Hackers are here. Where are you?

EC-Council Certified Ethical Hacker Program

Frequently Asked Questions

EC-Council Certified Ethical Hacker Program

Frequently Asked Questions

What is 'Hacking'?

Hacking is an act of penetrating computer systems to gain knowledge about the system and how it works. This is considered illegal since it is like breaking into someone's house.

What are 'Hackers'?

Hackers are people who try to gain unauthorized access to computers. This is normally done through the use of a 'backdoor' program installed on your machine. A lot of Hackers also try to gain access to resources through the use of password cracking software, which tries billions of passwords to find the correct one for accessing a computer.

What damage can a Hacker do?

This depends upon what backdoor program(s) are hiding on your PC. Different programs can do different amounts of damage. However, most allow a hacker to smuggle another program onto your PC. This means that if a hacker can't do something using the backdoor program, he can easily put something else onto your computer that can. Hackers can see everything you are doing, and can access any file on your disk. Hackers can write new files, delete files, edit files, and do practically anything to a file that could be done to a file. A hacker could install several programs on to your system without your knowledge. Such programs could also be used to steal personal information such as passwords and credit card information

How do Hackers hack?

Hackers use exploits and weakness in various operating systems and software programs. One of the popular methods of hacking is to exploit buffer overflow in applications.

What is a script kiddy?

A script kiddy is a wannabe cracker. These individuals lack knowledge of how a computer really works but they use well-known easy-to-find techniques and hacking tools on the Internet to break into a computer to steal passwords, music files, SPAM, etc.

What is Ethical Hacking?

The term ethical hacking refers to the co-ordinate and comprehensive check of security of a network and on systems inside it, in order to assess the actual risk level data is exposed to, and to propose possible corrective actions aimed at raising the security level. An ethical hacker is a computer security professional, a researcher constantly engaged in enhancing and widening his or her skills in several areas. A question may arise about the term « ethical » related to this kind of activity: « ethical » means that tools and techniques used are typically the same as those chosen by attackers, but they are applied wisely, without any risk for data integrity, service continuity and so forth. « Ethical » also means that privacy is guaranteed to accessed information, which is often particularly sensitive and valuable. Finally, « ethical » means suggestions are given in order to enhance the security level relating to the exposures found.

The role of a computer security policy is to prevent a malicious break-in into the network. What better way of assessing the effectiveness of such a policy than by carrying out realistic tests? Such simulations are called high end ethical hacking tests; the auditors carry out the simulations by using the same techniques as the ones used by real hackers. The only difference is that the systems are never disturbed during an audit.

After carrying out these tests, the auditors present an audit report to the client. It contains a precise assessment of the risks (and their potential costs), as well as a list of recommendations to implement in order to increase the network's security. The cost of such an implementation is also assessed.

Give me some examples of Hacking Threats?

"Inexperienced hackers specialized in defacing websites don't worry me"

One can define computer security in the following way: A computer network or system is regarded as secure when the information it contains is less valuable than the time required breaking into it.

Hacking threats can be divided into two main categories:

1. Attacks from inexperienced hackers:

    These attacks are quite frequent and often presented in the media. Their consequences are rarely dramatic but often visible:

- Disturbing the internet services provided by the victim
- Webpage defacement
- Etc.

The main risk is therefore bad publicity for the attacked organization. It is thus the main objectives of such malicious actions, which in general do not target specific servers (large sets of addresses are randomly scanned). Security systems of large organizations are often able to block such attacks.

2. Attacks from experienced hackers:

Becoming more and more frequent, they are however only rarely known to the public. Experienced hackers will choose specific targets and often spend a lot of time to achieve their goal:

- Industrial espionage on the behalf of third parties
- Stealing sensitive and/or confidential data on the behalf of third parties (client databases, etc.) or undermining the reputation of the victim
- Transferring money abroad (financial institutions)
- Stealing confidential data
- Etc.

The damages of such attacks are often quite important and can be of dramatic consequences for the targeted organization. One must unfortunately notice that the majority of organizations do not have nowadays a

satisfactory level of protection for such threats. The best way of protecting oneself against such threats is definitely by carrying out ethical hacking tests.

What is 'Penetration Testing'?

Penetration testing involves simulating an attack using tools and techniques available to external hackers and willful insiders to probe for weaknesses and ascertain the potential damage that could be caused. Damage to an insecure network may involve recording and tampering with network traffic, obtaining passwords and gaining administrator access or exploitation of published software weaknesses where patches have not been updated, to name but a few common examples. In real terms, such attacks can lead to loss, theft or alteration of business-critical and highly sensitive data.

