Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

White Hat Hacking

Varshitha.R,
Department Of Computer Science, St.Joseph's College Of Arts and Science For Women, Hosur, Tamilnadu, India

Abstract – "Hacking" is the word that shakes everyone whenever it is said or heard by someone. A Hacker needs a brilliant mind to hack anything. His/her skills should be so powerful that no other hacker can hack them. There are many rules that he/she should learn to become an Ethical Hacker. These rules include knowledge of HTML, Java script, Computer tricks, Cracking and breaking, etc..

Keywords: *Security, Hackers, Ethical Hacking, Malwares.*

I. INTRODUCTION

In their search for a way to approach the problem, organizations came to realize that one of the best ways to evaluate the intruder threat of their interests would be to have independent computer security professionals attempt to break into their computer systems. This scheme is similar to having independent auditors come into an organization to verify its book-keeping records. In the case of computer security, these "tiger teams" or "ethical hackers" would employ the same tools and techniques.

II. HACKER

The term hacker may refer to anyone with technical skills, but it often refers to a person who uses his or her abilities to gain unauthorized access to systems or networks in order to commit crimes. A hacker may, for example steal information to hurt people via identity theft, damage or bring down systems and often hold those system hostage to collect ransom.

Types of hackers

Hackers can be classified on the basis of why they are hacking system or why they are indulging hacking. There are mainly three types of hacker.

A. Black-hat hacker

A black hat hacker or crackers are individuals with extraordinary computing skills, resorting to malicious or destructive activities. That is black hat hackers use their knowledge and skill for their own personal gains probably by hurting others.

B.White-hat hacker

White hat hackers are those individuals professing hackers skills and using them for defensive purposes. This means that the white hat hackers use their knowledge and skills for the goods of others and for the common good.

C. Grey-hat hacker

These are individual who works both offensively and defensively at various times. We cannot predict their behavior. Sometimes they use their skills for the common good while in some others times he uses them for their personal gains.

III. ETHICAL HACKING

Ethical hacking or White Hat Hacking refers to the act of locating weakness and vulnerabilities of computer and information systems by duplicating the internet and actions of malicious hackers. Ethical hacking is also known as penetration testing.

A. What does an Ethical Hacker do?

An ethical hacker is a person doing ethical hacking that is he is a security personal who tries to penetrate in to a network to find if there is some vulnerability in the system .An ethical hacker will always have the permission to enter into the target network .An ethical hacker will first think with a mindset of a hacker who tries to get in to the system.

He will first find out what an intruder can see or what others can see. Finding these an ethical hacker will try to get into the system with that information in whatever method he can .If he succeeds in penetrating into the system that he will report to the company with a detailed report about the particular vulnerability exploiting which he got in to the system. He may also sometimes make patches for that particulars vulnerability or he may suggest some methods to prevent the vulnerability.

IV. ETHICAL HACKING COMMANDMENTS

Every ethical hacker must abide by few basic commandments. If not, bad things can happen. The commandments are as follows:

A. Working ethically

The word ethical in this context can be defined as working with high professional-morals and principles. Everything you do as an ethical hacker must be aboveboard and must support the company's goals. No hidden agendas are allowed! Trustworthiness is the ultimate tenet. The misuse of information is absolutely for bidden.

B. Respecting Privacy

Treat the information gathered with the utmost respect. All information you obtain during your testing from Web-application log files to clear-text passwords must be kept private. If you sense that someone should know there's problem, consider sharing that information with the appropriate manager.

C. Not crashing your systems

One of the biggest mistakes hackers tries to hack their own systems. The main reason for this is poor planning. These testers have not read the documentation or misunderstand the usage and power of the security tools and techniques.

V. METHODOLOGY OF HACKING

There are mainly five steps in hacking, but it is not the end of the process. The actual hacking will be a circular one. Once the hacker completed the five steps then the hacker will start the first step and preceding steps to get into the next level.

The various methodologies are

- Reconnaissance
- Scanning & Enumeration
- Gaining Access

- Maintaining Access
- Clearing Tracks

A. Reconnaissance

The literal meaning of the word reconnaissance means a preliminary survey to gain information. This is also known as foot-printing. This is the first stage in the methodology of hacking. This is the stage in which the hacker collects information about the company which the personal is going to hack. This is one of the pre-attacking phases. Reconnaissance refers to the preparatory phase where an attacker learns about all of the possible attack vectors that can be used in their plan.

B. Scanning & Enumeration

Scanning is the second phase in the hacking methodology in which the hacker tries to make a blue print of the target network. It is similar to a thief going through your neighborhood and checking every door and window on each house to see which one is locked. The blue print includes the IP addresses of the target network which are live, the services which are running on those systems and so on. Usually the services run on predetermined ports. There are different tools used for scanning war dialing and pingers were used earlier but nowadays both could be easily detected easily and hence are not in much use. Modern port scanning uses TCP protocol to do scanning and they could even detect the operating systems running on the particular hosts.

Enumeration is the ability of a hacker to convince some server to give them information that is vital to them makes an attack. By doing this the hacker aims to find what resources and shares can be found in the system, what valid user account and user groups are there in the network, what applications will be there etc. Hackers may use this also to find other hosts in the entire network.

