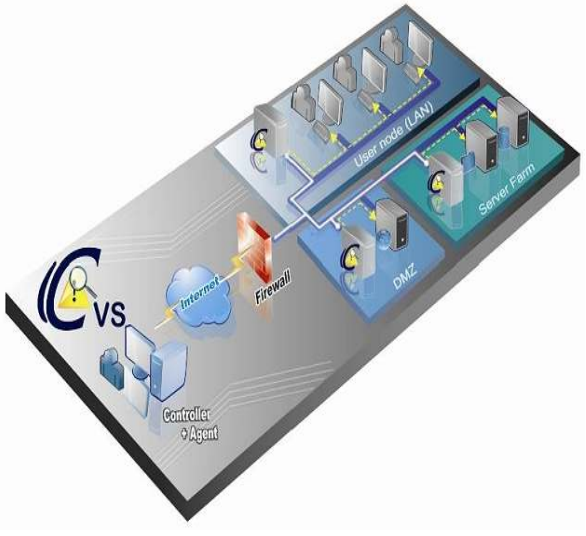
Industrial Science
ISSN 2347-5420

Impact Factor : 1.5015(UIF)
Volume - 1 | Issue - 12 | Aug - 2015

NETWORK VULNERABILITY DETECTION REPORTING SYSTEM WITH RECOMMENDATIONS & APPROPRIATE RESOLUTION

Uday Gobbur
[1]Master of Engineering student, Department of Computer science & Engineering
NK Orchid College of Engineering & Technology, Solapur , Maharashtra, India.

Suhas Raut
Ph.D. Professor, Department of Computer science & Engineering
NK Orchid College of Engineering & Technology, Solapur , Maharashtra, India.



ABSTRACT

Attacks against computer systems and the data contained within these systems are becoming increasingly frequent and evermore sophisticated. Organizations wishing to ensure security of their systems may look towards adopting appropriate measures to protect themselves against potential security breaches. One such measure is to hire the services of penetration testers to find vulnerabilities present in the organization's network, and provide recommendations as to how best to resolve such risks. In this paper we discuss role of the modern pen-tester and summarize current standards and professional qualifications and also further identify issues arising from pen-testers, thereby suggesting how to resolve loopholes in target system and generate report in printable format.

KEYWORDS :*Web application threats, Network application security, exploitation process and reporting.*

INTRODUCTION :

Generally in penetration testing process a simple way to test a system is held by primary analysis and formal methods, Based on the observation that most security flaws are triggered due to a flawed interaction with the environment. Here I have describe an approach for testing web application and database integration system for possible security flaws. This approach is to be included in a dynamic model which have the aim to bind the complex and lengthy procedure of penetration testing process. Proposed approach is prepared a model simplifies the complex penetration testing procedure and allow penetration tester to evaluate accurately what faults to be exist in the target system. The dynamic model of penetration testing can be implementing freely and efficiently on almost all type of applications. This scheme can be used to classify informatics, analytical, complex, logical, well-known and common security flaws of web application and network.

RELATED WORK:

Penetration tests are a great way to identify vulnerabilities that exists in a system or network that has an existing security measures in place. A penetration test usually involves the use o f attacking methods conducted by trusted individuals that are similarly used by hostile intruders or hackers. Depending on the type of test that is conducted ,this may involve a simple scan of an IP addresses to identify machines that are offering services with known vulnerabilities or even exploiting known vulnerabilities that exists in an unpatched operating system. The results of these tests or attacks are then documented and presented as report to the owner of the system and the vulnerabilities identified can then be resolved.

Penetration testing is often done for two reasons. This is either to increase upper management awareness of security issues or to test intrusion detection and response capabilities. It also helps in assisting the higher management in decision-making processes [5]. The management of an organization might not want to address all the vulnerabilities that are found in a vulnerability assessment but might want to address its system weaknesses that are found through a penetration test. This can happen as addressing all the weaknesses that are found in a vulnerability assessment can be costly and most organizations might not be able allocate the budget to do this.

EXISTING SYSTEM:

Security vulnerabilities in web applications may result in stealing of confidential data, breaking of data integrity or affect web application availability. Thus With the rapid growth of IT development the precaution are also big concerns for the research community against various threats and vulnerabilities. According to sophisticated vulnerability assessment tools 60% vulnerabilities can be found in most of web applications. Even due to automation in form of software many patches and security software are exist in the global world of IT for evade this type of threats such as antivirus, Intrusion detection system, Honey port, Firewall, application filtration software, source code reviewer etc. However the most common way of securing web applications are searching and eliminating vulnerabilities. Another ways of securing web application includes safe development while on other hand efficient way of finding security vulnerabilities from web applications is manual code review[1].

