International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Enhancing Feature of Open Source VA Tool: OpenVAS

Manju Pushkarsingh[1], Dr. Ravi K. Sheth[2]
[1, 2]*Department of IT, Raksha Shakti University, Ahmedabad, India*

Abstract: ***Data is like a 'Crown Jewel' not only for organizations but also for people associated with it. Cyber-attacks and threats are a real-world problem today with thousands of networks and websites and being compromised every day. As soon as any new product is developed it is tested for its quality and security. Same is the case with the software, hardware, applications, etc. As soon as any new application/software is developed they are checked for their level of security to minimize loss due to it to the company/organization. The purpose of this research is to make OpenVAS more reliable and enhanced to use. In this paper OpenVAS is presented for VAPT and its significance. Have gone through detailed study of OpenVAS to understand it.***
Keywords: Vulnerability Assessment; Penetration Testing; OpenVAS; AWS; Nagios,

I. INTRODUCTION

To ensure the security of the developed / developing applications, their regular security check up should be maintained. Unless newly developed software are not checked properly for their level of defense, they may prove their harmfulness instead of usefulness.

This is where Vulnerability Assessment and Penetration Testing (VAPT) secures it's place in Cyber security. It's almost beyond the bounds of possibility to imagine any kind of organization/institutes/business without systems/software and assuredly internet. The word internet brings many advantages to us along with huge list of challenges. The challenges can be of various types in terms of internet.

This virtual place of systems and internet is commonly known as Cyber Space. Approximately, all of the systems nowadays carry an internet connection with them. Vulnerabilities can originate not only from software but also from hardware devices. Due to overnight growth in use of hardware/software in various fields, the Cyber Space has grown to a huge and broader area which results in more chances of digging out new bugs and Vulnerability in them.

A vulnerability is any flaw/weakness left in an application, which if not patched can be put to wrong use by hackers/crackers. Gaining access to such vulnerability can be a golden chance for hackers to perform malicious and unintended activities. In this paper, the world's most advanced Vulnerability Scanner tool has been studied and explored to find out its base architecture. Also, the Master Slave configuration in OpenVAS has been implemented and deployed on Amazon Web Service(AWS) using Elastic Compute Cloud (EC2) instances.

Deploying it on cloud makes it easily accessible and increases the availability for the scan to perform on any slave systems using master scanner system. Much research have been done on various Vulnerability Assessment software including OpenVAS, including OpenVAS scanner.

Which shows that how important are these tools/scanners for the Cyber Security field. Apart from this the paper is organized as follows. Section 2 gives brief introduction of VAPT. Section 3 describes the various stages involved in Vulnerability Assessment and Penetration Testing. Under Section 4, prevailing VAPT techniques has been mentioned and basic difference between terms VA and PT. Section 5 is included with various TOP VAPT tools (Paid/Open source). In section 6 we describe how OpenVAS can be configured in AWS for Master-Slave configuration for efficient and reliable VA scanning. Ultimately last Section 7 concludes the work/research done and gives a glimpses for future work.

II. VULNERABILITY ASSESSMENT AND PENETRATION TESTING (WHAT AND WHY?)

Vulnerability Assessment and Penetration Testing is a well developed approach to evaluate the existing IT infrastructure to test it's security. With VAPT, we can find existing vulnerabilities in Operating Systems, Services, Mobile Applications, Web Applications, etc. It becomes crucial for any organization to perform periodic VAPT in order to ensure the security of their various assets. Any of the asset present in an organization can be vulnerable to some or other kind of cyber-attacks. To make sure that these assets are risk free and secure VAPT is required to be performed. Vulnerability Assessment and Penetration Testing is made up of two different

terms i.e. VA and PT. Vulnerability Assessment and Penetration Testing (VAPT) are both security services that focus on identifying vulnerabilities in the network, server and system infrastructure. Both the services serve a different purpose and are carried out to achieve different but complimentary goals. Vulnerability Assessment (VA) focuses on internal organizational security, while Penetration Testing (PT) focuses on external real-world risk. Both are different process but are correlated. The objective of Vulnerability Assessment is entire to search and find bugs. Penetration Testing is performed to see whether the vulnerability exists by exploring and exploiting the system.

