EC-Council

Hacking Technology

C|EH™

Certified Ethical Hacker

CourseWare v8

Course Description

CEHv8 is a comprehensive **Ethical Hacking** and **Information Systems Security Auditing** program focusing on latest security threats, advanced attack vectors, and practical real time demonstration of the latest **Hacking Techniques,** methodologies, tools, tricks, and security measures. Unlike other strictly theoretical training, you will be immersed in interactive sessions with hands-on labs after each topic. You can explore your newly gained knowledge right away in your classroom by pentesting, hacking and securing your own systems. The lab intensive environment gives you in-depth knowledge and practical experience with the current, essential security systems. You will first begin with understanding how perimeter defenses work and then move into scanning and attacking networks, of course, no real network is harmed. You will also learn how intruders escalate privileges and what steps can be taken to secure a system. You will also gain knowledge about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows, and Virus Creation. When you leave this intensive 5 day class you will have hands on understanding and experience in Ethical Hacking. This course prepares you for EC-Council Certified Ethical Hacker exam 312-50.

> “The course was very informative and provided a sound base upon which to build many other certifications and skills. I will personally be recommending that this course be mandatory for all personnel within our cyber threat section.”
>
> **- DoD Participant**

> “Having that quantity of tools is very useful, also because it is not focused to a specific provider, and I think it is a really positive thing.”
>
> **- Francisco Javier De La Chica Castellano,**
> **Senior Consultant, Altran, Spain**

Target Audience

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

Exam Details

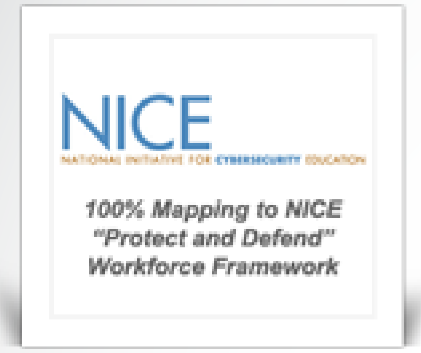
1. Exam Title: Certified Ethical Hacker (ANSI accredited)
2. Exam Code: 312-50 (IBT), 312-50 (VUE) or EC0-350 (APTC)
3. Number of Questions: 125
4. Duration: 4 hours
5. Availability: Prometric Prime/ Prometric APTC/ VUE
6. Test Format: Multiple Choice
7. Passing Score: 70%

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.

CEHv8 Recognition / Endorsement / Mapping


NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION
100% Mapping to NICE "Protect and Defend" Workforce Framework

The National Initiative for Cybersecurity Education (NICE)

American National Standards Institute (ANSI)

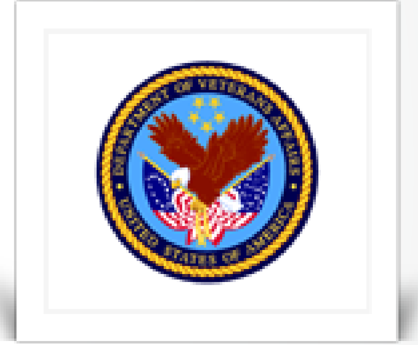
COMMITTEE ON NATIONAL SECURITY SYSTEMS
CNSS
SYSTEMS SECURITY FOR THE 21st CENTURY

Committee on National Security Systems (CNSS)

United States Department of Defense (DoD)

nicf
NATIONAL INFOCOMM COMPETENCY FRAMEWORK
Jointly developed by IDA and WDA

National Infocomm Competency Framework (NICF)



Department of Veterans Affairs

Malaysian Military Cyber Security Warfare Department (KOMLEK)

KOMLEK

MSC

> “Just completed a topic that covers SQL injection. Aware of the problem, but never knew there were so many exploitable methods.”
>
> **- Paul Mah,**
> **Fierce IT, Singapore**

