International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

Study on Ethical Hacking and Penetration Testing

Abhishek Gupta[1] , Dr. Jatinder Singh Mahnas[2]
[1]Research Scholar, AISECT University, Bhopal, Madhya Pradesh, India
[2]Sr. Assistant Professor, University of Jammu, Jammu and Kashmir, India

ABSTRACT

Ethical hacking refers to the act of tracing weaknesses and vulnerabilities of computer and information systems by duplicating the intent and actions of malicious hackers. Ethical hacking is also known as penetration testing, intrusion testing, or red teaming. Hacking is an activity in which, a person exploits the weakness in a system for self-profit or enjoyment. As public and private organizations migrate more of their critical functions or applications such as electronic commerce, marketing and database access to the Internet, then hackers have more opportunity and incentive to gain access to sensitive information through the Web application. Thus the need of protecting the systems from the hacking generated by the hackers is to promote the persons who will punch back the illegal attacks on our computer systems. Ethical hacking is an identical activity which aims to find and rectify the weakness and vulnerabilities in a system. Ethical hacking describes the process of hacking a network in an ethical way, therefore with good intentions. This paper describes what is ethical hacking, what are the types of ethical hacking, impact of Hacking on Businesses and Governments and penetration testing used for protection form hackers .

Keywords : Ethical Hacking, Penetration,Vulnerabilities, Hacker .

I. INTRODUCTION

Ethical Hacking

Ethical hacking is an extensive term that covers all hacking techniques, and other associated computer attack techniques. So, along with discovering the security flaws and vulnerabilities, and ensuring the security of the target system, it is beyond hacking the system but with a permission in order to safeguard the security for future purpose. Hence, we can that, it is an parasol term and penetration testing is one of the features of ethical hacking. 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

II. METHODS AND MATERIAL

Ethical hacking Phases:

The Ethical hacking process needs to be planned in advance. All technical, management and strategic 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 of 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 information:

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. The overall hacking methodology consists of certain steps which are as follows:

Step-1: Reconnaissance
Step-2: Scanning
Step-3: Enumeration
Step-4: Gaining Access
Step-5: Maintaining Access
Step-6: Creating Tracks

Step-1: **Reconnaissance:-**The literal meaning of the Word reconnaissance is a preliminary survey to gain the information. This is also known as foot-printing. The hacker collects information about the company which the person is going to hack. Information as DNS servers, administrator contacts and IP ranges can be collected. During the reconnaissance phase different kind of tools can be used – network mapping, network and vulnerability scanning tools etc can be commonly used. Cheops for example is a very good network mapping tool which is able to generate networking graphs.

They can be of great help later on during the attack phase or to get an overview about the network. A network mapping tool is very helpful when doing an internal ethical hack.

Step-2: **Scanning**:-The hacker tries to make a blue print of the target network. 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. Modern port scanning uses TCP protocol to do scanning and they could even detect the operating systems running on the particular hosts.

Step-3: **Enumeration**:- Enumeration is the ability of a hacker to convince some servers to give them information that is vital to them to make 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.

Step-4: **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 phase. Usually the main hindrance to gaining access to a system is the passwords. In the System hacking, first the hacker will try to get in to the system.

Step-5: **Maintaining Access**:- Now the hacker is inside the system . This means that he is now in a position to upload 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. This is analogous to making a small hidden door in the building so that he can directly enter in to the building through the door easily.

Step-6: Clearing Tracks:- Here the hacker eliminates the physical evidence of his/her hacking the system. Whenever a hacker downloads some file or installs some software, its log will be stored in the server logs. So in order to erase the

hacker uses man tools. One such tool is windows resource kit's auditpol.exe. Another tool which eliminates any physical evidence is the evidence eliminator. The Evidence Eliminator deletes all such evidences.

Penetration Testing

Penetration testing is a specific term and focuses only on discovering the vulnerabilities, risks, and target environment with the purpose of securing and taking control of the system. Or in other words, penetration testing targets respective organization's defense systems consisting of all computer systems and its infrastructure. Penetration techniques are used to protect from threats, the potential attackers are also swiftly becoming more and more sophisticated and inventing new weak points in the current applications. Hence, a particular sort of single penetration testing is not sufficient to protect your security of the tested systems. As per the report, in some cases, a new security loophole is discovered and successful attack took place immediately after the penetration testing. However, it does not mean that the penetration testing is useless. It only means that, this is true that with thorough penetration testing, there is no guarantee that

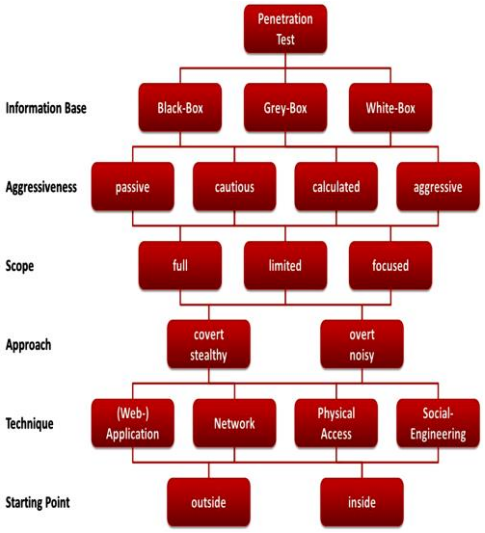
a successful attack will not take place, but definitely, the test will substantially reduce the possibility of a successful attack. Penetration testing is a process of systematic testing of hardware and software systems that involve in creating a complicated network for data storage and transmission. It is a method of understanding and evaluating the security ability of a network by simulating pretentious attacks and exploits. This understanding helps in elaborating the depth of the security system of any organization. This chapter considers all the different types of penetration testing based on the type of approach and also on the type of concentration. An overview of the different phases of penetration testing is described with block diagrams. Further, a description of the various tools that a pentester used are briefly listed. Towards the end, objectives and benefits of this testing methodology are explained.

