Article

on

Certified Ethical Hacker (C|EH)

About Author

Aparna Agarwal has done B.Tech, specialization in Information Technology from UPTU in 2013. Now working as a IT Security Consultant in Ducara Info Solutions Pvt. Ltd., Meerut (www.ducarainfo.com). She has done certifications- C|EH, E|CSP (.NET) from EC- Council and have a great experience of Network Security, Web Application Security, Cyber Forensics, OWASP top 10, Vulnerability Assessment, Information Security and secure programming in .net.

Abstract

As with most technological advances, there is also a dark side: criminal hackers. Governments, companies, and private citizens around the world are anxious to be a part of this revolution, but they are afraid that some hacker will break into their Web server and replace their logo with pornography, read their e-mail, steal their credit card number from an on-line shopping site, or implant software that will secretly transmit their organization's secrets to the open Internet. With these concerns and others, the ethical hacker can help. This paper describes ethical hackers: their skills, their attitudes, and how they go about helping their customers find and plug up security holes. In this article you will come to know:

- ✓ *What is Hacking?*
- ✓ *What is Ethical Hacking?*
- ✓ *What does Certified Ethical Hacker (C|EH) mean?*
- ✓ *Why C|EH is important for you?*
- ✓ *Who should attend?*
- ✓ *How you can be a Certified Ethical Hacker (C|EH)?*
- ✓ *What are the benefits of C|EH?*
- ✓ *From where you can get the training?*

HACKING:-

- *gain unauthorized access to data in a system or computer.*

- ✓ **Hacking** refers to exploiting system vulnerabilities and compromising security controls to gain unauthorized or inappropriate access to the system resources.
- ✓ **Hacking** is the practice of modifying system or application features, in order to accomplish a goal outside of the creator's original purpose. The person who is consistently engaging in hacking activities, and has accepted hacking as a lifestyle and philosophy of their choice, is called a **hacker**.
- ✓ **Computer hacking** is the most popular form of hacking nowadays, especially in the field of computer security, but hacking exists in many other forms, such as **phone hacking**, **brain hacking**, etc. and it's not limited to either of them.
- ✓ **Hacking** is the process of exploiting vulnerabilities to gain unauthorized access to systems or resources.

In the computer security context, a **hacker** is someone who seeks and exploits weaknesses in a computer system or computer network. Hackers may be motivated by a multitude of reasons, such as profit, protest, challenge or enjoyment. The subculture that has evolved around hackers is often referred to as the computer underground and is now a known community. While other uses of the word *hacker* exist that are not related to computer security, such as referring to someone with an advanced understanding of computers and computer networks, they are rarely used in mainstream context. They are subject to the longstanding hacker definition controversy about the term's true meaning. In this controversy, the term *hacker* is reclaimed by computer programmers who argue that someone who breaks into computers, whether computer criminal (black hats) or computer security expert (white hats), is more appropriately called a cracker instead. Some white hat hackers claim that they also deserve the title *hacker*, and that only black hats should be called "crackers".

Hacking is the practice of modifying the features of a system, in order to accomplish a goal outside of the creator's original purpose. The person who is consistently engaging in hacking activities, and has accepted hacking as a lifestyle and philosophy of their choice, is called a hacker.

Computer hacking is the most popular form of hacking nowadays, especially in the field of computer security, but hacking exists in many other forms, such as **phone hacking**, **brain hacking**, etc. and it's not limited to either of them.

Due to the mass attention given to **blackhat hackers** from the media, the whole hacking term is often mistaken for any security related cyber crime. This damages the reputation of all hackers, and is very cruel and unfair to the law abiding ones of them, from who the term itself originated.

With the growth of the technological aspects of business it is fast growing that all our data is to be made electronic; all business transactions are done electronically to try and bring us into the next generation. eBay for example is a global auction site that persuade businesses to sell their goods, allows an auction room in the comfort of our own homes. Ethical hackers can and may use their abilities to try and avoid paying for items they have brought because they know they can. They use their power to "help themselves" without being caught, at the expense of others, and can be seen as ethical hackers occasional job, essentially in this sense ethical hackers by day and wear black hats when they need to! *Unfortunately, some of the skilled professionals use their abilities to harm the society, by finding the vulnerabilities in the companies' systems and attacking them, creating and distributing virus containing codes, finding the ways to avoid payments for the desires service.*

Hacking on computer networks is often done through scripts or other *network programming*. These programs generally manipulate data passing through a network connection in ways designed to obtain more information about how the target system works. Many such pre-packaged scripts are posted on the Internet for anyone, typically entry-level hackers, to use. More advanced hackers may study and modify these scripts to develop new methods. A few highly skilled hackers work for commercial firms with the job to protect that company's software and data from outside hacking.

