International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 6, pp: 705-709 www.ijaem.net ISSN: 2395-5252

Effect of vulnerability assessment in network security

Muhammad A. Yau[1] and Adam Musa Safiyanu[2]
[1]*Department of Mathematics, Nasarawa State University Keffi, Nigeria.*
[2]*Information & Communication Technology Directorate, Nasarawa State University Keffi, Nigeria.*
Corresponding Author: Muhammad A. Yau

Date of Submission: 15-09-2020 Date of Acceptance: 29-09-2020

ABSTRACT: In this paper, we propose to provides the effect of vulnerability assessment using kali Linux Operating System with the help of Nessus and OpenVAS vulnerability scanner to scan and generate a report that could be used by the organization or network administrator in other to take a necessary measure on the network security and to be able to prevent a worm outbreak before it reaches critical mass. Regular assessments can give you a current and very useful understanding of the services offered on your network.

KEYWORDS: Vulnerability, Network Security, Linux OS, OpenVAS, Nessus

I. INTRODUCTION

Internet is becoming part and parcel in every human activities in this contemporary world, today we have E-commerce, E-banking, E-government, E-learning and E-voting etc. people are now using their android phone, blackberry, ipad and laptops as means of communication through the internet, it also used for buying and selling of product, E-transact, Remitta payment and other means on the internet, people were exchanging messages through e-mail, whatsapp, facebook by using the internet etc.

As a result of these development operating systems, applications, and network protocols that are used by different devices to communicate through the internet have grown so complex that manually reviewing each network for security hole is no longer feasible, each technological advancement brings a large number of security holes.

A new protocol might result in dozens of actual implementations, each of which contain exploitable programming errors, logical error, vendor-installed backdoor and misconfiguration. Also internet worm continuously assaulting every system attach to global internet

To combat these attacks, one needs the appropriate tools and knowledge to identify vulnerable system and resolve their security problems before they can be exploited, and one of the most powerful tools available today is the vulnerability assessment.

1. Vulnerability

Vulnerability can be defined as weaknesses or faults in a system design, procedure, implementation or security mechanism that exposes information or the supporting systems to an attack [1].

A weakness that is inherent in every network and device. This include routers, switches, desktops, server and even security.

Types of vulnerabilities

There are three main classes of vulnerability by which the distinction for the types of flaws (local and remote) can be made. These classes are generally divided into design, implementation, and operational categories:

i. **Design vulnerabilities:** These are discovered due to the weaknesses found in the software specifications
ii. **Implementation vulnerabilities:** These are the technical security glitches found in the code of a system
iii. **Operational vulnerabilities:** These are the vulnerabilities that may arise due to the improper configuration and deployment of a system in a specific environment

Based on these three classes, we have two generic types of vulnerabilities, local and remote, which can sit in to any class of the vulnerabilities explained.

i. Local Vulnerability

A condition on which the attacker requires local access in order to trigger the vulnerability by executing a piece of code is known as local vulnerability. By taking advantage of this type of vulnerability, an attacker can increase the access privileges to gain unrestricted access to the computer.

Let's look at this example in which Bad Man has local access to MS Windows Server 2012 (32-bit, x86 platform). His access has been restricted by the administrator through the implementation of a security policy, which will not allow him to run the specific application. Under extreme conditions, he found out that using a malicious piece of code can allow him to gain a system-level or kernel-level access to the computer. By exploiting this well-known vulnerability (for example, CVE-2013-0232, GP Trap Handler nt!KiTrap0D), he gained escalated privileges that allowed him to perform all the administrative tasks and gain unrestricted access to the application. This shows us a clear advantage that was taken by the malicious adversary to gain unauthorized access to the system.

ii. Remote Vulnerability

Remote vulnerability is a condition where the attacker has no prior access but the vulnerability can still be exploited by triggering the malicious piece of code over the network. This type of vulnerability allows an attacker to gain remote access to a computer without facing any physical or local barriers.

For instance, Nabil and Nabila are individually connected to the Internet. Both of them have different IP addresses and are geographically dispersed over two different regions. Let's assume that Nabila's computer is running on a Windows XP operating system, which holds secret biotech information. We also assume that Nabil already knows the operating system and IP address of Nabila's machine. Nabil is now desperately looking for a solution that can allow him to gain remote access to her computer. In the meantime, he comes to know that the MS08-067 Windows Server Service's vulnerability can be easily exploited against a Windows XP machine remotely. He then triggers the exploit against Nabila's computer and gains full access to it.