Key Features of CEHv8

1. Updated Content: CEHv8 contains updated information including concepts, methodologies, and tools.
2. It’s not what you know. It’s what you can do. Lab manuals in CEHv8 provide step-by-step walk-throughs of highly technical concepts and are designed to enforce the classroom learning
3. A result oriented, descriptive, and analytical lab manual - the labs showcased in the courseware are tested against the latest Operating Systems (including all patches and hot fixes applied)
4. Access to CEHv8 course at ASPEN, 24x7 from any geographical location with Internet access
5. CEHv8 includes more realistic hack websites to practice the learning and labs that are presented as a part of large case studies
6. Well organized DVD-ROM content - a repository of approximately 24GBs of the latest hacking and security tools
7. Focus on the attacks targeted to mobile platform and tablet computers and covers countermeasures to secure mobile infrastructure
8. CEHv8 courseware is enriched with stunning graphics and animations to demonstrate various hacking concepts and techniques
9. Concepts are presented in an easy-to-understand manner with diagrammatic representation of various hacking concepts for a better understanding and learning experience
10. CEHv8 is optimized for multi-platform delivery including pads, smartphones, and touch screens

Version Comparison

CEHv8 provides a comprehensive ethical hacking and network security-training program to meet the standards of highly skilled security professionals. Hundreds of SMEs and authors have contributed to the content presented in the CEHv8 courseware. CEHv8 focuses on the latest hacking attacks targeted to mobile platforms and tablet computers and covers countermeasures to secure mobile infrastructure. It has simplified advanced technical content with an emphasis on vulnerability assessment, risk assessment, penetration testing, and system protection.

The new version maps to several government and industry standards for infosec education and training including NICE, DoD 8570, etc. The new exam meets the rigorous requirements of the ANSI ISO/IEC 17024 standard.

The comprehensive instructor slides and student manual in CEHv8 empower the instructors and students with flawless flow and outstanding diagrammatic representation of investigation techniques, which makes it easier to teach and enables students to understand the concepts. Latest tools and exploits uncovered from the underground community are featured in the new package.

> “The certification has led to my recent promotion to the Corporate I am in. My company recognized the value of the CEH/CNDA and has moved me forward.”
>
> **- Tim Hoffman (CEH, CNDA)**
> **Corporate Information Assurance**
> **ITT Corporation Manager**

Course Outline Version 8

CEHv8 consists of 20 core modules designed to facilitate a comprehensive ethical hacking and penetration testing training.

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. Sniffing
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. Hacking Mobile Platforms
17. Evading IDS, Firewalls and Honeypots
18. Buffer Overflows
19. Cryptography
20. Penetration Testing

What will you learn?

Students going through CEH training will learn:

1. Key issues plaguing the information security world, incident management process, and penetration testing
2. Various types of footprinting, footprinting tools, and countermeasures
3. Network scanning techniques and scanning countermeasures
4. Enumeration techniques and enumeration countermeasures
5. System hacking methodology, steganography, steganalysis attacks, and covering tracks
6. Different types of Trojans, Trojan analysis, and Trojan countermeasures
7. Working of viruses, virus analysis, computer worms, malware analysis procedure, and countermeasures
8. Packet sniffing techniques and how to defend against sniffing
9. Social Engineering techniques, identify theft, and social engineering countermeasures
10. DoS/DDoS attack techniques, botnets, DDoS attack tools, and DoS/DDoS countermeasures
11. Session hijacking techniques and countermeasures
12. Different types of webserver attacks, attack methodology, and countermeasures

