BASICS OF ETHICAL HACKING

Chenchu Lakshmi S[1], P I Basarkod[2]
[1]M-Tech (DCN) Student, Reva institute of Technology and Management, Bangalore, India
[2]Sr. Associate Prof. (ECE), Reva Institute of Technology and Management, Bangalore, India

ABSTRACT

We are living in security era, where we are securing all our belongings under different modes of lock but it's different in the case of system security. We are carelessly leaving our datas and softwares unlocked. The state of security on the internet is bad and getting worse. One reaction to this state of affairs is termed as Ethical Hacking which attempts to increase security protection by identifying and patching known security vulnerabilities on systems owned by other parties. As public and private organizations migrate more of their critical functions to the Internet, criminals have more opportunity and incentive to gain access to sensitive information through the Web application. So, Ethical hacking is an assessment to test and check an information technology environment for possible weak links and vulnerabilities. Ethical hacking describes the process of hacking a network in an ethical way, therefore with good intentions. This paper describes what ethical hacking is, what it can do, an ethical hacking methodology as well as some tools which can be used for an ethical hack.

KEYWORDS: *Hacking, Hacker, Ethical Hacking, Vulnerabilities, Hacker, Cracker, Security, Tools*

I. INTRODUCTION

The vast growth of Internet has brought many good things like electronic commerce, email, easy access to vast stores of reference material etc. One of the more effective ways of testing network security is penetration testing or ethical hacking. Activities focus on the identification and exploitation of security vulnerabilities, and subsequent implementation of corrective measures (Using an Ethical Hacking Technique). Organizations are increasingly evaluating the success or failure of their current security measures through then use of ethical hacking processes. As, with most technological advances, there is also other side: criminal hackers who will secretly steal the organization's information and transmit it to the open internet. These types of hackers are called black hat hackers. So, to overcome from these major issues, another category of hackers came into existence and these hackers are termed as ethical hackers or white hat hackers. So, this paper describes ethical hackers, their skills and how they go about helping their customers. Ethical hackers perform the hacks as security tests for their systems. This type of hacking is always legal and trustworthy. In other terms ethical hacking is the testing of resources for the betterment of technology and is focussed on securing and protecting IP systems. Ethical hacking is a way of doing a security assessment. Like all other assessments an ethical hack is a random sample and passing an ethical hack doesn't mean there are no security issues**.**

What is Ethical Hacking?

Ethical hacking provides a way to determine the security of an information technology environment – at least from a technical point of view. As the name ethical hacking already tells, the idea has something to do with hacking. But what does "hacking" mean? "The word *hacking* has two definitions. The first definition refers to the hobby/profession of working with computers. The second definition refers to breaking into computer systems. While the first definition is older and is still used by many computer enthusiasts (who refer to cyber-criminals as "crackers"), the second definition is much more commonly used.” In the context of “ethical hacking”, hacking refers to the second definition – breaking into computer systems. It can be assumed that hacking is illegal, as breaking into a house would be. At this point, “ethical” comes into play. Ethical has a very positive touch and describes something noble which leads us to the following definition of ethical hacking: Ethical hacking describes the process of attacking and penetrating computer systems and networks to discover and point out potential security weaknesses for a client which is responsible for the attacked information technology environment. An ethical hack’s results is a detailed report of the findings as well as a testimony that a hacker with a certain amount of time and skills is or isn’t able to successfully attack a system or get access to certain information. Ethical hacking can be categorized as a security assessment, a kind of training, a test for the security of an information technology environment. An ethical hack shows the risks an information technology environment is facing and actions can be taken to reduce certain risks or to accept them. We can easily say that Ethical hacking does perfectly fit into the security life cycle shown in the below figure.

