International Journal of Computer and Communication Technology

Volume 7 | Issue 3 Article 11

July 2016

VULNERABILITY ASSESSMENT AND PENETRATION TESTING

SACHIN UMRAO
Department of Computer Application, KIET, Ghaziabad, India, sachin.umrao@rediffmail.com

MANDEEP KAUR
Department of Computer Application, KIET, Ghaziabad, India, deepan.mandeep@gmail.com

GOVIND KUMAR GUPTA
Department of Computer Application, KIET, Ghaziabad, India, mastergvnd.378@gmail.com

Recommended Citation
UMRAO, SACHIN; KAUR, MANDEEP; and GUPTA, GOVIND KUMAR (2016) "VULNERABILITY ASSESSMENT AND PENETRATION TESTING," *International Journal of Computer and Communication Technology*: Vol. 7 : Iss. 3 , Article 11.
DOI: 10.47893/IJCCT.2016.1367
Available at: https://www.interscience.in/ijcct/vol7/iss3/11

VULNERABILITY ASSESSMENT AND PENETRATION TESTING

SACHIN UMRAO[1], MANDEEP KAUR[2] & GOVIND KUMAR GUPTA[3]

[1,2&3]Department of Computer Application, KIET, Ghaziabad, India
Email: sachin.umrao@rediffmail.com, deepan.mandeep@gmail.com, mastergvnd.378@gmail.com

Abstract-In this modern world, all of the persons are using the facility of internet. SECURITY is one of the major issue of the internet. Everyday highly skilled hackers breach the security and take the advantage of vulnerabilities to access the confidential data. To overcome this problem one solution was suggested named Vulnerability Assessment and Penetration Testing (VAPT). Vulnerability Assessment is the art of finding an open door. Penetration Testing involves a series of activities undertaken to identify and exploit security vulnerabilities. Penetration testing is widely used to help ensure the security of the network. Traditional penetration testing were manually performed by tester according to scheme, the process is usually complex resulting in that it is labor-intensive and requires tester to be familiar with all kind of tools. So it is very desirable to use a unified method to describe the scheme which can be identified by computer, then the computer can be used to substitute for tester to perform penetration testing. This paper gives the overview of VAPT and describes the process & methodology of Vulnerability Assessment and Penetration Testing.

***Keywords**: Network security, Vulnerability assessment (VA), Penetration Testing (PT), Pen Tester.*

I. INTRODUCTION

In information system, we repeatedly hear that security is a journey and not a destination. That’s true because when managing the security of network, we always have to endeavour and stay one step ahead of our opponents – the criminals, malcontents, hackers, spies and miscreants. They steal data and information without breaking any glass. Keeping data confidential is one core mission of network security. Opponents are always honing their method and techniques each day to exploit network security and access the confidential information. These exploits are attacks against: *confidentiality*, *integrity* and *availability* of network resources.

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.

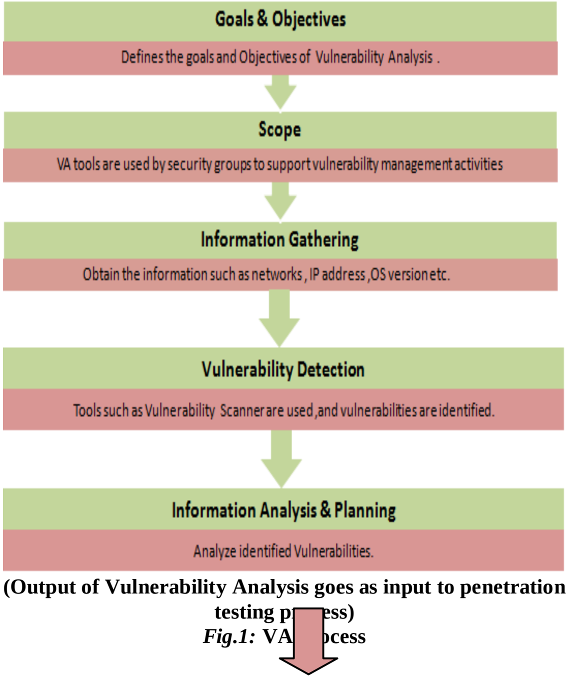
This paper is organized as follows Section: II describes the detail about VA include its process, strengths & weaknesses. Section III. Describe the detail about PT includes its process, strengths & weaknesses, Section IV. Comparison between VA &. PT, Section V. Conclusion & Future Scope.

