# ETHICAL HACKING: AN IMPACT ON SOCIETY

**Article** · April 2014

CITATIONS
9

READS
54,836

**1 author:**

Meenaakshi N. Munjal
Manav Rachna International University
**12** PUBLICATIONS **43** CITATIONS

SEE PROFILE

# ETHICAL HACKING: AN IMPACT ON SOCIETY

***Meenaakshi N. Munjal***
*HOD & Asst. Professor – Information Technology,*
*Manav Rachna International University,*
*minaximunjal2002@gmail.com*

## ABSTRACT

*Ethical hacking is the way to find out the weaknesses and vulnerabilities in the system or computer network. It is a way to describe the procedure of hacking in an ethical way for any network. The ethical hacker has the good purpose to do it. Actually it has become the general perception in our mind for hacker that he will be bad, fanatic, criminal and unethical. Basically some of the hacker has even done very badly with some organisations like they have stolen very important information of their customers. In some of the government organisations they have damaged very confidential information like social security numbers and other sensitive information. That is the reason hackers are not having very good reputation. To avoid such conditions many organisation have hired many ethical hackers to keep a track on their system and computer network. Ethical hackers are supposing to test and check vulnerabilities and weaknesses in the present system. There is one another face of the coin which tells that without hackers the vulnerabilities and holes of software would remain undiscovered [1]. In this paper I have tried to explain the good and bad face of hacker and even of ethical hackers also and what re the different impact on the different areas of our society. A study shows that almost 90% attacks happen on the inside which shows that easy it is to invade into the system or network for insiders.*

*I have tried to explore the ethics behind the ethical hacking and the problems lie with this particular field of information technology where security is concerned. Though ethical hacking has become a very upcoming technological subject from the last few years, now the doubt remains the true intentions of the hacker. Hackers in this context have had a very measurable impact on society. There are several fields in computing where hackers made measurable impact on society. In this paper I have tried to look into different ways how we can make ethical hacking safe and ethical.*

**KEYWORDS:** *Automated Security, Education and Training and Ethical Hacking, Hackers.*

## I. INTRODUCTION

Ethical hacking, as the name suggests a hacking which is ethical. It is also called as penetration testing. This is the technique which is being used by number of professionals to do hacking but that is not illegal it is rather ethical. That is the reason it is to be called as ethical hacking.

Though all the tools, tricks and techniques are used in this regard are the same as being used in hacking, but it is done with the consent of the target, that's why is not hacking it is ethical hacking. It is the way through which an ethical hacker will discover some vulnerability from the hacker's point of view so that the system can be made more secure and safe.

Ethical hacking also makes sure that the claim made by target should be genuine.

## II. WHAT IS EHICAL HACKING?

Ethical hacking is the term which is being used by professionals in order to make the system more secure and safe. A person will be called as an ethical hacker when he will not destroy the security of the system rather he will take care of the security and safety of the system from the view point of the hacker. The person who is doing all these efforts are to be known as ethical hacker or white hat hacker. In the ethical hacking we have to make sure about the security of the system as far as information technology is concerned. As the name says itself ethical hacking, it has two meanings or definitions – one which is the hobby or profession of a particular person who is interested to make career in this field. Another one who is breaking one's system for a purpose. Well the first definition has become older in

## IV. HACKERS?

Ethical hackers are mostly people with a good knowledge of operating systems and computer networks technology. An ethical hacker's knowledge is very much comparable to the one of a "real" hacker. It is known, that some black hats have been converted to white hats and are now using their knowledge on how to hack a system in an ethical way. Hiring ex-hackers as ethical hackers is very controversial. After all, an ethical hacker will see sensitive information and needs to be extremely trustworthy.

During his assignment an ethical hacker may get access to sensitive and confidential customer information where he will see and discover customers' weak points Therefore lot of companies don't believe to hire previous hackers to do their ethical hacks. As per their understanding by doing so the risk and insecurity level is very high. today's scenario whereas the second one has a meaning. The hacker culture began in the 1960s and 1970s as an intellectual movement: exploring the unknown, documenting the arcane, and doing what others cannot. Ethical hacking perfectly fits into the security life cycle as mentioned in the figure 1. It is actually a way to do the security assessment which can be checked from the technical point of view.