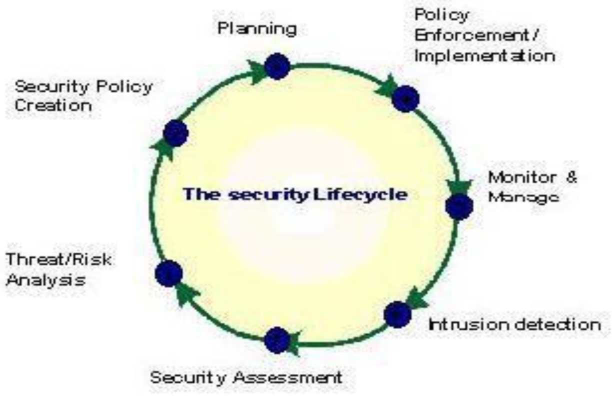

Fig. 1 Security life cycle

II. CATEGORIES OF HACKERS

White Hats
Ethical hacker is also known as White hat hacker, or white hat, they use programming skills to determine the vulnerabilities in computer systems.

Black Hats
Non-ethical hacker or black hat exploits these vulnerabilities for mischief, personal gain or other purposes. Ethical hacker introspect the weakness in computer security, points them out and may suggest changes to system to secure the information.

Grey Hats
Gray Hats hack for different reasons either ethically or unethically depending on the situation and circumstances at hand(Ethical Hacking: Student Courseware).

III. PENETRATION TESTING

Penetration testing also known as intrusion testing or red teaming is the method of examining the weakness and vulnerabilities of Computer and network security. Penetration testing helps to measure the effectiveness of system security or ineffectiveness of the system security.

Need of Penetration Testing: The main purpose of penetration testing is to identify the security weakness under controlled circumstances so that the security flaws can be eliminated before hackers exploit the system. Ethical hackers use their skills and apply penetration testing to discover the vulnerability Assessment, give importance to high sensitive data. Penetration testing may be done from business perspective to safeguard the organization against failure through preventing financial loss, as well as operational perspective to identify the risk and vulnerabilities.

Types of Penetration Test: Generally there are two type of penetration testing namely
1) Black Box Test
2) White Box Test

The type of penetration testing depends upon the situation of an organization wants to test, whether the scope is to simulate an attack by an insider (employee, network admin/ system admin, etc) or external source. The difference between the two is the amount of information provided to the penetration tester about the system is tested. In black box penetration testing is closely stimulated to that of an external attacker, giving little info or no knowledge about the systems to be tested. The penetration testers gather as much as information about the target system as possible to perform the test. In white box penetration testing the tester generally provided with detailed information about the network to be tested include the IP address.

Merits of Penetration Testing: Penetration testing are effective for many reasons
(1) avoid cost of network
(2) preserve the corporate image and customer loyalty
(3) meet the requirements
(4) manage vulnerabilities.

Penetration testing provides detailed information about actual, exploitable security threats. By doing penetration test we can easily identify the vulnerabilities are most critical as well as least significant. Penetration test benefits the organization by performing security patches and security resource more precisely to safeguard the information.

IV. WORKING OF AN ETHICAL HACKER

The working of an ethical hacker involves the under mentioned steps:

1) Obeying the Ethical Hacking Commandments: Every Ethical Hacker must follow few basic principles. If he does not follow, bad things can happen. Most of the time these principles get ignored or forgotten when planning or executing ethical hacking tests. The results are even very dangerous.
2) Working ethically: The word ethical can be defined as working with high professional morals and principles. Whether you’re performing ethical hacking tests against your own systems or for someone who has hired you, everything you do as an ethical Hacker must be approved and must support the company’s goals. No hidden agendas are allowed. Trustworthiness is the ultimate objective. The misuse of information is absolutely not allowed.
3) Respecting Privacy: Treat the information you gather with complete respect. All information you obtain during your testing from Web application log files to clear-text passwords — must be kept private.
4) Not crashing your systems: One of the biggest mistakes is when people try to hack their own systems; they come up with crashing their 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. You can easily create miserable conditions on your systems when testing. Running too many tests too quickly on a system causes many system lockups. Many security assessment tools can control how many tests are performed on a system at the same time. These tools are especially handy if you need to run the tests on production systems during regular business hours.
5) Executing the plan: In Ethical hacking, Time and patience are important. Be careful when you’re performing your ethical hacking tests.