II. VULNERABILITY ASSESSMENT

"*Vulnerabilities* are the doorways via which threats are revealed”. Vulnerabilities are actually weaknesses in system. A system is any of the following: computer system, network system, network nodes, routers, switches and firewalls and network or computer application. It is the inherit defects in systems, web applications or even in networks design. Vulnerabilities are open a door to exploitation.

This generates the possibility for penetration into the systems that may consequence in unauthorized access and a compromise of confidentiality, integrity, and availability of network resources. Vulnerability testing is a process to probe system from known vulnerabilities. *Vulnerability Assessment* is the process of pinpointing, computing and ranking the vulnerabilities in the system. In this process, such as operating systems & application software and network are scanned in order to identify the occurrence of well-known and unknown vulnerabilities. These vulnerabilities are occurs due to inappropriate software design, insecure authentication or even much vulnerabilities occurs as a result of misconfiguration.

A. *Process of Vulnerability Assessment*


Goals & Objectives
Defines the goals and Objectives of Vulnerability Analysis .
Scope
VA tools are used by security groups to support vulnerability management activities
Information Gathering
Obtain the information such as networks , IP address ,OS version etc.
Vulnerability Detection
Tools such as Vulnerability Scanner are used ,and vulnerabilities are identified.
Information Analysis & Planning
Analyze identified Vulnerabilities.

(Output of Vulnerability Analysis goes as input to penetration testing p ess)

Fig.1: **VA cess**

1. *Goals & Objectives*: Defines goals and objectives of Vulnerabilities analysis.
2. *Scope:* While performing assessments and tests, the scope of the assignment needs to be clearly defined. The scope is based on the assets to be tested. The following are the three possible scopes that exist*:*
   - *Black Box Testing:* Testing from an external network with no prior knowledge of the internal networks and systems.
   - *Gray Box Testing:* Testing from an external or internal network, with knowledge of the internal networks and systems. This is usually a combination of black box testing and white box testing.
   - *White Box Testing:* Performing the test from within the network with the knowledge of the network architecture and the systems. This is also referred to as internal testing.
3. *Information Gathering:* The process of information gathering is to obtain as much information as possible about the IT environment such as networks, IP addresses, operating system version, etc. This is applicable to all the three types of scope as discussed earlier.
4. *Vulnerability Detection:* In this process, tools such as vulnerability scanners are used, and vulnerabilities are identified in the IT environment by way of scanning.
5. *Information Analysis and Planning:* This process is used to analyze the identified vulnerabilities, combined with the information gathered about the IT environment, to devise a plan for penetrating into the network and system.

B. *Types of Vulnerabilities Assessment*

On the basis of vulnerabilities tool there are three board categories of vulnerabilities assessment: *Host Based, Network Based, and Database based.*

1. *Host Based:* Host Based VA identify an issue particular to an individual host or system. It is carried out via a host based scanner and able to diagnose system-level vulnerabilities. The host based tools load mediator software onto the target system that traces the events and reports it to the security analyst.
2. *Network Based:* Network Based VA detect open ports, identify unknown services running on these ports and disclose possible vulnerabilities associated with these service. This is done via a network based scanners, reside on the network to detect vulnerabilities.
3. *Database Based:* Database Based VA identify security exposures in database systems using tools and techniques to prevent from SQL- Injections exploit, can read sensitive data from the database and provides patch & update the DBMS.

