



AFRICAN ADVANCED LEVEL TELECOMMUNICATIONS INSTITUTE (AFRALTI)

TRAINING PROGRAM BROCHURE

Title: Penetration Testing
Duration: 5 Days (8.00am - 5.00pm)
Delivery: Face-to-face Training

Course Overview:

Target Audience:

This course will significantly benefit security officers, auditors, security professionals, site administrators, penetration testers, and anyone who is concerned about the integrity of the information systems.

Pre-requisites:

The participants are required to have some good understanding of information security principles.

Value Proposition

With the proliferation of attacks even on highly secure systems, today, there is no single system that is 100% secure. This is made possible by the availability of the myriad number of tools and applications that can be used to launch an attack without requiring much sophistication.

For security professionals to be in a position to mitigate and counter these attacks and reduce the associated business risks, they need a deep understanding of how these attacks are launched. This course arms the learner with the skills needed to turn them into ethical hackers who can guard the business organization against external and internal attacks.

Training Methodology:

The curriculum consists of instructor-led training practical lessons. Students will be provided with security related resources and all tools required to perform a successful penetration testing.

MAIN COURSE TOPICS

The trainers learn how to perform advanced techniques and attacks to identify SQL injection, Cross site scripting (XSS), LFI, RFI vulnerabilities in web applications. The following topics will be covered during the five days of intensive training:

1. Introduction to Vulnerability Assessment and Penetration Testing
2. Information Gathering Methodology
3. Scanning and Enumeration
4. Identify Vulnerabilities
5. Exploitation
6. Post Exploitation
7. Preparing a Report

LAB ACTIVITIES

This training is lab intensive and all lab activities will be completed in an advanced security and hacking lab environment.

Key Focus Areas

1. New Attack Vectors
2. Focus on Mobile Platforms and Tablet Computers Hacking
3. State of the Art Integrated Labs
4. Advanced Lab Environment
5. Latest Operating Environment includes Windows Server 2016,2012,2008, Windows 8/10, Linux OS, Kali Linux OS.

Expert Instructors and Accreditation

The course is conducted by experienced information system security specialists who possess the EC-Council's Certified Ethical Hackers (CEH) certification and are also Certified CEH Instructors. AFRALTI is an EC-Council Accredited Training Center (ATC)

For more information, please contact us on
Tel: +254 710 207 061, +254 733 444 421, +
training@afralti.org or info@afralti.org
www.afralti.org