V. ETHICAL HACKING METHODOLOGY

An ethical hacking methodology is quite similar to a hacking methodology as there are more or less the same goals. Anyhow, some differences exist. An ethical hacker doesn’t need to take that much care in hiding his traces and tracks. He can chose a more aggressive way and doesn’t need to bother with slowing down portscans (to avoid detection) or evading intrusion detection systems – at least most of the time unless it is specially desired by the client. Mostly, an ethical hacker just hasn’t the time to be that careful in blurring his traces and tracks unless the customer pays for. Nevertheless, a lot of similarities can be found to a hacking methodology. An ethical hacking methodology overview can be seen in figure 2. A similar setup could be used by a hacker for his attacks. The ethical hacking methodology described is based on eight possible phases where interactions between the phases are possible, even required as hacking is an iterative process; going back to an earlier phase is absolutely possible (and needed).

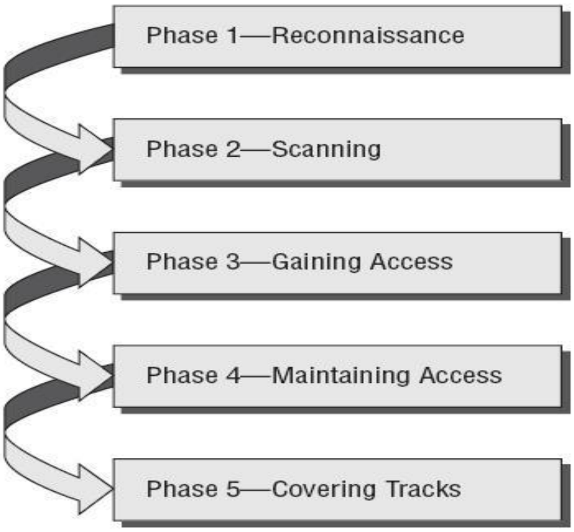

Figure 2: Ethical Hacking Methodology

1. Reconnaissance: It refers to gather as more information as we can about target in prior to perform an attack. It can be further classified into Active and Passive. Former involves information gathering with direct interaction like social engineering and the later without any direct interaction by searching news release or public records.
2. Scanning: It refers to scan for all the open as well as closed ports and even for the known vulnerabilities on the target machine.
3. Gaining Control: It can be gained at OS level, system level or even network level. From normal access hacker can even proceed with privilege escalation. It often includes password cracking, buffer overflows, DoS attack etc.
4. Maintaining Access: It is where hacker strives to retain its control over target with backdoors, root kits or Trojans. Compromised machines can even be used as Bots and Zombies for further attacks.
5. Covering Tracks : It is also known as Daisy Chaining. To avoid being exposed or caught, a good hacker will leave no impressions of his presence. So he attempts to overwrite the system and application logs.

VI. ETHICAL HACKING PROCESS

The Ethical hacking process needs to be planned in advance. All technical, management and strategical issues must be considered. Planning is important for any amount of testing – from a simple password test to all out penetration test on a web application. Backup off data must be ensured, otherwise the testing may be called off unexpectedly if someone claims they never authorises for the tests. So, a well defined scope involves the following in formation:

1. Specific systems to be tested.
2. Risks that are involved.
3. Preparing schedule to carry test and overall timeline.
4. Gather and explore knowledge of the systems we have before testing.
5. What is done when a major vulnerability is discovered?
6. The specific deliverables- this includes security assessment reports and a higher level report outlining the general vulnerabilities to be addressed, along with counter measures that should be implemented when selecting systems to test, start with the most critical or vulnerable systems.

VII. HACKING TOOLS

There are various characteristics for the use of tools for ethical hacking which are as follows:

1. Adequate documentation
2. Detailed reports on the discovered vulnerabilities, including how they can be fixed
3. Updates and support when needed
4. High level reports that can be presented to managers .