C. *Benefits of Vulnerability Assessment*

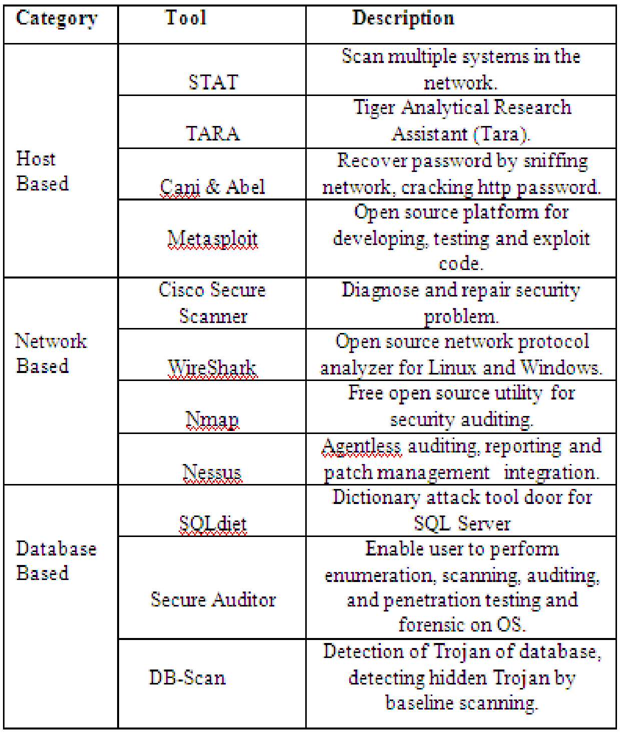
- Some freeware tools are available.
- Identifies almost all known vulnerabilities.
- Extremely automated for scanning.
- Easy to run on a regular basis.

D. *Weaknesses of Vulnerabilities Assessment*

- Have high false positive rate.
- Easily detect by Intrusion Detection System firewall.
- Cause a denial of services by generating bulk of packets.
- Often fail to notice latest vulnerabilities.

E. *Tools for vulnerability assessment*

TABLE I. Tools for VA



Category	Tool	Description
Host Based	STAT	Scan multiple systems in the network.
	TARA	Tiger Analytical Research Assistant (Tara).
	Cain & Abel	Recover password by sniffing network, cracking http password.
	Metasploit	Open source platform for developing, testing and exploit code.
Network Based	Cisco Secure Scanner	Diagnose and repair security problem.
	WireShark	Open source network protocol analyzer for Linux and Windows.
	Nmap	Free open source utility for security auditing.
	Nessus	Agentless auditing, reporting and patch management integration.
Database Based	SQLdict	Dictionary attack tool door for SQL Server
	Secure Auditor	Enable user to perform enumeration, scanning, auditing, and penetration testing and forensic on OS.
	DB-Scan	Detection of Trojan of database, detecting hidden Trojan by baseline scanning.

III. PENETRATION TESTING

Penetration testing is more of an art than a science [8]. It is the process of trying to gain unauthorized access to authorized resources. Penetration testing is also known as an ethical hacking as “breaking into your own system to see how hard it is to do.” It is a main branch of network security evaluation, which aims at providing analysis to discover the vulnerabilities and security threats in systems and networks. The purpose of penetration testing is to recognize technique of gaining access to a system by using common tools and techniques developed by hackers. After vulnerability assessments, which is are used to identify and inventory various exposures within the organization’s systems. Penetration testing attempts to exploit any one of the vulnerabilities to gain unauthorized access.

A. *Methodology*

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 organisation provides full information to test team.
3. *A partial knowledge Test:* Penetration test team has partial information about the target environment.

