Ethical hacking 1.0 (terms and rules)

Péter Török, Imre Négyesi, János Rikk

National University of Public Service, Hungary

Abstract

Ethical hacking is a buzzword of nowadays, but what does it mean exactly? Who the ethical hackers are and what they do? The main goal of this paper is to clearly define the most important notions. What does cybercrime mean, where is the threshold between white and dark zone. What types of hackers we can identify and what skills do they need.

Keywords: ethical hacker, cybercrime, security threats

„Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access."

Hacker is one of the most misunderstood and overused terms in the security industry. Everyone from the nightly news to authors to Hollywood and the rest of the media uses the term frequently. Thanks to overuse of the term and the fact that it is almost constantly attached to activities that are shady or even criminal in nature, the general public looks at anyone with the label hacker as up to no good. Hackers are viewed as those operating in the shadows, antisocial and antiestablishment in many cases. Other members of the public have even come to embrace hackers as the new social activists thwarting politicians, governments, large corporations, and others. Newsworthy events by loosely organized groups such as Anonymous and Lizard Squad have contributed to the public perception of the hacker. While many have taken different stances and have different opinions of whether hackers are good or bad, this paper will not seek to pass judgment either way on many of those who engage in hacking.

Computers have become mandatory to run a successful business. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. Hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cybercrimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks.

Among the many situations that have contributed to the increase in hacking and cybercrime are the amount of information being passed and the overall dependency on the Internet and digital devices. Over the last decade, the number of financial transactions online has increased, creating a tempting target for crooks. Also, the openness of modern devices such as smartphones and technologies such as Bluetooth has made hacking and stealing information more prevalent. Lastly, we can also point to the number of Internet-connected devices such as tablets and other gadgets that individuals carry around in increasing numbers. Each of these devices has attracted the attention of criminals with the temptation of stealing never before heard of amounts of money, data, and other resources. As computer crime laws began to be passed, the bragging rights for hacking a website became less attractive. Prank activity seems to have slowed down, whereas real criminal activity has increased. With online commerce, skills started going to the highest bidder, with crime rings, organized crime, and nations with hostile interests using the Internet as an attack vector.

Cybercrime is the use of computers and networks to perform illegal activities such as spreading computer viruses, online bullying, performing unauthorized electronic fund transfers, etc. Most cybercrimes are committed through the internet. Some cybercrimes can also be carried out using mobile phones via SMS and online chatting applications.

The following list presents the common types of cybercrimes:

Computer Fraud: Intentional deception for personal gain via the use of computer systems.

Privacy violation: Exposing personal information such as email addresses, phone number, account details, etc. on social media, websites, etc.

Identity Theft: Stealing personal information from somebody and impersonating that person.

Sharing copyrighted files/information: This involves distributing copyright protected files such as eBooks and computer programs etc.

Electronic funds transfer: This involves gaining an un-authorized access to bank computer networks and making illegal fund transfers.

Electronic money laundering: This involves the use of the computer to launder money.

ATM Fraud: This involves intercepting ATM card details such as account number and PIN numbers. These details are then used to withdraw funds from the intercepted accounts.

Denial of Service Attacks: This involves the use of computers in multiple locations to attack servers with a view of shutting them down.

Spam: Sending unauthorized emails. These emails usually contain advertisements.

Potential security threats

A computer system threat is anything that leads to loss or corruption of data or physical damage to the hardware and/or infrastructure. Knowing how to identify computer security threats is the first step in protecting computer systems. The threats could be intentional, accidental or caused by natural disasters.

Security Threat is defined as a risk that which can potentially harm computer systems and organization. The cause could be physical such as someone stealing a computer that contains vital data. The cause could also be non-physical such as a virus attack. In these tutorial series, we will define a threat as a potential attack from a hacker that can allow them to gain unauthorized access to a computer system.

physical threats

A physical threat is a potential cause of an incident that may result in loss or physical damage to the computer systems.

Internal: The threats include fire, unstable power supply, humidity in the rooms housing the hardware, etc.

