International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

ETHICAL HACKING TESTING TOOLS - A SURVEY PAPER

GATTU. RAMYA
Assistant Professor, Department of Computer Science and Engineering, Siddhartha Institute of Technology and Sciences, Narapally, Hyderabad, Telangana, India

ABSTRACT
The main aim of the paper is to emphasize the importance of Penetration Testing in Cyber Security domain. Penetration testing is a series of activities undertaken to identify and exploit security vulnerabilities. It helps confirm the effectiveness or ineffectiveness of the security measures that have been implemented. This paper provides an overview of different penetration testing tools which are required in securing the cyber world. This paper emphasizes the benefits and procedure of conducting penetration testing. We mentioned the best penetration tools based on our survey.
KEYWORDS: Security Testing, Vulnerability Assessment, Penetration Testing, Web Application Penetration Testing

1. INTRODUCTION

Security is one of the major issues of information systems. The growing connectivity of computers through the internet, the increasing extensibility of systems, and the unbridled growth of the size and complexity of systems have made software security a bigger problem now than in the past [1]. Furthermore, it is a business imperative to adequately protect an organization's information assets by following a comprehensive, and structured approach to provide protection from the risks an organization might face [2]. In an attempt to solve the security problem and comply with the mandated security regulations, security experts have developed various security assurance methods including proof of correctness, layered design, software engineering environments and penetration testing. Penetration testing is a comprehensive method to test the complete, integrated, operational, and trusted computing base that consists of hardware, software and people [1]. The process involves an active analysis of the system for any potential vulnerability, including poor or improper system configuration, hardware and software flaws, and operational weaknesses in the process or technical countermeasures [3]. Penetration testing is different from security functional testing. The latter demonstrates the correct behaviour of the system's security controls while penetration testing determines the difficulty for someone to penetrate an organization's security controls against unauthorized access to its information and information systems. It is done by simulating an unauthorized user attacking the system using either automated tools or manual method or a combination of both. This paper provides an overview of penetration testing. It discusses the benefits of penetration testing, penetration testing strategies and types, as well as the methodology for penetration testing. It further illustrates the process of

conducting web application penetration testing using two example web applications: TuneStore and BOG.

2. WHY PENETRATION TESTING

The main goal of vulnerability assessment is to identify security vulnerabilities under controlled circumstances so they can be eliminated before unauthorized users exploit them. Computing system professionals use penetration testing to address problems inherent in vulnerability assessment, focusing on high-severity vulnerabilities. Penetration testing is a valued assurance assessment tool that benefits both business and its operations.

2.1 Benefits of Penetration Testing from Business Perspective

From a business perspective, penetration testing helps safeguard the organization against failure through preventing financial loss; proving due diligence and compliance to industry regulators, customers and shareholders; preserving corporate image; and rationalize information security investment [4]. Organizations spend millions of dollars to recover from a security breach due to notification costs, remediation efforts, decreased productivity and lost revenue. The CSI study estimates recovery efforts alone to be $167,713.00 per incident [5]. Penetration testing can identify and address risks before security breaches occur, thus preventing financial loss caused by security breaches. Industry has mandated regulatory requirements for computing systems. Non-compliance can result in the organization's receiving heavy fines, imprisonment, or ultimate failure [4]. Penetration testing, as a proactive service, provides unassailable information that helps the organization to meet the auditing or compliance aspects of regulations. A single incident of compromised client data can be devastating. Loss of consumer confidence and business reputation can put the entire organization at risk. Penetration testing creates heightened awareness of security's importance at all levels of the organization. This helps the organization avoid security incidents that threaten its corporate image, put its reputation at risk and impact customer loyalty. Penetration testing evaluates the effectiveness of existing security products and provides the supporting arguments for future investment or upgrade of security technologies. It provides a "proof of issue" and a solid case for proposal of investment to senior management [5]. 2.2 Benefits of Penetration Testing from Operational Perspective From operational perspective, penetration testing helps shape information security strategy through quick and accurate identification of vulnerabilities; proactive elimination of identified risks; implementation of corrective measures; and enhancement of IT knowledge [4]. Penetration testing provides detailed information on actual, exploitable security threats if it is encompassed into an organization's security doctrine and processes [5]. This will help the organization to identify quickly and accurately real and potential vulnerabilities. By providing the information required to effectively and efficiently isolate and prioritize vulnerabilities, penetration testing can assist the organization fine-tune and test configuration changes or patches to proactively eliminate identified risks.

