AN OVERVIEW OF ETHICAL HACKING

Arockia Panimalar.S[1], Priyadharshini.P[2], Vijayabharathi.R[3], Abirami.P[4]

[1]*Assistant Professor, Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Tamilnadu*
[2,3,4] *III BCA Students, Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Tamilnadu*

Abstract: *Hacking is an unprivileged usage of computer and network resources. Hacking is a process to the security mechanisms of an information system on the network. Hacker is a generic term for a computer criminal. The practice of hacking without no malicious intent, the target system with a hacker's perspective. Today, more and more software's are developed and people are getting more and more options in their present software. The advent of new tools the hackers may make new schemes at least the software will be resistant to selected of the tools. The methods that can be used by a black hat hacker apart from the methodology are framed by the user. The operator should know at least some of these because specific hackers make use of those who are not aware of the various hacking systems to hack into a method.*

Keywords: Ethical Standards, Security, Hacking, Ethical Footprinting and Sniffing.

1. INTRODUCTION

Hacking is the act of finding the possible access points that exist in a computer system or a computer network. Hacking is commonly done for gain illegal access to a computer scheme or a computer system, either to harm the systems or to steal sensitive information available on the computer.

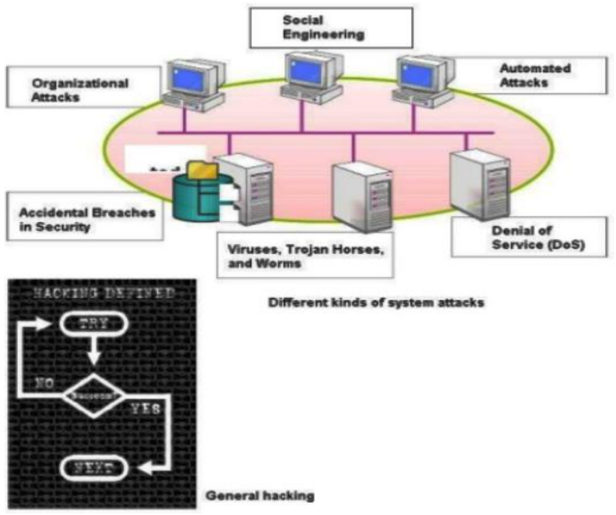

Fig 1: Hacking

Hacking is generally done to improvement unauthorized access to a computer scheme or a computer system, either to damage the systems or to bargain sensitive information existing on the computer. Hacking is generally legal as long as it is being done to find weaknesses in a computer or network system for the testing purpose. The explosive evolution of the internet has carried several moral effects of electronic commerce, easy access to vast stores of reference material, collaborative computing, e-mail, and new avenues advertising and information distribution, to name a few. As with most technological advances, there is also a dark side of hacking [1].

2. TYPES OF HACKING

A. Website Hacking

Hacking a website means taking illegal control over a web server and its associated software such as database and other interfaces.

B. Network Hacking

Hacking a network system gathering information immediate a scheme by using implements like Telnet, NS lookup, Ping, Tracer, Net stat, etc. with the determined to harm the network system and hamper its process.

C. Email Hacking

It includes getting illegal access to an Email account and using it without taking the consent of its owner.

D. Ethical Hacking

Ethical hacking includes finding weaknesses in a computer system or network scheme for testing purpose and finally getting them fixed.

E. Password Hacking

The procedure of improving secret passwords from data that has been stored in or communicated by a computer system.

F. Computer Hacking

The method of stealing computer identifications and passwords by applying hacking methods will leads to illegal access to a computer system [2].

3. ADVANTAGES OF HACKING

Hacking is quite useful in the following developments:
i. To improve loss of data, especially in case lost your password.
ii. To perform penetration testing to support computer system and network security.
iii. To put sufficient preventive measures in place to prevent security breaches.
iv. To have a computer network that prevents malicious hackers from gaining access [3].

4. DISADVANTAGES OF HACKING

Hacking is quite dangerous if it is done with harmful intent. It can cause:
i. Enormous security breach.
ii. Unauthorized system access on private data.
iii. Privacy violation.
iv. Hampering system process.
v. Denial of provision attacks.
vi. A Malicious attack on the scheme [4].

5. ELEMENTS OF SECURITY

5.1 Security

Security is the condition of existence protected against risk or loss. The security is a concept similar to security. In the case of networks, the security is also called the information security. Information security means protecting information and also information schemes from illegal access, usage, disclosure, disruption, modification, and also destruction. The security is termed in relations of CIA triads. The CIA is the basic principles of security, confidentiality, integrity and availability.