Cracking techniques on networks include creating **worms**, initiating **denial of service (DoS) attacks**, or in establishing **unauthorized *remote access* connections to a device**.

ETHICAL HACKING:-

- *To beat a hacker, you need to think like one!*

Ethical Hacking is often referred to as the process of penetrating one's own computer/s or computers to which one has official permission to do so as to determine if vulnerabilities exist and to undertake preventive, corrective, and protective countermeasures before an actual compromise to the system takes place.

- ✓ **Ethical Hacking** involves the use of hacking tools, tricks and techniques to identify vulnerabilities so as to ensure system security.
- ✓ **Ethical Hacking** focuses on simulating techniques used by attackers to verify the existence of exploitable vulnerabilities in the system security.
- ✓ **Ethical hacking** and **ethical hacker** are terms that describe hacking performed to help a company or individual identify potential threats on the computer or network.
- ✓ An ethical hacker attempts to hack their way past the system security, finding any weak points in the security that could be exploited by other hackers. The organization uses what the ethical hacker finds to improve the system security, in an effort to minimize, if not eliminate any potential hacker attacks.
- ✓ The term "**white hat**" in Internet slang refers to an ethical computer hacker, or a computer security expert, who specializes in penetration testing and in other testing methodologies to ensure the security of an organization's information systems.

Ethical hacking and **ethical hacker** are terms that describe hacking performed to help a company or individual identify potential threats on the computer or network. An ethical hacker attempts to hack their way past the system security, finding any weak points in the security that could be exploited by other hackers. The organization uses what the ethical hacker finds to improve the system security, in an effort to minimize, if not eliminate any potential hacker attacks.

Ethical hacking, often performed by white hats or skilled computer experts, is the use of programming skills to determine vulnerabilities in computer systems. Many companies utilize ethical hacking services from consultants or full-time employees to keep their systems and information as secure as possible. The work of ethical hacking is still considered hacking because it uses knowledge of computer systems in an attempt to in some way penetrate them

or crash them. This work is ethical because it is performed to increase the safety of the computer systems. It's reasoned that if a white hat can somehow break the security protocols of a system, so can a black hat. Thus, the goal of ethical hacking is to determine how to break in or create mischief with the present programs running, but only at the request of the company that owns the system and specifically to prevent others from attacking it.

Ethical hackers are highly paid professionals with a legitimate status and a means of access. They can minimize the risk of impact, clearly identifying benefits and flaws helping senior company directors to understand if such activities should be undertaken. Ethical hackers could explore vulnerabilities beforehand to minimize the risk. The company could undertake penetration tests to find if they are vulnerable to attack. Finding vulnerabilities for companies not only helps the company but also minimizes the risks of attacks, however ethical hackers have five days in general to perform tests, what happens if vulnerabilities are overlooked. If an ethical hacker fails to deliver results to the business and assumes the system is safe and that it has no problems, who can be liable for legal actions if a malicious hacker gets into the system? Surprisingly, a journal by IBM on ethical hacking reports, *"the client might ask "So, if I fix these things I'll have perfect security, right?" "Unfortunately, this is not the case. People operate the client's computers and networks, and people make mistakes. The longer it has been since the testing was performed, the less can be reliably said about the state of a client's security. A portion of the final report includes recommendations for steps the client should continue to follow in order to reduce the impact of these mistakes in the future*."

Ethical hacking is where a person hacks to find weaknesses in a system and then usually patches them. For example, a bank may pay a hacker to hack their systems to see if it is hack able. If he gets in, then they know there is potential for other people to hack in, and usually they will work with this ethical hacker to patch these holes. If he doesn't get in, then they pray that nobody is better at hacking than him. Let me add this. Hacking is simply exploring a computer's designed features, and learning how to exploit or take advantage of those features.

Google is a great search engine that allows valuable and sometimes illegal information to be obtained. Google causes privacy concerns, for the true people that understand how to obtain such information by using clever commands can use Google as a helpful tool into getting as much information as possible. Is it ethical for Google to hold such information about a certain individual or companies? Certainly, the answer here would be no, it allows us to obtain sensitive information about our targets, good for the hacker, but bad for the target. Though it is still available, companies must ensure that all employees don't send any sensitive information across the internet. Google can play a major part as to giving valuable and sometimes sensitive information. This causes great concern for the individuals that purchase or have web servers with valuable information. With further investigation Google allows retrieving valuable information.