PROPOSED SYSTEM:

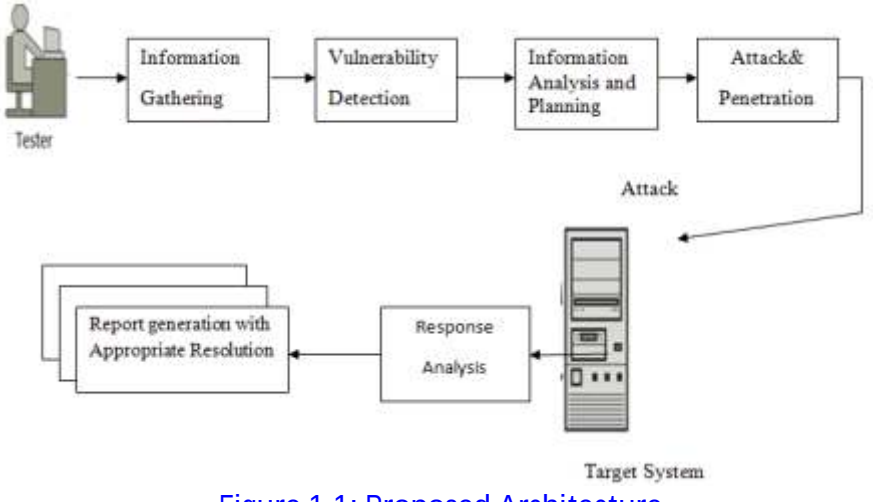


Figure 1.1: Proposed Architecture

System it follows following steps:

•Collect information about target system or network such as operating system, open ports, services running.

•Take all these information as input and find weaknesses of the target system.

•Analyze this entire information find out the risk of all weaknesses.

•To Perform various attacks on the target system and appropriately resolve vulnerabilities in the target system.

THE PROCESS AND METHODOGY:

•Planning and Preparation

In order to make the penetration test done on an organization a success, a great deal of preparation needs to be done. Ideally a kickoff meeting should be called between the organization and the penetration testers. The kick off meeting must discuss matter concerning the scope and objective of the penetration test as well as the parties involved. There must be a clear objective for the penetration test to be conducted.

•Information Gathering

Information gathering is the initial stage of any information security audit, which many people tend to overlook [2]. When performing any kind of test on an information system, information gathering and is essential and provides the testers with all possible information about the target to continue with the test.

•Vulnerability Detection

After having gathered the relevant information about the targeted system, the next step is to determine the vulnerability that exists in each system. Penetration testers should have a collection of exploits and vulnerabilities at their disposal for this purpose [2]. The knowledge of the penetration tester in this case would be put to test. An analysis will be do ne on the information obtained to determine any possible vulnerability that might exist. This is called manual vulnerability scanning as the detection of vulnerabilities is done manually.

The completion of the vulnerability detection will produce a definite list of targets to investigate in depth. These lists of targets will be used in the next stage. A penetration will be attempted at these targets that have their vulnerabilities defined.

•Information analysis and planning

In this stage tester collating the information gathered in previous stages and find the risk of the vulnerability and then decide which attack we have to perform. After determining the vulnerabilities that exist in the systems, the next stage is to identify suitable targets for a penetration attempt [2].

•Attack and Penetration

After choosing the suitable targets, the penetration attempt will be performed o n these chosen targets. There are some tools available for free via the Internet but they generally require customization. Knowing that a vulnerability exist on a target does not always imply that it can be exploited easily. Therefore it is not always possible to successfully penetrate even though it is theoretically possible[2]. In any case exploits that exist should be tested o n the target first before conducting any other penetration attempt.

•Report Generation

In this stage all information from above stages can be given as input for generating report. For example, organizations might accept the risk incurred from the less effective vulnerabilities and only address to fix the more affected ones [4].

CONCLUSION:

It is important to make a distinction 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 emulate 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 where as penetration testers need to possibly find all if not as many as possible holes that exist.

REFERENCES

[1]Seven Phrase Penetration Testing Model,ParvinAmi Assist. Professor B.K. Mehta IT Center, PalanpurBanaskantha, Gujarat -385001, India ,AshikaliHasan Chief Technical OfficerXeniar Technology Pvt Ltd Ahmadabad, Gujarat-380015, India,Volume 59– No.5, December 2012.
[2] http://www.sans.org/reading-room/whitepapers/auditing/67.php
[3]Penetration Testing, Stephen Northcutt, Jerry Shenk, Dave Shackleford, TimRosenberg, RaulSiles,andSteveMancini,http://www.sans.org/reading_room/analysis_program/PenetrationTesting_June06.pdf accessed on 1st march 2013.
[4]TheArtofWritingPenetrationTestReports, http://resources.infosecinstitute.com/writing-penetration-testing-reports accessed on 1st March 2013
[5]http://www.netragard.com/penetration-testing- definition
[6]VulnerabilityAnalysishttp://www.penteststandard.org/index.php/Vulnerability_Analysis.
[7]http://www.networkworld.com/article/2193965/tech-primers/top-10vulnerabilities inside-the-network.html
[8] http://www.softwaretestinghelp.com/penetration-testing-guide/
[9] Improving penetration testing through static and dynamic analysis, William G. J. Halfond, Shauvik Roy Choudhary and Alessandro Orso,Softw. Test. Verif. Reliab.(2011) Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/stvr.450
[10] Laura Chappell's session TUT233,"Cyber Crime at Packet Level", at Novell BrainShare 2001.
[11]Sample Network & Computer Security Policies, http://www.cpcstech.com/sample-network-computer-security-policies.html