AFRICAN ADVANCED LEVEL TELECOMMUNICATIONS INSTITUTE (AFRALTI)

TRAINING PROGRAM BROCHURE

Title:	**Certified Ethical Hacker (CEH) Version 10**
Duration:	**5 Days (8.00am - 5.00pm)**
Venue:	**AFRALTI, Nairobi, Kenya**
Fees:	**Inclusive of Training, Official Courseware, Exam Voucher**

Course Overview:

This course is a comprehensive ethical hacking and information systems security assessment program focusing on latest security threats, advanced attack vectors and practical real time demonstration of latest hacking techniques, methodologies, tools, tricks and security measures.

The course also focuses on the latest hacking attacks targeted to mobile platform and tablet computers and covers countermeasures to secure mobile infrastructure. It addresses latest development in mobile and web technologies including Andriod OS 4.1 and Apps, iOS 6 and Apps, BlackBerry 7 OS, Windows Phone 8 and HTML 5.

When a student leaves this intensive 5-day class they will have hands on understanding and experience in Ethical Hacking. This course prepares you for EC-Council Certified Ethical Hacker exam.

This course is recognized by National Security Agency (NSA) and the Committee on National Security Systems (CNSS). The course is also accredited by ANSI and is compliant with National Initiative For Cybersecurity Education (NICE).

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.

Prior to attending this course, you will be asked to sign an agreement stating that you will not use the newly acquired advanced hacking skills for illegal or malicious attacks and you will not use such tools in an attempt to compromise any computer system.

Value Proposition

This course delivered through our partnership with the EC-Council – the architects of the Ethical Hacking certification, promises to create ethical hackers who understand all security vulnerabilities and how to mitigate the associated risks. This training is delivered by certified Ethical Hackers who are also qualified CISA-ISACA auditors and CCNP certified.

Pain Point

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 covering both theory and practical lessons. Students will be provided with security related resources and all tools required to perform a successful ethical hacking.

It is conducted using courseware developed by subject matter experts from all over the world and constantly updated to ensure that the students are exposed to the latest advances in the hacking/security space. Students practice various hacking techniques in a real time and simulated environment.

Students will receive the following:

- Official EC-Council Course Materials
- Exam Voucher for the CEH Certification - Exam code 312-50
- Gigabytes of the most effective Hacking and Security tools

MAIN COURSE TOPICS

The following topics inclusive of theory and labs will be covered during the five days of intensive training:

1. Introduction to Ethical Hacking - Key issues plaguing the information security world, incident management process, and penetration testing
2. Footprinting and Reconnaissance - Various types of footprinting, footprinting tools, and countermeasures
3. Network scanning techniques and scanning countermeasures
4. Enumeration techniques and enumeration countermeasures
5. Vulnerability Analysis - identify security loopholes in the target organization’s network, communication infrastructure, and end systems. This module covers the vulnerability management life cycle, and various approaches and tools.
6. System hacking methodology, steganography, steganalysis attacks, and covering tracks
7. Malware Threats - Different types of Trojans, Trojan analysis, and Trojan countermeasures, Working of viruses, virus analysis, computer worms, malware

analysis procedure, and countermeasures; Ransomware, banking and financial malware, IoT botnets, Android malwares etc.

8. Packet sniffing techniques and how to defend against sniffing
9. Social Engineering techniques, identify theft, and social engineering countermeasures
10. DoS/DDoS attack techniques, botnets, DDoS attack tools, and DoS/DDoS countermeasures
11. Session hijacking techniques and countermeasures
12. Evading Firewall, IDSs, and Honeypots - evasion techniques, evasion tools, and countermeasures
13. Different types of webserver attacks, attack methodology, and countermeasures
14. Hacking Web Applications - Different types of web application attacks, web application hacking methodology, and countermeasures
15. SQL injection attacks and injection detection tools
16. Hacking Wireless Networks - Wireless Encryption, wireless hacking methodology, wireless hacking tools, and wi-fi security tools
17. Hacking Mobile Platforms - Mobile platform attack vector, android vulnerabilities, jailbreaking iOS, windows phone 8 vulnerabilities, mobile security guidelines, and tools
18. IoT Hacking - Understand the potential threats to IoT platforms and learn how to defend IoT services securely.
19. Cloud Computing - Various cloud computing concepts, threats, attacks, and security techniques and tools
20. Cryptography - Different types of cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools

LAB ACTIVITIES

More than 40 percent of class time is dedicated to the learning of practical skills and this is achieved through EC-Council labs. Theory to practice ratio for C|EH program is 60:40 providing students with a hands-on experience of the latest hacking techniques, methodologies, tools, tricks, etc.

The C|EH v10 course includes a library of tools that is required by security practitioners and pentesters to find and uncover vulnerabilities across different operation platforms. This provides a wider option to students than any other programs in the market.