External: These threats include Lightning, floods, earthquakes, etc.

Human: These threats include theft, vandalism of the infrastructure and/or hardware, disruption, accidental or intentional errors.

To protect computer systems from the above mentioned physical threats, an organization must have physical security control measures.

non-physical threats

A non-physical threat is a potential cause of an incident that may result in:

- Loss or corruption of system data
- Disrupt business operations that rely on computer systems
- Loss of sensitive information
- Illegal monitoring of activities on computer systems
- Cyber Security Breaches
- Others

The non-physical threats are also known as **logical threats**.

Common types of non-physical threats: Virus, Trojans, Worms, Spyware, Key loggers, Adware, Denial of Service Attacks, Distributed Denial of Service Attacks, Unauthorized access to computer systems resources such as data, Phishing, Other Computer Security Risks

Types of hackers

A Hacker is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.

Hackers are classified according to the intent of their actions. The following list classifies hackers according to their intent.

Symbol	Description
	**Ethical Hacker (White hat):** A hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration testing and vulnerability assessments.
	**Cracker (Black hat):** A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.
	**Grey hat:** A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner.
	**Script kiddies:** A non-skilled person who gains access to computer systems using already made tools.
	**Hacktivist:** A hacker who use hacking to send social, religious, and political, etc. messages. This is usually done by hijacking websites and leaving the message on the hijacked website.

1. Table

Skill required

As a hacker, you will need to develop skills that will help you get the job done. These skills include learning how to program, use the internet, good at solving problems, and taking advantage of existing security tools. What languages? It depends on your target computer systems and platforms.

LANGUAGES	DESCRIPTION	PLATFORM	PURPOSE
HTML	Language used to write web pages.	*Cross platform	**Web hacking** Login forms and other data entry methods on the web use HTML forms to get data. Been able to write and interpret HTML, makes it easy for you to identify and exploit weaknesses in the code.
JavaScript	Client-side scripting language	*Cross platform	**Web Hacking** JavaScript code is executed on the client browse. You can use it to read saved cookies and perform cross site scripting etc.
PHP	Server-side scripting language	*Cross platform	**Web Hacking** PHP is one of the most used web programming languages. It is used to process HTML forms and performs other custom tasks. You could write a custom application in PHP that modifies settings on a web server and makes the server vulnerable to attacks.
SQL	Language used to communicate with database	*Cross platform	**Web Hacking** Using SQL injection, to by-pass web application login algorithms that are weak, delete data from the database, etc.
Python **Ruby** **Bash** **Perl**	High level programming languages	*Cross platform	**Building tools & scripts** They come in handy when you need to develop automation tools and scripts. The knowledge gained can also be used in understand and customization the already available tools.
C & C++	High level programming	*Cross platform	**Writing exploits, shell codes, etc.** They come in handy when you need to write your own shell codes, exploits, root kits or understanding and expanding on existing ones.

2. Table

* Cross platform means programs developed using the particular language can be deployed on different operating systems such as Windows, Linux based, MAC etc.

The process

- **Gather Information**: This is the first stage, the learns as much as he can about the intended victim. The information is gathered from company websites, other publications and sometimes by talking to the users of the target system.
- **Plan Attack**: The attackers outline how he/she intends to execute the attack
- **Acquire Tools**: These include computer programs that an attacker will use when launching the attack.
- **Attack**: Exploit the weaknesses in the target system.

- **Use acquired knowledge**: Information gathered during the social engineering tactics such as pet names, birthdates of the organization founders, etc. is used in attacks such as password guessing.

Information plays a vital role in the running of business, organizations, military operations, etc. **Information in the wrong hands can lead to loss of business or catastrophic results. To secure communication, a business can use cryptology to cipher information**.

Social engineering is the art of manipulating users of a computing system into revealing confidential information that can be used to gain unauthorized access to a computer system. The term can also include activities such as exploiting human kindness, greed, and curiosity to gain access to restricted access buildings or getting the users to installing backdoor software.