5.2 Need for Security

There may be several methods of damage which is clearly interrelated which is produced byte intruders.

These include:
i. Loss of private data
ii. Damage or destruction of data
iii. Damage or destruction of computer scheme
iv. Loss of reputation of a company

5.3 Confidentiality

Confidentiality is the property of preventing disclosure of information to unauthorized individuals or systems. This implies that the individual data should be seen only by the authorized personals. Those persons who are a passive person should not see those data. For example in the case of a credit card transaction, the authorized person should see the credit card numbers and he should see that data. Nobody others should see that number because they may use it for some other activities. Thus the confidentiality is very important. The required data for maintaining the privacy of the persons whose personal information a system holds.

5.4 Integrity

The data cannot be modified without authorization. The data seen by the legal persons should be correct or the data should maintain the property of integrity without that integrity the data is of no use. Integrity is violated by computer network illness infects a computer:

i. When an employee is able to modify his own salary in a payroll database.
ii. When an unauthorized user vandalizes a website.
iii. When someone is able to cast a very large number of votes in an online poll.

5.5 Availability

For any information system to serve its purpose, the information must be available when it is needed. Consider the case in which the data should have integrity and confidentiality. The data is not available to the user or it is not available. The data is of no use even if it has all the other characteristics. The computing systems used to store the data and process the information, the security controls used to protect, and the communication networks used to access its requirement to be operative properly. The issues are considered to be important since data lacking any of the above characteristics is useless. The security is described as the CIA. Lacking any one of the CIA means there is a security breach [5].

6. TYPES OF HACKERS

Hackers can be generally classified as the source of the hacking system. There are four types of hackers on this basis.

6.1 Black Hat Hacker

Black-hat hackers or crackers are individual with extraordinary computing skills, resorting to malicious actions. The black hat hackers use their knowledge and skills. Their own individual gains probably by down others.

6.2 White Hat

White hat hackers are those individuals allowing hacker skills and using them for protective purposes. The white hat hackers use their information and skill for the good of others and for the common good.

6.3 Grey-Hat Hackers

These are individuals who work both offensively and defensively at various times. It cannot predict their behavior.

Sometimes they use their skills for the common good while in some other times he uses them for their personal gains.

6.4 Criminal Hackers

Management enterprises and secluded citizens around the world are anxious to be a part of this revolution, but they are troubled that some hacker will break into their web server and implant software that will secretly transfer their organization's secrets to the open internet. The intent of ethical hacking is to determine exposures from a hacker's viewpoint systems can be better secured. It is a part of an overall information risk management program that allows for ongoing security improvements. Ethical hacking can also ensure that vendor's rights to the security of their products are authentic [6].

7. METHODS ETHICAL HACKING

The method of ethical hacking in different methods, but the intact process can be considered into the following six phases.

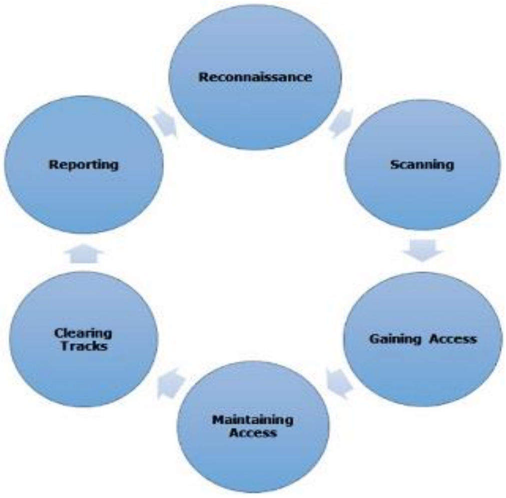

Fig 2: Ethical Hacking Methods

7.1 Reconnaissance

Reconnaissance is the phase where the attacker collects information about an object using active or passive. The tools that are widely used in this process are NMAP, Hoping, Malt ego, and Google Dorks.

Reconnaissance hacking methods as two parts Active-Reconnaissance, Passive- Reconnaissance.

A) Active Reconnaissance

The information can be related and accurate. But there is a risk of getting detected and planning active reconnaissance without permission. It detected the system admin can take severe action against you and trail your subsequent activities.

B) Passive Reconnaissance

It used to gather essential information without always interacting with the target systems.