How are Penetrating Testing conducted?

Penetration testing can be conducted using one of two approaches: black-box (with no prior knowledge of the infrastructure to be tested) and white-box (with a complete knowledge of the network infrastructure).

Black-Box Testing

Black-box testing simulates a true web-hacking attack, beginning with nothing but the client's corporate name. From here the evaluator will gather information about the network and the business from as many outside sources as possible. Scanning tools such as port scanners aid in network mapping and publicly available information from sources such as web sites and media publications supply useful information about the business. Social

engineering techniques may also be used where information is gathered from unwitting employees. The evaluator then begins probing the network for exploitable vulnerabilities based on a network map created from the initial investigations.

White-Box Testing

White-box testing has fundamental similarities in terms of the testing involved but assumes a full knowledge of the client's organization and network infrastructure from the outset. The evaluators are privy to all system design and implementation documentation, which may include listings of source code, manual and circuit diagrams. Adopting a structured and formal approach, a good evaluator will also test the validity of the information initially provided, rather than work under the assumption that it is true. A white-box test can also be used to simulate an attack from inside the company or by ex-employees with knowledge of the systems.

Who conducts these Penetration Tests?

These tests are conducted by highly knowledgeable security experts called “Ethical Hackers”.

Who is an ‘Ethical Hacker’?

An ethical hacker is a security professional who will use hacking skills and the tools used by the real hackers to try to break into a company's network and uncover holes in its security.

What do ethical hackers do?

An ethical hacker's evaluation of a system's security seeks answers to three basic questions:

- What can an intruder see on the target systems?
- What can an intruder do with that information?
- Does anyone at the target notice the intruder's attempts or successes?
- What are you trying to protect?
- What are you trying to protect against?
- How much time, effort, and money are you willing to expend to obtain adequate protection?

What is CEH program?

EC-Council's unique five day security training course called the Ethical Hacking & Countermeasures, prepares the students for the CEH exam 310-50. As the only course of its kind in the world leading to an Ethical Hacker Certification, it teaches how hackers hack, the tools they use, how to hack via Linux and Windows 2000, how to hack firewalls and how to implement an effective security framework for both e-commerce and day to day operation and how to apply countermeasures to avoid those risks.

The Certified Ethical Hacker (CEH) program expands the horizon of the thinking of the average systems engineer. While traditionally all they do is to think defense, now they are thought to "think outside the box" and prepare and predict the worst ever possible attack on their system. They are thought how to configure, deploy and manage hacking tools and techniques as well as ensure that they are properly secured within their company' infrastructures.

How would my company benefit from the CEH program?

Companies benefit from the CEH certification program, allowing them to have the appropriate level of education and understanding on how hackers think and function to allow them to deploy and test hacking tools on their own. “This is meant to be as a preemptive strike against any real or potential hacking attempt to any site as candidates are required to launch an attack on their own system”.

What are the skills covered in the CEH program?

The Ethical Hacking and Countermeasures course covers the following 21 domains.

1. Ethics and Legal Issues
2. Footprinting
3. Scanning
4. Enumeration
5. System Hacking
6. Trojans and Backdoors
7. Sniffers
8. Denial of Service
9. Social Engineering
10. Session Hijacking
11. Hacking Web Servers
12. Web Application Vulnerabilities
13. Web Based Password Cracking Techniques
14. SQL Injection
15. Hacking Wireless Networks
16. Virus and Worms
17. Physical Security
18. Hacking Linux

19. IDS, Firewalls and Honeypots
20. Buffer Overflows
21. Cryptography
22. Penetration Testing Methodologies

How can I become 'Certified Ethical Hacker'?

There are two simple steps in becoming certified as CEH.

1. Attend EC-Council's Ethical Hacking and Countermeasures Training at an Accredited Training Center
2. Pass the CEH exam 312-50 conducted by Thomson Prometric.

How well is CEH certification recognized?

The CEH credential is a growing certification and recognized by IBM, Microsoft, HP, and Nortel and endorsed by leading associations such as AIP, NCCA and Singapore's NICC. The CEH program is globally recognized and adopted by training centers around the world. The CEH exams are translated to Japanese. EC-Council has trained US Navy, BFI, CIA, US Military divisions, Microsoft, Dell etc on Ethical Hacking.

How is the CEH program different from CISSP, Security+ and SCP programs?

The CEH program is based on hacking skills rather than defense and security skills. The CISSP program focuses on general security knowledge based on ISC2 published security domain. The CISSP program is non-technical while the CEH program is very technical.

How many people are certified as CEH till today?