**Figure 1: The Security Life Cycle**

## III. WHO ARE ETHICAL

According to them previous employees know each and every thing from the root so they can easily destroy the present system. As already pointed out, one of the main requirements for an ethical hacker is its trustworthiness. The customer needs to be 100% certain that information found by the ethical hacker won't be abused. Another very important ability is patience. An ethical hacker is most trustworthy employee for the organisation who is hired to check about the vulnerabilities and other issues in the computer network system to maintain its security and safety. One another truth is lying in this case that gaining access to somebody's computer system or network without his consent is a crime whereas the penetration testing with the consent of target is not a crime rather in this case target is interested to make proper arrangement and other security for his system. There are so many certified ethical hackers are in the IT

field those who are working for the same reason for the targets. In the last I would like to mention this fact also that it is the culture or religion of a particular person how he is behaving in different in different environment moreover he has his own right or wrong perception towards the understanding of few things [5].

# V. TYPES OF ETHICAL HACKING

There are mainly four different types of ethical hacking depending on the knowledge of the hacker. There are many hackers whose intentions are not to harm. Basically the term ethical hacking itself says that hacking which is done for the purpose of not to harm rather take preventive measures to maintain the security and safety and check the vulnerabilities in the current system.

## A. HACKTIVISTS

This is the technique through which a hacker is hacking into any computer system illegally for any reason may be social or political. In this activity a hacker can leave a very large message on the main page of any well-known website or any other so called important message so that visitor will see that message and react accordingly. It may display any kind of speech or any social message which can attract users and they may participate in the discussion or forum. This may lead to hacking the system without the consent of the target. It may have any social message like ethical hacking is ethical or not which may attract number of users and they can participate in the discussion.

## B. CYBERWARRIOR

Cyber warrior is a kind of hacker who is being hired by an organisation or by an individual to creep into the system or computer network. Cyber warrior will act as a wicked hacker will try to find out the vulnerabilities or weaknesses in the present system. This hacker is not having any prior knowledge of system or computer network in which he is gaining access. By doing this activity he will come to know about the vulnerabilities in the present system or computer network and can tell the organisation or individual to work upon on it so that the website or other data can be secured from hacking in future.

## C. WHITE BOX PENETRATION TESTERS

White box penetration testers are also called as white box hackers. They are the employees those are hired by the organisation to break into their current system or computer network. They are the legal penetration testers. They are legally breaking into the system or computer network for the organisation or for an individual to help them by telling the vulnerabilities and weaknesses in the present system.

White box testers are working in the same way as cyber warriors are working the only difference is that cyber warriors do not have knowledge of the system or computer network of the organisation or of individual whereas white box hackers are having full knowledge of the system or computer network of the target. We can also consider it as that the attack is being simulated by an insider of the organisation.

## D. CERTIFIED ETHICAL HACKER / LICENSED PENETRATION TESTER

As the name says itself that certified ethical hacker or licensed penetration tester are those certified or licensed professional in the field of hacking who are performing the duties of both i.e. black box hacker and white box hackers. They are responsible to look into the system and networks to find out the vulnerabilities and weaknesses.

These certifications or license are given by International Council of E-Commerce Consultants. Ethical hackers are required to recertify themselves after every three years.

# VI. TYPES OF HACKERS

There are basically three types of hackers on the basis of their way of doing and what their intentions behind for hacking are.

### A. WHITE HAT HACKER

White hat hackers are those hackers who are gaining access into the system or computer network with the consent of the target to find out the vulnerabilities and security flaws in the present system. They are actually helping the organisation or individual by making them aware about such flaws. These types of professionals are hired by computer security companies. White hat hackers are also called as sneakers. In the company when there are more than one sneaker then the group of such professionals are called as "tiger team". So we can say that white hat hacker is actually an ethical hacker who is opposing all exploitation in the computer system, ethically.