Become a Certified Ethical Hacker

A Certified Ethical Hacker is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s). The CEH credential certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective.

- *To beat a hacker, you need to think like one!*

CERTIFIED ETHICAL HACKER

C|EH 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. Certified Ethical Hackers are professionals that have completed the EC-Council CEH Program. The Certified Ethical Hacker certification requires participants to attend an Ethical Hacking and Countermeasures Course and pass the Ethical Hacking and Countermeasures Exam offered by EC-Council.

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

What does *Certified Ethical Hacker (C|EH)* mean?

Certified Ethical Hacker (C|EH) is a professional designation for hackers that perform legitimate services for IT companies and other organizations. A C|EH is hired to locate and repair application and system security vulnerabilities to preempt exploitations by black hat hackers and others with potentially illegal intentions.
C|EH oversight is provided by the International Council of **E-Commerce Consultants (EC-Council).**

Explains Certified Ethical Hacker (C|EH)

Individuals that pass the C|EH examination after training from an Accredited Training Center (ATC) or self study receive the C|EH designation. Self study learners must back up their qualifications with two years of practical working experience in Information Security (IS). Without this experience, a detailed educational background is required for review on a case-by-case basis.

The **Certified Ethical Hacker** is a professional certification, provided by the International Council of E-Commerce Consultants (EC-Council.)

An ethical hacker is usually employed by an organization who trusts him or her to attempt to penetrate networks and/or computer systems, using the same methods as a hacker, for the purpose of finding and fixing computer security vulnerabilities. Unauthorized hacking (i.e., gaining access to computer systems without prior authorization from the owner) is a crime in most countries, but penetration testing done by request of the owner of the victim system(s) or network(s) is not.

A Certified Ethical Hacker has obtained a certification in how to look for the weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a hacker.

The code for the C|EH exam is 312-50.

The C|EH credential establishes and governs minimum standards for information security specialists in ethical hacking and information system auditing.

To beat a hacker, you need to think like one! A Certified Ethical Hacker is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of the target system(s). The CEH credential certifies

individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective.

The purpose of the CEH credential is to:

- Establish and govern minimum standards for credentialing professional information security specialists in ethical hacking measures.
- Inform the public that credentialed individuals meet or exceed the minimum standards.
- Reinforce ethical hacking as a unique and self-regulating profession.

Why is C|EH exam important for you?

This is the world's most advanced ***ethical hacking*** *course* with 20 of the most current security domains any ethical hacker will ever want to know when they are planning to beef up the information security posture of their organization. The goal of this course is to help you master an ethical hacking methodology that can be used in a penetration testing or ethical hacking situation. You walk out the door with hacking skills that are highly in demand, as well as the internationally recognized ***certified ethical hacker certification***! Ethical hacking course prepares you for EC-Council Certified Ethical Hacker exam 312-50.

Examination

Certification is achieved by taking the C|EH examination after having either attended training at an ATC (Accredited Training Center) or done self-study. If a candidate opts for self-study, an application must be filled out and proof submitted of 2 years of relevant information security work experience. In case you do not have two years of information security related work experience, you can send them a request detailing your educational background and request for consideration on a case basis. The current version of the C|EH is V8 uses EC-Council's exam 312-50, as did the earlier versions. Although the new version V8 has recently been launched. This exam has 125 multiple-choice questions, a 4 hour time limit, and requires at least a score of 70% to pass. The earlier v7 had 150 multiple-choice questions and a four hour time limit. The version 7 and version 8 exams costs US$500 for the actual test and US$100 as a nonrefundable fee for registration. Prices apply in the United States (prices in other countries may differ), and is administered via computer at an EC-Council Accredited Training Center, Pearson VUE, or Prometric testing center (in the United States).

Recertification

EC-Council Continuing Education (ECE) points serve to ensure that all certified professionals maintain and further their knowledge. Professionals must meet ECE requirements to avoid revocation of certification. Members holding the C|EH/C|NDA designation (as well as other EC-Council certifications) must recertify under this program every three years for a minimum of 120 credits.

Controversy

Certain computer security professionals have objected to the term ethical hacker: "There's no such thing as an 'ethical hacker' - that's like saying 'ethical rapist' - it's a contradiction in terms." Part of the controversy may arise from the older, less stigmatized, definition of hacker, which has since become synonymous with computer criminal.

On the other hand, some companies do not seem to mind the association. According to EC-Council, there has been an increase of careers where C|EH and other ethical hacking certifications are preferred or required. Even the US government accepts this association and requires C|EH accreditation for some jobs per DoD 8570.01-M guidelines.