There are thousands of Certified Ethical Hackers around the world.

Who sits on the council?

The council is represented by academic professors and lecturers. Corporate bodies also sit on the council namely Microsoft, IBM, Nortel, HP etc. Please visit http://www.eccouncil.org/members.htm for the complete list of honorary members.

Who accredits the council?

EC-Council certification programs are accredited and endorsed by Association of Internet Professionals (http://www.association.org). The Association of Internet Professionals is the premier professional association for Internet professionals worldwide. The AIP Certification Accreditation Council is made up of industry certification companies, educational institutions, software, hardware, and staffing companies, as well as other non-profit representative groups. The purpose of the Council is to determine standards for certification programs and then accredit the programs that meet those standards.

How many training centers are there around the world?
There are more than 100 training centers around that conduct EC-Council programs.

What type of IT professional should take the CEH certification?

The CEH certification is designed for the network or systems practitioner who typically has responsibilities for penetration testing in job function and in job title. It is intended for those practitioners who desire to improve their security practitioner expertise, as well as position themselves as demonstrated and knowledgeable Ethical Hacking security professionals. Typically, these candidates will have two or more years in information security and IT experience, and are responsible for their organizations' primary systems and networks.

What is the benefit of having the CEH certification?

CEH certification demonstrates that IT personnel have the essential knowledge and ability to be active stakeholders in today's enterprise security, helping the organization achieve a more operationally secure posture.

How does this certification differ from others, such as CISSP?

CEH certification is unique in the IT security market in that it focuses on the essential aspects of Ethical Hacking and Penetration Testing. Unlike other security certifications, CEH takes the “Hacking” approach toward security and risk management, in that it focuses on the absolute "Attack" vs. “Defense”, ensuring that baseline approaches have been researched and implemented. CEH is complementary to CISSP, since it is designed for the IT practitioner responsible for ensuring security principles are applied in the context of their daily job scope. CISSP is non-technical certification suited for IT practitioners at managerial level while CEH is highly technical subject and targeted towards Security Administrators.

Comparison between CISSP and CEH

CISSP	CEH
ISC2 is the program vendor.	EC-Council is the program vendor.
Exam administered by selected ISC2 centers.	Exam administered by Thomson Prometric around the world.
Exam must be pre-registered and can be taken only on scheduled dates.	The Exam 312-50 can be taken at anytime by registering directly with Prometric.
ISC2 requires 2-years proof of work experience as prerequisite to take the exam.	None
The certification is targeted towards IT security at managerial level.	The certification is targeted towards security administrators at technical level.
Depth of coverage: General security concepts	Depth of coverage: Very technical involving vulnerability testing and assement.
Skills required to pass the exam: None	Skills required to pass the exam: Windows 2000, Linux, C++, Assembly Language, Programming, Web Server Administration, SQL

	Server 2000, Oracle, Cisco router and firewall configuration.
Topics covered on the exam: 1. Access Control Systems & Methodology 2. Applications & Systems Development 3. Business Continuity Planning 4. Cryptography 5. Law, Investigation & Ethics 6. Operations Security 7. Physical Security 8. Security Architecture & Models 9. Security Management Practices 10. Telecommunications, Network & Internet Security	Topics covered on the exam: 1. Ethics and Legal Issues 2. Footprinting 3. Scanning 4. Enumeration 5. System Hacking 6. Trojans and Backdoors 7. Sniffers 8. Denial of Service 9. Social Engineering 10. Session Hijacking 11. Hacking Web Servers

	12. Web Application Vulnerabilities 13. Web Based Password Cracking Techniques 14. SQL Injection 15. Hacking Wireless Networks 16. Virus and Worms 17. Physical Security 18. Hacking Linux 19. IDS, Firewalls and Honeypots 20. Buffer Overflows 21. Cryptography 22. Penetration Testing Methodologies

How does CEH compare with SANS GIAC certifications?

CEH is vendor/training neutral. GIAC is SANS only, which is based on their training specifically.

I am working on by GIAC certification and have 5 years of security background plus networking, is this certification designed for someone like me?

Yes, absolutely. One of EC-Council goals is to increase the number of skilled network security practitioners and professionals in the industry.

I am pursuing my CCIE, how would your certification differ from what Cisco offers?

Cisco is product-focused and product specific, CEH addresses the "hacking principles" to sound security across the spectrum of networks/systems/products/components, etc. CEH is vendor neutral.

How long is the certification valid, and what about re-certification?

The CEH certification is valid for life since you are certified on a particular version. The current version of the exam is 4.