Cryptography is the study and application of techniques that hide the real meaning of information by transforming it into nonhuman readable formats and vice versa.

Cryptanalysis is the art of trying to decrypt the encrypted messages without the use of the key that was used to encrypt the messages. Cryptanalysis uses mathematical analysis & algorithms to decipher the ciphers.

The success of cryptanalysis attacks depends

- Amount of time available
- Computing power available
- Storage capacity available

commonly used Cryptanalysis attacks:

- **Brute force attack**– this type of attack uses algorithms that try to guess all the possible logical combinations of the plaintext which are then ciphered and compared against the original cipher.
- **Dictionary attack**– this type of attack uses a wordlist in order to find a match of either the plaintext or key. It is mostly used when trying to crack encrypted passwords.
- **Rainbow table attack**– this type of attack compares the cipher text against pre-computed hashes to find matches.

So, What Is an Ethical Hacker?

Ethical Hacking is identifying weakness in computer systems and/or computer networks and coming with countermeasures that protect the weaknesses. Ethical hackers must abide by the following rules.

- Get written permission from the owner of the computer system and/or computer network before hacking.
- Protect the privacy of the organization been hacked.
- Transparently report all the identified weaknesses in the computer system to the organization.
- Inform hardware and software vendors of the identified weaknesses.

WHY?

Information is one of the most valuable assets of an organization. Keeping information secure can protect an organization's image and save an organization a lot of money. Hacking can lead to loss of business for organizations that deal in finance such as PayPal. Ethical hacking puts them a step ahead of the cyber criminals who would otherwise lead to loss of business.

What Are Your Responsibilities?

One of the details you need to understand early and never forget is permission. As an ethical hacker you should never target a system or network that you do not own or have permission to test. If you do so, you are guilty of any number of crimes, which would be detrimental not only to your career but perhaps to your freedom as well. Before you test a target, you should have a contract in hand from the owner giving you permission to do so.

Also remember that you should test only those things you have been contracted to test. If the customer or client decides to add or remove items from the test, the contract must be altered to keep both parties out of legal trouble. Take special notice of the fact that ethical hackers operate with contracts in place between themselves and the target. Operating without permission is unethical; operating without a contract is downright stupid and illegal.

In addition, a contract must include verbiage that deals with the issue of confidentiality and privacy. It is possible that during a test you will encounter confidential information or develop an intimate knowledge of your client's network. As part of your contract you will need to address whom you will be allowed to discuss your findings with and whom you will not. Generally, clients will want you to discuss your findings only with them and no one else.

According to the International Council of Electronic Commerce Consultants (EC-Council) you, as a CEH, must keep private any confidential information gained in your professional work (in particular as it pertains to client lists and client personal information). You cannot collect, give, sell, or transfer any personal information (such as name, email address, Social Security number, or other unique identifier) to a third party without your client's prior consent. Keep this in mind since a violation of this code could not only cause you to lose trust from a client but also land you in legal trouble. Contracts are an important detail to get right; if you get them wrong it could easily mean legal problems later. The problem with contracts is that most people find the legalese nearly impossible to understand and the amount of preparation intimidating to say the least. I strongly recommend that you consider getting a lawyer experienced in the field to help you with contracts.

A contract is essential for another extremely important reason as well: proof. Without a contract you have no real proof that you have permission from the system owner to perform any tests.

Once ethical hackers have the necessary permissions and contracts in place, they can engage in penetration testing, also known as pen testing. This is the structured and methodical means of investigating, uncovering, attacking, and reporting on the strengths and vulnerabilities of a target system. Under the right circumstances, pen testing can provide a wealth of information that the owner of a system can use to plan and adjust defenses.

Ethical Hacking and Penetration Testing

Ethical hackers engage in sanctioned hacking—that is, hacking with permission from the system's owner. In the world of ethical hacking, most tend to use the term pentester, which is short for penetration tester. Pentesters do simply that: penetrate systems like a hacker but for benign purposes.