III. LIFE CYCLE OF VAPT

Vulnerability Assessment and Penetration Testing consists of various steps to be followed one by one. These steps can be shown as below in figure.

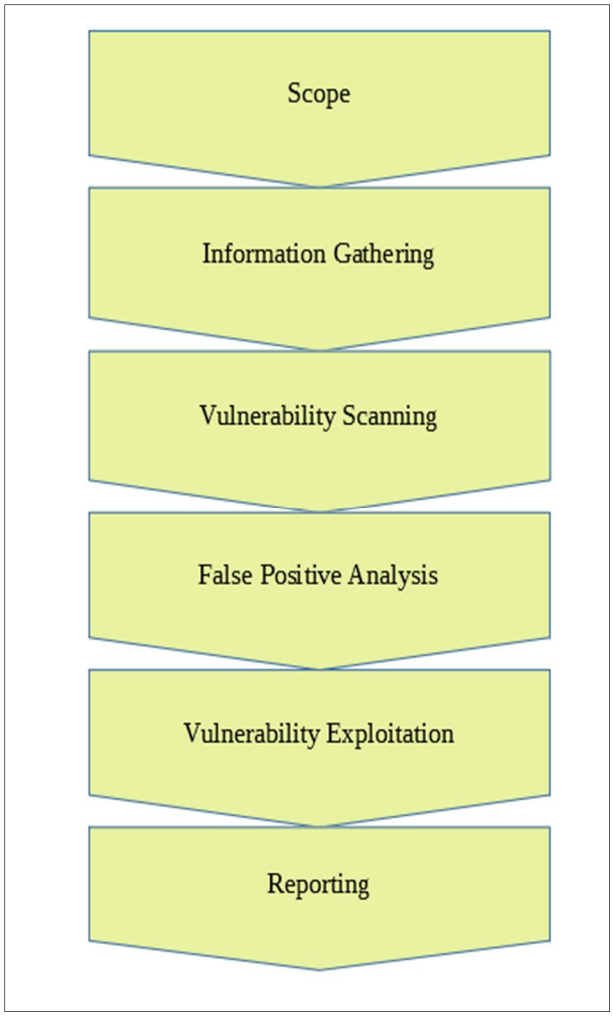

Fig. 1. Vulnerability Assessment and Penetration Testing Life Cycle

Before starting the process for VAPT, the initial step to consider is Scope. It is the primary step of any security testing. It helps the tester in deciding what to test and what not to test. Once the boundaries has been decided for testing, tester will now start gathering as much as information he/she can dig out related to Operating System, Networks, IPs, Software, etc. After this tester uses various vulnerability scanning tools and techniques to uncover the hidden vulnerabilities, if they exist. Once the vulnerabilities are obtained tester can have an analyzing look at it and prepares for exploitation of those discovered vulnerabilities. Tester prepares a plan for it and implements it on target. Once done with exploitation part, tester analyses the results and provides the amendatory and corrective tips for those vulnerabilities. Finally, all these activities are formed in a well documented report which are then forwarded to the management to take the appropriate action.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

IV. VAPT TECHNIQUES

Vulnerability Assessment and Penetration Testing can be achieved using various tools and methods. VAPT can be done with automated tools and it can be done manually as well. Depending on the criticality of the target to test, different methods/tools for testing can be selected. In most cases manual approach is preferred over automated tools, but in some cases automated tools can be a great choice.

VAPT can be performed on different domain, some are shown as below:

VAPT can be performed on different platforms to find hidden vulnerabilities in them.

