**Certified Ethical Hacker**



**Certified Ethical Hacker**

**Course Objective**

* Describe how perimeter defenses function by ethically scanning and attacking networks
* Conduct information systems security audits by understanding the latest security threats, advanced attack vectors, hacking techniques, methodologies and security measures
* Identify intruders, understand how they escalate privileges, and take the necessary steps to secure a system
* Conduct vulnerability assessments, risk assessments, penetration testing, and system protection measures
* Create policies and apply countermeasures against social engineering, Distributed Denial-of Service (DDoS) attacks, buffer overflows, and virus creation
* Apply countermeasures to secure mobile infrastructure against the attacks to mobile platforms and tablet computers

**Target Audience**

* IT professionals, security professionals, auditors, site administrators, general management and anyone tasked with managing and protecting the integrity of the network infrastructure. This also includes anyone already familiar and involved with IT/Cyber/Digital Security and seeking to build on their fundamental principles of security. This course will also prepare professionals wishing to take the EC-Council ANSI accredited Certified Ethical Hacker exam 312-50.

**Course Outline**

**Day 1**

* Introduction to Ethical Hacking
* Short History of hacking
* Current developments
* Evolution and growth
* What is an “Ethical” Hacker
* Types of hackers

**Day 2**

* Hacking methodologies
* Key issues plaguing the information security world
* Penetration testing
* System fundamentals
* Incident management processes
* Identifying the systems at risk
* Wireless networking
* Mobile platform security guidelines
* Mobile platform security tools

**Day 3**

* Web servers
* Web applications
* Footprinting tools
* Footprinting reconnaissance
* Scanning networks
* Enumeration of services
* System hacking techniques and countermeasures
* Types of Trojans
* Working of viruses
* Computer worms
* Covert channels
* Sniffers
* Social engineering

**Day 4**

* Denial of Service (DoS)
* Cryptography
* Public Key Infrastructure (PKI)
* Cryptanalysis tools
* Hacking your own system
* Gaining access to a system
* Session hijacking
* Wireless hacking tools

**Day 5**

* Hacking mobile platforms
* Structured Query Language (SQL) injection
* Evading an Intrusion Detection System (IDS)
* Firewalls
* Honeypots
* Penetration testing
* Types of penetration testing
* Vulnerability assessment
* Penetration testing roadmap
* **The Feature Of Asia Master Training And Development Center**
* we pick up the customer from the airport to the hotel.
* we give the participant training bag includes all the necessary tools for the course.
* Working within groups to achieve the best results.
* All our courses are confirmed and we do not postpone or cancel the courses regardless of the number of participants in the course.
* We can assist you in booking hotels at discounted prices if you wish to book through us.
* We offer the certificate from Asia Masters Center for Training and Administrative Development.

The Cost Of The Training Program Includes The Following:

1. Scientific article on flash memory.
2. Training Room.
3. Training.
4. Coffee break.
5. The training bag includes all the tools for the course.

|  |
| --- |
| Price (USD) |
| Communicate with the training department  to know the participation fees   * There are offers and discounts for groups |
| The details of the bank account |
| Bank name: CIMB Bank Berhad  Account name: Asia Masters Center SDN. BHD  Bank account number: 80-0733590-5  Swift code: CIBBMYKL  IBAN: Null |