### B. BLACK HAT HACKER

A black hat hacker is a person who is exploiting the computer system or computer network without the consent or permission from any authorised party. His main goal is to do any kind of mishap to the system. Basically black hat hacker is a kind of person who uses his knowledge of vulnerabilities to exploit any system. He is much more concerned with his private gain. These persons are not interested to reveal them in the public. They may write their own code to destroy the entire system and its security for their private interest and gain.

### C. GREY HAT HACKER

A grey hat hacker is a person who is skilled enough to act as a good or bad in both ways. At times grey hat hacker can act legally and at times he may act illegally. Grey hat hackers generally do not hack the system for their personal gain. They normally don't have any kind of nasty intentions, but they may commit a crime while using technology. A grey hat hacker will not report to the system administrator for any kind of dissemination.

# VII. ETHICAL HACKING METHODOLOGY

Ethical hacking procedure has basically five different stages. Any ethical hacker will follow these stages one by one and will reach to his goal. Figure 3 demonstrates the five stages of ethical hacking which are being followed by any ethical hacker in a computer system.

### A. RECONNAISSANCE

This is the first stage of attack in which hacker is supposed to collect all the information of that company whose data need to be hacked. This term is also called as foot printing. The literal meaning of reconnaissance means preliminary survey to gain the information. In this stage hacker has to ensure that all information must collect. We can call this stage as pre-attacking phase in hacking. During this phase different types of tools like network mapping and network vulnerability scanning can be used. In this context cheops is a very good tool for network mapping through which network graphs can be generated. The network mapping tool is mainly used for internal ethical hacking. It is not mush used for external purpose.

### B. SCANNING

The next stage in ethical hacking is scanning. With this technique a penetration

tester can easily find out the open doors for any network. In this stage a hacker always tries to make an outline of the target network. The outline includes the IP addresses of the end or target network which are live, other services which are running on those systems and so on. In some of the cases most vulnerabilities scanners do wonderful job of minimizing false positives, and many organisations use them to recognize out-of-date systems or probable new experience that might be exploited by hackers [2].

There are three types of scanning:

**(i) Port Scanning**

With the help of modern port scanning which uses TCP protocol we can even come to know that which operating system is running on the particular hosts. In the technological term port scanning is mainly used to find out the vulnerabilities and weak points in the used port in the network. In this process we have to locate the active host, operating system which is getting used, firewalls, intrusion detection systems, different servers and services running on those servers, boundary devices, routing topologies and other topologies used in the network of the target organisation. By using the foot printing technique we can trace the IP address of the target organisation. Once the IP address is found scanning of TCP and UDP ports of the target system become quite easy for the ethical hacker to map the network. The most common and popular network mapper tool is Nmap which is very powerful and flexible and very easy to use. Nmap network mapper is available for both the operating system i.e. Linux and Windows. Apart of Nmap there are so many network mapper tools are available on the internet like netscantools, Superscan, Unicornscan, Scanrand and Portscan 2000.

**(ii) Network Scanning**

In the network scanning we identify all active hosts which are present on a network. The purpose of this exercise is either to attack them or there is a requirement to assess the network security. In this procedure we will come to know about IP addresses of individual host. All the network scanning tools will be able to tell us about the active hosts and their corresponding IP addresses on the network.

**(iii) Vulnerability Scanning**

In the vulnerability scanning the hacker will come to know about the operating system of the system and other related details of operating system such as its version, service pack if it is installed. The vulnerability scanner will identify the weakness of the operating system so that later can be attacked. Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet.

## C. GAINING ACCESS

This is the most important phase where attackers will get the access of the system or network and have the ability to spoil it completely. Moreover this is also truth that attacker always need not to have access of the system to damage it. I must say that this is the stage where actually a real hacking takes place. Those weak points and vulnerabilities which are exposed during the reconnaissance and scanning phase they are further exploited to gain access in the target system. The method of connection which will be used by an attacker or hacker to damage the system it can be local area network, local access to computer and internet. There are few more examples of the same they are: stack based buffer overflows, session hijacking and denial of service etc. Gaining access also known as owns the system in the hacker world which means now attacker or hacker will have the full access to the target system. Factors that influence the chances of an attacker gaining

access into a target system include the architecture and configuration of the target system, the skill level of the perpetrator, and the primary level of access obtained. One of the most harmful types of the denial-of-service attacks which can be further distributed into several denial-of-service attacks, where a hacker uses a special type of software called "zombie" and he distributes it on number of machines on internet in such an organised manner so that maximum number of machines can be damaged.

