IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

Penetration Testing: Attacking Oneself to Enhance Security

Gurline Kaur[1], Gurpreet Kaur[2]

Assistant Professor, P.G. Dept. of Comp. Science & Applications, Kanya Maha Vidyalaya, Jalandhar, Punjab[1]

Student, M.Sc. IANS (Information & Network Security) Sem. IV, P.G. Dept of Comp. Science & Applications, Kanya Maha Vidyalaya, Jalandhar, Punjab[2]

Abstract: Penetration Testing is one tool of cyber security which is very common. This is a type of testing where in any organization attacks itself to know its own vulnerabilities. But this attack is stopped when any vulnerability or security loophole is encountered. Generally to have such a penetration testing or pen test a team of penetration testers or pen testers are hired. This testing is also bounded through various legal agreements as it deals with any organization's confidentiality and privacy. Thus, this paper is aimed at studying penetration testing from various topics thereby explaining the major types of penetration testing. There is a line of difference between hacking and penetration testing. This paper will also explain that demarcation.

Keywords: Penetration testing, vulnerability, intrusion, router, firewall, pentest.

I. INTRODUCTION

Penetration Testing is oldest methods for assessing the security of computer system. In the early 1970's, the Department of Defense used this penetration testing method to demonstrate the security weakness in computer systems or networks. Penetration Testing is the process of testing the organization in order to find any loopholes and vulnerabilities. It is done with acceptance of the organization. Once the loopholes and vulnerabilities are found, then the report is generated and the counter measures are taken to remove them or to reduce them. The penetration testing can determine the internal and external resources. A penetration tester is the attested, programmed and effective technique used to find the vulnerabilities.

II. LITERATURE SURVEY

In [1] Swarnjeet Kaur and Harmandeep Singh described that Penetration testing is a number of events to demonstrate the security exposures. Penetration testing is a method to perform a appropriate attack on a IT companies to find a danger harm and security risks, using a tools and a particular task that gives a popular description of what real-world malicious attacker would perform. A penetration testing is a technique to make an attempt to achieve resources information without awareness of private information or data. User finds the weakness and security of the companies as a particular way of cracker or attacker.

In [2] Aileen G. Bacudio, Xiaohong Yuan, Bei-Tseng Bill Chu and Monique Jones have proposed that Penetration testing is a inclusive method to test the complete, integrated, operational, and trusted computing base that consists of hardware and software. The process includes an active analysis of the system for any potential vulnerability, including poor system configuration or improper system configuration, hardware and software flaws, and operational weaknesses in the complicated countermeasures. Penetration testing is different from security functional testing. The latter demonstrates the accurate performance of the system's security controls while penetration testing determines the complexity for someone to penetrate an organization's protection control in objection, to the illegitimate access to its information and information systems. It is done by mimic an unauthorized user attacking the system using each automated tools or manual method or both of these manual and automated tools.

In [3] Brandon F. Murphy has described that this paper will illustrate the research done to test aptitude to penetrate a network without user interface, in order to retrieve private information from a targeted host. BlackBuntu is a Linux-based distribution for penetration testing. BlackBuntu was particularly designed for security training for students and practitioners of IT security. BlackBuntu is penetration testing linux based distribution with GNOME Desktop Environment.

In [4] Emily Chow has suggested that Ethical hacking and penetration testing is a defensive technique which consists of a chain of legitimate tools that recognize and exploit an organization's security weaknesses. It uses the identical or related mechanism of malicious hackers to attack key vulnerabilities in the company's security system, which then can be mitigated and closed. These tests reveal how simple an organization's security controls can be penetrated, and to obtain contact to its confidential and sensitive information asset by hackers. As a result, ethical hacking is an successful tool that can help support CA professionals to enhanced recognize the organization's information systems and its approach, as well as to

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

improve the stage of assurance and IS audits if used properly.

In [5] V.V.N. SURESH KUMAR has described that Penetration testing helps to evaluate the helpfulness of system security or ineffectiveness of the system security inside testing is performed from within the organization's technology environment. The main reason of penetration situation so that the security flaws can be eliminated earlier than hackers exploit the computer. Ethical hackers use their skills and apply penetration testing to determine the weakness consideration, offer the value to high sensitive data of Penetration testing. The type of penetration testing depends upon the condition of an institute wants to test, whether the scope is to replicate an attack by an internal (employee, network admin/ system admin, etc) or external source.