B. *Process of Penetration Testing*

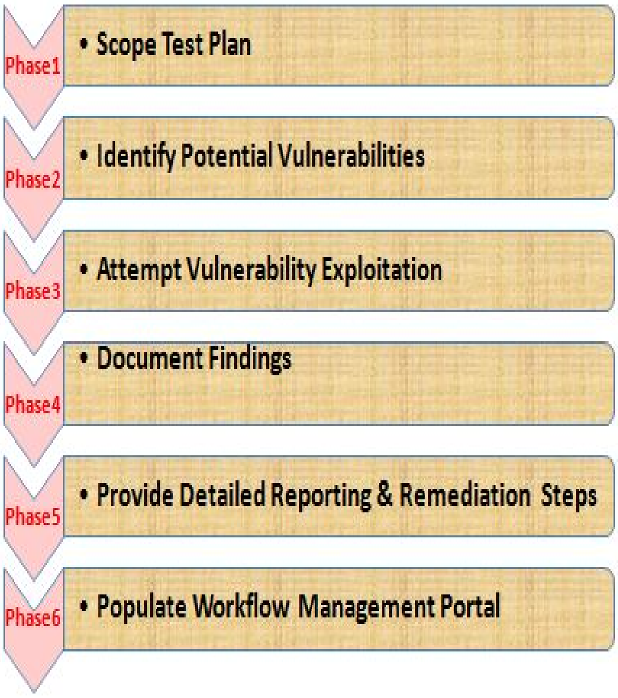

Phase1
• Scope Test Plan
Phase2
• Identify Potential Vulnerabilities
Phase3
• Attempt Vulnerability Exploitation
Phase4
• Document Findings
Phase5
• Provide Detailed Reporting & Remediation Steps
Phase6
• Populate Workflow Management Portal

***Fig.2:* PT process**

1. *Scope test Plan:* In first step we narrow the scope of our test to what is meaningful to the client.

   Identify Potential Vulnerabilities: In this step potential vulnerabilities are identified by using some tools. As vulnerabilities are identified then vulnerabilities are patched.
2. *Attempt Vulnerability Exploitation:* In this step, we find out the greatest possible advantage that we can take from vulnerabilities .The assigned security analyst utilizes a set of tools to exploit and gain access to key systems (core servers, domain controllers, e-mail platforms, ERP, and ERM systems, etc.)
3. *Document Finding:* While testing in-scope systems, the analyst documents all test findings within the Frontline Services Platform (FSP), a secure multi-function portal that allows clients to receive centralized and standardized reporting functionality.
4. *Provide Detailed and Remediation Steps*: At completion of previous step, the client is provided full executive and technical reporting via the FSP client portal, Frontline. Clients can optionally contract for access to a workflow management tool that is also available with Frontline. This tool enables you to efficiently manage and track remediation of the penetration test findings.
5. *Populate Workflow Management Portal:* Now clients can take advantage of the integrated workflow management tool to quickly and effectively deal with discovered issues.

C. *Penetration Testing Strategies*

There are two types of Penetration Testing Strategies: external and internal 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.

D. *Benefits of Penetration Testing*

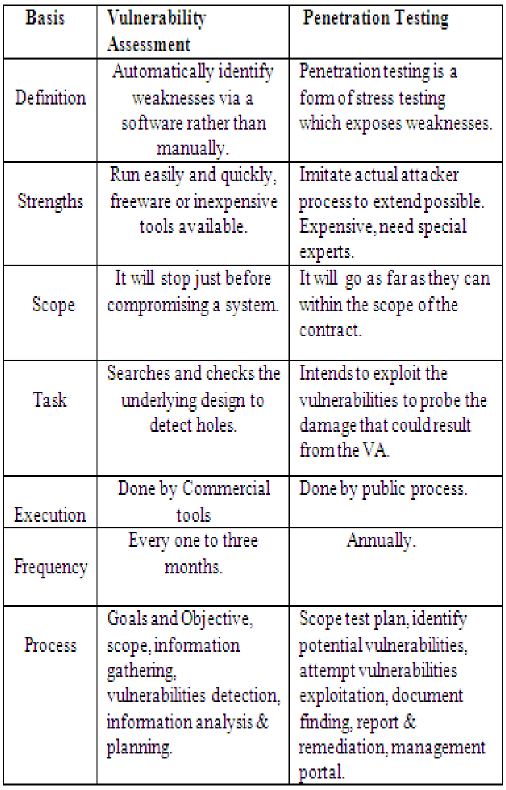
- Test network or system using the tools and techniques that attackers use.
- Demonstrate at what depth vulnerabilities can be exploited.
- Validate vulnerabilities.
- Can provide the realism and evidence needed to address security issue.

