ISSN:0975-9646

Survey: Secured Techniques for Vulnerability Assessment and Penetration Testing

Sushilkumar Yadav, Chandrakant Navdeti

Department of Information Technology, SGGSIE&T,
Nanded, Maharashtra, India

***Abstract*-- Now days, all of the computer users are using the facility of internet and different cloud applications. SECURITY is one of the major issues of the internet which are dealt with an immense important issue priority. Everyday well skilled invaders breach the security and take the advantage of security issues and flaws to access the confidential data and change them to inaccessible accounts. To overcome this problem one solution was suggested named Vulnerability Assessment and Penetration Testing (VAPT) for Security of Web applications. Vulnerability Assessment is the way by which we can find flaws in the system. Penetration Testing will detect the vulnerabilities and breach them to get access to the system through security issues. Penetration testing is widely used to help ensure the security of the network and host system. The usual way of penetration testing involves the manual tests by the hacker or a tester according to the given scheme, it requires a lot of work one by people and also it requires expertise on the system and every tool that we are going to use for penetration testing. We need to have some unique mechanism which will give detailed information on the scheme used for designing the system and will deal with the existing flaws that are susceptible to the attacks done by hackers. This paper will check for the existing systems for VAPT and will check for the features that it offers to the user and will propose the unique approach to it in a secured and unified way which will overcome the disadvantages of the existing systems and will provide some new features.**

***Keywords*— Secure Vulnerability Assessment.**

I. INTRODUCTION

In information system, we day to day hear that security is a journey and not a destination. While we are designing the system we need to manage the security issues of the system such that hackers will not be able to breach the security and insert the content like-malicious data, error prone information and insecure code. Hackers and malicious users will try getting access to the system and will get the confidential information from the system affected, without the knowledge of the user. We usually focus on the data privacy and its integrity in order to get the user safe and secured from the different types of security attacks. Hackers and the competitor people are always in search of the flaws in our system and breach that they can apply to our system. These breaches are mainly focused on the three important concepts in information and network security. Those are as below.

Confidentiality *(being safe from unauthorized access)* Confidentiality refers to limiting information access and disclosure to authorized user and preventing access and disclosure from unauthorized ones.

Integrity *(correctness and comprehensiveness of data)* Integrity refers to the credibility of information resources. It ensures that data have not been changed inappropriately either by deliberately or inadvertently malign activity.

Availability *(resources are always available to authorized user)* Availability refers to the accessibility of the information resources. It ensures that information must be available to authorized user when they accessed.

This paper is organized as follows Section: II describes the detail about Secure Vulnerability Assessment include its definition, steps in assessment. Section III. Describe the detail about Penetration Testing includes the steps involved and detailed description about the PT. Section IV. Contains Existing System Section V. Proposed system and Section VI. contains Conclusion

II. SECURE VULNERABILITY ASSESSMENT

"*Vulnerabilities* are the doorways via which threats are revealed". Security of the system can be tested by using the different doorways and security issues. There can be different types system like: Desktop system, Client-Server system, network nodes, routers, switches and defective firewalls and network or computer web application.

Vulnerabilities, security issues and flaws are the predefined issues in systems, web applications or even in networks design. Vulnerabilities are easily detectable by hacker for breaches and attacks. This will lead to the entry of hacker to the system which may lead to breaches in security such as Confidentiality, Integrity, Availability, Nonrepudiation, Authentication, authorization and access control. Secure Vulnerability assessments are carried out to know the easily traceable vulnerabilities as well as the vulnerabilities those are not traceable.

Secure Vulnerability Assessment is the process of detecting, evaluating and grading the Security vulnerabilities in the system. In this process we are not only scanning operating system but also scanning the web application for security flaws which may leads to a huge loss of an individual or an enterprise. The vulnerabilities are there in the system due to the software development flaws and coding standard use by that organization. Sometimes there can be a case that an enterprise is unaware of the standard secure coding practices. There can be flaws such as design flaws, security certificate use, insecure methods to call the different actions that may lead to secure transaction breach and misconfigured data in the application backend.