### D. MAINTAINING ACCESS

After gaining the access of the target system by a hacker it would be very easy for him to use the system itself and all its resources and exploit them. This is also the case in this context that hacker can use this target system as launch pad so that he can scan other systems and can damage them. This way an entire organisation can be exploited. There are so many attackers or hackers who believe to be undetected and keep on removing all the proofs of their entry in the target system. They use the backdoor or Trojan to get the repeated access in the target system. There is one another option is with them that they can install the rootkit at the kernel level of the operating system and can have the super access in the system. With the help of Trojan horse hackers are able to have user names their passwords and other confidential information like credit card number its passwords etc. of the target.

### E. CLEARING TASKS

This is the last and final stage where hacker want to remove or destroy all evidence of his/her presence and activities for various reasons such as maintain access and evading punitive actions. This is one of the best methods to evade track back. Erasing evidence is the requirement for a hacker to remain obscure. It is really very crucial for invaders to make the system look like it as the same before they gained access and established backdoors for their use. Any files, which have been modified or altered, need to be changed back to their original attributes or format. Information listed, such as file size and date, is just attribute information contained within the file. Following are few activities which are present during this phase.

- Steganography
- Using a tunnelling protocol
- Altering log files

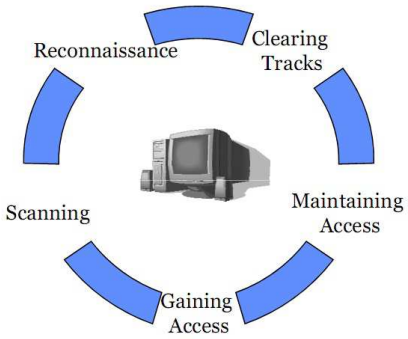


**Figure 2: A complete methodology of ethical hacking**

## VIII. IMPACT ON SOCIETY OF ETHICAL HACKING

Hackers are having very measurable impact on the society. They are attracting more and younger generation. Though ethical hacking is not bad but it is also very important to know that what exactly ethical hackers are doing for the interest of society. If we treat hacker is the person who pushes technology beyond perceived norms, there are several fields in computing where ethical hacking or ethical hackers made a measurable impact. Now a day's internet has become the gateway for any computer to connect to the entire world, which also makes it vulnerable to attacks from the hackers across the world.

### A. IMPACT ON EDUCATION

It is really very hard to teach students hacking. Though students are more

interested to learn this new technique. It is again a hard reality that if teacher is teaching them the concept of hacking he/she can ensure that how a student is taking it. It is very much possible that student will be curious to hack the other computer and may do some bad activities as well. It is not the task of argument that what an instructor is teaching them and we cannot say this also that why they have opted this course for learning. I believe that entire class is taking the lecture in a simple manner but there may be few students who are having bad intentions and can do hacking. As far as global technological knowledge is concerned it is very important to give the latest knowledge to students in the field of IT and other related areas. "A very big problem with undergraduate students to teach this approach that a teacher is effectively providing a loaded gun to them "[4]. There is one another a very big problem with undergraduate students that they actually don't understand the importance and effectiveness of the hacking, but yes definitely they want to apply it either for good or bad purpose. There are number of students even of first semester are always come with this request that when we can have workshop or special classes for Ethical Hacking. It is really very surprising that they don't know about even the ethics of computer but they want to go for hacking which is ethical, as per their understanding.
There are few measures which can take place at the university or college level for students to not indulge in hacking activity which may harm at later stage. University can take personal interview, checking for the criminal background and some sort of professional certification from the students.