The list and description of various tools used in the ethical hacking process are as follows:
Scanning tools: The Scanning tools are quite helpful in the ethical hacking process. In technical detail, a scanner sends a message requesting to open a connection with a computer on a particular port. (A port is an interface where different layers of software exchanges information).

Port Scanners:

- Nmap
- Superscan
- Angry IP Scanner
- Nikto
- Unicornscan
- Autoscan

Packet Sniffers: They allow you to capture and visualise the traffic that is coming on your website.

- Wireshark
- TCPdump
- Ethercap
- Dsniff
- EtherApe

Vulnerability Exploitation: These are the tools you would use in order to gain access to various places.

- Metasploit
- Sqlmap
- Sqlninja
- Social Engineer Toolkit
- Netsparker
- BeEF
- Dradis

Vulnerability Scanners: These are designed to access a computer or network's vulnerability to attacks. The functionaility of these tools varies from one to the other, but they all present a detailed analysis of how vulnerable your system is.

- Nessus
- OpenVAS
- Nipper
- Retina
- QualysGuard
- Nexpose

Hacking Operating System: These are OS that have been designed specifically for hackers.

- Backtrack5r3
- Kalilinux
- SE Linux
- Knoppix
- Backbox linux
- Pentoo
- Matriux Krypton
- NodeZero
- Blackbuntu
- CAINE
- DEFT
- Helix

Intrusion Detection Systems: These tools are one of the most important part of any security arrangement. They allow you to detect those threats that are potentially dangerous for your system.

- Snort
- NetCap

VIII. CONCLUSION

Ethical hacking seems to be a new buzz word although the techniques and ideas of testing security by attacking an installation aren't new at all. But, with the present poor security on the internet, ethical hacking may be the most effective way to plug security holes and prevent intrusions. On the other hand ethical hacking tools have also been notorious tools for crackers. So, at present the tactical objective is to stay one step ahead of the crackers. Ethical Hacking is a tool, which if properly utilized, can prove useful for understanding the weaknesses of a network and how they might be exploited. After all, ethical hacking will play a certain role in the security assessment offerings and certainly has earned its place among other security assessments. 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.

REFERENCES

[1]. Gurpreet K. Juneja, "*A Technique to Enhance Information Security"*, dec 2013.

[2]. Aileen G. Bacudio, 1Xiaohong Yuan, 2Bei-Tseng Bill Chu, 1Monique Jones*, "An Overview of Penetration Testing"*, Volume3.no.6, Nov 2011

[3]. Monika Pangaria1, Vivek Shrivastava2," *Need of Ethical Hacking in Online World"*, Volume.2. Issue 4.Apr 2014

[4]. K.BalaChowdappa,S. Subbulakshmi,P.N.V Pavan Kumar, Ethical Hacking Techniques with Penetration Testing, Volume 5(3).2014

[5]. Regina D. Hartley, Ethical Hacking: Teaching Students to Hack, East Carolina University.

[6]. Monika Pangaria, Vivek Shrivastava, "*Need of Ethical Hacking in Online World",* International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064, Volume 2 Issue 4, April 2013.

[7]. Rashmi Hegde, "Biometrics Authentication Technique with Kerberos for Email Login", International Journal of Advances in Engineering & Technology, Vol. 7, Issue 6, pp. 1735-1744, Jan., 2015.

[8]. Amitesh Kumar Gupta, Asish Srivastava, Tinesh Kumar Goyal, Piyush Saxena, "*ETHICAL HACKING: An Approach towards Penetration Testing "*,International Journal of Modern Communication Technologies & Research (IJMCTR) ISSN: 2321-0850, Volume-2, Issue-5, May 2014

[9]. Aniruddha P Tekade, Pravin Gurjar, Pankaj R. Ingle, Dr.B.B.Meshram, "*Ethical Hacking in Linux Environment",* International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 , Vol. 3, Issue 1, January -February 2013, pp.1854-1860