

# Master the Hacking Technologies. Become a Certified Ethical Hacker.



**C | E H** <sup>TM</sup>  
Certified Ethical Hacker

<http://www.eccouncil.org>

**EC-Council**

## Course Description

This class will immerse the student into an interactive environment where they will be shown how to scan, test, hack and secure their own systems. The lab intensive environment gives each student in-depth knowledge and practical experience with the current essential security systems. Students will begin by understanding how perimeter defenses work and then be lead into scanning and attacking their own networks, no real network is harmed. Students then learn how intruders escalate privileges and what steps can be taken to secure a system. Students will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation. 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 312-50.

## Who Should Attend

This course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure.

## Duration:

5 days (9:00 – 5:00)

## Certification

The Certified Ethical Hacker certification exam 312-50 will be conducted on the last day of training. Students need to pass the online Prometric exam to receive CEH certification.

## Legal Agreement

Ethical Hacking and Countermeasures course mission is to educate, introduce and demonstrate hacking tools for penetration testing purposes only. Prior to attending this course, you will be asked to sign an agreement stating that you will not use the newly acquired skills for illegal or malicious attacks and you will not use such tools in an attempt to compromise any computer system, and to indemnify EC-Council with respect to the use or misuse of these tools, regardless of intent.

## Topics Covered v4

- |  |                                       |
|--|---------------------------------------|
| 1. Ethics and Legal Issues                 | 14. SQL Injection                     |
| 2. Footprinting                            | 15. Hacking Wireless Networks         |
| 3. Scanning                                | 16. Virus and Worms                   |
| 4. Enumeration                             | 17. Physical Security                 |
| 5. System Hacking                          | 18. Hacking Linux                     |
| 6. Trojans and Backdoors                   | 19. IDS, Firewalls and Honeypots      |
| 7. Sniffers                                | 20. Buffer Overflows                  |
| 8. Denial of Service                       | 21. Cryptography                      |
| 9. Social Engineering                      | 22. Penetration Testing Methodologies |
| 10. Session Hijacking                      |                                       |
| 11. Hacking Web Servers                    |                                       |
| 12. Web Application Vulnerabilities        |                                       |
| 13. Web Based Password Cracking Techniques |                                       |