7.2 Scanning

The hackers begin to actively review a target mechanism or system for capabilities that can be exploited. The tools used in this process are Nessus, Nexpose, and NMAP.

7.3 Gaining Access

The ability is located and your effort to the activity it in order to enter into the scheme. The primary tool that is used in this method is Metasploit.

7.4 Maintaining Access

The hacker has a gained access to a scheme. After gaining access, the hacker connects some backdoors in order to enter into the system when hacker needs access to this owned system in future.

7.5 Clearing Tracks

The process is actually an unethical activity. It has to do with the deletion of logs of all the actions that take place through the hacking process.

7.6 Reporting

The Ethical Hacker collects a report with systems results and the job that was done such as the implements are used, the success rate, abilities found, and the action methods. Reporting is the last stage of final the ethical hacking method [7].

8. ETHICAL FOOTPRINTING

Foot printing could be both passive and active. Foot printing is mostly the first step to hacker gathers as much information as possible to find ways to interrupt into a target system or at least decide what type of attacks will be more suitable for the target.

During this part, a hacker can collect the ensuing information as

- Domain name
- IP Addresses
- Namespaces
- Employee information
- Phone numbers
- E-mails
- Job Information [5].

9. SNIFFING

Sniffing is the process of monitoring and capturing all the packets passing complete a known network by sniffing tools. It is a method of "tapping phone wires" and get to know about the conversation. It is also called wiretapping applied to the computer networks.

The following sensitive information from a network is:

- Email traffic
- FTP passwords
- Web traffics
- Telnet passwords
- Router configuration
- Chat sessions
- DNS traffic [4].

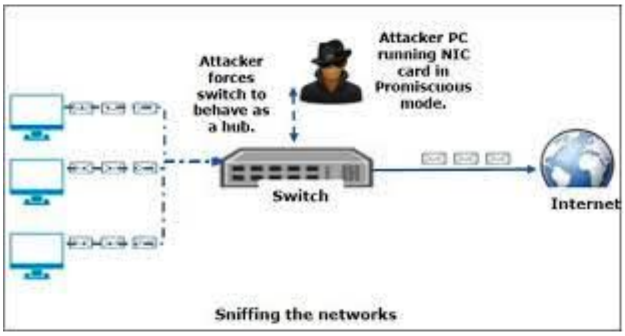
Attacker forces switch to behave as a hub.
Attacker PC running NIC card in Promiscuous mode.
Switch
Internet
Sniffing the networks

Fig 3: Sniffing Process

10. CONCLUSION

One of the main goals of the discussion is to make others understand that there are many tools through which a hacker can become in to a scheme. It checked its several needs from various perspectives. A student should understand that no software is made with zero Vulnerability. So though they are learning they must learn the various possibilities and must learn how to check that as they are the authorities of tomorrow. Professionals must appreciate that business is straight connected to Security. So they should make new software with vulnerabilities as less as possible [3].

11. FUTURE ENHANCEMENT

Hacking enhanced software's should be used for optimum security. Tools are used, need to be updated regularly and more efficient ones need to be developed [3].

12. REFERENCES

[1]Patrick Engebretson, The Basics of Hacking and Penetration Testing Ethical Hacking and Penetration Testing Made Easy, Elsevier Inc., 2013.

[2]Beggs Robert, Mastering Kali Linux for Advanced Penetration Testing A practical guide to testing your network's security with Kali Linux the preferred choice of penetration testers and hackers, Packt Publishing Ltd, 2014.

[3] Joseph Muniz, Amir Lachine, Penetration Testing With Raspberry Pi Construct a hacking arsenal for penetration testers or hacking enthusiasts using Kali Linux on a Raspberry Pi, Packt Publishing Ltd, 2015.

[4] H. M. David, "Three Different Shades of Ethical Hacking: Black White and Gray", GSEC Practical Assignment Version 1.4b Option 1, 2004.

[5] J. Danish, A.N. Muhammad, "Is Ethical Hacking Ethical?", International journal of Engineering Science and Technology, vol. 3, no. 5, pp. 3758-3763, 2011.

[6] Ajinkya A. Far sole, Marta G. Kashia, Aura Zunzunwala, "Ethical Hacking", International journal of Computer Applications, vol. 1, no. 10, pp. 14-20, 2010.

[7] Gurpreet K. Juneja, "Ethical hanking: A technique to enhance information security", International journal of computer applications, vol. 2, no. 12, 2013.