13. Different types of web application attacks, web application hacking methodology, and countermeasures

14. SQL injection attacks and injection detection tools

15. Wireless Encryption, wireless hacking methodology, wireless hacking tools, and wi-fi security tools

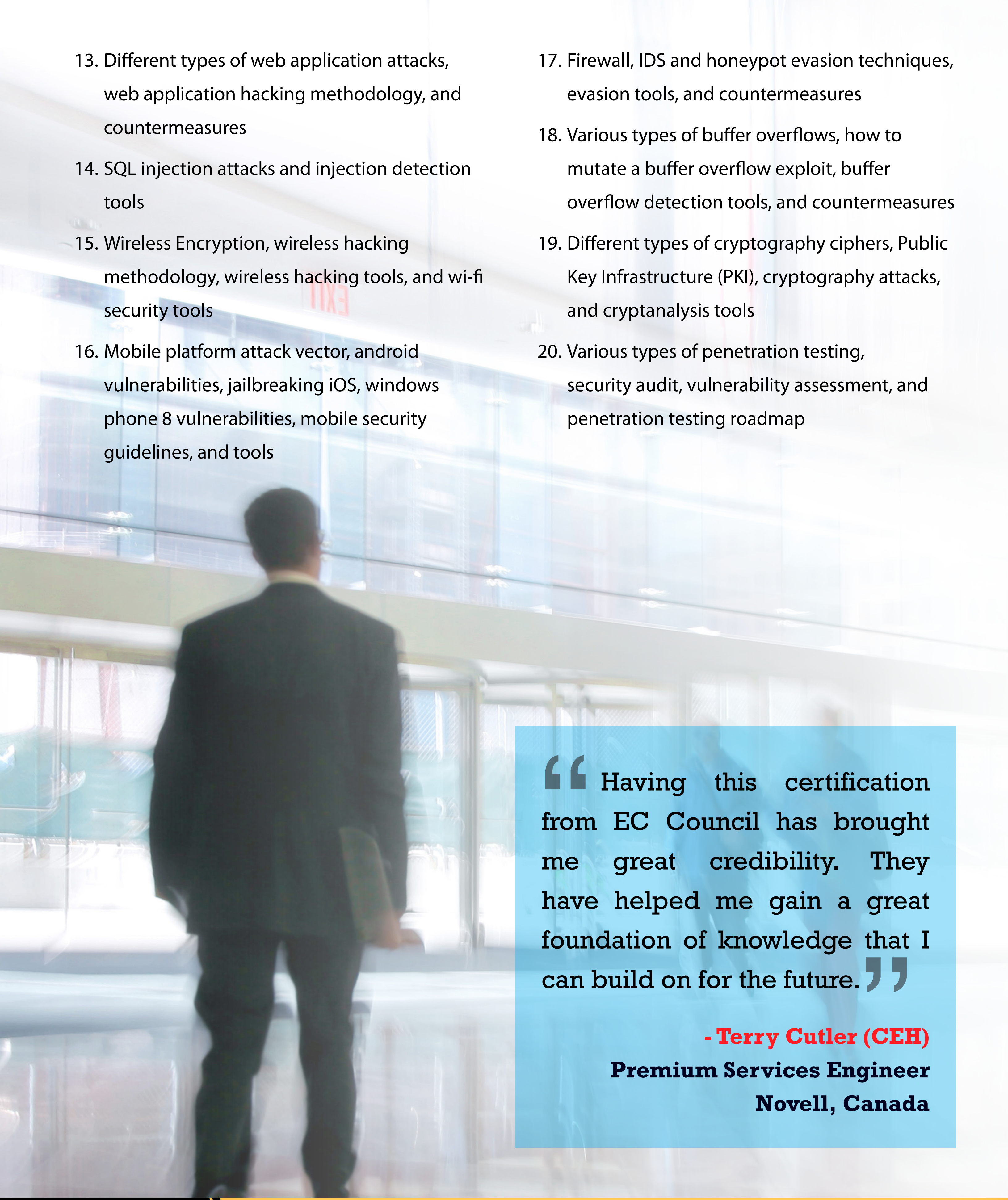
16. Mobile platform attack vector, android vulnerabilities, jailbreaking iOS, windows phone 8 vulnerabilities, mobile security guidelines, and tools

17. Firewall, IDS and honeypot evasion techniques, evasion tools, and countermeasures

18. Various types of buffer overflows, how to mutate a buffer overflow exploit, buffer overflow detection tools, and countermeasures

19. Different types of cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools

20. Various types of penetration testing, security audit, vulnerability assessment, and penetration testing roadmap



> “Having this certification from EC Council has brought me great credibility. They have helped me gain a great foundation of knowledge that I can build on for the future.”
>
> **- Terry Cutler (CEH)**
> **Premium Services Engineer**
> **Novell, Canada**