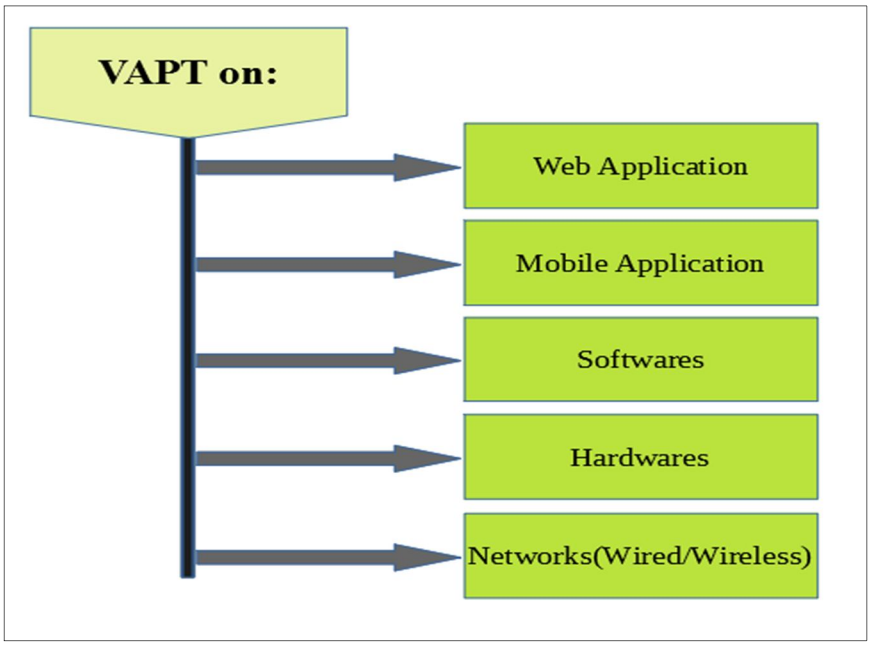

Fig. 2. Vulnerability Assessment and Penetration Testing Techniques

Vulnerability Assessment and Penetration Testing has broad application in different domain i.e. VAPT is useful in both the situation either the target to be assessed is hardware based or software based. VAPT can be carried out in order to ensure cyber security for different applications like: software, hardware, network, applications, databases, devices, process, etc. VAPT is a kind of security testing which should be carried out in a regular span of time for continuous improvements. It is an organized approach to meet the security perimeters for the organizations and data. Following a systematic and continuous approach can prove beneficial to the cyber space. As per the need of the organization/individual we can select the different technique and domain to perform VAPT. System and process can be vulnerable to certain kind of attacks due to diverse reasons, these vulnerabilities can be removed using VAPT practice. VAPT can be performed using some automated tools available and it can also be done using manual approach. Both approaches play crucial role for securing the assets.

V. VAPT TOOLS

Plenty of tools are available for performing VAPT process some are paid and others are open source. Some of them are listed here and all have their own advantages and limitations. All tools possess some specific and important feature that can be really helpful in VAPT. One or more tools can be used in order to get an accurate and efficient result during VAPT process. Along with using these automated tools, the results can be enhanced by adding manual approach to it. If required/possible custom scripts/programs can be developed for better result and process. OpenVAS has its plugins written in NASL, so as new attack/vulnerability is encountered in cyber world the custom script/code can be developed for that vulnerability because the previous/old plugins can't detect the newly discovered vulnerabilities. Together with plugins, OpenVAS also has other records of vulnerabilities in form of Common Vulnerability Exposure (CVE), Computer Emergency Response Team (CERT) data, etc.

The following table summarizes some of the well known tools for VAPT process. Their basic description and some features are listed in front of each tool name, which can help us to differentiate and understand different tools. Understanding a tool for the features provided by it very important as on the basis of this understanding we have to select the tool for real VAPT process.

Table 1 – Various VAPT tools and comparison

Tool Name	Company	Description	Max # of Hosts Available	Vulnerability Detection List
Nessus	Tenable	Large-scale vulnerability assessment tool with 80,000+ plug-ins designed to access various vulnerabilities	Default – 30 Licensed – Unlimited	Systems, Networks, Applications, Malware, Control Systems, Mobile, etc.
OpenVAS	Open Source	Similar to Nessus, except Open Source	Default-30	Network, Server, and Web Application
Nexpose	Rapid7	Integrates Metasploit for vulnerability assessment	Default – 32 Express & Consultant– 1,024 Enterprise & Ultimate – Unlimited	Browser and Operating Systems
GFI LanGuard	GFI Software	Designed to help with patch management and network/software audits	No default or max number specified	Multi-platform Vulnerability Scans available for Windows, Max, Linux, iOS, Android, Windows Phone, etc.
QualysGuard	Qualys	Offers network discovery, mapping, prioritization, and reporting	Default – 30 Express Lite – 256 Express – 5,120 Enterprise – unlimited	Web-Application, Malware, Firewall, IT systems, etc.
MBSA	Open Source	Checks to see if Microsoft products are secure	64 hosts	Passwords, IIS administration, SQL Server administration, Security, Web-Application, etc.
Retina	BeyondTrust	Assesses and prioritizes vulnerabilities in networks	Community – 256	Network Systems, Web Applications, Databases, Virtual Environments
Nipper	Titania	Audits network configuration files	No default or max number specified	Web Application, Banking and Financial Systems, SSL Scanners, etc.
SAINT	SAINT	Vulnerability assessment	Scans all hosts in a target's subnet	Operating Systems, Databases, and Web Applications
Core Impact	Core Security	Powerful exploitation tool, can import other tools such as Burp Suite, SAINT, etc.	No default or max number specified	Web Application, Password, Mobile Device, Wireless Network, etc.
Secunia PSI	Flexera Software	Free security tool that is able to detect vulnerable and outdated programs and vulnerable plug-ins	No default or max number specified	Hardware, Firmware, Middleware, ICS, etc.