Students are mainly going for the security courses there they can easily learn the hacking and its effectiveness. They are getting attracted towards this new aspect of learning where they can hack anybody's computer or any peripheral device in few minutes. By taking some kind of workshops and training we can make them understand that ethical hacking is not good if it is not containing ethics. Again it is also a hard reality that ethical hackers are highly paid individuals. We have to make sure that by doing such activities ethical hacking should be ethical. If we don't have above measures in place then we have to ensure it manually that our systems are safe and secure. So ethical hacking can also ensure about the safety and security of our system if it is done ethically.

## B. IMPACT ON BUSINESS

In today' world no business is without the use of IT. With the help of IT all our data is made electronic. Due to this reason maximum or I can say all business transactions are done electronically. We can also say this demand of today's generation. With the growth of Internet there are number of shopping and auctions websites those are influencing customers and selling their goods online. These sites are giving very good rewards and other discounts as well. It is very easy for an ethical hacker to buy number of goods and can avoid to pay the amount because they know that they can easily do it. They can even use other's personal data or account information to solve their own purposes. It is really a hard fact that some computer programmers are very good and ethical and doing their job effectively and well but they can use their ability as and when they require doing so. It is very unfortunate that some skilled professionals use their skills and ability to harm the society by finding vulnerabilities in their company's system, attacking them, creating virus programs, making code for not to accept the payment for the desired service. As we know that the corruption is the major fact in the today's world it is very difficult to find out the trust worthy and perfect resource to do ethical hacking for us. If in case an ethical hacker is good and doing his job very well it is again very hard to know about his true intentions. At times

this situation has also come up that if an ethical hacker is corrupt then may be the company is corrupt if they refuse any mishap. By seeing above all problems and difficulties with ethical hackers it is always advisable that counseling and motivations are the only way out to let them understand that they have to work for good reasons and with good intentions also.

## C. IMPACT ON WORK PLACE AND ITs SECURITY

At the workplace it is very important to maintain its security and safety in a well-defined manner. As we know that today's world every data of the company is in the electronic form. Ethical hacker can easily take this data and manipulate it according to his need and requirement. Few days back I have read in a book that a lady's apartment in Mumbai was been hacked by a person sitting in another corner in the world and he has also switched on her Webcam as well. This is really very hard to digest that somebody can do this also. Ethical hacker can steal all the information and personal data related to employees. He may even make information inaccurate as well. Ethical hacker is in the company as the name of security person in IT but we will never come to know what exactly he can do. He may write the virus code or even allow the virus code to enter into the company's server to harm it. At times ethical hackers even don't realize the fact and effect of certain virus and worms. Being into the company's insider he has all the rights to access all the confidential data of the company. It is really depends on the true intentions of the ethical hackers that how they do their job well. Besides that there certain tools are also available through which we can easily come to know that whether information are being used for good purpose or for bad purpose. It is now the observation and deeper analysis that correctly programmed systems would improve the system security. By the name of hacking an ethical hacker may gain the access of data and can exploit them. He may also demand for a heavy amount from the company to release the data and other personal information. It is always a risk to have an ethical hacker in the company, but there are certain tools which may help to come out from any of this situation. As I have already told that providing training and some other motivations may help them to bring the good intentions in the field of ethical hacking.

## D. IMPACT ON TECHNOLOGY

There is no harm to say that almost nothing is secure in the technological world. Information are available to everyone for very reason. There are certain tools available through which anybody can easily get the information related to any system either local or remote. Ethical hacker can easily get the IP addresses of any system and may harm it. For ethical hackers there are many tools available in the global market to help them to do their job effectively. NMap is the effective tool which is available on internet to download and use, it help an ethical hacker to find open ports of the different systems. Acunetix is the tool which tests for web applications vulnerabilities and it is available on internet for an ethical hacker it is very easy to use and get the information. These tools are being used by a normal hacker or by an ethical hacker without any discrimination. Hackers may use them for criminal intentions whereas ethical hackers will use them for the organizations benefits and to identify the weaknesses and flaws in the network security.