Penetration testing can also help an organization quantify the impacts and likelihood of the vulnerabilities. This will allow the organization to prioritize and implement corrective measures for reported known vulnerabilities. The process of carrying out a penetration test entails a lot of time, effort and knowledge to deal with the complexities of the test space. Penetration testing will therefore enhance the knowledge and skill level of anyone involved in the process.

3. WHAT IS INVOLVED IN PENETRATION TESTING

There are two areas that should be considered when determining the scope and objectives of penetration testing: testing strategies and testing types used [2].

3.1 Penetration Testing Strategies

Based on the amount of information available to the tester, there are three penetration-testing strategies: black box, white box and gray box. In black box penetration testing, the testers have no knowledge about the test target. They have to figure out the loopholes of the system on their own from scratch. This is similar to the blind test strategy in [2], which simulates the actions and procedures of a real attacker who has no information concerning the test target. On the contrary, in white box penetration testing, the testers are provided with all the necessary information about the test target. This strategy is referred to in [2] as targeted testing where the testing team and the organization work together to do the test, with all the information provided to the tester prior to test. Partial disclosure of information about the test target leads to gray box penetration testing. Testers need to gather further information before conducting the test. Based on the specific objectives to be achieved, there are two penetration testing strategies which include external and internal testing. External testing refers to any attacks on the test target using procedures performed from outside the organization that owns the test target [2]. The objective of external testing is to find out if an outside attacker can get in and how far he can get in once he has gained access. Internal testing is performed from within the organization that owns the test target. The strategy is useful for estimating how much damage a disgruntled employee could cause. Internal testing is centred on understanding what could happen if the test target was successfully penetrated by an authorized user with standard access privileges.

3.2 Penetration Testing Types

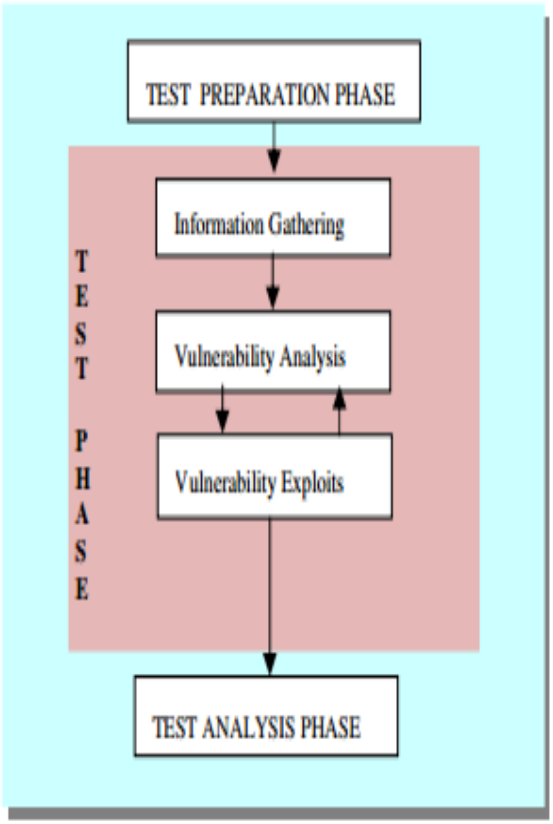
There are three areas to test in penetration testing: the physical structure of the system, the logical structure of the system, and the response or workflow of the system [6]. These three areas define the scope and the types of penetration testing which are network, application, and social engineering. Network penetration testing is an ethical and safe way to identify security gaps or flaws in the design, implementation or operation of the organization's network. The testers perform analysis and exploits to assess whether modems, remote access devices and maintenance connections can be used to penetrate the test target. Application penetration testing is an attack simulation intended to expose the effectiveness of an application's security controls by

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

highlighting risks posed by actual exploitable vulnerabilities [7]. Although organizations use firewall and monitoring systems to protect information, security can still be compromised since traffic can be allowed to pass through the firewall.Social engineering preys on human interaction to obtain or compromise information about an organization and its computer systems [8]. It is used to determine the level of security awareness among the employees in the organization that owns the target system. This is useful to test the ability of the organization to prevent unauthorized access to its information and information systems [2]. Thus, this is a test focused on the workflow of the organization.