Students can also purchase separately the C|EH integrated labs (iLabs) to emphasize the learning objectives. The iLabs provides additional labs that students can practice post training on their own time

Key Focus Areas

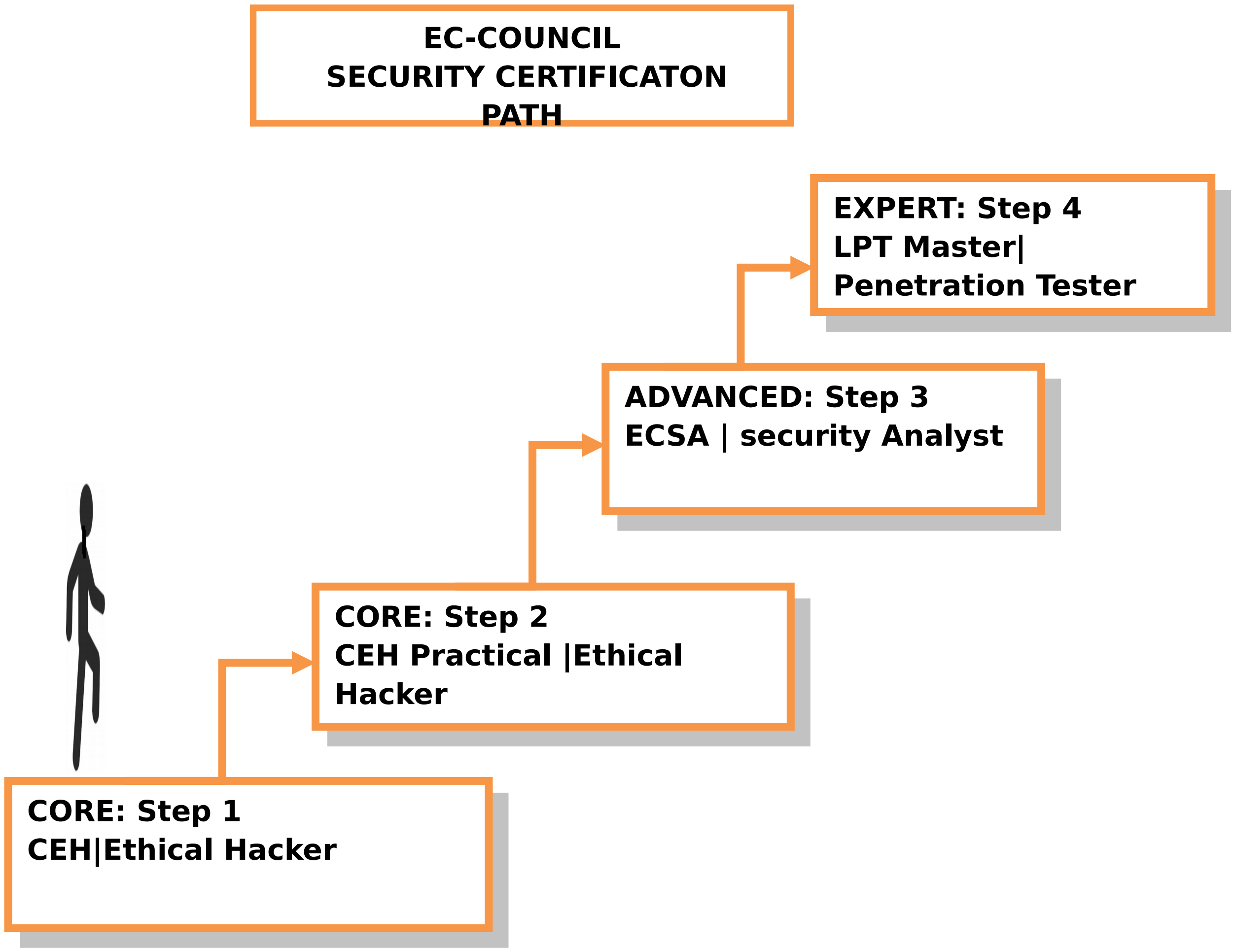
1. Hacking IoT Systems
2. Vulnerability Analysis
3. New Attack Vectors
4. Focus on Mobile Platforms and Tablet Computers Hacking
5. State of the Art Integrated Labs
6. Advanced Lab Environment

7. Latest Operating Environment includes Windows Server 2016, Windows 8/10, Linux OS, Kali Linux OS, Visual Content Technology

Expert Instructors and Accreditation
The course in conducted by experienced information system security specialists who possess the Certified EC-Council Instructor (CEI) certification and are also Certified CEH and ECSA Certified Instructors.

AFRALTI is an EC-Council Accredited Training Centre (ATC) and all the EC-Council certifications are taken at the centre.

Recommended Certification path at AFRALTI



EC-COUNCIL
SECURITY CERTIFICATON
PATH

EXPERT: Step 4
LPT Master|
Penetration Tester

ADVANCED: Step 3
ECSA | security Analyst

CORE: Step 2
CEH Practical |Ethical Hacker

CORE: Step 1
CEH|Ethical Hacker

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