2. Vulnerability Assessment

Vulnerability assessment has become the preferred method of managing security flaws for many organizations. The ability to quickly identify misconfiguration and unpatched systems, combined with the ease of use and accuracy of many assessment tools has changed the way many administrators manage their system.

Vulnerability assessment are simply the process of locating and reporting vulnerabilities. This provides you with a way to detect and resolve security problems before someone or something can exploit them [2]. Vulnerability assessment provides a snapshot of the security posture of your network.

With the help of assessment tools you can be able to locate vulnerabilities in a network and that will allows you to write a report about the vulnerabilities found for proper action before it can be exploited by an attacker. So now the effect of vulnerability assessment is locating and reporting the flaws that are found on the network as a result of using assessment tools eg. Nessus, OpenVAS, web application analysis tools for the assessment. All of these tools can be install on Kali Linux distribution from Offensive Security.

3. Kali Linux Distribution from Offensive Security

Kali Linux, or simply Kali, is the newest Linux distribution from Offensive Security. It is the successor to the Backtrack Linux distribution. Unlike most Linux distributions, Kali Linux is used for the purposes of penetration testing. Penetration testing is a way of evaluating the security of a computer system or network by simulating an attack.

Kali Linux is a penetration testing and security auditing platform with advanced tools to identify, detect, and exploit any vulnerabilities uncovered in the target network environment. Kali Linux is a distribution based on the Debian GNU/Linux distribution aimed at digital forensics and penetration testing use. It is a successor to the popular BackTrack distribution [3].

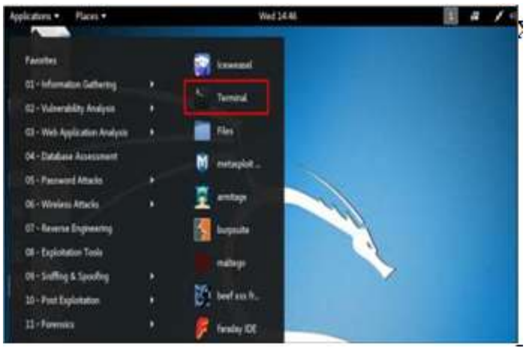
Kali Linux is one of the best security packages of an ethical hacker, containing a set of tools divided by the categories. Generally, Kali Linux can be installed in a machine as an Operating System, you can also install it on Oracle VM VirtualBox and VMware on windows, mac and Ubuntu etc.

Kali Linux window

4. Kali Linux Tools

Kali Linux contains a number of tools that can be used during the penetration testing process.

The penetration testing tools included in Kali Linux can be categorized into the following categories:



Kali Linux Assessment Tools

I. **Information gathering:** This category contains several tools that can be used to gather information about DNS, IDS/IPS, network scanning, operating systems, routing, SSL, SMB, VPN, voice over IP, SNMP, e-mail addresses, and VPN.

II. **Vulnerability assessment:** In this category, you can find tools to scan vulnerabilities in general. It also contains tools to assess the Cisco network, and tools to assess vulnerability in several database servers. This category also includes several fuzzing tools.

III. **Web applications:** This category contains tools related to web applications such as the content management system scanner, database exploitation, web application fuzzers, web application proxies, web crawlers, and web vulnerability scanners.

IV. **Password attacks:** In this category, you will find several tools that can be used to perform password attacks, online or offline.

V. **Exploitation tools:** This category contains tools that can be used to exploit the vulnerabilities found in the target environment. You can find exploitation tools for the network, Web, and database. There are also tools to perform social engineering attacks and find out about the exploit information.

VI. **Sniffing and spoofing:** Tools in this category can be used to sniff the network and web traffic. This category also includes network spoofing tools such as Ettercap and Yersinia.

VII. **Maintaining access:** Tools in this category will be able to help you maintain access to the target machine. You might need to get the highest privilege level in the machine before you can install tools in this category. Here, you can find tools for backdooring the operating system and web application. You can also find tools for tunneling.

VIII. **Reporting tools:** In this category, you will find tools that help you document the penetration-testing process and results.

IX. **System services:** This category contains several services that can be useful during the penetration testing task, such as the Apache service, MySQL service, SSH service, and Metasploit service[4].