VI. RELATED WORK - OPEN SOURCE VA SCANNER: OPEN VAS

Among various Vulnerability Assessment tools available, OpenVAS is one of the important tool. It's not just a VA tool/scanner also it is a whole framework of several services and tools which combinedly offers vulnerability scanning along with vulnerability management. It contains huge numbers of plugins to perform VA scanning. OpenVAS software can be used to easily test your Internet infrastructure. It can be installed on different platforms like: Windows, Linux, Virtual appliance. It is a fork of Nessus.

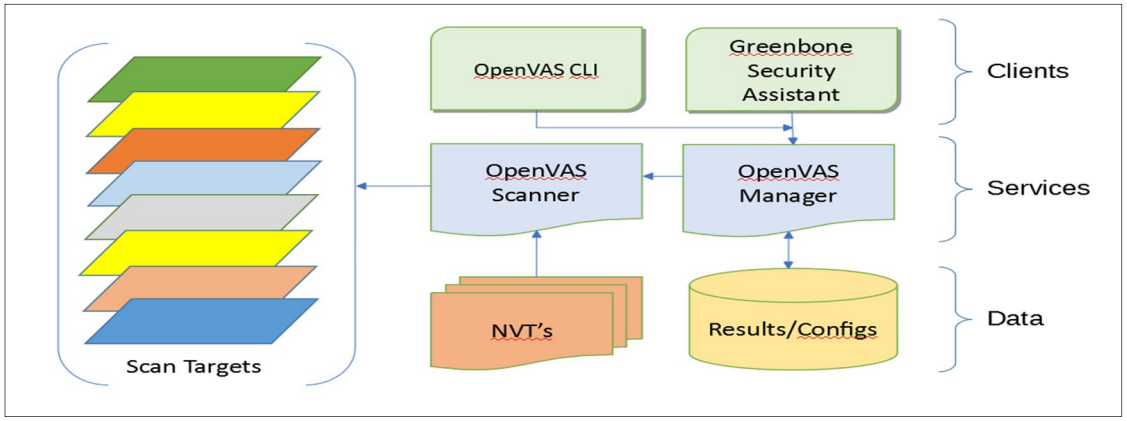

Fig. 3. OpenVAS Architecture

OpenVAS can be configured in Master-Slave configuration, where Master can create scan task for all the slaves connected to it. Once Master-OpenVAS creates the scan tasks for Slave-OpenVAS connected to it, it can generate the results of scan in form of report in various formats like PDF, HTML, CSV, etc. When there are large numbers of system to scan it becomes tedious task to handle all those scan results and reports. When there are multiple slaves/systems to scan through Master system, it becomes a tedious task to manage a huge bunch of newly created reports and results.

So, for handling all these numbers of reports we can use Nagios Monitoring system which can help in monitoring the task and handle them easily. Apart from this, the Master-Slave configuration for OpenVAS can be implemented on Amazon Web Services (AWS) for better handling of scans, scalability, availability, etc. Master-Slave architecture has been implemented and Nagios monitoring System is installed.