1. Basic Concepts

"Penetration testing is the simulation of an attack on a system, network, piece of equipment or other facility, with the objective of proving how vulnerable that system or "target" would be to a real attack". This process is carried out by a potential ethical hacker. In simple words, it is the procedural auditing of the security features of an established network or application. Based on the type of approach, penetration testing is classified into three types, namely Black box, White box and Gray box..This also narrows down the classification into two major types i.e. external and internal. In simple words, it depends on whether the attacker system is inside the network or is targeting from outside.

1.1 Black-Box

The Black-Box penetration testing is the most practical attack that a tester implements without having any prior knowledge of the target systems. It is the most effective way to evaluate a system for its security controls. In simple words, the penetration tester would have no access to any sort of information regarding the network, making a real world type of attack. This eliminates the application type, location of the network, types of physical equipment, etc. The attacker has to study the target completely from scratch in a systematic way to reach his goal. The aim of the black box attack on a network is to study the cyber warfare attack completely. the network.



1.2 White-Box

The White-Box provides a formal way of testing certain infrastructure as the tester is provided all the basic information that understands the network layout, IP address and the application details . With this basic knowledge of the target network, the tester would be able to infiltrate the network's infrastructure with the key goal to mitigate the weak points. The tester basically works from inside the network and establishes concrete base to setup a strong system. In simple words, the tester and the organization work hand in hand to enable a tough security system.

1.3 Gray-Box

By the name, the Gray-Box is the combination of white box and black box types of penetration testing. Here, the tester is partially provided with the target system's infrastructure. This type is not popular in the usual classification. The available information may include the server IP address or the source code of the application. The tester might not always test the system from inside the network, rather pretend to be a hacker to test the robustness of the network environment. Furthermore, based on the assessment requirements, penetration testing typically can be divided into four types.

a) Applications

Applications based penetration testing is mainly the focused on the vulnerabilities in the data monitoring applications along with the firewall security issues. Also, the client-server

communication based applications that transfer information to sources might have critical loop holes that count big for the target system. In the current scenario, a lot of major web-based 9 applications have wide proven vulnerabilities that are yet to be mitigated. These aspects are concentrated while testing the network for its security using penetration testing.

b)Network

Network based penetration testing is one the major aspects in performing a testing over an organization's network. Based on the scale of the organization, the physical network might reflect security gaps that usually go unnoticed during the setup. To ensure an unbreakable network and maintain a strong back bone, penetration testing is performed on routers, switches, modems and hubs to fill in the gaps. It is a process where a tester ethically attacks the network operations in an organization to find flaws, vulnerabilities using exploits and aims to patch and fix the loop holes.

c) Physical

The scope of weakness in this area would be the unauthorized physical access to the target machines in an organization. Authentications and restricted access are thoroughly reviewed and tested while dealing with the physical technique penetrating testing. This plays a major role as it 10 helps gather information of the target system in a much more comfortable way of physically being inside the network. This is concentrated to synthesize the effectiveness of the authorization authentication and access to the physical systems.

d) Social

Social engineering targets on the social websites that can easily be reached using Google and other engines. With the high social exchange over websites like Facebook, LinkedIn and Twitter, a huge amount of information is being shared that could be a starting point of the attackers to build on. Also, public meetings, human interaction are the main weaknesses that are focused on by the attackers . This particular field of penetration testing is useful to evaluate the unauthorized access to the confidential information.

III. RESULTS AND DISCUSSION

Penetration tests on a large scale are beneficial in tracing critical vulnerabilities on any Logistic network, helping individual companies to either advance their technology or enhance the security by mitigating the loop holes. The main objectives of a successful penetration include security incidents credentials, determining the ease of the vulnerable aspects, and examining the extent of reachability. Benefits include proving the status of network infrastructure with detailed reports and identification of critical network points that are attack prone. These tests performed regularly protect an organization's security potential.

IV. CONCULSION

It is important to make a difference between penetration testing and network security assessments. A network security or vulnerability assessment may be useful to a degree, but do not always reflect the extent to which hackers will go to exploit a vulnerability. Penetration tests attempt to rival a 'real world' attack to a certain degree. The penetration testers will generally compromise a system with vulnerabilities that they successfully exploited. If the penetration tester finds 5 holes in a system to get in this does not mean that hackers or external intruder will not be able to find 6 holes. Hackers and intruders need to find only one hole to exploit whereas penetration testers need to possibly find all if not as many as possible holes that exist. This is a daunting task as penetration tests are normally done in a certain time frame. Finally, a penetration test alone provides no improvement in the security of a computer or network. Action to taken to address these vulnerabilities that is found as a result of conducting the penetration test.

V. REFERENCES

[1]. http://www.articlesbase.com/security-articles/ethical-hacking-an-introduction-402282.html

[2]. http://www.ehacking.net/2011/06/top-6-ethical-hacking-tools.html#sthash.nszGZw4y.dpuf

[3]. OWASP. "Web Application PenetrationTesting,"http://www.owasp.org/index .php/Web_Application_Pene tration_Testing.

[4]. http://www.corecom.com/external/livesecurity/pentest.html

[5]. http://www.networkdefense.com/papers/pentest.html
[6]. Internet Security Systems, Network and Host-based Vulnerability Assessment
[7]. http://www.infosecinstitute.com/blog/ethicalhacking_computer_forensics.html
[8]. http://searchnetworking.techtarget.com/generic/0,295582,sid7_gci1083715,00.html
[9]. http://www.owasp.org/index.php/Testing:_Information_Gathering