A. *Steps in secure vulnerability assessment*

Secure Vulnerability assessment is carried out through following steps:

1. Goals & Objectives: Why we are going to carry out the security assessment and what we will achieve from this is determined at the first step.

2. Scope: Security assessment is carried out by keeping in mind the scope of the application, whether it is going to be used for general use or for money transaction and the parts of the applications that ate much important to be assessed.

Black box security assessment: Security assessment from the network which is foreign to the system which don't have the basic info of the system and its components.

White Box Security Assessment: Carry out the security assessment for the given application which mainly consists of static code and dynamic code analysis.

Generally static code analysis is carried out by manual process and dynamic code analysis is carried out by using different tools. White Box security assessment is a pure source code check of an application. We need to take significant precautions when performing source code security assessments due to the sensitive nature of the applications. The entire application is checked and line by line inspected to ensure proper measures are there to protect the application from security attack. A mixed way by is used by VA using automated source code analysis tools and manual checking, in gives rise to a significant way which will help us to check with flaws and different issues that will detect the breaches in the web application. White Box application security assessments are the most comprehensive security assessment that can be performed on an application.

A White Box code review for security issues is the most accurate way to find and diagnose many security problems such as Cross Site Scripting, Broken Authentication, Injection etc. many of the security issues are detected by using this approach. Additionally, a code analysis for security is the only way to ensure that security has correctly been deployed. White Box code security assessments are the most accurate way to find security vulnerabilities.

3. Data Collection for application uses: This is the main task to get the more and detailed information of the system I order to carry out the security assessment in a proper and controlled way. Data is specifically related to the IT infrastructure such as networks, development environment, coding language, operating system version, deployment targets etc. it is applicable to both types of scope that are white box security assessment and black bo security assessment.

4. Identifying security breaches: this step mainly comprises of security scanning tools and human intelligence and security vulnerabilities are discovered in the given application by way of security assessment.

5. Data, Code and information analysis and Security measurement implementation: by this process we usually detect security issues and get them used for preventing security attacks.

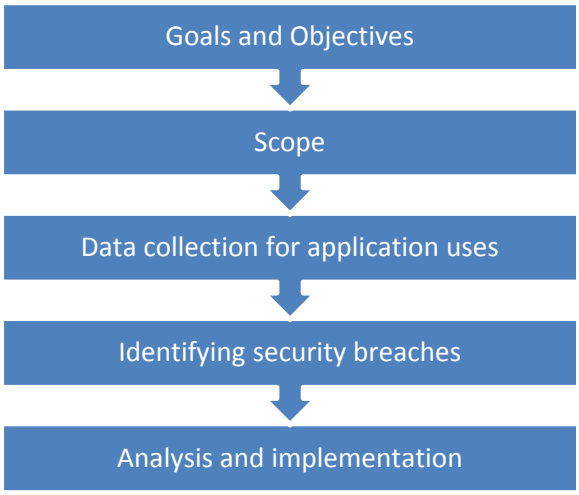

Fig.1: Steps involved in vulnerability assessment

III. PENETRATION TESTING

It is the process of trying to gain unauthorized access to authorized resources, systems and applications. Penetration testing is also known as an ethical hacking as "breaking into your own system to see how hard it is to do". Network security measurement is the task which aims at supplying the scanning to check the security flaws and security threats in applications and networks. The purpose of penetration testing is to recognize technique of accessing a system by using common tools and techniques designed by malicious user. After secure vulnerability assessments, which is are used to identify and invent various exposures within the web application. Penetration testing attempts to breach any one of the flaws to gain unauthorized access.