4. HOW TO CONDUCT PENETRATION TESTING

Penetration testing is not merely the serial execution of automated tools and generation of technical reports as it is frequently viewed. It should provide a clear and concise direction on how to secure an organization's information and information systems from real world attacks. One critical factor in the success of penetration testing is its underlying methodology. A systematic and scientific approach should be used to successfully document a test and create reports that are aimed at different levels of management within an organization. It should not be restrictive to enable the tester to fully explore his intuitions. Generally, penetration testing has three phases: test preparation, test, and test analysis as shown in Figure 1.



All the necessary documents for the test are organized and finalized during the test preparation phase. The testers and the organization meet to decide the scope, objectives, timing, and duration of the test. Issues such as information leakages and downtime are resolved and put into legal agreement document. Other legal agreements that are deemed necessary are concluded and signed during this phase. The bulk of the penetration testing process is done during the test phase. A variety of automated tools can be used in this phase. Table 1 lists some of these tools. This phase involves the following steps: information gathering, vulnerability analysis, and vulnerability exploits.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Name of Tool	Specific Purpose	Cost	Portability
Nmap [8]	• network scanning • port scanning • OS detection	Free	Linux, Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga
Hping [6]	port scanning • remote OS fingerprinting	free	Linux, FreeBSD, NetBSD, OpenBSD, Solaris, Mac OS X, Windows
SuperScan [8]	• detect open TCP/UDP ports determine which services are running on those ports • run queries like whois, ping, and hostname lookups	free	Windows 2000/XP/Vista/7
Xprobe2 [8]	• remote active OS fingerprinting • TCP fingerprinting • port scanning	free	Linux
p0f [8]	• OS fingerprinting • firewall detection	free	Linux, FreeBSD, NetBSD, OpenBSD, Mac OS X, Solaris, AIX, Windows
Httprint [8]	• web server fingerprinting • detect web enabled devices (e.g., wireless access points, routers, switches, modems) which do not have a server banner string • SSL detection	free	Linux, Mac OS X, FreeBSD, Win32 (command line and GUI)
Nessus [8]	• detect vulnerabilities that allow remote cracker to control or access sensitive data • detect misconfiguration, default password, and denial of service	free for personal edition, nonenterprise edition	Mac OS X, Linux, FreeBSD, Oracle Solaris, Windows, Apple
Shadow Security Scanner [8]	• detect network vulnerabilities, audit proxy and LDAP servers	free trial version	Windows but scan servers built on any platform
Iss Scanner [7]	• detect network vulnerabilities	free trial version	Windows Server 2003/2008, Windows 2000 Professional, Windows 7 Ultimate/ Vista Business/XP Professional/Small Business Sever 2000/2003/2008
Brutus [8]	• Telnet, ftp, and http password cracker	free	Windows 9x/NT/2000
Metasploit Framework[8]	• develop and execute exploit code against a remote target • test vulnerability of computer systems	Free	All versions of Unix and Windows

The information gathering step requires that the tester scan the physical and logical areas of the test target and identify all pertinent information needed in the vulnerability analysis phase. Depending on the information gathered or provided by the organization, the tester then analyzes the vulnerabilities that exist within the target's network, host and application. The tester may opt to use the manual method to do this step but automated tools also exist to help the tester. The last step allows the tester to find exploits for the vulnerabilities found in the previous steps. When exploits do not lead to what is intended, for example, root access, then further analysis should be done. This is represented by the loop between vulnerability analysis and vulnerability exploit phases. The results of the test are thoroughly investigated during the test analysis phase. These results are provided to the organization so it must be comprehensive and systematic. Preparation of a mitigation plan is important in penetration testing [8]. It is therefore

mandatory to include a mitigation plan section in the analysis report.

5. WEB APPLICATION PENETRATION TESTING

Penetration testing is the systematic probing of a system that could be any combination of applications, hosts, or networks [6]. The general methodology of penetration testing described in Section 4 is a useful process to uncover and resolve security weaknesses of applications, especially web applications. This section illustrates the process of penetration testing using two example web applications, TuneStore and BOG. It should be noted that the areas tested here consist of only a small subset of the areas that should be tested. Therefore, the penetration testing process may be more comprehensive and may take more time and effort when performed on more complicated web applications. It is assumed that the test preparation phase has been completed prior to the test phase. There are three steps involved in the test phase: information gathering, vulnerability analysis, and vulnerability exploit. These phases are called discovery phase, vulnerability phase and attack simulation phase in [4]. The test phase is followed by test analysis phase.