C. Gaining Access

This is the actual hacking phase in which the hacker gains access to the system. The hacker will make use of all the information he collected in the pre-attacking phases. Usually the main hindrance to gaining access to a system is the passwords. System hacking can be considered as many steps. First the hacker will try to get in the system; once he gets in to the system the next thing he wants will be to increase his privileges so that he can have more control over the system. As a normal user hacker may not be able to see the confidential details or cannot upload or run the different hack tools for his own personal interest. Another way to crack in to a system is by the attacks like man in the middle attack.

Password Cracking

There are many methods for cracking the password and then get in to the system. The simplest method is to guess the password. But this is a tedious work. But in order to make this work easier there are many automated tools for password guessing like legion. Legion actually has an inbuilt dictionary in it and software. The software itself it generates the password using the dictionary and will check the responses. Techniques used in password cracking are:

- Dictionary Cracking
- Brute force Cracking
- Hybrid Cracking
- Social Engineering

Privilege Escalation

Privilege escalation is the process of raising the privileges once the hacker gets into the system. That is the hacker may get in as an ordinary user. And now he tries to increase his privileges to that of an administrator who can do many things. There are some tools like get admin attaches the user to some kernel routine rather than user initiated program. The privilege escalation process usually uses the vulnerabilities present in the host operating system or the software. There are many tools like hk.exe, metasploit etc. One such community of hackers is the metasploit.

D. Maintaining Access

Now the hacker is inside the system by some means by password guessing or exploiting some of its vulnerabilities. This means that he isnow in a position toupload some files and download some of them. The next aim will be to make an easier path to get in when he comes the next time. So that the hacker will upload some software like Trojan horses, Sniffers, Key stroke loggers etc.

E.Clearing Tracks

This is the final step in hacking. In this the hackers clear tracks or any records that may present in the network to prove that he was here. Whenever a hacker downloads some files or installs some software, its log will be stored in the server logs. So in order to erase that hacker uses man tools. One such tool is windows resource kit's auditpol.exe. This is a command line tool with which the intruder can easily disable to auditing. Another tool which eliminates any physical evidence is the evidence eliminator. Sometimes apart from the server logs some other information may be stored temporarily. The evidence eliminator deletes all such evidences.

VI. REQUIRED SKILLS OF AN ETHICAL HACKER

- Microsoft: skills in operation, configuration and management.
- Linux: knowledge of Linux / UNIX; security setting, configuration and services.
- Firewalls: configuration and operation of intrusion detection systems.
- Routers: knowledge of routers, routing protocols and access control lists.
- Mainframes
- Network protocols: TCP/IP; how they function and can be manipulated.
- Project management: leading, planning, organizing and controlling a penetration testing team.

A. Top 10 Mal Viruses

Here are some types of malicious virus which are founded and used by Black Hat Hackers. They are:

- Sobig
- I Love You
- Storm worm
- Code Red
- Slammer
- Melissa
- Sasser
- My Doom
- Mebroot
- Leap

B. Top 10 Software Used For Hacking

- Metasploit framework
- Nmap
- Acunetix WVS
- Maltego
- SET
- Nessus
- Hydra
- Aircrack-ng
- Wireshark
- Nikto

VII. ETHICAL HACKING TOOLS

Ethical hackers utilize and have developed variety of tools to intrude into different kinds of systems and to evaluate the security levels. The nature of those tools differs widely. The tools which are used widely are:

A. Samspade

Samspade is a simple tool which provides us information about a particular host. This tool is very much helpful in finding the addresses, phone numbers etc.

B. Email tracker and visual route

We often used to receive many spam messages in our mail box. We don't know where it comes from. Email tracker is software which helps us to find from which server the mail does actually came from. Every message we receive will have a header associated with it. The email tracker uses this header information to find the location.

Visual route GUI have a world map drawn to it. The software willlocate the position of the server in that world map. It will also depict the path through which the message came to our system. This software will actually provide us with information about the routers through which the message or the path traced by the mail from the source to the destination.

Some other important tools used are:

- War Dialing
- Pincers
- Super Scan
- Nmap etc…

VIII. SECURITY

Security is the condition of being protected against danger or loss. In the general sense, security is the concept similar to safety. In the case of networks the security is also called the information security. Information security means protecting information and information systems from unauthorized access, us, disclosure, disruption, modification, or destruction.

A. Need For Security

There may be several forms of damage which are obviously interrelated which are produced by intruders. These include:

- Loss of confidential data
- Damage or destruction of data
- Damage or destruction of computer system
- Loss of reputation of a company

IX. ADVANTAGES AND LIMITATIONS

Ethical hacking nowadays is the backbone of network security. Each day its relevance is increasing, the major pros & cons of ethical hacking are given below

Advantages

- Helps in closing the open holes in the system network
- Provides security to banking and financial establishments
- Prevents website defacements
- An evolving technique

Limitations

- All depends upon the trustworthiness of the ethical hacker
- Hiring professionals is expensive.

CONCLUSION

The word "hacker" carries weight. People strongly disagree as to what a hacker is. Hacking may be defined as legal or illegal, ethical or unethical. Ethical hacking is legal way to securing your system in hands of ethical hacker so that he can make your system full proof. Thus, the ethical hacker attacks are done in a non-destructive manner.

References

[1] MCA-Ethical hacking-report.pdf
[2] Palmer-Ethical Hacking.pdf