A. *Process of Penetration Testing*

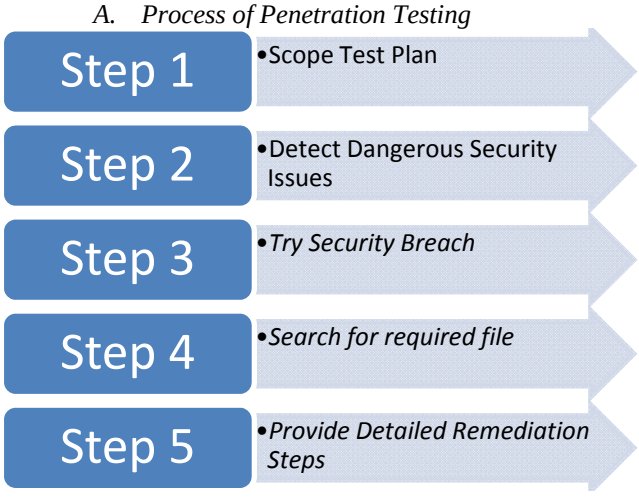

Fig.2: Penetration testing step-by-step execution

1. Scope Test Plan: In first step we lessen the scope of our test to what is meaningful to the client so that it can easily be identified.

2. Detect dangerous security issues: In this step dangerous security issues are detected and verified by using the tools used for PT. Those vulnerabilities are identified will be patched to get the resultant application state.
3. Try Security Breach: We can identify and verify that these are the vulnerabilities that occurred. We can breach into those security issues. The person who is dealing with the different tools will use the tools to breach the vulnerabilities and will find the ways by which system can be compromised. There can be systems such as (Important coding data servers, domain creation and controller servers, etc.)
4. Search for required file: The document for carrying out the breach or exploitation is provided to the client and is used to check with the issue that occurred in that same way or the way unique to itself.
5. Provide Detailed Remediation Steps:
At the completion of the previous steps the client is provided with the steps that he needs to take as a remediation task for a particular breach. Remediation is done according to the type of breach t and the consequences that are going to occur with the particular system.

IV. EXISTING SYSTEMS

A. Types of Security Vulnerabilities Assessment

In consideration with of vulnerability tools used there are three broad categories of security vulnerabilities assessment:
Host Based, Network Based, and Database based.

1. *Host Based:* Host Based Vulnerability Assessment detects the security issues in regards to an individual system or application. It is processed by using the tools used for host based assessment and will to deal with host based vulnerabilities. The tool will scan the whole application and will tell you actual spot of the application issues in regards with system.
2. *Network Based:* Network Based VA identify unused open ports, check the unused applications running on these ports and identify possible security issues associated with these applications. This is done by using the network scanning tools.
3. *Database Based:* Database Based VA detect security flaws in database systems using tools and techniques to prevent from SQL- Injections attack, can read unbearable data from the database and provides some data modification & change the DBMS.

a. Benefits of Security Vulnerability Assessment

- Freeware and open source tools are used to carry the out the secure vulnerability assessment.
- Detects most of known security issues that needs user's attention.
- Easy to do assessment due to no manual intervention required.

b. Weaknesses of Security Vulnerability Assessment

- The tools usually find much of the false positives.
- Not fully automated to generate the reports.
- Check for the directories that are not required for security assessment.
- Generate excess issues that are used for application to run faster.
- All the latest issues cannot be detected by the system as they are not added to the system.

B. Penetration Testing Strategies

Penetration testing methodology includes three types:
1. *A zero-knowledge Test:* Penetration test team has no real information about the target environment.
2. *A full knowledge test*: The client organization provides full information to test team.
3. *A partial knowledge Test:* Penetration test team has partial information about the target environment.

Types of Penetration Testing
External and internal testing are the two types of penetration testing.
1. External Testing: It includes Internet and
Dial-in. In internet, attack on the target network from outside the network. In Dial-in, War dialing is the systematic calling of each number in the number in the target rang in search of listening modems.
2. Internal Testing: It is performed from inside the network. The goal is to ascertain the internal network topology which gives the mapping of the critical access path.

a. Benefits of Penetration Testing

- Test network or system using the tools and techniques that attackers use.
- Demonstrate at what depth vulnerabilities can be exploited.
- Validate vulnerabilities.
- It can give common sense and confirmation required for to deal with the security issues.

b. Weaknesses of Penetration Testing

- It requires lot of efforts to be imparted to get the solution and it requires the trained and highly skilled person to address those needs.
- Dangerous when conducted by inexperienced tester.
- Revel source code to third party.
- Expensive.
- Some of the tools are not recommended as they not secure to use as a testing tool for certain application due to their mal-functionality.
- It requires the estimated time to carry out the test and it should be done periodically.
- We need to test the service in order to ensure the security or insecurity of that particular system or service.