E. *Weaknesses of Penetration Testing*

- Labor intensive, require great expertise.
- Dangerous when conducted by inexperienced tester.
- Revel source code to third party.
- Expensive.
- Some tools and methods may be banned by agency regulation.
- Conducted in limited time period.
- If a service is not tested then there will be no information about its security or insecurity.

IV. VULNERABILITY ASSESSMENT Vs PENETRATION TESTING

TABLE II. Comparison of VA with PT



Basis	Vulnerability Assessment	Penetration Testing
Definition	Automatically identify weaknesses via a software rather than manually.	Penetration testing is a form of stress testing which exposes weaknesses.
Strengths	Run easily and quickly, freeware or inexpensive tools available.	Imitate actual attacker process to extend possible. Expensive, need special experts.
Scope	It will stop just before compromising a system.	It will go as far as they can within the scope of the contract.
Task	Searches and checks the underlying design to detect holes.	Intends to exploit the vulnerabilities to probe the damage that could result from the VA.
Execution	Done by Commercial tools	Done by public process.
Frequency	Every one to three months.	Annually.
Process	Goals and Objective, scope, information gathering, vulnerabilities detection, information analysis & planning.	Scope test plan, identify potential vulnerabilities, attempt vulnerabilities exploitation, document finding, report & remediation, management portal.

V. CONCLUSION AND FUTURE WORK

In this article we focused on the vulnerability and penetration tests that give security, an ethical way to identify and evaluate system weaknesses and then mitigate the risks based on the results of such tests.

Thus we have reached to a point that to prevent attacker from stealing our confidential data, Vulnerability Assessment & Penetration Testing is necessary. Through VA we can identify the vulnerabilities and then by PT we can patch the vulnerabilities.

In future we will concentrate on practical implementation of Vulnerability Analysis & Penetration Testing by using tools such as *NESSUS, NMAP, WIRESHAPR, METASPLOIT, ETTERCAP, and CAIN & ABEL.*

REFERENCES

[1]. The Canadian Institute of Chartered Accountants Information Technology Advisory Committee, (2003) "Using an Ethical hacking Technique to Assess Information Security Risk", Toronto Canada.

[2]. http://www.cica.ca/research-and-guidance/documents/it-advisory-committee/item12038.pdf, accessed on 11/ 23/ 2011.

[3]. 2. Edith Cowan University-Research Online, International Cyber Resilience conference Security Research Centre Conferences 2010 on Penetration testing and Vulnerability Assessment: A Professional Approach

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

[5]. SANS GIAC Security Essentials Training Manual.

[6]. © 2003 by RMA. Joel Lenz leads a technology assurance and advisory CPA practice; he is the leader of the New York State Society of CPAs Technology Assurance Committee Task Force on Security and Privacy; and he is an adjunct faculty member at Pace University.

[7]. © Appin |Appin Knowledge Solutions

[8]. https://www.schell.com/Top_Ten_Database_Threads.pdf

[9]. K. Scarfone, M. Souppaya, A. Cody and A.Orebaugh, "Technical Guide to Information Security Testing and Assessment", National Institute of Standards and Technology, Sep. 2008, pp. 36-39.9.

[10]. Hamisi, N.Y., Mvungi, N.H., Mfinanga, D.A. and Mwinyiwiwa, B.M.M., "Intrusion detection by penetration test in an organization network", ICAST 2009.

[11]. G. J. William, Halfond, S. R. Choudhary and A. Orso, "Penetration Testing with Improved Input Vector Identification", International Conference on Software Testing Verification and Validation, 2009, pp. 346-355, doi:10.1109/ICST.2009.26.

[12]. Z.Q. XU, "Study on the Penetration Platforin of Network Information Security", Guangdong University of Technology, May. 2008.

[13]. L. Jehyun, L. Heejo and H. P. In, "Scalable attack graph for risk assessment," in Information Networking, 2009. ICOIN 2009.International Conference on, 2009, pp. 1-5.

[14]. A.Bechtsoudis and N.Sklavos "Aiming at Higher Network Security Through Extensive Penetration Tests" IEEE latin america transactions, vol. 10, no. 3, april 2012, p.p 1752-1756.