Hacking Case Studies

News #1

Internet hacker wanted in US arrested in Thailand

A Ukrainian man wanted in the United States for large-scale Internet fraud and causing more than $100 million in business

losses has been arrested in Thailand, US and Thai officials said on Wednesday.

US embassy officials identified the suspect as Maksym Kovalchuk, although he was thought to use a number of aliases. Thai authorities identified him as 25-year-old Maksym Vysochanskyy. He was arrested late on Tuesday while shopping with his wife in Bangkok.

The man, who has denied any wrongdoing, is accused of distributing thousands of fake software programs worth more than $3 million and pioneered a new form of Internet theft and account takeover known as Web-spoofing, a US Embassy spokesman said.

"This Web-spoofing activity has accelerated identity-based Internet crimes in the US and internationally," the spokesman said.

The programmes contained computer code which granted him "a back door" to businesses that installed the programmes on their computers, posing "a huge danger" to their financial security, the spokesman said.

Kovalchuk is wanted in northern California on charges of criminal copyright infringement, trafficking in counterfeit goods, money laundering, conspiracy to launder money and the possession of unauthorized access devices.

Appearing before reporters on Wednesday, the suspect denied the charges, saying: "They took the wrong person. I didn't do anything wrong in the Net."

With tears in his eyes, he also complained about being treated badly by Thai police while in detention.

The United States is expected to file an extradition request with Thai authorities, the spokesman said. The maximum penalty faced by the suspect if he is found guilty of the charges was not immediately known.

The arrest follows a lengthy investigation by US officials. A US Secret Service attache at the US Embassy in Thailand, James Gehr said that the police had been following the suspect for more than two years, and that he had caused more than $100 million in losses.

News #2

Youth Hacked Into Database, Los Angeles School Says

A 17-year-old junior at Don Lugo High School in Chino, in the Los Angeles area, allegedly hacked into his school's computer system this month, changing his and a classmate's grades and also tapping into confidential student information, including Social Security numbers, officials said Tuesday. The male student, whose name is being withheld because he is a minor, was arrested May 14 at the Chino Valley Unified School District offices on suspicion of violating state theft and privacy laws. He was released to his parents' custody. The Chino Police Department has turned the case over to the San Bernardino County district attorney's office. District officials mailed letters Tuesday to the school's 2,400 students, notifying parents and recommending that they contact the nation's three major credit bureaus and place a fraud alert on their child's file. Officials said 1,744 students had their Social Security numbers in the database. The teenager acknowledged to district officials that

he broke into the computer system, school officials said. He remained on suspension Tuesday and could face expulsion. The other student's role is still being investigated, they said.

"This is a unique occurrence," said Bob Blackery, the district's director of instructional support and technology. No other schools in the district were affected, he said. Blackery said that, until this incident, he believed the school's computer system had never been tampered with by a student. The company that provides the software, Orange County-based Eagle Software, also said its programs had never been hacked into. The firm provides software to about 280 districts in the state, Blackery said. School officials said they suspect the student gained entry to the database from a computer on school property. In his backpack, they allegedly found a disk with a copy of the school's database. Authorities are investigating whether the data were misused or further disseminated. "Things like this happen," said John Pruitt Jr., vice president of the district's school board. He and other officials noted that hackers have attacked the Pentagon, NASA and major corporations. "What I'm proud of is how quickly we acted." After a teacher discovered the grade change in the computer, officials said they identified the suspected student within 16 working hours. They immediately began securing the system by working with the software manufacturer to change all passwords and computer pathways into the main computer. The district is also seeking an external audit of its network security procedures.

Yesterday's story was about a Texas student hacking the school grades and today it is Los Angeles. Forget about the lame cyberterrorist alert stuff and let's call for a CODE ORANGE ALERT on the school networks.

News #3

Hackers hijack computers remotely in new surge of spam

The Flint Hills School, a prep academy in Oakton, Va., might seem an unlikely place to find an Internet spammer. But late last year, technicians at America Online were able to trace the origin of a new torrent of spam, or unsolicited e-mail advertisements, to the school's computer network.

On further investigation, though, AOL determined that the spammers were not enterprising students or moonlighting teachers. Instead, a spam-flinging hacker -- who still has not been found -- had exploited a software vulnerability to use the school's computers to relay spam while hiding the e-mail's true origins.

It was not an isolated incident. As spam has proliferated -- and with it the attempts by big Internet providers to block messages sent from the addresses of known spammers -- many mass e-mailers have become more clever in avoiding the blockades by aggressively bouncing messages off the computers of unaware third parties.

