



Online Certified Ethical Hacker Course

100 Hours / 6 Months

Course Description

Are you interested in network security and information technology—but perhaps want more of a challenge than typical IT provides? If so, ethical hacking certification is a unique way to set yourself apart from other IT professionals and add more value to your organization. As a certified ethical hacker, you'll use the same techniques as the bad guys to assess security and identify weaknesses, except you'll use these hacking powers for good because to beat a hacker, you need to think like a hacker.

This course will immerse you into the hacker mindset, putting you in the driver's seat of hands-on activities. You will scan, test, hack, and secure your own systems. You will learn the five phases of ethical hacking (reconnaissance, gaining access, enumeration, maintaining access, and covering your tracks) and the ways to approach your target and succeed at breaking in every time.

This course provides you with advanced hacking tools and techniques so that you can assess the security posture of an organization with the same approach these malicious hackers use. You'll be able to identify weaknesses and fix the problems before they are identified by the enemy, preventing what could potentially be catastrophic damage to your organization. This is sure to help you get ahead in your current and future positions.

Upon completion of this course, you will be prepared to sit for the Certified Ethical Hacker Exam 312-50, offered by EC-Council. This course also includes a voucher which covers the fee of the exam.

Hardware Requirements

- This course can be taken on either a PC or Mac.

Software Requirements

- PC: Windows 8 or later.
- Mac: OS X Yosemite 10.10 or later.
- Browser: The latest version of Google Chrome or Mozilla Firefox are preferred. Microsoft Edge and Safari are also compatible.
- Adobe Flash Player. [Click here](#) to download the Flash Player.
- Adobe Acrobat Reader. [Click here](#) to download the Acrobat Reader.
- All software must be installed and fully operational before the course begins.
- Email capabilities and access to a personal email.

Prerequisites

There are no mandatory prerequisites prior to taking Certified Ethical Hacker (CEH). However, students must have a very strong knowledge of network infrastructure, computer hardware, software and security.

Course Outline

MODULE	TOPICS COVERED
1: Certified Ethical Hacking	<ul style="list-style-type: none"> Key issues plaguing the information security world Incident Management Process Penetration Testing
2: Footprinting and Reconnaissance	<ul style="list-style-type: none"> Various types of footprinting Footprinting tools Countermeasures
3: Scanning Networks	<ul style="list-style-type: none"> Network scanning techniques Scanning countermeasures
4: Enumeration	<ul style="list-style-type: none"> Enumeration techniques Enumeration countermeasures
5: System Hacking	<ul style="list-style-type: none"> System hacking methodology Steganography Steganalysis Attacks and covering tracks
6: Malware Threats	<ul style="list-style-type: none"> Different types of Trojans Trojan Analysis Trojan Countermeasures Working of Viruses Virus Analysis Computer Worms Malware Analysis Procedure
7: Evading IDS, Firewalls and Honeypots	<ul style="list-style-type: none"> Firewall IDS and Honeypot Evasion Techniques Evasion Tools Countermeasures
8: Sniffing	<ul style="list-style-type: none"> Packet sniffing techniques How to defend against sniffing
9: Social Engineering	<ul style="list-style-type: none"> Social Engineering techniques Identify theft Social Engineering Countermeasures
10: Denial of Service	<ul style="list-style-type: none"> DoS/DDoS attack techniques Botnets DDoS attack tools DoS/DDoS Countermeasures
11: Session Hijacking	<ul style="list-style-type: none"> Session hijacking techniques Countermeasures
12: Hacking Web Servers	<ul style="list-style-type: none"> Different types of webserver attacks Attack methodology Countermeasures
13: Hacking Web Applications	<ul style="list-style-type: none"> Different types of web application attacks Web Application Hacking Methodology

	<ul style="list-style-type: none"> Countermeasures
14: SQL Injection	<ul style="list-style-type: none"> SQL injection attacks Injection detection tools
15: Hacking Wireless Networks	<ul style="list-style-type: none"> Wireless Encryption Wireless hacking methodology Wireless Hacking Tools Wi-Fi- Security Tools
16: Hacking Mobile Platforms	<ul style="list-style-type: none"> Mobile Platform Attack Vector Android Vulnerabilities Jailbreaking D. iOS, windows phone 8 vulnerabilities Mobile Security Guidelines and Tools
17: Cloud Computing	<ul style="list-style-type: none"> Various Cloud Computing Concepts Threats, Attacks, and Security Techniques and Tools
18: Cryptography	<ul style="list-style-type: none"> Different types of Cryptography Ciphers Public Key Infrastructure (PKI) Cryptography Attacks Cryptanalysis Tools