ASPEN System

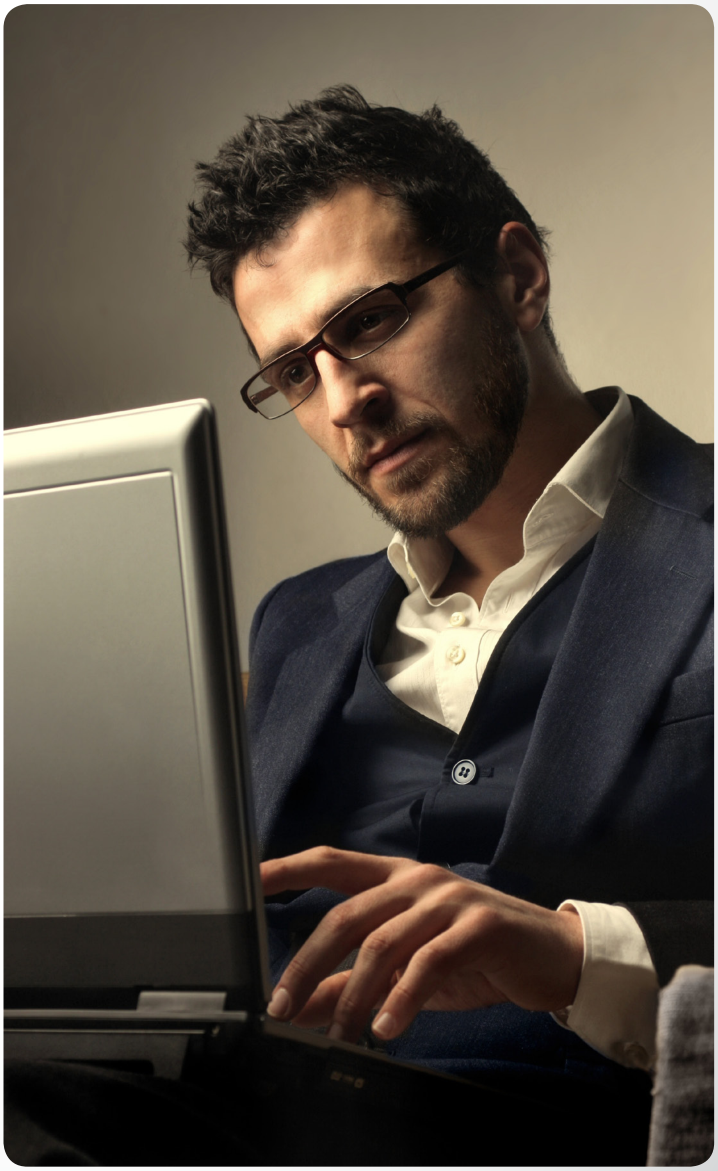
ASPEN is a cloud-based training delivery platform that facilitates an excellent streamlined learning experience in a single place. It is a one-step gateway to multiple portals, products, and services provided by EC-Council for its registered members. ASPEN is an integrated environment and a user-friendly portal where users can navigate to various EC-Council member pages through a single login. ASPEN registered users can place orders for products and courseware at their convenience with just a few mouse clicks. ASPEN not only acts as a portal to EC-Council's services, but also as a social communication medium between its users. ASPEN is an innovative concept that offers easy access to a wide variety of EC-Council's contributions to the information security industry under one platform.

iLabs

The iLabs is a subscription based service that allows students to log on to a virtualized remote machine running Windows 2008 Server to perform various exercises featured in the CEHv8 Lab Guide. All you need is a web browser to connect and start experimenting with our immersive labs. The virtual machine setup reduces the time and effort spent by instructors and partners prior to the classroom engagement. It is a hassle free service available 24/7 for however long you are subscribed.

Benefits

1. Enables students to practice various hacking techniques in a real time and simulated environment
2. The course tools and programs are preloaded on the iLabs machine, thereby saving productive time and effort



EC-Council