5. Vulnerability Assessment Tools

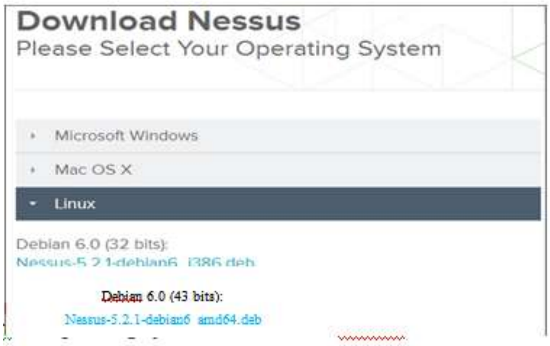
Both Nessus and OpenVAS have similar sets of vulnerabilities that they can scan for on a target host. These vulnerabilities include:

I. Linux vulnerabilities
II. Windows vulnerabilities
III. Local security checks
IV. Network service vulnerabilities

1. Nessus Vulnerability Scanner

Nessus has features such as flexible results filtering and report creation and simplify policy creation.

Before you start scanning, you need to download and install new version of Nessus from their website (www.nessus.org).



Download Nessus
Please Select Your Operating System

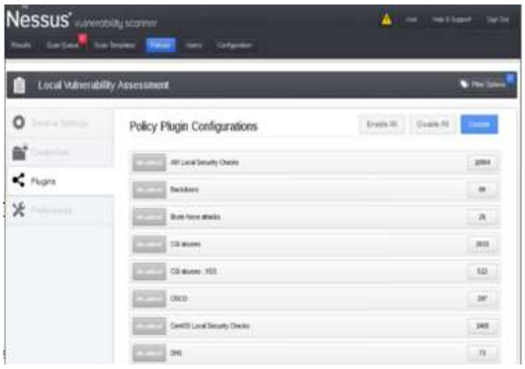
- Microsoft Windows
- Mac OS X
- Linux

Debian 6.0 (32 bits):
Nessus-5.2.1-debian6_i386.deb

Debian 6.0 (43 bits):
Nessus-5.2.1-debian6_amd64.deb

select the operating system to download Nessus

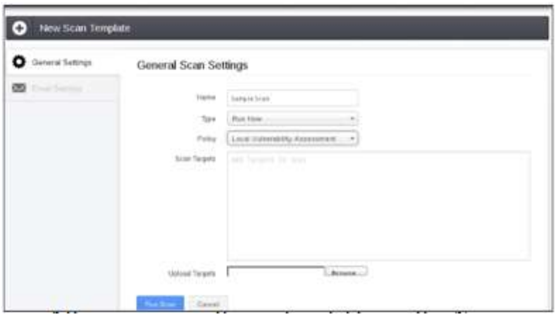
after finishing installing the Nessus vulnerability scanner, you can now open the Nessus and start scanning of the vulnerabilities


Nessus vulnerability scanner
Local Vulnerability Assessment
Policy Plugin Configurations
Plugins

Nessus Vulnerability Scanner

After when you have installed Nessus scanner, you can used it to scan vulnerabilities, those vulnerabilities could be either local or remote vulnerabilities assessment.

Open new scan template and select a policy for now we choose local vulnerability assessment.



New Scan Template

General Settings

Email Settings

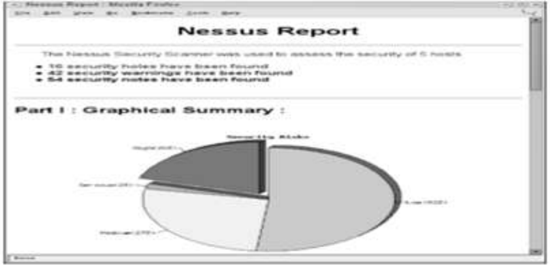
General Scan Settings

Name: Sample Scan
Type: Run Now
Policy: Local Vulnerability Assessment
Scan Targets: Add Targets for Scan
Upload Targets: Browse

Local Vulnerability Assessment policy

After scanning the vulnerability with Nessus vulnerability scanner the result of the scanned vulnerability will be as follows.