5.1 Information-Gathering Step

In this step, the testers collect as much information about the web application as possible and gain understanding of its logic. The deeper the testers understand the test target, the more successful the penetration testing will be [4]. The information gathered will be used to create a knowledge base to act upon in later steps. The testers should gather all information even if it seems useless and unrelated since no one knows at the outset what bits of information are needed. This step can be carried out in many different ways: by using public tools such as search engines; using scanners; sending simple HTTP requests or specially crafted requests [7]; or walking through the application. The testers can identify the purposes of the application by browsing them. They can fingerprint the web server, spot the applications on both the client and the server side, and determine the content and functionality manually or using an automated tool. Table 2 lists some common tools that can be used in web application penetration testing. In what follows, we describe how to conduct information gathering on two example applications, BOG and TuneStore.

5.2 Test Analysis Phase

This phase is the interface of the results, the testers and the target entity [4]. It is important that the target entity is aware of typical attacker modus operandi, techniques and tools attackers rely on, exploits they use, and any needless exposure of data the target is suffering from. The reactive and corrective steps that need to be taken to address the problems should be included in this phase. Considering the findings for BOG and TuneStore, one of the remediation strategies could be to sanitize the user's input data before placing it within a SQL query. By requiring that the username and password being passed to the database do not contain any bad characters, the systems could be protected against SQL injection attacks. 6. DISCUSSION Penetration

testing can be an efficient and cost-effective strategy to protect the organization's systems against attacks. If done properly, it helps the organization identify the internal practices that give rise to vulnerabilities and other sources of vulnerabilities. The identified sources enable the organization to remove the vulnerabilities, properly direct the system's security efforts, pressure vendors to improve their products, improve its internal business security practices and prove to customers, shareholders and regulatory agencies that it is making a good faith effort to properly protect critical business data. Selecting a penetration team is a pertinent factor towards the success of penetration testing process. In evaluating the team, consideration should be given to their qualifications, experience and knowledge, reputation in the e-business community, access to, and use of, stateof-the art tools. A rule of thumb is to eliminate a team who provides the systems to be tested. Penetration testing cannot be expected to identify all possible security vulnerabilities since it is but just one aspect of testing. The organization should develop an overall security testing strategy that is tailored to its threat models and security policies. Finally, penetration testing should never be regarded as a one-off-service. It is conducted at a point of time. System changes, threats emerge, business strategies advance, and hacker tools evolve. Fixing or patching the vulnerability detected does not mean an end to your security worries and nightmare, it is just the beginning of a never ending cycle. In addition, a penetration test does not offer any guarantee of absolute security, it is just a measurement of security posture [8].

6. CONCLUSION

Penetration testing is a comprehensive method to identify the vulnerabilities in a system. It offers benefits such as prevention of financial loss; compliance to industry regulators, customers and shareholders; preserving corporate image; proactive elimination of identified risks. The testers can choose from black box, white box, and gray box testing depending on the amount of information available to the user. The testers can also choose from internal and external testing, depending on the specific objectives to be achieved. There are three types of penetration testing: network, application and social engineering. One of the most important parts of the test analysis phase is the preparation of remediation which includes all necessary corrective measures for the identified vulnerabilities. The final report needs to have enough detail and substance to allow those doing remediation to simulate and follow the attack pattern and respective findings [8].

REFERENCES

[1] McGraw, G. (2006). Software Security: Building Security In, Adison Wesley Professional.

[2] The Canadian Institute of Chartered Accountants Information Technology Advisory Committee, (2003) "Using an Ethical hacking Technique to Assess Information Security Risk", Toronto Canada. http://www.cica.ca/research-and-guidance/documents/it-advisory-committee/item12038.pdf, accessed on Dec. 09, 2016.

[3] Mohanty, D. "Demystifying Penetration Testing HackingSpirits," http://www.infosecwriters.com/text_resources/pdf/pen_test2.pdf, accessed on Dec. 09, 2016.
[4] "Penetraion Testing Guide", http://www.penetration-testing.com/
[5] iVolution Security Technologies, "Benefits of Penetration Testing," http://www.ivolutionsecurity.com/pen_testing/benefits.php, accessed on Dec. 05, 2016.
[6] Shewmaker, J. (2008). "Introduction to Penetration Testing," http://www.dts.ca.gov/pdf/news_events/SANS_InstituteIntroduction_to_Network_Penetration_Testing.pdf, accessed on Dec. 02, 2016.
[7] "Application Penetration Testing," https://www.trustwave.com/apppentest.php, accessed on Dec. 09, 2016.
[8] "Kali Linux Penetration Testing and Ethical Hacking ", http://docs.kali.org/ , accessed on Dec. 09,2016