In [6] Daisy Suman, Sarabjit Kaur and Geetika Mannan have suggested that A penetration test generally involves the use of attacking methods conducted by trusted persons that are also used by aggressive intruders or hackers. Pen tests can be automated with software applications. Penetration testing can be performed manually. Penetration tests are an brilliant method for determining the strengths and weaknesses of a network consisting of systems and network devices. However, the process of penetration test is composite, and if it is taken out carelessly then it can have fatal effects.

III. TYPES OF PENETRATION TESTING

The different types of penetration testing are:

A. External Network Penetration Testing
External Network Penetration Testing refers to attack on the organization network perimeter using procedures performed from outside the organization systems, that is from the internet or extranet. This test may be performed with no or full disclosure of the environment in question. It involves analysis of publicly available information, a network enumeration phase and behavior of security services analyzed.

B. Internal Network Penetration Testing
Internal Network Penetration Testing is performed from within the organization's technology environment. This test mimics an attack on the internal network by a disaffected employee or an authorized visitor having standard access privileges. This testing is often performed from different network access points that include both the physical and logical segments.

C. Router Penetration Testing
Router Penetration Testing is done for testing misconfiguration of router product specific vulnerabilities. Routing devices are used to direct network traffic, and one router can be used to manipulate network traffic if router is misconfigured or unsecure. A compromise on routing device compromises the entire network traffic.

D. Firewall Penetration Testing
Firewall Penetration Testing means that the firewall too needs to check so that it is working properly or not Firewall Penetration Testing attempts to penetrate the firewall and host within the target network are initiated from a host outside of the network. Firewall Penetration Testing attempts to compromise the firewall security software, configuration settings or operating system itself from hosts within the network. With this vulnerabilities as well as misconfigurations and badly implemented security policies are exploited.

E. Application Penetration Testing
Application Penetration Testing organization perform conscientious testing of an applications to check for code related or back end vulnerabilities that provided access to the application itself, the underlying operating system, or the data that the application can access. Application Penetration Testing and Security Assessment services can be employed to test your trade web applications as well as standard applications like antivirus, embedded applications, games, and other computer system applications.

F. Intrusion Detection System Penetration Testing
Intrusion Detection System Penetration Testing attempts to penetrate IDS from outside as well as inside to find loop holes and weak security policies weak signatures or rules, attempts to figure out the misconfigurations of IDS. To circumvent IDS, you need to find holes in its rules, signatures and / or thresholds. Though it is unlikely to have complete information on the rule set of existing IDS, many hackers and security consultants do have an understanding of the common IDS rule set, including typical threshold values. They develop their penetration strategy around bypassing the common IDS configuration.

G. Password Cracking Penetration Testing
Password Cracking Penetration testing team will extract/ etc/ password and /etc/shadow files in Linux or extract SAM files in windows. The various password cracking tools are used for password cracking penetration testing. Some of the passwords cracking tools are john the ripper, pwdump3, l0phtcrack. The Team will identify the target person's personal profile and will try various password cracking tools to break password protected files. Then the password cracking team makes a report and presents it to the organization.

IV. TOOLS OF PENETRATION TESTING

There are a wide variety of tools that are used in Penetration Testing and the important tools are:

A. NMap
NMap which is also called Network Mapper In order to develop network services and maps, Nmap (network mapper) a scanner is used which is written by Gordon Lyon. To accomplish its goal, NMap sends specifically crafted packets to the target host and then analyses the

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

responses. NMap supports the scanning of the various types of protocols and most of the existing systems. It is free software.

B. Cain and Abel

Cain and Abel is a penetration tool. This tool is mostly used for password cracking. If cracking encrypted passwords or network keys is what you want, then Cain& Abel is the tool for you. It uses network sniffing, Dictionary attack, Brute-Force and Crypt analysis attacks, and routing protocol analysis methods to accomplish this. Test out information about this free to use tool at below page.

This is entirely for Microsoft operating systems. Cain and Abel is predominantly developed in order to help for security professionals and Network admins. The new version of Cain and Abel supports ARP Poison routing attacks.