Nessus sample report



Nessus Report

The Nessus Security Scanner was used to assess the security of 5 hosts

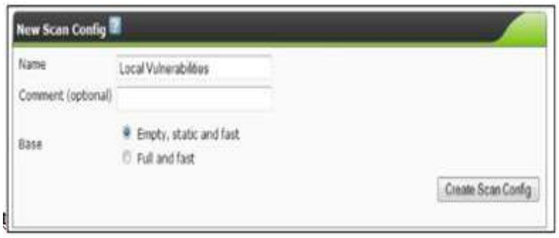
- 16 security holes have been found
- 42 security warnings have been found
- 54 security notes have been found

Part I : Graphical Summary :

2. OpenVAS vulnerability scanner

OpenVAS, the **Open Vulnerability Assessment System**, is an excellent framework that can be used to assess the vulnerabilities of our target. It is a fork of the Nessus project. Unlike Nessus, OpenVAS offers its feeds completely free of charge. As OpenVAS comes standard in Kali Linux, we will begin with configuration [5].

you need to download and installed OpenVAS on your Kali Linux to be able to perform vulnerability assessment.

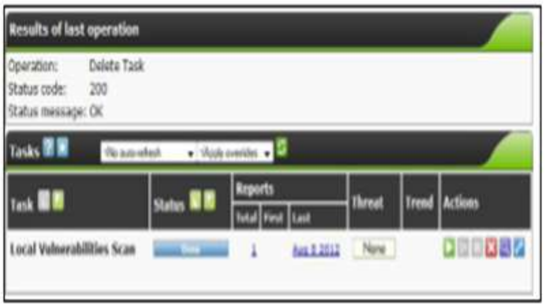


New Scan Config

Name: Local Vulnerabilities
Comment (optional):
Base: ● Empty, static and fast
○ Full and fast

OpenVAS new scan config

Once your scan has been performed, you can see the results by viewing the report.



Results of last operation

Operation: Delete Task
Status code: 200
Status message: OK

Task	Status	Reports			Threat	Trend	Actions
		Total	First	Last			
Local Vulnerabilities Scan	Done	1		Aug 8 2012	None		

Scanned Report

Report Generation

Generating report is the main target of every vulnerability assessment. This report provides a snapshot of all the identified vulnerabilities on the network at a given time. .Although the primary purpose of an assessment is to detect vulnerabilities; the assessment report can also be used as an inventory of the systems on the network and the services they expose. Since enumerating hosts and services is the first part of any vulnerability assessment, regular assessments can give you a current and very useful understanding of the services offered on your network. Assessments assist in crises: when a new worm is released, assessment reports are often used to generate task lists for the system administration staff, allowing them to prevent a worm outbreak before it reaches critical mass.

In conclusion the network administrator has to be very vigilant about the work by performing frequent vulnerability assessment in other to generate a useful report to the organization for proper action, and this is the main effect of vulnerability assessment in network security.

REFERENCES

[1]. Pfleeger, P., & Pfleeger, S. (2003) Security in Computing, 3rd edition, Upper Saddle River, New Jersey: Prentice Hall.

[2]. A practical guide to installing, configuring, and administering the CentOS community-based enterprise server

[3]. Linux Shell Scripting Cookbook, Second Edition, Over 110 practical recipes to solve real-world shell problems, guaranteed to make you wonder how you ever lived without them.

[4]. Zabbix 1.8 Network Monitoring, Monitor your network hardware, servers, and web performance effectively and efficiently.

[5]. A practical guide to implementing penetration testing strategies on websites, web applications, and standard web protocols with Kali Linux. Effectively perform efficient and organized social engineering tests and penetration testing using Kali Linux acceleration and deceleration of valve
d)Reduction in size and weight
e)Fuel economy Increases
f)Power and Torque increase

REFERENCES

[1]. Anderson, M; Tsao, T-C; and Levin, M., 1998, "Adaptive Lift Control for a Camless Electrohydraulic Valvetrain," SAE Paper No. 98102
[2]. Ashhab, M-S; and Stefanopoulou, A., 2000, "Control of a Camless Intake Process – Part II," ASME Journal of Dynamic Systems, Measurement, and Control – March 2000
[3]. Gould, L; Richeson, W; and Erickson, F., 1991, "Performance Evaluation of a Camless Engine Using Valve Actuation with Programmable Timing," SAE Paper No. 910450.
[4]. Schechter, M.; and Levin, M., 1998, "Camless Engine," SAE Paper No. 960581
[5]. INTERNATIONAL JOURNAL OF ROBUST AND NONLINEAR CONTROL, Int. J. Robust Nonlinear Control 2001; 11:1023}1042 (DOI: 10.1002/rnc.643) **(10)**