Who Should Attend?

Ethical hacking training 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 AM – 5:00 PM)

Certification Target Audience

The Certified Ethical Hacker certification 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.

Exam Info

- Number of Questions: 125
- Passing Score: 70%
- Test Duration: 4 Hours

If you are attempting Exam 312-50 or 312-50v7 the web based Prometric Prime exam, you can contact your ATC to schedule the exam.

If you are attempting Exam EC0-350 at any authorized Prometric Testing center (APTC), you can schedule the exam by contacting Prometric directly. You can use the voucher number given to you by EC-Council upon approval of your eligibility application form. Please note that Prometric will NOT schedule exams without the voucher number.

For VUE, please visit http://www.vue.com/eccouncil. EC-Council reserves the right to revoke the certification status of candidates that do not comply to all EC-Council examination policies found here.

Clause: Age Requirements and Policies Concerning Minors

The age requirement for attending the training or attempting the exam is restricted to any candidate that is at least 18 years old.

If the candidate is under the age of 18, they are not eligible to attend the official training or eligible to attempt the certification exam unless they provide the accredited training center/EC-Council a written consent of their parent/legal guardian and a supporting letter from their institution of higher learning. Only applicants from nationally accredited institution of higher learning shall be considered.

Disclaimer: EC-Council reserves the right to impose additional restriction to comply with the policy. Failure to act in accordance with this clause shall render the authorized training center in violation of their agreement with EC-Council. EC-Council reserves the right to revoke the certification of any person in breach of this requirement.

CEHv8 Recognition / Endorsement / Mapping

The National Initiative for Cybersecurity Education (NICE)

American National Standards Institute (ANSI)

Committee on National Security Systems (CNSS)

United States Department of Defense (DoD)

National Infocomm Competency Framework (NICF)

Department of Veterans Affairs

KOMLEK

MSC

CEH Accredited by ANSI

EC-Council has been accredited by the ANSI to meet the ANSI/ISO/IEC 17024 Personnel Certification Accreditation standard for its Certified Ethical Hacker certification.

About ANSI: As the voice of the U.S. standards and conformity assessment system, the American National Standards Institute (ANSI) empowers its members and constituents to strengthen the U.S. marketplace position in the global economy while helping to assure the safety and health of consumers and the protection of the environment.

The Institute oversees the creation, promulgation and use of thousands of norms and guidelines that directly impact businesses in nearly every sector: from acoustical devices to construction equipment, from dairy and livestock production to energy distribution, and many more. ANSI is also actively engaged in accrediting programs that assess conformance to standards – including globally-recognized cross-sector programs such as the ISO 9000 (quality) and ISO 14000 (environmental) management systems.

The American National Standards Institute (ANSI) is a private non-profit organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system. It is the sole representative of both the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC) in the United States. ANSI is the only personnel certification accreditation body in the United States to meet nationally accepted practices for accreditation bodies. The ANSI/ISO/IEC 17024 standard addresses the general requirements for certification entities.

Key Features of CEH

I. Updated Content: CEH contains updated information including concepts, methodologies, and tools.
II. It's not what you know. It's what you can do. Lab manuals in CEH provide step-by-step walk-through of highly technical concepts and are designed to enforce the classroom learning
III. 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)
IV. Access to CEH course at ASPEN, 24x7 from any geographical location with Internet access
V. CEH includes more realistic hack websites to practice the learning and labs that are presented as a part of large case studies
VI. Well organized DVD-ROM content - a repository of approximately 24GBs of the latest hacking and security tools
VII. Focus on the attacks targeted to mobile platform and tablet computers and covers countermeasures to secure mobile infrastructure
VIII. CEH courseware is enriched with stunning graphics and animations to demonstrate various hacking concepts and techniques
IX. Concepts are presented in an easy-to-understand manner with diagrammatic representation of various hacking concepts for a better understanding and learning experience
X. CEH is optimized for multi-platform delivery including pads, smart phones, and touch screens

What will you learn?

