WHY TAKE CEH-CERTIFIED ETHICAL TRAINING?

The Certified Ethical Hacker (CEH) will only be considered as White Hats if they are fully certified by the EC-council CEH, (The international Council of E-Commerce Consultants). This certification is called C/EH or Certified Ethical Hacker. This is obtained through specialized training and an examination. The certified ethical hacker certification can be renewed every three years and the recent version is CEHv9, CEH v10.

Who Should Take CEH-Certified Ethical Certification Training?

CEH training is critical for security professionals; you need to think like a hacker but use your skills lawfully to uncover and repair system vulnerabilities. We've developed an ethical hacking course boot camp that introduces the concept of key security tools and perimeter defenses — then leads students into scanning, hacking and compromising networks in an immersive, interactive environment.

CEH training will fortify the application knowledge of security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure. CEH candidates will be immersed in an interactive network hacking environment where they will be shown how to scan, test, hack and secure their systems. Candidates will begin by understanding how perimeter defenses work and then be led into scanning and attacking their own networks.

CEH candidates then learn how intruders escalate privileges and what steps can be taken to secure a system. Candidates will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows, and Virus Creation. Learn the art of penetration testing (pen testing) to create a network intrusion vulnerability prevention strategy.

Listed as a component of the United States Department of Defense Directive 8570, CEH is a respected certification in the industry.

What Jobs Can You get with CEH-Certified Ethical Certification in DC?

Are you intrigued by the world of digital forensics? Our combined CEH + CHFI training class is designed to take you from a novice cybersecurity practitioner to a fully certified forensic investigator, quickly and at a great price. More detailed information about the CEH and CHFI designations are as follows.

Certified Ethical Hacker (CEH). Once you have your basic IT certification and experience down, EC-Councils CEH certification is the next step into the fascinating world of ethical hacking and penetration testing. Our hands-on, instructor-led class will teach you all you need to know about the fundamentals of offensive hacking and the ability to use hacking knowledge and skills for

good. We'll show you how to utilize your curiosity and computer skills to hack into systems with the goal of identifying and fixing holes in an organization's IT infrastructure.

Computer Hacking Forensic Investigator (CHFI). Expanding on the skills you learned studying for the CEH exam, our CHFI training class takes you into the fascinating world of digital forensics. EC-Councils CHFI Certification proves your ability to identify the origins of computer intrusions, and how to gather and present evidence in support of resulting prosecutions. This is a great certification for anyone working in law enforcement, banking, security, and systems administration.

Our CEH and CHFI classes are hands-on, instructor-led programs, designed to ensure you can apply your skills in the real world, as well as pass the certification exams. The whole program takes 80 hours, with the two classes running consecutively. This CEH + CHFI Combo training is a great way to progress your skills quickly through expert teaching and study.

Is a CEH-Certified Ethical Certification in the Washington Metropolitan area Worth It?

Absolutely, the EC-Council CEH course and certification are more essential than ever. It's a great time for uncertified IT professionals to consider taking the course and exam. This certification was the first to involve "black hat" hacking techniques in the classroom. These are the tactics that cybercriminals use to exploit networks. By learning the techniques, they use, IT professionals who are responsible for the protection of their organizations' IT infrastructure, can better combat cybercriminals. CEH training provides the knowledge required to prevent and respond to cybercriminal techniques. This ensures the safety of important data.

There are many benefits to becoming CEH certified. The course and certification will:

- **Increase your knowledge of vulnerabilities and risks** – Cybercriminals are intelligent and resourceful, continuously coming up with new ways to exploit vulnerabilities and attack IT infrastructure. Studying for the CEH certification exam and becoming certified will provide "white hat" hackers with the tools they need to identify and resolve vulnerabilities and risks.
- **Increase your earning potential** – CEH certification shows that professionals have the knowledge and skills to protect IT infrastructure from cybercriminals. That's an experience that organizations will pay for. CEH certified professionals earn higher salaries than non-certified IT professionals. They also have more career advancement opportunities. Computer security is a global issue, and it's the job of an ethical hacker to make the cyberspace safe, now and forever. Career opportunities and growth in EC Council Ethical Hacker Certification (CEH) will always be recognized in the industry.
- **Teach you to use real hacking tools** – Through the CEH certification, you will learn how to use the tools and techniques that unethical hackers to exploit organizations. Learning

how cybercriminals perform attacks and use tools will allow you to better protect your applications, networks, and other assets from being exploited.

How Much Can You Make with a CEH-Certified Ethical Certification in DC?

This is compensated by a great paycheck that every CEH receives. In 2018, the average annual pay for a certified ethical hacker ranges from $75,000.00 to as much as $110,000. However, great companies usually give bonuses to employees which can further increase the total annual certified ethical hacker salary.

WHO CAN DO THE ETHICAL HACKING COURSE?

This CEH course is perfect for people who work in the role that involves maintaining the integrity of network infrastructure. It's also a good fit for anyone who wants to get started in the cybersecurity industry. Whether you work for a private business, a government agency, or a public organization in Maryland, Washington DC, or Northern Virginia, the knowledge, and skills you will gain from our conveniently located CEH training and certification will benefit you and your organization. You will learn how to protect the systems, data, and infrastructure of your employer.

Additionally, the CEH course and certification are essential to anyone who wants to work in an its role for the US Department of Defense (DOD). The DOD requires that its employees have several certifications, including the CEH certification.

EXAM AND CERTIFICATION REQUIREMENTS:

This course helps you prepare for EC-Council's CEH v10 certification exam 312-50. The examination is 4 hours long, consists of 125 multiple choice questions and the passing score is 70%. Ask about our Certified Ethical Hacker exam pass guarantee and the DoD Directive 857.

Who needs CEH Certification?

CEH certification satisfies requirements for CSSP Analyst, CSSP Infrastructure Support, CSSP Incident Responder, and CSSP Auditor roles, as part of DoD 8570.

CEH certification will prepare you for a wide range of IT job roles including:

- Network Security Specialist
- IT Security Specialist
- Security Administrator
- IT Security Consultant
- Ethical Hacker
- Penetration Tester
- Site Administrator
- IT Auditor
- Computer Forensics Analyst
- Homeland Security Specialist