International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 11 | Nov 2019 www.irjet.net p-ISSN: 2395-0072

Study of Hacking and Ethical Hacking

Mrs. Kavita Ganesh Kurale

Sr. Lecturer, Dept of Computer Engineering, Sant Gajanan Maharaj Rural Polytechnic, Mahgaon.

Abstract – Hacking is the process of finding entry points that exist in a computer system or a computer network and finally make control on system. Ethical hacking is legal form of hacking. Ethical hacking is performed with the target's permission. This paper describes what is hacking, ethical hacking, types of hackers, advantages and disadvantages of hacking, purpose of hacking and process of hacking.

Key Words: **Hacking, hackers, ethical hackers**

1. INTRODUCTION

Hacking is the process of finding entry points that exist in a computer system or a computer network and finally make control on system. Hacking is nothing but unauthorized control on a computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer. Many organizations has sensitive data, hackers stole their sensitive data, damage the system.

Hacking is process to find problems in a computer system for testing purpose. This type of hacking is called Ethical Hacking. A person who hack the system is called a "Hacker". Hackers are those who has knowledge how systems operate, how system are designed, and then they play with these systems.

2. TYPES OF HACKING [2]

There are different types of Hacking

2.1 Website Hacking

Hacking a website means unauthorized person make control on webserver and databases of servers and other interfaces.

2.2 Network Hacking

Network hacking means information about network are collected and he network system and its operations are harmed.

2.3 Email Hacking:

It means hacking the password and email login id of an Email account and using it.

2.4 Ethical Hacking

Ethical hacking means finding problems in a computer or network system for testing purpose and fixing that problem to make a better system.

2.5 Password Hacking

Sensitive passwords are stolen by the unauthorized persons to harm the computer.

2.6 Computer Hacking

This is the process of finding computer username and password to access to a computer system.

3. TYPES OF HACKERS[3]

3.1 White Hat Hackers

White Hat hackers are also Ethical Hackers. They doesn't harm a system, they try to find the problems in a computer or a network system. They do testing of computers or networks. Ethical hacking is not illegal type of hacking there are numerous companies that appoints ethical hackers for testing their systems.

3.2 Black Hat Hackers

Black Hat hackers also hackers those hack system and get unauthorized access to a system and harm its operations or steal sensitive information. Black Hat hacking is always illegal users because they hack the system with bad intention like stealing corporate data, violating privacy, damaging the system, blocking network communication, etc.

3.3 Grey Hat Hackers

Grey hat hackers also black hat and white hat hackers. They don't have any intention but work for their fun, they break security in a computer system or network without the permission or knowledge. Their intention is to focus on the weakness of computer and make the attention of the owners and get appreciate from the owners.

3.4 Miscellaneous Hackers [2]

Apart from the above well-known classes of hackers, we have the following categories of hackers based on what they hack and how they do it –

1. Red Hat Hackers

Red hat hackers are also both black hat and white hat hackers. They are usually hacks government sites, secret information, and sensitive information.

2. Blue Hat Hackers

A blue hat hacker is used to bug-test a system prior to system launch. They look for loopholes available in the system and try to fill these gaps.

3. Elite Hackers

This is a social status among hackers, which is used to describe the most skilled. Newly discovered exploits will circulate among these hackers.

4. Script Kiddie

A script kiddie is a non-expert who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept, hence the term Kiddie.

4. ADVANTAGES OF HACKING

Hacking is quite useful in the following scenarios –

1. To recover lost information when computer password is lost,
2. Helps us to find the loopholes in the system.
3. Make system more secure by self-hacking of system.
4. Understand the hackers techniques
5. Prepare for hacker attack.
6. Develop the quality of system

5. DISADVANTAGES OF HACKING

Hacking is quite dangerous if it is done with harmful intent. It can cause –

1. Corrupt the files of Computer system
2. Unauthorized access for private information.
3. System Privacy violated.
4. Hampering system operation.
5. Ethical hacker will send and/or place malicious code, viruses, malware and other destructive and harmful things on a computer system

6. PURPOSE OF HACKING

There could be various positive and negative intentions behind performing hacking activities. Here is a list of some probable reasons why people indulge in hacking activities –

