

An overview of ethical hacking and its impact on society

Ms. Athira Raj

Assistant Professor, PG Department of Computer Science, JPM Arts and science College, Labbakkada, Kerala, India

Abstract: Hacking is the process of find out the vulnerabilities in a computer system or a computer network. Hacking is done to gain unauthorized access to a computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer. Legal hacking is called Ethical hacking. This paper discusses Ethical hacking and its impact on society.

Keywords: Ethical hacking, Types of Hackers, Types of hacking, Impact on society

I. INTRODUCTION

As the name implies Ethical hacking which is ethical. It is also referred to as penetration testing. Ethical hacking is done by professionals to do hacking but that is not illegal it is ethical. This is why it is known as ethical hacking. This is the way to discover the weaknesses and vulnerabilities in the system or computer network. The ethical hacker has a good determination to do it.

II. ETHICAL HACKING DEFINITION

Ethical hacking is performed by computer professionals to detect vulnerability in the computer system or computer network. Ethical hacker or white hats those who perform ethical hacking. They work to make a stronger and safer system. They know how to identify the weak points and places where black hats could attack the system. Using that knowledge, they can assist companies and the government in creating more protected systems. These hackers can only do so if they are asked by companies. White hats can explain to companies how they can upgrade their systems.

III. TYPES OF HACKERS

3.1. White hat hackers

White hat hackers are computer professionals. They are certified or authorized to hack the systems. They work for companies, organizations, and governments by getting into the systems. They hack the system from the weak points. This hacking is done to test the level of security of their computer system. By doing this they can identify the vulnerabilities and fix the problems. White hat hackers work as per the rules and regulations of the government.

3.2. Black hat hackers.

A black hat hacker is a person who is exploiting the computer system or computer network without permission from any authorized party. He uses his knowledge of vulnerabilities to exploit any system. He may write his code to destroy the entire system and its security for his private interest.

3.3. Gray hat hackers

A grey hat hacker is a person who can act as a good or bad in both ways. At times grey hat hackers can act legally and at times he may act illegally. They generally do not hack the system for their interest. They 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.

IV. ETHICAL HACKING METHODOLOGY

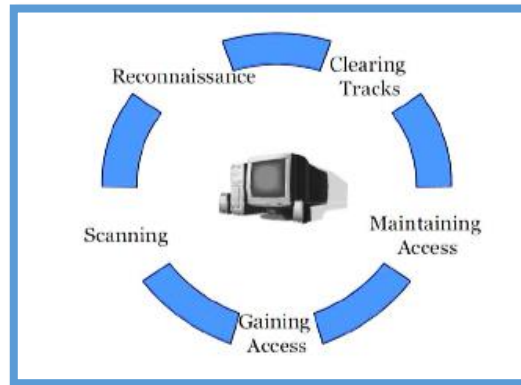
Ethical hacking is a process of crack the vulnerabilities in the network which a malicious attacker may exploit. Ethical hackers use some methods to hacking with the permission of an authorized person.

There are mainly 5 phases in hacking methodology. They are,

- Reconnaissance
- Scanning
- Gaining access
- Maintaining access
- Clearing tracks



The below figure illustrates the methodology of ethical hacking,



Fig; Ethical Hacking Methodology

4.1 Reconnaissance

This phase contains a set of techniques like footprinting, scanning, and enumeration along with processes used to discover and find information about the target system.

4.2 Scanning

Scanning is a set of steps. These are used for identifying live hosts, ports, services and discovering operating systems, and identifying vulnerabilities, threats in the network by scanning which is used to create a profile of the target organization.

4.2.1. Types of Scanning

4.2.1.1. Port Scanning

This method gives the attacker an idea of where to probe for weakness. Typically, this approach consists of sending a message to each port, one by one. The responses received indicate whether the port is used and can therefore be probed for weakness.

4.2.1.2 Network Scanning

It is an important element. It allows the user to map the network as well as to find the devices that would be hard to find manually. It allows a security analyst to locate the devices on the network that could be likely to begin a breach into the network.

4.2.1.3 Vulnerability Scanning

In this scanning, it finds a weakness in the system or network and reports any false positive. The result of a vulnerability scan is a list of all the systems that are found and identifies on the network and highlighting any known weakness that needs the hacker's whole attention.

4.3 Gaining Access

This is the main phase where attackers will get the access of the system or network and have the ability to spoil it completely. The main activities involved in these steps are, system hacking, Acquire passwords etc.

4.4 Maintaining Access

In this step 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.

4.5 Clearing Tracks

An intelligent hacker always clears all evidence. so, no one will find any traces leading to him. This is the last and final stage where hackers want to remove or destroy all evidence. This is one of the best methods to evade trackback. Erasing evidence is the requirement for a hacker to remain obscure. This involves modifying/corrupting / deleting the values of logs, modifying registry values and uninstalling all applications he used, and deleting all folders he created.

V.IMPACT ON SOCIETY OF ETHICAL HACKING

Hackers have a great impact on society. Ethical hacking is not a bad thing, but we should know what ethical hackers doing in society. 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 hackers across the world



5.1 Impact on Education

Students are very interested to study new technologies. It is hard to teach hacking to students. Because they are very curious to learn about it. They want to learn about hacking and take its benefit. we can make them understand that ethical hacking is not good if it is not containing ethics. So ethical hacking can also ensure the safety and security of our system if it is done ethically.

5.2 Impact on Business

Nowadays we use the advantages of IT in business. As a result, the rate of e-commerce using is increased day by day. It is very easy for an ethical hacker to buy several goods and can avoid paying the amount because they know that they can easily do it. But there are also some ethical hackers are here, they do their job neatly and ethically. IT world has grown up day by day, also ethical hackers are increased. We can not predict the intention of the hacker. We can not stop them from hacking, but we can advise them to use their ability to do something good for society, or do hacking ethically

5.3 Impact on workplace and its security

Now we are in a digital world. Most companies store their data in digital format. So, a hacker can steal the data from a company. He can hack the employee details and other private data about the company. So, it is necessary to improve the security features of the company system. Today most companies have their own IT professionals to handle their security system.

5.4 Impact on technology

We can say that nothing in this digital world is secure. Hence a brilliant hacker can hack anything. Because all is in his fingertip. There are many tools to help them to hack. Like, Nmap, Acunetix. Hackers may use this to crime and an ethical hacker can use this to find the weakness and imperfections in the system.

5.5 Impact on confidential Information

We can say that no confidential data is secure in the modern world. Many hackers work in the financial field so they can steal confidential information from the customer. He can retain their accounts detail and may make any kind of transaction, blackmailing etc.

VI.CONCLUSION

The hacking technique may legal or illegal or in other words, it may ethical or unethical. Technology has grown up every day and hacking also. Hacking may good or bad, it depends on the situation and the character of the hacker. We cannot stop them from hacking. we can only do that advise them to use their skills for society. so always be alert in your data and try to improve yourself to learn about new technologies to prevent hacking.

REFERENCES

1. The figure taken from www.researchgate.com
2. Points based on the observation from www.medium.com
3. Points taken from www.researchgate.com
4. Reference from Ethical hacking : An Impact On society; Meenakshi N Mungal.

BIOGRAPHY



Athira Raj, Is serving as Assistant Professor in the PG Department of Computer Application, JPM Arts and Science College, Kanchiyar, Kerala. Has 3 years of experience in the teaching field. Also worked as an assistant professor in IHRD college and Published Many research papers. Secured with the second rank from MG university for Msc .computer science.