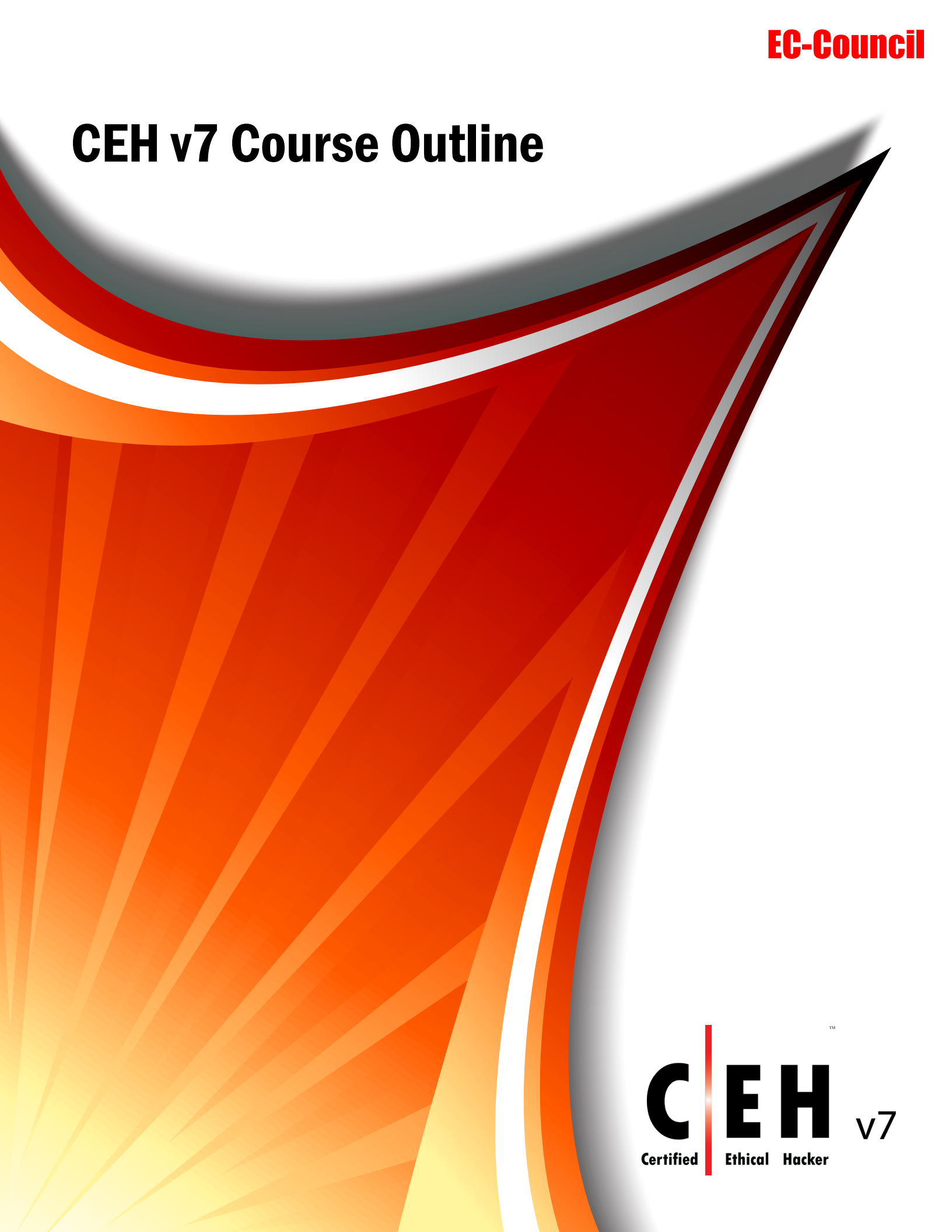
EC-Council

CEH v7 Course Outline



C|EH™ v7
Certified Ethical Hacker

Course Description

This class will immerse the students 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 exam 312-50 may be taken on the last day of the training (optional). 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.

Not anyone can be a student — the Accredited Training Centers (ATC) will make sure the applicants work for legitimate companies.

Course Outline Version 7

CEHv7 Curriculum consists of instructor-led training and self-study. The Instructor will provide the details of self-study modules to the students beginning of the class.

1. Introduction to Ethical Hacking
2. Footprinting and Reconnaissance
3. Scanning Networks
4. Enumeration
5. System Hacking
6. Trojans and Backdoors
7. Viruses and Worms
8. Sniffers
9. Social Engineering
10. Denial of Service
11. Session Hijacking
12. Hacking Webservers
13. Hacking Web Applications
14. SQL Injection
15. Hacking Wireless Networks
16. Evading IDS, Firewalls and Honeypots
17. Buffer Overflows
18. Cryptography
19. Penetration Testing

For more details, class schedules, enquiries contact info@eccouncil.org

EC-Council

6330 Riverside Plaza Ln NW
Suite 210
Albuquerque, NM 87120

Tel: +1.505.341.3228
Fax: +1.505.341.0050

http://www.eccouncil.org
E-mail: info@eccouncil.org