1. Just for fun
2. Show-off
3. Steal important information
4. Damaging the system
5. Hampering privacy
6. Money extortion
7. System security testing
8. To break policy compliance

7. ETHICAL HACKING

You need protection from hacker. Ethical hackers perform the hacking of the system for security tests. Ethical hacking — additionally referred to as penetration testing or white-hat hacking — involves the identical tools, tricks, and techniques that hackers use, however with one major difference. Ethical hacking is legal form of hacking. Ethical hacking is performed with the target's permission. The intention of ethical hacking is to get vulnerabilities from a hacker's viewpoint thus systems may be higher secured. It's part of an overall information risk management program that that permits for current security enhancements. Ethical hacking can also ensure that vendors' claims about the security of their products are legitimate.

8. WHY WE TEND TO HACK OUR OWN SYSTEM

"To catch a felon, assume sort of a thief".

This is often the idea for ethical hacking. You don't protect your systems from everything. The only protection against everything is to unplug your laptops, computer and lock them away nobody will bit them — not even you. That's not the most effective approach to information security.

With the increased numbers and expanding knowledge of hackers combined with the growing number of system vulnerabilities and other unknowns, the time can come when all computer systems are hacked or compromised in some way. Protecting your systems from the dangerous guys — and not simply the generic vulnerabilities that everybody is aware of regarding knows about — is absolutely critical.

Hacking preys on weak security practices and converts vulnerabilities. Firewalls, encryption, and nonpublic networks (VPNs) can produce a false feeling of safety. These security systems usually focus on high-level vulnerabilities, like as viruses and traffic through a firewall, without affecting how hackers work. Attacking your own systems to get vulnerabilities is a step to

Making them safer. This is often the sole evidenced methodology of greatly hardening your systems from attack. If you don't identify weaknesses, it's a matter of time before the vulnerabilities are exploited. As hackers expand their knowledge, so should you. You must think like them to protect your systems from them. You, as

the ethical hacker, must know activities hackers perform and the way to prevent their efforts. You should know what to look for and how to use that information to thwart hackers' efforts. You don't have to protect your systems from everything

9. ETHICAL HACKING PROCESS

Following is the process of Ethical hacking. [4]

9.1 Reconnaissance

Reconnaissance is the step where the attacker gathers information about a target using active or passive means. The tools that are widely used in this process are NMAP, Hping, Maltego, and Google Dorks.

9.2 Scanning

In this process, the attacker begins to actively probe a target machine or network for vulnerabilities that can be exploited. The tools used in this process are Nessus, Nexpose, and NMAP.

Fig-1 Process of Ethical Hacking

9.3 Gaining Access

In this process, the vulnerability is located and you attempt to exploit it in order to enter into the system. The primary tool that is used in this process is Metasploit.

9.4 Maintaining Access

It is the process where the hacker has already gained access into a system. After gaining access, the hacker installs some backdoors in order to enter into the system when he needs access in this owned system in future. Metasploit is the preferred tool in this process

9.5 Clearing Tracks

This process is actually an unethical activity. It has to do with the deletion of logs of all the activities that take place during the hacking process.

9.6 Reporting

Reporting is the last step of finishing the ethical hacking process. Here the Ethical Hacker compiles a report with his findings and the job that was done such as the tools used, the success rate, vulnerabilities found, and the exploit processes.

10. Conclusion

Hacking has both its benefits and risks. Hackers are very diverse. They may bankrupt a company or may protect the data, increasing the revenues for the company. Ethical Hackers help organizations to understand the present hidden problems in their servers and corporate network. In conclusion, it must be said that the ethical hacker is an educator who seeks to enlighten not only the customer, but also the security industry as a whole. In an effort to accomplish this, let us welcome the Ethical Hacker into our ranks as a partner in this quest.

REFERNCES

[1] Wikipedia

[2] Tutorialpoint.com

[3] K.Bala Chowdappa et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014, 3389-3393

[4] Gurpreet K. Juneja,"Ethical hanking: A technique to enhance information security"international journal of computer applications (3297: 2007), vol. 2, Issue 12, December 2013.