evasion Techniques

Module 9: Web Pen Testing & Database Injection

- Bypassing Authentication using Cross Site Scripting
- Revealing User Accounts and Passwords through Database Injection

Module 10: Documentation, Reporting & Presentation

- Writing Pen Testing Reports

Business & IT Center
Tel: +961 (0)1 362 289
Mob:+961 (0)3 615 786

www.bitc-edu.com
info@bitc-edu.com

Examination & Certification:

- The ICSI|CPTA Certified Penetration Tester Associate certification exam covers theoretical material from all 10 modules and mainly consists of 100 Multiple Choice Questions test.
- The exam duration is 2 hours.
- Passing Grade = 60%.

- The ICSI|CPT Certified Penetration Tester certification exam covers Hands-On material from all 10 modules and mainly consists of 40 Fill in the Blanks and Multiple Choice Questions test with access to a Controlled Online Lab Environment.
- The exam duration is 4 hours.
- Passing Grade = 70%.