

## Certified Ethical Hacker



### Course Description:

The Certified Ethical Hacker (CEH) program is the core of the most desired information security training system any information security professional will ever want to be in. The CEH, is the first part of a 3 part EC-Council Information Security Track which helps you master hacking technologies. You will become a hacker, but an ethical one!

As the security mindset in any organization must not be limited to the silos of a certain vendor, technologies or pieces of equipment,

This course was designed to provide you with the tools and techniques used by hackers and information security professionals alike to break into an organization. As we put it, “To beat a hacker, you need to think like a hacker”. This course will immerse you into the Hacker Mindset so that you will be able to defend against future attacks. It puts you in the driver’s seat of a hands-on environment with a systematic ethical hacking process.

Here, you will be exposed to an entirely different way of achieving optimal information security posture in their organization; by hacking it! You will scan, test, hack and secure your own systems. You will be thought the Five Phases of Ethical Hacking and thought how you can

approach your target and succeed at breaking in every time! The five phases include Reconnaissance, Gaining Access, Enumeration, Maintaining Access, and covering your tracks.

The tools and techniques in each of these five phases are provided in detail in an encyclopedic approach to help you identify when an attack has been used against your own targets. Why then is this training called the Certified Ethical Hacker Course? This is because by using the same techniques as the bad guys, you can assess the security posture of an organization with the same approach these malicious hackers use, identify weaknesses and fix the problems before they are identified by the enemy, causing what could potentially be a catastrophic damage to your respective organization.

Throughout the CEH course, you will be immersed in a hacker's mindset, evaluating not just logical, but physical security.

## **Course Prerequisites:**

Prior experience or knowledge of Networking and programming.

## **Target Audience:**

This course is specially designed for the B.Tech /B.E(CSE/IT/EEE/ECE/Mech) and all other IT related Graduates and Post Graduate students. Mission Professionalism has conquered the job scenario and companies seek for well qualified, professional and skilled manpower. Quality Education and Performance Oriented Training is our motto.

## **What Student/Professionals Will Learn?**

- Identify any and all networks they will test
- Learning how exploits evolve
- Detail the testing interval
- Gather Information Intelligence
- Find Security Vulnerabilities
- Develop Exploits
- Scan and Produce Vulnerability Assessments
- Learn Network Attacking Techniques

## **COURSE-CONTENT**

- 1. Introduction to Ethical Hacking**
- 2. Foot printing and Reconnaissance**
- 3. Scanning Networks**
- 4. Enumeration**
- 5. System Hacking**
- 6. Malware Threats**
- 7. Sniffing**
- 8. Social Engineering**
- 9. Denial of Service**
- 10. Session Hijacking**
- 11. Hacking Web Servers**
- 12. Hacking Web Applications**
- 13. SQL Injection**
- 14. Hacking Wireless Networks**
- 15. Hacking Mobile Platforms**
- 16. Evading IDS, Firewalls, and Honeypots**
- 17. Cloud Computing**
- 18. Cryptography**

## **INTEGER Innovation will provide:**

- Training Slides taught during training by trainers
- Programmatic Examples
- Assignments of each topic in a module
- Demos executed during training session.
- Software's and installation guide (for future help)
- E-books for further reading in depth
- Reference links
- 24X7 online support for any queries or doubts.