Students going through CEH training will learn:

- Key issues plaguing the information security world, incident management process, and penetration testing.
- Various types of footprinting, footprinting tools, and countermeasures.
- Network scanning techniques and scanning countermeasures.
- Enumeration techniques and enumeration countermeasures.
- System hacking methodology, steganography, steganalysis attacks, and covering tracks.
- Different types of Trojans, Trojan analysis, and Trojan countermeasures.
- Working of viruses, virus analysis, computer worms, malware analysis procedure, and countermeasures.
- Packet sniffing techniques and how to defend against sniffing.
- Social Engineering techniques, identify theft, and social engineering countermeasures.
- DoS/DDoS attack techniques, botnets, DDoS attack tools, and DoS/DDoS countermeasures.
- Session hijacking techniques and countermeasures.
- Different types of webserver attacks, attack methodology, and countermeasures.
- Different types of web application attacks, web application hacking methodology, and countermeasures.
- SQL injection attacks and injection detection tools.
- Wireless Encryption, wireless hacking methodology, wireless hacking tools, and wi-fi security tools.
- Mobile platform attack vector, android vulnerabilities, jailbreaking iOS, windows phone 8 vulnerabilities, mobile security guidelines, and tools.
- Firewall, IDS and honeypot evasion techniques, evasion tools, and countermeasures.
- Various types of buffer overflows, how to mutate a buffer overflow exploit, buffer overflow detection tools, and countermeasures.
- Different types of cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools.
- Various types of penetration testing, security audit, vulnerability assessment, and penetration testing roadmap.

About EC-Council

The International Council of **E-Commerce Consultants (EC-Council)** is a member based organization that certifies individuals in various information security and e business skills. EC-Council has been certified by ***American National Standards Institute*** to meet its **ANSI 17024 standard**. It is the owner and creator of the world famous **Certified Ethical Hacker** (CEH), **Computer Hacking Forensics Investigator** (CHFI) and **EC-Council Certified Security Analyst** (ECSA)/**License Penetration Tester** (LPT) programs, and as well as many others programs, that are offered in over 92 countries through a training network of more than 450 training partners globally.

As of end 2012, EC-Council has trained over 160,000 individuals and certified more than 66,000 security professionals. Many of these certifications are recognized worldwide and have received endorsements from various government agencies including the **US Federal Government** via the Montgomery GI Bill, **National Security Agency** (NSA) and the **Committee on National Security Systems** (CNSS). And the United States Department of Defense has included the CEH program into its Directive 8570, making it as one of the mandatory standards to be achieved by **Computer Network Defenders Service Providers (CND-SP).**

Individuals who have achieved EC-Council certifications include those from some of the finest organizations around the world such as the US Army, the FBI, Microsoft, IBM and the United Nations.
EC-Council has also been featured in internationally acclaimed publications and media including Fox Business News, CNN, The Herald Tribune, The Wall Street Journal, The Gazette and The Economic Times as well as in online publications such as the ABC News, USA Today, The Christian Science Monitor, Boston and Gulf News.

EC-Council is the owner of the Hacker Halted conference and workshop series, which had been organized in international cities such as Miami, Myrtle Beach, Dubai, Singapore, Kuala Lumpur, Mexico City, among others. Hacker Halted features renowned international speakers who are experts in the field of information security. **The objective of Hacker Halted conference series is to raise international awareness towards increased education and ethics in information security.** The EC-Council University, based in the state of New Mexico, United States of America, is a fully licensed degree granting university that offers both bachelors and masters degree programs.

Currently, EC-Council is supporting the International Multilateral Partnership against Cyber Threats (IMPACT) that is a partner organization of the United Nations/International Telecommunication Union (UN/ITU) to provide training and technical support to governments of its 191 member states.

Conclusion

To beat a hacker, you need to think like one! This is exactly what this class will teach you. It is the pinnacle of the most desired information security training program any information security professional will ever want to be in. To master the hacking technologies, you will need to become one.

*The **Certified Ethical Hacker class** will immerse the students into a hands-on environment where they will be shown how to conduct ethical hacking. They will be exposed to an entirely different way of achieving optimal information security posture in their organization; by hacking it! They will scan, test, hack and secure their own systems.*

References:

1. *DANISH JAMIL and MUHAMMAD NUMAN ALI KHAN-"* ***IS ETHICAL HACKING ETHICAL?", 2011***
2. *CEH v7 and v8 module: EC Council*
3. *http://www.globalknowledge.com*
4. *http://www.eccouncil.org*
5. *http://www.esecurityplanet.com*
6. *http://www.ijest.info/docs/IJEST11-03-05-186.pdf*
7. *http://eprints.binadarma.ac.id/1000/1/KEAMANAN%20SISTEM%20INFORMASI%20MATERI%201.pdf*
8. *http://en.wikipedia.org/wiki/Certified_Ethical_Hacker*
9. *http://volgenau.gmu.edu*
10. *http://en.wikipedia.org/wiki/EC-Council*
11. *http://en.wikipedia.org/wiki/Hacking/*
12. *http://www.computerhope.com/*
13. *http://www.eccouncil.org/Certification/certified-ethical-hacker/*
14. *http://www.ansi.org*