As an ethical hacker, you must become familiar with the lingo of the trade. Here are some of the terms you will encounter in pen testing:

Hack Value This term describes a target that may attract an above-average level of attention from an attacker. Presumably because this target is attractive, it has more value to an attacker because of what it may contain.

Target of Evaluation A target of evaluation (TOE) is a system or resource that is being evaluated for vulnerabilities. A TOE would be specified in a contract with the client.

Attack This is the act of targeting and actively engaging a TOE.

Exploit This is a clearly defined way to breach the security of a system.

Zero Day This describes a threat or vulnerability that is unknown to developers and has not been addressed. It is considered a serious problem in many cases.

Security This is a state of well-being in an environment where only actions that are defined are allowed.

Threat This is considered to be a potential violation of security.

Vulnerability This is a weakness in a system that can be attacked and used as an entry point into an environment.

Daisy Chaining This is the act of performing several hacking attacks in sequence with each building on or acting on the results of the previous action.

As an ethical hacker, you will be expected to take on the role and use the mind-set and skills of an attacker to simulate a malicious attack. The idea is that ethical hackers understand both sides, the good and the bad, and use this knowledge to help their clients. By understanding both sides of the equation, you will be better prepared to defend yourself successfully. Here are some things to remember about being an ethical hacker:

You must have explicit permission in writing from the company being tested prior to starting any activity. Legally, the person or persons who must approve this activity or changes to the plan must be the owner of the company or their authorized representative. If the scope changes, you must update the contract to reflect those changes before performing the new tasks.

You will use the same tactics and strategies as malicious attackers. You have the potential to cause the same harm that a malicious attack will cause and should always consider the effects of every action you carry out.

You must have knowledge of the target and the weaknesses it possesses.

You must have clearly defined rules of engagement prior to beginning your assigned job.

You must never reveal any information pertaining to a client to anyone but the client.

If the client asks you to stop a test, do so immediately.

You must provide a report of your results and, if asked, a brief on any deficiencies found during a test.

You may be asked to work with the client to fix any problems that you find. As I will discuss several times in this text, never accept a verbal agreement to expand test parameters. A verbal agreement has no record, and there is a chance of getting sued if something goes wrong and there's no record.

Under the right circumstances and with proper planning and goals in mind, you can provide a wealth of valuable information to your target organization. Working with your client, you should analyze your results thoroughly and determine which areas need attention and which need none at all. Your client will determine the perfect balance of security versus convenience. If the problems you uncover necessitate action, the next challenge is to ensure that existing usability is not adversely affected if security controls are modified or if new ones are put in place. Security and convenience often conflict: The more secure a system becomes, the less convenient it tends to be.

Although ethical hacking sometimes occurs without a formal set of rules of engagement, pen testing does require rules to be agreed on in advance in every case. If you choose to perform a pen test without having certain parameters determined ahead of time, it may be the end of your career if something profoundly bad occurs. For example, not having the rules established before engaging in a test could result in criminal or civil charges, depending on the injured party and the attack involved. It is also entirely possible that without clearly defined rules, an attack may result in shutting down systems or services and stopping the functioning of a company completely, which again could result in huge legal and other issues for you.

We hope to successfully clarify some basic concepts. Knowing them, we can play with clear rules, protecting ourselves from serious problems.

Real learning can begin…

References

1. Négyesi I.: A megfigyelés és információgyűjtés múltja, jelene és jövője; SZAKMAI SZEMLE: A KATONAI NEMZETBIZTONSÁGI SZOLGÁLAT TUDOMÁNYOS-SZAKMAI FOLYÓIRATA 2009/3:(3. szám) pp. 35-50. (2009)

2. Linus Torvalds: Just for Fun; 2001.

3. Pekka Himanen: The Hacker Ethic; 2001.

4. E. S. Raymond, G. L. Steele: Jargon File; 1983.

5. Imre Négyesi: Open source apps; Henderson DEVLART LLC. 2017. ISBN 978-0-9977210-7-2

6. Török Péter, Rikk János: BASH scripting Henderson DEVLART LLC, 2017. 68 p. (ISBN:978-0-9977210-6-5)