In the past two years, more than 200,000 computers worldwide have been hijacked without the owner's knowledge and are currently being used to forward spam, according to AOL and other Internet service providers. And each day thousands of additional PCs are compromised at companies, institutions and -- most commonly of all -- homes with high-speed Internet connections shared by two or more computers.

Mostly, the spammers are exploiting security holes in existing software, but increasingly they are covertly installing e-mail forwarding software, much like a computer virus.

“This is not about a hacker trying to show off, or give you a hard time," said William Hancock, the chief security officer for Cable & Wireless, the British telecommunications company. ‘This is about money. As long as there are people who want spam to go out, this is not going to go away.''

News #4

Some sites and web host make easy marks for hackers on the Web

There is an epidemic of graffiti on the Internet. The Web sites of Al-Jazeera and Madonna are among the thousands defaced during recent months. According to mi2g, a British company, the number of vandalized sites is likely to reach more than 185,000 this year - more than double the number during 2002. These defacements occur when cybervandals replace existing Web pages with other material, such as political slogans or obscene messages. Could it really be so easy to deface a Web site? Apparently it is. "It's incredibly easy to do," says Paul Henry, an expert in defacements and vice president of CyberGuard, a Fort Lauderdale, Fla., network-security company. "Any 13-year-old with an Internet connection and a little spare time can be a hacker." This is because experienced hackers have created easy-to-use software tools enabling typical computer users to become cybervandals. One program mentioned by Henry - I won't reveal the name - runs on Windows PCs. The program looks for certain types of vulnerabilities in Web servers - the computer systems for storing and delivering Web pages to browsers. To use the program, you simply enter the address of the

site you are hoping to vandalize, then let the program attempt to find a vulnerability. If it finds one, you are able to change the content of a Web page at the site and forward the vandalized page as a replacement for the real one. "It can literally be done in seconds," Henry says. "It's point-and-click Web site defacement."

News #5

Canuck Web sites hacked

Another front of the war on Iraq is being fought on the Internet as hackers have increased attacks by 450%, with Canadian Web sites among the most popular targets, says a Toronto-based security consultant.

Hacker activity has increased dramatically since the U.S. and U.K. started their war against Iraq, said Claudiu Popa, of LSM Consulting. She said one group of hackers reportedly single-handedly defaced 800 Web sites with anti-war messages.

Popa said Canadian Web sites are at the top of list of the targets for hackers with attacks increasing by 1,000% from last year.

News #6

Japanese Web Sites Hacked

TOKYO, Jan. 25 — Japan suffered an embarrassment today when hackers penetrated two government Web sites, leaving a message in one of them criticising the Japanese government's position on the 1937 Nanjing Massacre.

Computer systems at Japan's Management and Coordination Agency were raided on Monday and its homepage was replaced with derogatory messages insulting the Japanese in the first-ever hacking of the country's government computer system. The hackers left a message on the Web site in Chinese blasting the Japanese government for refusing to acknowledge that the Nanjing Massacre took place, media reports said. Call for Protest

Jiji news agency said it had deciphered the message, which originally came in garbled, to read: "The Chinese people must speak up to protest the Japanese government for refusing to acknowledge the historical misdeed of the 1937 Nanjing Massacre." Hundreds and thousand of civilians were massacred by Imperial Army troops during the 1937-38 occupation of the central Chinese city. A meeting by ultra-rightist Japanese in Osaka last weekend to whitewash the incident, also called the Rape of Nanking, has whipped up new anger in China, where hundreds marched through the streets of Nanjing to denounce the conference.

Statistics

"Web spending on IT products and services [is expected] to more than double from $119.1 billion in 2000 to $282.5 billion in 2003."

From The Computer Security Institute with the participation of the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad, 22 March 2000, http://www.gocsi.com/prelea_000321.htm, out of 643 respondents:

- 25% of respondents detected system penetration from the outside.
- 27% of respondents detected denial of service attacks.
- 79% detected employee abuse of Internet access privileges (for example, downloading pornography or pirated software, or inappropriate use of e-mail systems).
- 85% detected computer viruses
- 93% of respondents have WWW sites.
- 43% conduct electronic commerce on their sites (in 1999, only it was only 30%).
- 19% suffered unauthorized access or misuse within the last twelve months.
- 32% said that they didn't know if there had been unauthorized access or misuse.
- 35% of those acknowledging attack, reported from two to five incidents.
- 19% reported ten or more incidents.
- 64% of those acknowledging an attack reported Web-site vandalism.
- 60% reported denial of service.
- 8% reported theft of transaction information.
- 3% reported financial fraud.
- 273 organizations that were able to quantify their losses reported a total of $265,589,940