C. BeEF

BeEF is stands for The Browser Exploitation Framework. It is a penetration testing tool that focuses on the web browser. It has a GUI interface, works on Linux, Apple Mac OS X and Microsoft Windows. It is open source and can be found at this page. BeEF allows the professional penetration tester to assess the actual security posture of a target environment. It investigates the exploitability in the context of web browsers. BeEF works on the base of hooking one or more web browsers like Google, internet explorer, Mozilla Firefox etc as beachhead for the launching of directed command modules.

D. Metasploit

This is the most popular Framework that can be used to for pen-testing. Metasploit is test tools that test for weaknesses in operating systems and applications. This penetration testing tool is based on the concept of 'exploit' which is a code that can most excellent the security measures and enter a definite system.

If entered, it runs a 'payload', a code that performs operations on a target host, thus creating the perfect framework for penetration testing. It is an advanced open-source platform for developing and testing. It can be used on web applications, networks, servers etc. It has a command-line and a GUI interface, works on multiple operating systems like: Linux, Apple Mac OS X and Microsoft Windows. This is a commercial invention, although there might be free limited trials available.

E. Nessus

Nessus is most popular penetration testing tool and remote security scanner, meaning that it is typically run on one machine to scan all the services offered by a remote machine in order to determine whether the later is safeguarded against all known security exploits. Nessus is the world's most popular vulnerability scanner that is used in over 75,000 organizations worldwide. This tool allows the user to script and run specific vulnerability checks. These checks provide a lot of control where most products do not. It is non – destructive.

V. DIFFERENCE BETWEEN PENETRATION TESTING AND HACKING

Penetration Testing is the process of attacking any organization in order to determine whether there exists any loopholes or not. This is usually done with the acceptance of the organization.

Hacking can be defined as the process of attacking any organization without the permission of the organization.

The main difference between penetration testing and hacking is as given below in the form of TABLE I.

TABLE I Difference between Hacking & Penetration Testing

Sr.No.	Penetration Testing	Hacking
1	In Penetration Testing the organization is attacked with the purpose of finding any loopholes or vulnerabilities in order to remove them.	In Hacking, the organization is attacked with the purpose ofobtaining the valuable data and information of the organization to be exploited.
2	Penetration Testing is done with the acceptance of the organization.	Hacking is done with the purpose of stealing the data and the information of the network without the permission of the organization.
3	Penetration Testing is done by the third party or the penetration testing team hired by the organization.	The Hacker can be a single person or a group but never acquired by the organization.
4	In Penetration Testing the organization employees the people for doing the Penetration Testing of their organization.	In Hacking the organization employees the people for not doing the Penetration Testing of their organization.
5	Penetration Testing is considered legal because everything happens with the acceptance of the organization.	Hacking is considered illegal because not everything happens with the acceptance of the organization.
6	In Penetration Testing, once the loopholes are founded then the organization takes various countermeasures to recover from the loopholes or a remove them.	Hacking only aims to steal the important data and the important information.

DOI 10.17148/IJARCCE.2016.54141

7	In Penetration Testing, there is not any kind of loss to the organization. All is the files of the Penetration Testers are saved and returned to the organization in the form of a report. This is all done under various legal documents.	In Hacking the organization can be in loss if the hacker becomes successful in obtaining the access to the organization data and the information.

VI. CONCLUSION

After studying this paper one can easily obtain the knowledge about what penetration testing is, how it is done and also about the various tools available. There are a number of tools available for such purpose; a few of them are explained.

REFERENCES

[1] Swarnjeet Kaur and Harmandeep Singh, A Descriptive Review of Different Penetration Testing Tools and Methods, March, 2016 International Journal Of Engineering Sciences & Research Technology.
[2] Aileen G. Bacudio, Xiaohong Yuan, Bei-Tseng Bill Chu and Monique Jones, AN OVERVIEW OF PENETRATION TESTING, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011.
[3] Brandon F. Murphy, Network Penetration Testing and Research, July 30 2013.
[4] Emily Chow, Ethical Hacking & Penetration Testing, July 1, 2011.
[5] V.V.N. Suresh Kumar, Ethical Hacking and Penetration Testing Strategies, Volume 11 Issue 2 –NOVEMBER 2014 IJETCSE.
[6] Daisy Suman, Sarabjit Kaur and Geetika Mannan, Penetration Testing, International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 10, October 2014.

DOI 10.17148/IJARCCE.2016.54141