I will take an example of Google search engine, while searching some information over the internet on Google we don't find the valuable information because of the privacy concern of the Google to those companies. It is actually not ethical for Google to hold any kind of information for

any company; it may good for hacker but not good for target. In this context companies must ensure that none of the sensitive or secure information should send across the internet. It should not the responsibility of the search engine to show which information and which not to show to the targets rather it is should be prime responsibility of the company and its employees for not to give the sensitive information on the internet. It is like the same way that for shipping the some valuable package and it is decided to send using online system to save the time but it has to go to the post office.

### E. IMPACT ON CONFIDENTIAL INFORMATION

Confidential information in any field is not at all secure in the presence of hacker. There are so many ethical hackers are working in banks where all financial transactions takes place. A hacker can easily have access to the valuable data of all account holders. He can steal or memorize their accounts detail and may make any kind of transaction. He can further blackmail them also. There are so many online shopping and other transactions where frauds being committed. While using the email spam has become an extremely big problem for all the email users which is further the cause of virus attack.

A recent report exposed that spam contributed 70% of all the emails on the internet [3]. It is really a great problem for an ethical hacker to track down all the scenarios. At times it is observed that having access to account will in effect blame on ethical hacker in such a way that even if they have not done anything in any regard. It is really very important to know that hacking is different from ethical hacking. But at times because of all access with ethical hacker they may come in this circle also. Sometimes for an ethical hacker it becomes so difficult to prove that he is not the victim. Here I would like to address on this issue that a respectful job is given to the ethical hacker to cross check the vulnerabilities in the system of any organization, after few days some information were hacked then who is responsible for that an organization or an ethical hacker?

The same case may apply in any defense academy. An ethical hacker is hired to check the vulnerabilities in the security and other issues. After some time if some confidential information is leaked out then who will be responsible for that.

Having access to all confidential information it may assume that ethical hacker may have given/ leaked the private or confidential information. In one another example if one resident has given access to system for administrator for safety measures. Certainly no one would like that any system administrator is watching each and every activity in his home. This is further raising another ethical issue.

## IX. CONCLUSION

To conclude the paper I must say that the work “hacker” carries weight. Hacking may be defined as legal or illegal, ethical or unethical. As we all know that technology is growing so fast and it will continue to do so. With the technological development there are many faces of one technology.

Human mind is very powerful tool and actually has no control. Hackers will always find some way out to get into the system, irrespective of seeing good or bad intentions. It is my hope that in future hackers and ethical hackers will have different ways out for doing the things.

They will be differentiated according to the work given to them. No ethical hacker will be considered as hacker. But as an end user we also make sure for few things like we

have to keep ourselves updated and have sufficient knowledge about those software which are being used for official purpose. We have to use only that software which is coming from reliable sources. We have to use every potential security dealings like Honey Pots, Intrusion Detection Systems and Firewalls etc. We also make sure that every time our passwords must be strong and difficult to crack by any hacker.

## ACKNOWLEDGEMENT

I would like to express my deepest appreciation to all those who provided me the possibility to complete this paper. A special gratitude I give to my husband Mr. Narender Munjal, whose contribution in stimulating suggestions and encouragement helped me to coordinate my paper especially in writing this paper. A very special thanks to my son Kabir N. Munjal without his co-operation I may not complete this paper. Last but not least my parents who are main source of motivation for letting me do this job so peacefully.

## REFERENCES

[1] Jon Erickson, 2008, *"Hacking : The Art of Exploitation"*, 2nd Edition, No Starch Press Inc., ISBN-13: 978-1-59327-144-2, ISBN-10: 1-59327-144-1

[2] David Kennedy, Jim O'Gorman, Devon Kearns and Mati Aharoni, 2011, "Metasploit : The Penetration Tester's Guide", 1st Edition, No Starch Press Inc., ISBN-13: 978-1593272883, ISBN-10: 59327288X

[3] Ankit Fadia, 2005, "The Ethical Hacking: Guide to Corporate Security",1st Edition, ISBN: 989-615-004-4

[4] Tom Wulf, 2003, "Teaching Ethics in Undergraduate Network", Consortium for Computing Sciences in College, Vol 19 Issue 1, 2-3.

[5] Syed A. Saleem, 2006, "Ethical Hacking as a risk management technique", USA, New York, ACM, 201-203