V. PROPOSED SYSTEM

The proposed system will overcome the different disadvantages of the existing system.

- Existing system will not find the issues that are once found as false positive
- We propose the system that will provide the automation of reports after security assessment.

- Proposed system has a facility of Check for the directories that are not required for security assessment.
  We can exclude the directories such as libraries, jars and tools directories from the data to be scanned.
- The proposed system generates the issues that are severe and it will remove the issues that are generated and false positive.
- Proposed systems provide a GUI to add the latest issues and also it has a auto detection system for new issues which will find issues.
- The system is automated so requires only one person to look after it, who will monitor the activities. We have also planned to automate it as a web application which will be accessed it from your location with the help of a URL. The system has an easy readme to understand the system which will reduce the expertise required for the system.
- As the system is easy to understand so we can easily operate it.
- The system will not give the data to any third party as it has designed its security mechanism with three way authentication.
- It's not that much expensive as we have designed the system using the freeware and inbuilt tools.
- The tools that we used are valid by OWASP organization so that are not banned by any agency.
- The different tools are used for testing the system for different types of assessment and we are going to use it as a standard for the testing the applications.

Also the proposed system will contain the all types of assessment in the same system. Also it adds some more strength to the system as we have added the reporting part in the proposed system.

VI. CONCLUSION

The proposed system will solve the problems that we are facing right now such as we have to use different tools from different organization for carrying out the assessment of each type. So we are going to get a single system which has different tools integrated into the single system and we have automated them as a web application. We can carry out the different types of assessment like host, network as well as database based by using this single system.

REFERENCES

[1] "*Vulnerability Assessment and Penetration Testing*", Ankita Gupta, Kavita, Kirandeep Kaur

[2] "*Vulnerability Assessment And Penetration Testing*", Sachin Umrao, Mandeep Kaur & Govind Kumar Gupta

[3] "*A Modern Approach to Cyber Security Analysis Using Vulnerability Assessment and Penetration Testing*", Sugandh Shah, B. M. Mehtre

[4] Vulnerability Assessment and Penetration Testing http://www.aretecon.com/aretesoftwares/ vapt.html

[5] http://searchsoftwarequality.techtarget.com/definition/penetration-testing http://www.netragard.com/penetration-testing- definition

[6] Introduction to t h e Premier Pen Testing Informa- tion Security Certification (Advanced EthicalHacking)

[7] Laura Chappell's session TUT233, "Cyber Crime at PacketLevel", at Novell BrainShare 2001.

[8] C. Anley,"Advanced SQL injection in SQL server applications,", 2002.

[9] Open Web Application Security Project, https://www.owasp.org/index.php/Category: Vulnerability

[10] Vulnerability Analysis, http://www.pentest-standard.org/index.php/ Vulnerability_Analysis

[11] Penetration Testing Limits http://www. praetorian.com/blog/penetration-testing/ limitations-of-penetration-testing/, 2008

[12] Audit your website security with Acunetix Web Vulnerability

[13] Xiaowei Li and Yuan Xue, "A Survey on Web Application Security", Technical report, Vanderbilt University, 2011.

[14] Shahriar H. and Zulkernine M., " Automatic Testing of Program Security Vulnerabilities", proceeding of 33rd International Conference of Computer Software and Applications (COMPSAC), 2009 IEEE, pages 550-555.

[15] Steven Palmer, " Web Application Vulnerabilities: Detect, Exploit, Prevent", Syngress Publishing, 2007, ISBN: 1597492094 9781597492096.