Nagios, a system and network monitoring application can be integrated with OpenVAS for better management of the 'Scan results'. Nagios offers monitoring and alerting services for servers, switches, applications and services. Some of the features provided in Nagios are:

1) Monitoring of network services (SMTP, POP3, HTTP, ICMP, SNMP, FTP, SSH)
2) Monitoring of host resources
3) Monitoring of any Hardware
4) Monitoring of Application, Database, Log, and Bandwidth.
5) Monitoring remotely via Nagios Remote Plugin Executor and many more.

a) *Significance*: Integrating Monitoring tools with a vulnerability scanner can be an efficient solution in various scenario, some of them are as under:

i) Easy monitoring of System/Infrastructure
ii) Open Source application
iii) Quick access to scan results
iv) Reliable scans Creation/Management
v) Scalability and Flexibility

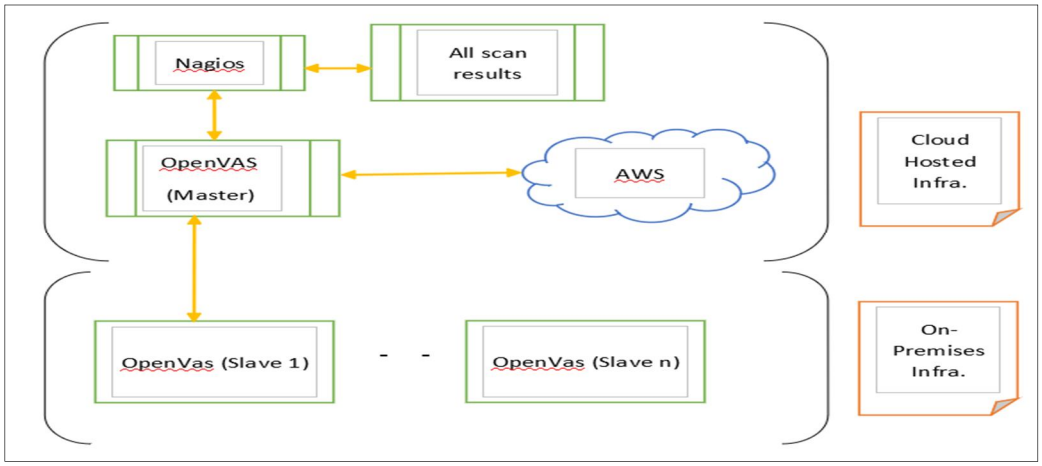

Fig. 4. Master-Slave (OpenVAS) with AWS and Nagios

VII. CONCLUSION AND FUTURE WORK

In this paper we explained how Open Source Vulnerability Assessment tool – OpenVAS can be efficiently used for performing Vulnerability Assessment on any IT infrastructure. It has been shown that using cloud computing service AWS, we can achieve better manageability and scalability. Some of top VAPT tools are also shown here. This paper helps in understanding use of OpenVAS for Vulnerability Assessment. This paper can be helpful to future researcher in getting the core idea of VAPT and the OpenVAS scanner. Also, it will be helpful in differentiating various VAPT tools listed in this paper. Implementing VAPT at every organization can help a lot in securing the virtual digital space, we call as Cyber Space. As a part of future work, it can be considered to develop some efficient plugins for OpenVAS which can be written in Nessus Attack Scripting Language (NASL). Developing more efficient plugins for various vulnerabilities/attacks can make OpenVAS to work in more accurate and efficient way. Also OpenVAS can be automated for certain tasks and some proactive can be developed.

REFERENCES

[1] OpenVAS official guide. URL: http://www.openvas.org/#about
[2] Greenbone guide. URL: https://community.greenbone.net/t/master-slave-configuration- troubleshooting/388
[3] Setup Master-Slave OpenVAS. URL: https://blog.haardiek.org/setup-openvas-as-master-and-slave.html
[4] OpenVAS to perform scan on AWS. URL: https://skywide.in/blog/using-openvas-perform-security-scan- ec2/
[5] EC2 Instance AWS. URL: https://docs.aws.amazon.com/efs/latest/ug/gs-step-one-create-ec2-resources.html
[6] Install Nagios on OpenVAS system. URL: https://www.howtoforge.com/tutorial/ubuntu-nagios/
[7] Nagios. URL: http://www.bujarra.com/monitorizando-vulnerabilidades-con-nagios-y-openvas/?lang=en
[8] VAPT. URL: https://opensourceforu.com/2017/06/basics-vulnerability- assessment-penetration- testing/
[9] OpenVAS different components. URL: https://github.com/greenbone.